**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ**

**КАФЕДРА** **КОМП’ЮТЕРИЗОВАНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ**

ДОПУСТИТИ ДО ЗАХИСТУ

Завідувач кафедри

\_\_\_\_\_\_\_\_\_\_\_\_ А.В. Ільєнко

«\_\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_ 20\_\_ р.

На правах рукопису

УДК 004.056.5:510.22(043.3)

**МАГІСТЕРСЬКА АТЕСТАЦІЙНА РОБОТА**

**ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ**

**«МАГІСТР»**

**Тема**:Актуальні методи захисту інформації в умовах інформаційної війни

|  |  |
| --- | --- |
| **Автор:** студент БІ-241м Марголін Максим Вадимович |  |
| **Науковий керівник: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Єлізаров А.Б.** |  |
| **Нормоконтролер:** |  |

**НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ**

**Факультет:** Кібербезпеки, комп’ютерної та програмної інженерії

**Кафедра:** Компютеризованих систем захисту інформації

**Освітній ступінь:** Магістр

**Спеціальність:** 125 «Кібербезпека»

**Освітньо-професійна програма**: «Безпека інформаційних і комунікаційних систем»

ЗАТВЕРДЖУЮ

Завідувач кафедри

\_\_\_\_\_\_\_\_ А.В. Ільєнко

«\_\_» \_\_\_\_\_\_\_\_\_ 20\_\_ р.

**ЗАВДАННЯ**

**на виконання магістерської атестаційної роботи**

**магістранта Марголіна Максима Вадимовича**

1. Тема: *Актуальні методи захисту інформації в умовах інформаційної війни*

затверджена наказом ректора від «\_\_» \_\_\_\_\_\_\_\_\_\_ 20\_\_ № \_\_\_\_\_/ст*.*

1. Термін виконання з \_\_.\_\_.20\_\_р. по \_\_.\_\_.20\_\_р*.*
2. Вихідні дані: проаналізувати існуючі системи та методики захисту інформації; на основі аналізу виділити вхідні і вихідні параметри, завдяки яким можливо провести порівняння існуючих методів захисту інформації, виявлення їх переваг і недоліків; розробити методику, алгоритм та програмне забезпечення системи захисту інформації.
3. Зміст пояснювальної записки: аналіз існуючих систем та алгоритмів інформаційної безпеки; розробка методики системи захисту інформації на основі актуальних методів; розробка програмного забезпечення запропонованої системи, верифікація отриманих результатів.
4. Календарний план-графік

|  |  |  |  |
| --- | --- | --- | --- |
| № з/п | Завдання | Термін виконання | Підпис керівника |
| 1 | Аналіз літературних джерел |  |  |
| 2 | Обґрунтування вибору рішення |  |  |
| 3 | Збір інформації |  |  |
| 4 | Аналіз даних та їх класифікація |  |  |
| 5 | Ознайомлення із загальними теоретичними відомостями шифрування та хешування |  |  |
| 6 | Розробка алгоритмів захисту інформації |  |  |
| 7 | Створення системи заисту інформації |  |  |
| 8 | Оцінка ефективності защихеності |  |  |

1. Дата видачі завдання:

Керівник дипломної роботи: \_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(підпис керівника) (П.І.Б.)

Завдання прийняв до виконання*:* \_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_

(підпис) (П.І.Б)

**РЕФЕРАТ**

Пояснювальна записка до дипломної роботи «Актуальні методи захисту інформації в умовах інформаційної війни»: 87 с., 18 рис., 20 літературних джерел.

ЗАХИСТ, ПРОТОКОЛ, КРИПТОГРАФІЯ, ChaCha20, AES, Twofish., БЕЗПЕКА, ШИФРУВАННЯ.

Предмет дослідження - актуальні процедури захисту данних.

Об’єкт дослідження - основи функціонування методів критографічних перетворень.

Мета дипломної роботи - аналіз та захист данних в умові інформаційної війни.

Методи дослідження – створення програмного засобу що базується на сучасних методах захисту інформації.

Технічні та програмні засоби - для процедур аналізу, захисту використовувалися: один персональний компютер, віртуальна машина VMWare з встановленими операційними системами Windows 10 і Windows 7.

Безпека даних у відкритих інформаційних мережах, а саме Інтернет, завжди буде джерелом будь-яких атак. Тому вкрай важливо створити безпечне середовище для передачі та обробки інформації. Найчастіше передані дані мають різні вимоги щодо захисту даних, серед яких: конфіденційність, достовірність і цілісність. Також варто звертати увагу на фали які зберігаються на компютері, особливо якщо до ньго має доступ декілька людей з різним рівнем достпу.

В результаті виконання данної роботи було створено праграмне рішення що дає змогу для розподілення доступу та гарантує цілістність та конфіденційність персональніх данних. Кількість викрадених даних зростає з кожним днем, особливо в умови інформаційної війни, тому потрібно прийняті захисні заходи. Розроблений проект дає змогу захистити необхідну інформацію, а також має гнучкий функіонал який дозволяє підібрати необхідний рівень захищеності самому користувачу. Адже чим складніше алгоритми – тим надійніша система але у той самий час збільшується час на читання, зберігання, модифікування інформації, усе залежить від технічних засобів користувача – саме тому й необхідна гучка кастомізація.

**ЗМІСТ**

[ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ 8](#_Toc30348901)

[ВСТУП 9](#_Toc30348902)

[РОЗДІЛ 1 12](#_Toc30348903)

[ОСНОВНІ ПОЛОЖЕННЯ ПРО ЗАХИСТ ІНФОРМАЦІЇ 12](#_Toc30348904)

[1.1. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» 12](#_Toc30348905)

[1.2. Закон України «Про основні засади забезпечення кібербезпеки України» 17](#_Toc30348906)

[1.3. Стратегія кібербезпеки України 24](#_Toc30348907)

[1.4. Вимоги до захисту інформації web – сторінки від несанкціонованого доступу 36](#_Toc30348908)

[1.5. Висновки по розділу 42](#_Toc30348909)

[РОЗДІЛ 2 43](#_Toc30348910)

[АНАЛІЗ КРИПТОГРАФІЧНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ 43](#_Toc30348911)

[2.1. Проблема захисту інформації 43](#_Toc30348912)

[2.2. Методи і способи захисту інформації 53](#_Toc30348913)

[2.2.1. Цифрові сертифікати 57](#_Toc30348914)

[2.3. Аналіз стійкості обраного методу шифрування 62](#_Toc30348915)

[2.4. Висновки по розділу 63](#_Toc30348916)

[РОЗДІЛ 3 64](#_Toc30348917)

[ЗАХИСТ ІНФОРМАЦІЇ НА ОСНОВІ РОЗРОБЛЕНОЇ МЕТОДОЛОГІЇ 64](#_Toc30348918)

[1.1. Створення середовища для виконання дипломної роботи 64](#_Toc30348919)

[1.1.1. Visual Studio - інтегроване середовище розробки ПЗ. 67](#_Toc30348920)

[1.2. Обрані алгоритми шифрування 68](#_Toc30348921)

[1.2.1. Алгоритм AES 68](#_Toc30348922)

[1.1.2. Алгоритм ChaCha20 74](#_Toc30348923)

[1.3. Створення ключів 74](#_Toc30348924)

[1.4. Інтерфейс програми 74](#_Toc30348925)

[1.5. Оцінка ефективності 86](#_Toc30348926)

[1.6. Висновки по розділу 87](#_Toc30348927)

[СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ ВИКОРИСТАНИХ ДЖЕРЕЛ 89](#_Toc30348928)

[ДОДАТОКА 93](#_Toc30348929)

# ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

БД – база даних.

ПК – персональний комп’ютер.

ОС – операційна система.

ПЗ – програмне збезпечення.

# ВСТУП

**Актуальніть дослідження.** Розвиток інформаційних комп’ютерних технологій надав можливість не тільки обмінюватися інформацією, а і змогу ведення бізнесу, збереженню інформації у мережі, тобто розширив можливості нашого кібер-простору. Зараз, по всій Україні, з’явились тисячі туристичних агентств, інтернет-магазинів, інтернет-банків, які ведуть розрахунки онлайн. А безпечне зберігання та передавання цих розрахунків гарантувати ніхто не може. Розвиток інформаційних технологій дозволяє в значній мірі скоротити дистанцію між виробником і споживачем банківських послуг. Цей напрямок в Україні в останні роки активно розвивається і вдосконалюється.

Але на данний момент при вирішенні технічних проблем захисту інформації, велику загрозу конфіденцільнсті становлять організвційні та комунікаційні проблеми.   
 Ось на приклад: зі зростанням як внутрішнього так і зовнішнього ринку в країні зростає чило програмістів, дизайнерів, архітекторів та багато інших спеціалістів в області інформаційних послуг. Зазвичай акі професії вимгають навіть для навчання сучасні та швидкі компбтери але не всі мають можливість придбати професіні машини, які необхідні для їх діяльності. Попит породжує пропозиції тому зараз існують офіси в яких в аренду здатюся робочі місця разом із професійними та не дешевими комплектуючими, які підходять для буд яких, навіть, графічних робіт. За дуже вигідними цінами. Наіть студет може користуватися подібними послугами. Але що робити, якщо необхідно працювати із інформацією яка не підлягає розголошенню, а можливості придбати свій компютер – нема. Нікто не дасть гарантію, ніхто не стане працювати з вашим комп’ютером у час вашої відсутності. Велика кількість людей, а також не усі навість знають один одного – це великий прострір для махінацій різного роду.

Такі самі загрози мають місце навіть державних підприємстваї та службах. Так, зараз більшість програм перейшла на хмарні технології, але навіть і вони не захищені від організаційних проблем, через які злоумисник може здобудти небхідну інформацію, не зважаючі на передові методи аутентифікації та найбезпечніші систмеи передачі данних. Адже усі звикли до комфорту і користуються автозаповненням паролів та форм, записуванням паролів на папірцях – це не пристумо але людський фактор залишає дуже багато можливостей для злодіїв. Адже більшість звикла, що злоумисники десь там – дуже далекою.

Безпека даних у відкритій інформаційній мережі, а саме Інтернет, завжди буде джерелом будь-яких атак. Тому вкрай важливо створити безпечну передачу та обробку інформації, так само як на персональніх компютерах, адже якщо існує мережевій захист, усі програми перенесені на хмарні технології – всеодно дуже важливо, щоб данні для вільного доступу до русурсів не потрапили зоумиснику, навіть якщо злодій - інсайдер.

Через те, що з'явилися атаки на протоколи - стає актуальною проблема розробки методики тестування конфігураційних параметрів протоколу, реалізації методики для клієнтських і серверних веб-додатків, які використовують протокол, формування і застосування рекомендацій щодо захисту.

**Мета та завдання** – аналіз та захист данних в умові інформаційної війни.

Для досягнення поставленої мети вирішуються такі **задачі:**

* дослідження відомих методів криптографічних систем та перетворень;
* розробка та вибір методик та підходів для розподілення прав доступу та уникання витоку конфіденційної інформації на основі зроблених досліджень;
* розробка алгоритмів і програмного забезпечення на основі обраних та розораблених методик.

**Об’єктом дослідження** є основи функціонування методів критографічних перетворень.

**Предметом дослідження** є актуальні процедури захисту данних.

Актуальність дослідження полягає у наданні захищеного сховища для забезпечення конфіденційності конфіденційних данних. Кількість викрадених персональних даних зростає з кожним днем, тому потрібно прийняті захисні заходи. Хешування та шифрування – це криптографічні методи, які вирішують проблему з викраденням, модифікацією цінної інформації.

**Новизна одержаних результатів полягає в наступному:**

* розроблена система аналізу данних, яка може зімінити стандартні формми зберігання паролів та уникнуті їх витоку персональніх данних.

**Практичне значення отриманих результатів:**

* розроблено інструмент для аналізу данних та розподілееня прав доступу для уникнення витоку персональніх данних та конфіденційної інформацції.
* розроблено гнучкий інструиент для маштабуваняя необхідного рівня захищеності, адже надійність криптографічних алгоритмів залежить від часу обробки функцій тому можливість використовувати на старих та повільних комп’ютерах сучасні та дієві технології захсту інформації – один із основних параметрів.
* розроблено гнучкий та зрозумілий інтерфейс, який відображає ступінь надійності створеної системи загалом, через оціку надійності ключа доступу. Таких підхід робить зрозумілим для кожного користувача ступінь надійності системи.

**Апробація.** Було опублікована стаття, присвячена темі, що розглядалась в дипломній роботі:

* + 1. Єлізаров А.Б., Марголін М.В. «Захист інформаційно-комунікаційної мережі із забезпеченням надійності обслуговування» / Збірник тез доповідей “Образование и наука без границ”.

# РОЗДІЛ 1

# ОСНОВНІ ПОЛОЖЕННЯ ПРО ЗАХИСТ ІНФОРМАЦІЇ

## 1.1. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»

“Стаття 1. Визначення термiнiв

У цьому Законi наведенi нижче термiни вживаються в такому значеннi:

* блокування iнформацiї в системi - дiї, внаслiдок яких унеможливлюється доступ до iнформацiї в системi;
* виток iнформацiї - результат дiй, внаслiдок яких iнформацiя в системi стає вiдомою чи доступною фiзичним та/або юридичним особам, що не мають права доступу до неї;
* володiлець iнформацiї - фiзична або юридична особа, якiй належать права на iнформацiю;
* власник системи - фiзична або юридична особа, якiй належить право власностi на систему;
* доступ до iнформацiї в системi - отримання користувачем можливостi обробляти iнформацiю в системi;
* захист iнформацiї в системi - дiяльнiсть, спрямована на запобiгання несанкцiонованим дiям щодо iнформацiї в системi;
* знищення iнформацiї в системi - дiї, внаслiдок яких iнформацiя в системi зникає;
* iнформацiйна (автоматизована) система - органiзацiйно-технiчна система, в якiй реалiзується технологiя обробки iнформацiї з використанням технiчних i програмних засобiв;
* iнформацiйно-телекомунiкацiйна система - сукупнiсть iнформацiйних та телекомунiкацiйних систем, якi у процесi обробки iнформацiї дiють як єдине цiле;”[1]
* “комплексна система захисту iнформацiї - взаємопов'язана сукупнiсть органiзацiйних та iнженерно-технiчних заходiв, засобiв i методiв захисту iнформацiї;
* користувач iнформацiї в системi (далi - користувач) - фiзична або юридична особа, яка в установленому законодавством порядку отримала право доступу до iнформацiї в системi;
* криптографiчний захист iнформацiї - вид захисту iнформацiї, що реалiзується шляхом перетворення iнформацiї з використанням спецiальних (ключових) даних з метою приховування/вiдновлення змiсту iнформацiї, пiдтвердження її справжностi, цiлiсностi, авторства тощо;
* несанкцiонованi дiї щодо iнформацiї в системi - дiї, що провадяться з порушенням порядку доступу до цiєї iнформацiї, установленого вiдповiдно до законодавства;
* обробка iнформацiї в системi - виконання однiєї або кiлькох операцiй, зокрема: збирання, введення, записування, перетворення, зчитування, зберiгання, знищення, реєстрацiї, приймання, отримання, передавання, якi здiйснюються в системi за допомогою технiчних i програмних засобiв;
* порушення цiлiсностi iнформацiї в системi - несанкцiонованi дiї щодо iнформацiї в системi, внаслiдок яких змiнюється її вмiст;
* порядок доступу до iнформацiї в системi - умови отримання користувачем можливостi обробляти iнформацiю в системi та правила обробки цiєї iнформацiї;
* телекомунiкацiйна система - сукупнiсть технiчних i програмних засобiв, призначених для обмiну iнформацiєю шляхом передавання, випромiнювання або приймання її у виглядi сигналiв, знакiв, звукiв, рухомих або нерухомих зображень чи в iнший спосiб;
* технiчний захист iнформацiї - вид захисту iнформацiї, спрямований на забезпечення за допомогою iнженерно-технiчних заходiв та/або програмних i технiчних засобiв унеможливлення витоку, знищення та блокування iнформацiї, порушення цiлiсностi та режиму доступу до iнформацiї.

Стаття 2. Об'єкти захисту в системi”[1]

“Об'єктами захисту в системi є iнформацiя, що обробляється в нiй, та програмне забезпечення, яке призначено для обробки цiєї iнформацiї.

Стаття 3. Суб'єкти вiдносин

Суб'єктами вiдносин, пов'язаних iз захистом iнформацiї в системах, є:

* володiлцi iнформацiї;
* власники системи;
* користувачi;
* спецiально уповноважений центральний орган виконавчої влади з питань органiзацiї спецiального зв'язку та захисту iнформацiї i пiдпорядкованi йому регiональнi органи.

Стаття 4. Доступ до iнформацiї в системi

Порядок доступу до iнформацiї, перелiк користувачiв та їх повноваження стосовно цiєї iнформацiї визначаються володiльцем iнформацiї.

Порядок доступу до державних iнформацiйних ресурсiв або iнформацiї з обмеженим доступом, вимога щодо захисту якої встановлена законом, перелiк користувачiв та їх повноваження стосовно цiєї iнформацiї визначаються законодавством.

У випадках, передбачених законом, доступ до iнформацiї в системi може здiйснюватися без дозволу її володiльця в порядку, встановленому законом.

Стаття 5. Вiдносини мiж володiльцем iнформацiї та власником системи

Власник системи забезпечує захист iнформацiї в системi в порядку та на умовах, визначених у договорi, який укладається ним iз володiльцем iнформацiї, якщо iнше не передбачено законом.

Власник системи на вимогу володiльця iнформацiї надає вiдомостi щодо захисту iнформацiї в системi.

Стаття 6. Вiдносини мiж власником системи та користувачем

Власник системи надає користувачевi вiдомостi про правила i режим роботи системи та забезпечує йому доступ до iнформацiї в системi вiдповiдно до визначеного порядку доступу.”[1]

“Стаття 7. Вiдносини мiж власниками систем

Власник системи, яка використовується для обробки iнформацiї з iншої системи, забезпечує захист такої iнформацiї в порядку та на умовах, що визначаються договором, який укладається мiж власниками систем, якщо iнше не встановлено законодавством.

Власник системи, яка використовується для обробки iнформацiї з iншої системи, повiдомляє власника зазначеної системи про виявленi факти несанкцiонованих дiй щодо iнформацiї в системi.

Стаття 8. Умови обробки iнформацiї в системi

Умови обробки iнформацiї в системi визначаються власником системи вiдповiдно до договору з володiльцем iнформацiї, якщо iнше не передбачено законодавством.

Державнi iнформацiйнi ресурси або iнформацiя з обмеженим доступом, вимога щодо захисту якої встановлена законом, повиннi оброблятися в системi iз застосуванням комплексної системи захисту iнформацiї з пiдтвердженою вiдповiднiстю. Пiдтвердження вiдповiдностi здiйснюється за результатами державної експертизи в порядку, встановленому законодавством.

Для створення комплексної системи захисту державних iнформацiйних ресурсiв або iнформацiї з обмеженим доступом, вимога щодо захисту якої встановлена законом, використовуються засоби захисту iнформацiї, якi мають сертифiкат вiдповiдностi або позитивний експертний висновок за результатами державної експертизи у сферi технiчного та/або криптографiчного захисту iнформацiї. Пiдтвердження вiдповiдностi та проведення державної експертизи цих засобiв здiйснюються в порядку, встановленому законодавством.

Стаття 9. Забезпечення захисту iнформацiї в системi

Вiдповiдальнiсть за забезпечення захисту iнформацiї в системi покладається на власника системи.

Власник системи, в якiй обробляються державнi iнформацiйнi ресурси або iнформацiя з обмеженим доступом, вимога щодо захисту якої встановлена"[1] “законом, утворює службу захисту iнформацiї або призначає осiб, на яких покладається забезпечення захисту iнформацiї та контролю за ним.

Про спроби та/або факти несанкцiонованих дiй у системi щодо державних iнформацiйних ресурсiв або iнформацiї з обмеженим доступом, вимога щодо захисту якої встановлена законом, власник системи повiдомляє вiдповiдно спецiально уповноважений центральний орган виконавчої влади з питань органiзацiї спецiального зв'язку та захисту iнформацiї або пiдпорядкований йому регiональний орган.

Стаття 10. Повноваження державних органiв у сферi захисту iнформацiї в системах

Вимоги до забезпечення захисту державних iнформацiйних ресурсiв або iнформацiї з обмеженим доступом, вимога щодо захисту якої встановлена законом, встановлюються Кабiнетом Мiнiстрiв України.

Спецiально уповноважений центральний орган виконавчої влади з питань органiзацiї спецiального зв'язку та захисту iнформацiї:

* розробляє пропозицiї щодо державної полiтики у сферi захисту iнформацiї та забезпечує її реалiзацiю в межах своєї компетенцiї;
* визначає вимоги та порядок створення комплексної системи захисту державних iнформацiйних ресурсiв або iнформацiї з обмеженим доступом, вимога щодо захисту якої встановлена законом;
* органiзовує проведення державної експертизи комплексних систем захисту iнформацiї, експертизи та пiдтвердження вiдповiдностi засобiв технiчного i криптографiчного захисту iнформацiї;
* здiйснює контроль за забезпеченням захисту державних iнформацiйних ресурсiв або iнформацiї з обмеженим доступом, вимога щодо захисту якої встановлена законом;
* здiйснює заходи щодо виявлення загрози державним iнформацiйним ресурсам вiд несанкцiонованих дiй в iнформацiйних, телекомунiкацiйних та”[1] “iнформацiйно-телекомунiкацiйних системах та дає рекомендацiї з питань запобiгання такiй загрозi.

Державнi органи в межах своїх повноважень за погодженням вiдповiдно iз спецiально уповноваженим центральним органом виконавчої влади з питань органiзацiї спецiального зв'язку та захисту iнформацiї або пiдпорядкованим йому регiональним органом встановлюють особливостi захисту державних iнформацiйних ресурсiв або iнформацiї з обмеженим доступом, вимога щодо захисту якої встановлена законом.

Особливостi захисту iнформацiї в системах, якi забезпечують банкiвську дiяльнiсть, встановлюються Нацiональним банком України.

Стаття 11. Вiдповiдальнiсть за порушення законодавства про захист iнформацiї в системах

Особи, виннi в порушеннi законодавства про захист iнформацiї в системах, несуть вiдповiдальнiсть згiдно iз законом.

Стаття 12. Мiжнароднi договори

Якщо мiжнародним договором, згода на обов'язковiсть якого надана Верховною Радою України, визначено iншi правила, нiж тi, що передбаченi цим Законом, застосовуються норми мiжнародного договору.

Стаття 13. Прикiнцевi положення

Цей Закон набирає чинностi з 1 сiчня 2006 року.

Нормативно-правовi акти до приведення їх у вiдповiднiсть iз цим Законом дiють у частинi, що не суперечить цьому Закону.”[1]

## Закон України «Про основні засади забезпечення кібербезпеки України»

“Цей Закон визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів,”[2] “підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.

«Стаття 1. Визначення термінів

У цьому Законі наведені нижче терміни вживаються в такому значенні:

* індикатори кіберзагроз - показники (технічні дані), що використовуються для виявлення та реагування на кіберзагрози;
* 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;”[2] “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;
* кібероборона - сукупність політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в кіберпросторі та спрямовані на забезпечення захисту суверенітету та обороноздатності держави, запобігання виникненню збройного конфлікту та відсіч збройній агресії;
* кіберпростір - середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з’єднаних) комунікаційних систем та”[2] “забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних;
* кіберрозвідка - діяльність, що здійснюється розвідувальними органами у кіберпросторі або з його використанням;
* кібертероризм - терористична діяльність, що здійснюється у кіберпросторі або з його використанням;
* кібершпигунство - шпигунство, що здійснюється у кіберпросторі або з його використанням;
* критична інформаційна інфраструктура - сукупність об’єктів критичної інформаційної інфраструктури;
* критично важливі об’єкти інфраструктури (далі - об’єкти критичної інфраструктури) - підприємства, установи та організації незалежно від форми власності, 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;
* Національна телекомунікаційна мережа - сукупність спеціальних телекомунікаційних систем (мереж), систем спеціального зв’язку, інших комунікаційних систем, які використовуються в інтересах органів державної влади та органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону, призначена для обігу (передавання, приймання, створення, оброблення, зберігання) та захисту національних інформаційних ресурсів, забезпечення захищених електронних комунікацій, надання спектра сучасних захищених інформаційно-комунікаційних (мультисервісних) послуг в інтересах здійснення управління державою у мирний час, в умовах надзвичайного стану та в особливий період, та яка є мережею (системою)”[2] “подвійного призначення з використанням частини її ресурсу для надання послуг, зокрема з кіберзахисту, іншим споживачам;
* національні електронні інформаційні ресурси (далі - національні інформаційні ресурси) - систематизовані електронні інформаційні ресурси, які містять інформацію незалежно від виду, змісту, форми, часу і місця її створення (включаючи публічну інформацію, державні інформаційні ресурси та іншу інформацію), призначену для задоволення життєво важливих суспільних потреб громадянина, особи, суспільства і держави. Під електронними інформаційними ресурсами розуміється будь-яка інформація, що створена, записана, оброблена або збережена у цифровій чи іншій нематеріальній формі за допомогою електронних, магнітних, електромагнітних, оптичних, технічних, програмних або інших засобів;
* об’єкт критичної інформаційної інфраструктури - комунікаційна або технологічна система об’єкта критичної інфраструктури, кібератака на яку безпосередньо вплине на стале функціонування такого об’єкта критичної інфраструктури;
* система управління технологічними процесами (далі - технологічна система) - автоматизована або автоматична система, яка є сукупністю обладнання, засобів, комплексів та систем обробки, передачі та приймання, призначена для організаційного управління та/або управління технологічними процесами (включаючи промислове, електронне, комунікаційне обладнання, інші технічні та технологічні засоби) незалежно від наявності доступу системи до мережі Інтернет та/або інших глобальних мереж передачі даних;
* системи електронних комунікацій (далі - комунікаційні системи) - системи передавання, комутації або маршрутизації, обладнання та інші ресурси (включаючи пасивні мережеві елементи, які дають змогу передавати сигнали за допомогою проводових, радіо-, оптичних або інших електромагнітних засобів, мережі мобільного, супутникового зв’язку, електричні кабельні мережі в частині, в якій вони використовуються для цілей передачі сигналів), що забезпечують електронні комунікації (передачу електронних інформаційних ресурсів), у тому”[2] “числі засоби і пристрої зв’язку, комп’ютери, інша комп’ютерна техніка, інформаційно-телекомунікаційні системи, які мають доступ до мережі Інтернет та/або інших глобальних мереж передачі даних.

Терміни "національна безпека", "національні інтереси", "загрози національній безпеці" вживаються в цьому Законі у значенні, визначеному Законом України "Про основи національної безпеки України".

Стаття 4. Об’єкти кібербезпеки та кіберзахисту

Об’єктами кібербезпеки є:

* конституційні права і свободи людини і громадянина;
* суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища;
* держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність;
* національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави;
* об’єкти критичної інфраструктури.

Об’єктами кіберзахисту є:

* комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону;
* об’єкти критичної інформаційної інфраструктури;
* комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу.

Порядок формування переліку об’єктів критичної інформаційної інфраструктури, перелік таких об’єктів та порядок їх внесення до державного реєстру об’єктів критичної інформаційної інфраструктури, а також порядок формування”[2] “та забезпечення функціонування державного реєстру об’єктів критичної інформаційної інфраструктури затверджуються Кабінетом Міністрів України.

Повноваження щодо формування та забезпечення функціонування реєстру об’єктів критичної інформаційної інфраструктури у банківській системі України покладаються на Національний банк України.

Стаття 5. Суб’єкти забезпечення кібербезпеки

* Координація діяльності у сфері кібербезпеки як складової національної безпеки України здійснюється Президентом України через очолювану ним Раду національної безпеки і оборони України.
* Національний координаційний центр кібербезпеки як робочий орган Ради національної безпеки і оборони України здійснює координацію та контроль за діяльністю суб’єктів сектору безпеки і оборони, які забезпечують кібербезпеку, вносить Президентові України пропозиції щодо формування та уточнення Стратегії кібербезпеки України.
* Кабінет Міністрів України забезпечує формування та реалізацію державної політики у сфері кібербезпеки, захист прав і свобод людини і громадянина, національних інтересів України у кіберпросторі, боротьбу з кіберзлочинністю; організовує та забезпечує необхідними силами, засобами і ресурсами функціонування національної системи кібербезпеки; формує вимоги та забезпечує функціонування системи аудиту інформаційної безпеки на об’єктах критичної інфраструктури (крім об’єктів критичної інфраструктури у банківській системі України).
* Суб’єктами, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, є:
* міністерства та інші центральні органи виконавчої влади;
* місцеві державні адміністрації;
* органи місцевого самоврядування;
* правоохоронні, розвідувальні і контррозвідувальні органи, суб’єкти оперативно-розшукової діяльності;”[2]
* “Збройні Сили України, інші військові формування, утворені відповідно до закону;
* Національний банк України;
* підприємства, установи та організації, віднесені до об’єктів критичної інфраструктури;
* суб’єкти господарювання, громадяни України та об’єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов’язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом.

Суб’єкти забезпечення кібербезпеки у межах своєї компетенції:

* здійснюють заходи щодо запобігання використанню кіберпростору у воєнних, розвідувально-підривних, терористичних та інших протиправних і злочинних цілях;
* здійснюють виявлення і реагування на кіберінциденти та кібератаки, усунення їх наслідків;
* здійснюють інформаційний обмін щодо реалізованих та потенційних кіберзагроз;
* розробляють і реалізують запобіжні, організаційні, освітні та інші заходи у сфері кібербезпеки, кібероборони та кіберзахисту;
* забезпечують проведення аудиту інформаційної безпеки, у тому числі на підпорядкованих об’єктах та об’єктах, що належать до сфери їх управління;
* здійснюють інші заходи із забезпечення розвитку та безпеки кіберпростору.”[2]

## Стратегія кібербезпеки України

“Загальні положення

Стрімкий розвиток інформаційних технологій поступово трансформує світ. Відкритий та вільний кіберпростір розширює свободу і можливості людей,”[3] “збагачує суспільство, створює новий глобальний інтерактивний ринок ідей, досліджень та інновацій, стимулює відповідальну та ефективну роботу влади і активне залучення громадян до управління державою та вирішення питань місцевого значення, забезпечує публічність та прозорість влади, сприяє запобіганню корупції.

Водночас переваги сучасного цифрового світу та розвиток інформаційних технологій обумовили виникнення нових загроз національній та міжнародній безпеці. Поряд із інцидентами природного (ненавмисного) походження зростає кількість та потужність кібератак, вмотивованих інтересами окремих держав, груп та осіб.

Поширюються випадки незаконного збирання, зберігання, використання, знищення, поширення, персональних даних, незаконних фінансових операцій, крадіжок та шахрайства у мережі Інтернет. Кіберзлочинність стає транснаціональною та здатна завдати значної шкоди інтересам особи, суспільства і держави.

Метою Стратегії кібербезпеки України (далі - Стратегія) є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави.

Для досягнення цієї мети необхідними є:

* створення національної системи кібербезпеки;
* посилення спроможностей суб'єктів сектору безпеки та оборони для забезпечення ефективної боротьби із кіберзагрозами воєнного характеру, кібершпигунством, кібертероризмом та кіберзлочинністю, поглиблення міжнародного співробітництва у цій сфері;
* забезпечення кіберзахисту державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, а також інформаційної інфраструктури, яка знаходиться під юрисдикцією України, та порушення сталого функціонування якої матиме негативний вплив на стан національної безпеки і оборони України (критична інформаційна інфраструктура).

Забезпечення кібербезпеки України як стану захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі, що ”[3] “досягається комплексним застосуванням сукупності правових, організаційних, інформаційних заходів, має базуватися на принципах:

* верховенства права і поваги до прав та свобод людини і громадянина;
* забезпечення національних інтересів України;
* відкритості, доступності, стабільності та захищеності кіберпростору;
* державно-приватного партнерства, широкої співпраці з громадянським суспільством у сфері забезпечення кібербезпеки та кіберзахисту;
* пропорційності та адекватності заходів кіберзахисту реальним та потенційним ризикам;
* пріоритетності запобіжних заходів;
* невідворотності покарання за вчинення кіберзлочинів;
* пріоритетного розвитку та підтримки вітчизняного наукового, науково-технічного та виробничого потенціалу;
* міжнародного співробітництва з метою зміцнення взаємної довіри у сфері кібербезпеки та вироблення спільних підходів у протидії кіберзагрозам, консолідації зусиль у розслідуванні та запобіганні кіберзлочинам, недопущення використання кіберпростору в протиправних та воєнних цілях;
* забезпечення демократичного цивільного контролю над утвореними відповідно до законів України військовими формуваннями та правоохоронними органами держави, що діють у сфері кібербезпеки.

Розвиток та безпека кіберпростору, запровадження електронного урядування, гарантування безпеки й сталого функціонування електронних комунікацій та державних електронних інформаційних ресурсів мають бути складовими державної політики у сфері розвитку інформаційного простору та становлення інформаційного суспільства в Україні.

Ця Стратегія базується на положеннях Конвенції про кіберзлочинність, ратифікованої Законом України від 7 вересня 2005 року № 2824-ІV, законодавства України щодо основ національної безпеки, засад внутрішньої та зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та”[3] “інформації, вимога щодо захисту якої встановлена законом та спрямована на реалізацію до 2020 року Стратегії національної безпеки України, затвердженої Указом Президента України від 26 травня 2015 року № 287 "Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про Стратегію національної безпеки України".

Загрози кібербезпеці

Кіберпростір поступово перетворюється на окрему, поряд із традиційними "Земля", "Повітря", "Море" та "Космос", сферу ведення бойових дій, у якій все більш активно діють відповідні підрозділи збройних сил провідних держав світу. З урахуванням широкого застосування сучасних інформаційних технологій у секторі безпеки і оборони, створення єдиної автоматизованої системи управління Збройних Сил України оборона нашої держави стає більш уразливою до кіберзагроз.

Економічна, науково-технічна, інформаційна сфера, сфера державного управління, оборонно-промисловий і транспортний комплекси, інфраструктура електронних комунікацій, сектор безпеки і оборони України стають все більш уразливими для розвідувально-підривної діяльності іноземних спецслужб у кіберпросторі.

Сучасні інформаційно-комунікаційні технології можуть використовуватися для здійснення терористичних актів, зокрема шляхом порушення штатних режимів роботи автоматизованих систем керування технологічними процесами на об'єктах критичної інфраструктури. Більшого поширення набуває політично вмотивована діяльність у кіберпросторі у вигляді атак на урядові та приватні веб-сайти в мережі Інтернет.

Дедалі частіше об'єктами кібератак та кіберзлочинів стають інформаційні ресурси фінансових установ, підприємств транспорту та енергозабезпечення, державних органів, які гарантують безпеку, оборону, захист від надзвичайних ситуацій. Новітні технології застосовуються не лише для скоєння традиційних видів злочинів, але і для скоєння принципово нових видів злочинів, притаманних суспільству з високим рівнем інформатизації.”[3]

“Загрози кібербезпеці актуалізуються через дію таких чинників, зокрема, як:

* невідповідність інфраструктури електронних комунікацій держави, рівня її розвитку та захищеності сучасним вимогам;
* недостатній рівень захищеності критичної інформаційної інфраструктури, державних електронних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, від кіберзагроз;
* безсистемність заходів кіберзахисту критичної інформаційної інфраструктури;
* недостатній розвиток організаційно-технічної інфраструктури забезпечення кібербезпеки та кіберзахисту критичної інформаційної інфраструктури та державних електронних інформаційних ресурсів;
* недостатня ефективність суб'єктів сектору безпеки і оборони України у протидії кіберзагрозам воєнного, кримінального, терористичного та іншого характеру;
* недостатній рівень координації, взаємодії та інформаційного обміну між суб'єктами забезпечення кібербезпеки.

Національна система кібербезпеки, основні суб'єкти забезпечення кібербезпеки

Національна система кібербезпеки має насамперед забезпечити взаємодію з питань кібербезпеки державних органів, органів місцевого самоврядування, військових формувань, правоохоронних органів, наукових установ, навчальних закладів, громадських об'єднань, а також підприємств, установ та організацій незалежно від форми власності, які провадять діяльність у сфері електронних комунікацій, захисту інформації та/або є власниками (розпорядниками) об'єктів критичної інформаційної інфраструктури.

Рада національної безпеки і оборони України відповідно до Конституції України та у встановленому законом порядку має здійснювати координацію та контроль діяльності суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку України.”[3]

“Основу національної системи кібербезпеки становитимуть Міністерство оборони України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція України, Національний банк України, розвідувальні органи, на які мають бути покладені в установленому порядку такі основні завдання:

* на Міністерство оборони України, Генеральний штаб Збройних Сил України відповідно до компетенції - здійснення заходів з підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони); здійснення військової співпраці з НАТО, пов'язаної з безпекою кіберпростору та сумісним захистом від кіберзагроз; забезпечення у взаємодії з Державною службою спеціального зв'язку та захисту інформації України і Службою безпеки України кіберзахисту власної інформаційної інфраструктури;
* на Державну службу спеціального зв'язку та захисту інформації України - формування та реалізація державної політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту критичної інформаційної інфраструктури, державний контроль у цих сферах; координація діяльності інших суб'єктів кібербезпеки щодо кіберзахисту; здійснення організаційно-технічних заходів із запобігання, виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків, інформування про кіберзагрози та відповідні методи захисту від них; забезпечення функціонування державного центру кіберзахисту; проведення аудиту захищеності об'єктів критичної інформаційної інфраструктури на вразливість;
* на Службу безпеки України - попередження, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, які вчиняються у кіберпросторі; здійснення контррозвідувальних та оперативно-розшукових заходів, спрямованих на боротьбу з кібертероризмом та кібершпигунством, а також щодо готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів; протидія кіберзлочинності, можливі наслідки якої безпосередньо створюють загрозу життєво важливим інтересам України; розслідування кіберінцидентів та кібератак щодо”[3] “державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечення реагування на комп'ютерні інциденти у сфері державної безпеки;
* на Національну поліцію України - забезпечення захисту прав і свобод людини та громадянина, інтересів суспільства і держави від злочинних посягань у кіберпросторі; запобігання, виявлення, припинення та розкриття кіберзлочинів; підвищення поінформованості громадян про безпеку в кіберпросторі;
* на Національний банк України - формування вимог щодо кіберзахисту критичної інформаційної інфраструктури у банківській сфері;
* на розвідувальні органи України - здійснення розвідувальної діяльності щодо загроз національній безпеці України у кіберпросторі, інших подій і обставин, що стосуються сфери кібербезпеки.

Мають бути створені умови для залучення підприємств, установ та організацій незалежно від форми власності, які провадять діяльність у сфері електронних комунікацій, захисту інформації та/або є власниками (розпорядниками) об'єктів критичної інфраструктури, до забезпечення кібербезпеки України. Зокрема, мають бути врегульовані питання щодо обов'язковості вжиття ними заходів із забезпечення захисту інформації та кіберзахисту відповідно до вимог законодавства, а також щодо сприяння ними державним органам у виконанні завдань із забезпечення кібербезпеки та кіберзахисту.

Держава сприятиме залученню наукових установ, навчальних закладів, організацій, громадських об'єднань і громадян до розробки та реалізації заходів із кібербезпеки і кіберзахисту.

Пріоритети та напрями забезпечення кібербезпеки України

Розвиток безпечного, стабільного і надійного кіберпростору має полягати, насамперед, у:

* виробленні і оперативній адаптації державної політики у сфері кібербезпеки, спрямованої на розвиток кіберпростору, досягненні сумісності з відповідними стандартами ЄС та НАТО;”[3]
* “створенні вітчизняної нормативно-правової та термінологічної бази у цій сфері, гармонізації нормативних документів у сфері електронних комунікацій, захисту інформації, інформаційної та кібербезпеки відповідно до міжнародних стандартів і стандартів ЄС та НАТО;
* формуванні конкурентного середовища у сфері електронних комунікацій, наданні послуг із захисту інформації та кіберзахисту;
* розвитку технологій кіберзахисту засобів рухомого зв'язку, забезпеченні апаратної, контентної безпеки, безпеки додатків та сервісів зв'язку;
* залученні експертного потенціалу наукових установ, професійних та громадських об'єднань до підготовки проектів концептуальних документів у сфері кібербезпеки;
* підвищенні цифрової грамотності громадян та культури безпекового поводження в кіберпросторі, комплексних знань, навичок і здібностей, необхідних для підтримки цілей кібербезпеки, впровадженні державних і громадських проектів підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту;
* проведенні навчань щодо надзвичайних ситуацій та інцидентів у кіберпросторі;
* розвитку та удосконаленні системи державного контролю за станом захисту інформації, а також системи незалежного аудиту інформаційної безпеки, запровадженні кращих світових практик і міжнародних стандартів з питань кібербезпеки та кіберзахисту;
* розвитку інфраструктури електронних комунікацій, включаючи широкосмуговий доступ до мережі Інтернет, цифрове та інтерактивне телебачення;
* розвитку мережі команд реагування на комп'ютерні надзвичайні події;
* створенні системи своєчасного виявлення, запобігання та нейтралізації кіберзагроз, у тому числі із залученням волонтерських організацій;
* розвитку та вдосконаленні системи технічного і криптографічного захисту інформації;”[3]
* “розвитку міжнародного співробітництва у сфері забезпечення кібербезпеки, підтримці міжнародних ініціатив у сфері кібербезпеки, які відповідають національним інтересам України, поглибленні співпраці України з ЄС та НАТО для посилення спроможностей України у сфері кібербезпеки, участі у заходах зі зміцнення довіри у кіберпросторі, які проводяться під егідою ОБСЄ;
* створенні умов для впровадження в Україні сучасних технологій кіберзахисту.

Кіберзахист державних електронних інформаційних ресурсів та інформаційної інфраструктури, призначеної для обробки інформації, вимога щодо захисту якої встановлена законом, має полягати, насамперед, у:

* створенні та забезпеченні функціонування національної телекомунікаційної мережі - єдиної платформи захищених електронних комунікацій органів державної влади;
* упровадженні організаційно-технічної моделі національної системи кібербезпеки, оперативному реагуванні на кібератаки та кіберінциденти;
* розгортанні (відповідно до компетенції) єдиної системи ситуаційних центрів профільних органів державної влади сектору безпеки і оборони на базі захищеної інформаційної інфраструктури;
* розбудові захищеної інтегрованої системи електронних державних реєстрів, баз даних, дата-центрів, у тому числі єдиного дата-центру резервного збереження інформації і відомостей державних електронних інформаційних ресурсів;
* удосконаленні системи зберігання, передачі та обробки даних державних реєстрів і баз даних із застосуванням сучасних інформаційно- комунікаційних технологій (включаючи технології онлайн-доступу);
* розробленні нових методів запобігання кібератакам, кіберінцидентам та поширенню інформації про них;
* розробленні вимог (правил, настанов) щодо безпечного використання мережі Інтернет та надання електронних послуг державними органами;”[3]
* “підвищенні обізнаності працівників державних органів у сфері інформаційної безпеки та кібербезпеки, проведенні відповідних тренінгів, навчань.

Кіберзахист критичної інфраструктури має полягати, насамперед, у:

* комплексному вдосконаленні правової основи кіберзахисту об'єктів критичної інфраструктури, визначенні критеріїв віднесення інформаційних (автоматизованих), телекомунікаційних, інформаційно-телекомунікаційних систем до критичної інформаційної інфраструктури;
* формуванні та забезпеченні функціонування державного реєстру об'єктів критичної інформаційної інфраструктури;
* регламентації вимог до кіберзахисту об'єктів критичної інфраструктури;
* створенні та забезпеченні функціонування власниками (розпорядниками) об'єктів критичної інфраструктури підрозділів кіберзахисту;
* установленні кваліфікаційних вимог для окремих категорій працівників об'єктів критичної інфраструктури з урахуванням сучасних тенденцій кібербезпеки та актуальних кіберзагроз, упровадження для таких працівників обов'язкової періодичної атестації на предмет відповідності зазначеним вимогам;
* налагодженні співробітництва між суб'єктами забезпечення кіберзахисту критичної інфраструктури, розвитку державно-приватного партнерства у запобіганні кіберзагрозам, реагуванні на кібератаки та кіберінциденти, усуненні їх наслідків, зокрема в умовах кризових ситуацій, надзвичайного і воєнного стану, в особливий період;
* розробленні та запровадженні механізму обміну інформацією між державними органами, приватним сектором і громадянами стосовно загроз критичній інформаційній інфраструктурі.

Розвиток потенціалу сектору безпеки і оборони у сфері забезпечення кібербезпеки передбачатиме здійснення в установленому порядку, зокрема, таких заходів:

* здійснення захисту технологічних процесів на об'єктах критичної інфраструктури, в яких управління або моніторинг здійснюється за допомогою”[3] “інформаційно-комунікаційних технологій, від несанкціонованого втручання у їх роботу;
* періодичне проведення огляду національної системи кібербезпеки, розроблення галузевих індикаторів стану кібербезпеки;
* розроблення та впровадження протоколів спільних дій, зокрема інформаційного обміну у режимі реального часу, суб'єктів забезпечення кібербезпеки під час виявлення кібератак та кіберінцидентів;
* проведення навчань суб'єктів сектору безпеки і оборони щодо реагування на кібератаки та кіберінциденти, зокрема, проведення кібернавчань Збройних Сил України, інших суб'єктів сектору безпеки і оборони України, участь у таких навчаннях у рамках заходів колективної оборони;
* реалізація державного стратегічного планування та програмно- цільового забезпечення у сфері розвитку електронних комунікацій, інформаційних технологій, захисту інформації та кіберзахисту;
* здійснення воєнно-політичних, військово-технічних та інших заходів для розширення можливостей Воєнної організації держави, сектору безпеки і оборони у кіберпросторі, створення, розвиток сил, засобів та інструментів можливої відповіді на агресію у кіберпросторі, яка може застосовуватись як засіб стримування військових конфліктів та загроз у кіберпросторі (активний кіберзахист);
* створення єдиного підрозділу із забезпечення кібербезпеки та кіберзахисту Збройних Сил України на стратегічному, оперативному та тактичному рівнях;
* розвиток підрозділів кібербезпеки та кіберзахисту Збройних Сил України, Державної служби спеціального зв'язку та захисту інформації України, Служби безпеки України, Національної поліції України, розвідувальних органів, досягнення сумісності із відповідними підрозділами кібербезпеки та кіберзахисту держав - членів НАТО;
* сприяння розвитку системи оперативного реагування на комп'ютерні надзвичайні події;”[3]
* “удосконалення системи контррозвідувального та оперативно-розшукового забезпечення кібербезпеки держави;
* розвиток та координація проведення наукових досліджень у галузі кібербезпеки та кіберзахисту для потреб національної безпеки і оборони;
* підвищення спроможності суб'єктів боротьби з кібертероризмом щодо протидії кібератакам на державні електронні інформаційні ресурси, об'єкти критичної інфраструктури, а також розвідувально-підривної діяльності іноземних спецслужб, організацій, груп та осіб проти України у кіберпросторі;
* обмеження участі у заходах із забезпечення інформаційної та кібербезпеки будь-яких суб'єктів господарювання, які знаходяться під контролем держави-агресора, визнаної Верховною Радою України, або держав та осіб, стосовно яких діють спеціальні економічні та інші обмежувальні заходи (санкції), прийняті на національному або міжнародному рівні внаслідок агресії щодо України, а також обмеження використання продукції, технологій та послуг таких суб'єктів для забезпечення технічного та криптографічного захисту державних інформаційних ресурсів, посилення державного контролю у цій сфері;
* розмежування кримінальної відповідальності за злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, вчинені щодо державних та інших інформаційних ресурсів, щодо об'єктів критичної інформаційної інфраструктури та інших об'єктів, а також відповідне розмежування підслідності;
* розвиток системи підготовки кадрів для потреб органів сектору безпеки і оборони України та розвиток науково-виробничого потенціалу такої системи.

Боротьба з кіберзлочинністю передбачатиме здійснення в установленому порядку, серед іншого, таких заходів:

* створення ефективного і зручного контакт-центру для повідомлень про випадки кіберзлочинів та шахрайства у кіберпросторі, підвищення оперативності реагування на кіберзлочини правоохоронних органів, зокрема їх регіональних підрозділів;”[3]
* “удосконалення процесуальних механізмів щодо збирання доказів в електронній формі, що стосуються злочину, удосконалення класифікації, методів, засобів і технологій ідентифікації та фіксації кіберзлочинів, проведення експертних досліджень;
* запровадження блокування операторами та провайдерами телекомунікацій визначеного (ідентифікованого) інформаційного ресурсу (інформаційного сервісу) за рішенням суду;
* унормування порядку внесення обов'язкових до виконання операторами та провайдерами телекомунікацій приписів про термінове фіксування та подальше зберігання комп'ютерних даних, збереження даних про трафік;
* врегулювання питання можливості термінового здійснення процесуальних дій у режимі реального часу із застосуванням електронних документів та електронного цифрового підпису;
* упровадження схеми (протоколу) координації правоохоронних органів щодо боротьби з кіберзлочинністю;
* підготовка суддів (слідчих суддів), слідчих та прокурорів для роботи з доказами, що стосуються злочину, отриманими в електронній формі, з урахуванням особливостей кіберзлочинів;
* запровадження особливого порядку зняття інформації з каналів телекомунікацій у випадку розслідування кіберзлочинів;
* підвищення кваліфікації співробітників правоохоронних органів.

Прикінцеві положення

Положення Стратегії враховуються у розробленні інших документів стратегічного планування суб'єктів сектору безпеки і оборони України у сфері кібербезпеки. “[3]

## Вимоги до захисту інформації web – сторінки від несанкціонованого доступу

“Галузь використання

Цей нормативний документ системи технічного захисту інформації (НД ТЗІ) встановлює вимоги до технічних та організаційних заходів захисту інформації WEB-сторінки в мережі Інтернет.

Згідно з визначеними НД ТЗІ 2.5-004-99 специфікаціями він встановлює мінімально необхідний перелік послуг безпеки інформації та рівнів їх реалізації у комплексах засобів захисту інформації WEB-сторінки від несанкціонованого доступу.

Мета цього НД ТЗІ – надання нормативно-методологічної бази для розроблення комплексу засобів захисту від несанкціонованого доступу до інформації WEB-сторінки під час створення комплексної системи захисту інформації.

Цей НД ТЗІ призначений для суб’єктів відносин (власників або розпорядників WEB-сторінки, операторів (провайдерів), користувачів), діяльність яких пов’язана з розробкою та експлуатацією WEB-сторінки, розробників комплексної системи захисту інформації та постачальників окремих її компонентів, а також для фізичних та юридичних осіб, які здійснюють оцінку захищеності WEB-сторінки на відповідність вимогам ТЗІ.

Встановлені цим НД ТЗІ вимоги є обов’язковими для виконання державними органами, Збройними Силами України, іншими військовими формуваннями, утвореними відповідно до законів України, Радою Міністрів Автономної республіки Крим та органами місцевого самоврядування, а також підприємствами, установами та організаціями (далі - установи) усіх форм власності під час захисту інформації, що належить до державних інформаційних ресурсів на WEB-сторінках.

Для захисту інших видів інформації власники WEB-сторінок користуються цим НД ТЗІ на власний розсуд.

Визначення

У цьому НД ТЗІ використовуються терміни та визначення, що відповідають встановленим ДСТУ 2226 та НД ТЗІ 1.1-003.

Інші терміни, ужиті в цьому НД ТЗІ, мають такі значення:”[4]

“Інтернет (мережа Інтернет) – сукупність мереж та обчислювальних засобів, які використовують стек протоколів TCP/IP, спільний простір імен та адрес для забезпечення доступу до інформаційних ресурсів мережі будь-якій особі;

Оператор (провайдер, provider) – юридична або фізична особа, яка надає користувачам доступ до мережі Інтернет;

Браузер (browser) – програмне забезпечення, що надає інтерфейс для доступу до інформації WEB-сторінок та їх перегляду;

Робоча станція (клієнт мережі) – окрема (персональна) ЕОМ або віддалений термінал мережі, з яких користувачі отримують доступ до ресурсів мережі Інтернет;

Сервер (server) – об’єкт комп’ютерної системи (програмний або програмно-апаратний засіб), що надає послуги іншим об’єктам за їх запитами;

WEB-сервер – сервер, який обслуговує запити користувачів (клієнтів) згідно з протоколом HTTP, забезпечує актуалізацію, збереження інформації WEB-сторінки, зв’язок з іншими серверами;

WEB-сторінка (WEB-сайт) – мережевий інформаційний ресурс, що надається користувачу у вигляді HTML-документу і має у мережі свою унікальну адресу;

HTML-документ – файл текстової або нетекстової природи (звук, відео, зображення), створений за допомогою мови гіпертекстової розмітки HTML;

Посилання (гіпертекстове посилання) – адреса іншого мережевого інформаційного ресурсу у форматі URL, який тематично, логічно або будь-яким іншим способом пов’язаний з документом, у якому це посилання визначене.

Загальні вимоги

* + Установа, під час створення WEB-сторінки та визначення операторів, вузли яких будуть використовуватися для підключення до мережі Інтернет, повинна керуватися законами України, іншими нормативно-правовими актами, що встановлюють вимоги з технічного захисту інформації.
  + WEB-сторінка установи може бути розміщена на власному сервері або на сервері, що є власністю оператора. Власник сервера зобов’язаний гарантувати власнику інформації рівень захисту у відповідності до вимог цього НД ТЗІ.”[4]
  + “Функціонування WEB-сторінки забезпечується АС, за допомогою якої здійснюється актуалізація розміщених на WEB-сторінці інформаційних ресурсів та керування доступом до них.
  + Для забезпечення захисту інформації WEB-сторінки в цій АС створюється КСЗІ, що є сукупністю організаційних і інженерно-технічних заходів, а також програмно-апаратних засобів, які забезпечують захист інформації.
  + Створення КСЗІ здійснюється відповідно до технічного завдання, розробленого згідно з НД ТЗІ 3.7-001.
  + КСЗІ підлягає державній експертизі у порядку, передбаченому Положенням про державну експертизу в сфері технічного захисту інформації.
  + Захист інформації на всіх етапах створення та експлуатації WEB-сторінки здійснюється відповідно до розробленого установою плану захисту інформації, зміст якого визначено НД ТЗІ 1.4-001. План захисту затверджується керівником установи, а у випадку використання сервера оператора – погоджується з власником сервера.
  + Перелік інформації, призначеної для публічного розміщення на WEB-сторінці, визначається з урахуванням вимог діючого законодавства та затверджується керівником установи, що є власником WEB-сторінки.
  + Організація робіт із захисту інформації та забезпечення контролю за станом її захищеності на WEB-сторінці в установі здійснюється відповідальним підрозділом або відповідальною особою (далі - службою захисту інформації, СЗІ).
  + У випадку користування послугами оператора щодо розміщення, експлуатації та адміністрування WEB-сторінки власник інформацїі укладає з оператором договір (угоду), яким визначаються права і обов’язки сторін, умови підключення, розміщення інформації та забезпечення доступу до неї, інші питання, що вимагають урегулювання між власником інформації WEB-сторінки та оператором, виходячи з вимог законодавства у сфері захисту інформації та цього НД ТЗІ.
  + Окремі питання із захисту інформації можуть оформлятися у вигляді додатків, які є невід’ємною частиною договору.”[5]

“Характеристика типових умов функціонування та вимоги до захисту інформації WEB-сторінки

До складу АС, яка забезпечує функціонування WEB-сторінки, входять: ОС, фізичне середовище, в якому вона знаходиться і функціонує, середовище користувачів, оброблювана інформація, у тому числі й технологія її оброблення. Під час забезпечення захисту інформації мають бути враховані всі характеристики зазначених складових частин, які впливають на реалізацію політики безпеки WEB-сторінки.

У випадку, якщо WEB-сторінка містить посилання на інформаційні ресурси іншої WEB-сторінки, умови функціонування останньої не повинні порушувати встановлену для даної WEB-сторінки політику безпеки.

У цьому розділі визначаються типові умови функціонування всіх складових АС, вводяться обмеження до умов функціонування та встановлюються загальні вимоги із захисту інформації до окремих компонентів АС. Для визначеної таким чином типової схеми функціонування АС встановлюються можливі варіанти для вибору функціональних профілів захищеності інформації від НСД.

Інформація WEB-сторінки та технологія її оброблення

Характеристика

* Інформація WEB-сторінки поділяється на дві категорії:

1. загальнодоступна інформація;
2. технологічна інформація.

* До загальнодоступної інформації відноситься публічно оголошувана інформація, користуватися якою можуть будь-які фізичні або юридичні особи (користувачі інформаційних ресурсів), що мають доступ до мережі Інтернет.
* До технологічної інформації WEB-сторінки відноситься технологічна інформація КСЗІ та технологічна інформація щодо адміністрування та управління обчислювальною системою АС і засобами обробки інформації – дані про мережеві адреси, імена, персональні ідентифікатори та паролі користувачів, їхні повноваження та права доступу до об’єктів, інформація журналів реєстрації дій користувачів,”[6] “інша інформація баз даних захисту, встановлені робочі параметри окремих механізмів або засобів захисту, інформація про профілі обладнання та режими його функціонування, робочі параметри функціонального ПЗ тощо.

Технологічна інформація призначена для використання тільки уповноваженими користувачами з числа співробітників та персоналу, що забезпечує функціонування АС.

* + - * Способи і методи обробки інформації WEB-сторінки (зберігання, супроводження, передачі, введення, актуалізації та використання інформації) визначають технології оброблення інформації.
      * Технологічні особливості роботи користувачів із загальнодоступною інформацією WEB-сторінки визначаються особливостями системного та функціонального ПЗ, зокрема броузерів, які ними використовуються.
      * Технологічні особливості роботи користувачів інших категорій визначаються, крім того, архітектурою АС, способами оброблення та передавання інформації між компонентами АС і способами здійснення доступу до неї.

Вимоги

* + - * КСЗІ повинна забезпечувати реалізацію вимог із захисту цілісності та доступності розміщеної на WEB-сторінці загальнодоступної інформації, а також конфіденційності та цілісності технологічної інформації WEB-сторінки.
      * Технологія оброблення інформації повинна відповідати вимогам політики безпеки інформації, визначеної для АС, що забезпечує функціонування WEB-сторінки.
      * Вимоги щодо забезпечення цілісності загальнодоступної інформації WEB-сторінки та конфіденційності й цілісності технологічної інформації вимагають застосування технологій, що забезпечують реалізацію контрольованого і санкціонованого доступу до інформації та заборону неконтрольованої й несанкціонованої її модифікації.

Технологія оброблення інформації повинна бути здатною реалізовувати можливість виявлення спроб несанкціонованого доступу до інформації ”[7]

“WEB- сторінки та процесів, які з цією інформацією пов’язані, а також забезпечити реєстрацію в системному журналі визначених політикою відповідної послуги безпеки подій (як НСД, так і авторизованих звернень).

* + - * Для користувачів, які порушили встановлені правила розмежування доступу до WEB-сторінки, засоби КСЗІ на період сеансу роботи повинні забезпечити блокування доступу до WEB-сторінки.
      * Технологічними процесами повинна бути реалізована можливість створення резервних копій інформації WEB-сторінки та процедури їх відновлення з використанням резервних копій.
      * Технологія оброблення інформації повинна передбачати можливість аналізу використання користувачами і процесами обчислювальних ресурсів АС і забезпечувати керування ресурсами.”[4]

## Висновки по розділу

На наш час зберігання даних не можливе без застосування як криптографічних перетворень так і розмежування прав доступу. Процедури ідентифікації та автентифікації широко користуються усіма сучасними засобами криптографії, а більшість сервісів та служб використовується видаленно, через інтернет. Забезпечення якісного контролю за цілісністю та доступністю інформації – головні критериї які повинні виконуватись у сучасних системах. Для розмежування прав доступу використовуються різні варіації автентифікації від біометричних до парольних але це не має сенсу якщо інформація буду зберігатися в не захищеному форматі.

# РОЗДІЛ 2

# АНАЛІЗ КРИПТОГРАФІЧНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

## Проблема захисту інформації

Інформаційні ресурси держави або суспільства в цілому, а також окремих організацій і фізичних осіб являють собою певну цінність, мають відповідне матеріальне вираження і вимагають захисту, оскільки несанкціонований доступ може, завдати збитків та призвести до зниження цінності інформаційних ресурсів. Впливи, які призводять до зниження цінності інформаційних ресурсів, називаються несприятливими. Потенційно можливий несприятливий вплив називається загрозою.

Захист інформації, що обробляється, полягає в створенні і підтримці в дієздатному стані системи заходів, як технічних, інженерних, програмно-апаратних, так і нетехнічних, правових, організаційних, що дозволяють запобігти або ускладнити можливість реалізації загроз, а також знизити потенційні збитки. Такий захист э необхіний як у мирний час так і під час інформаційної війни. Приватні та державні підприємства та організації мають конфіденційні та персональні данні які необхідно захищати, для уникнення витоку даних та збитків. Іншими словами, захист інформації спрямовано на забезпечення безпеки оброблюваної інформації в цілому, тобто такого стану, який забезпечує збереження заданих властивостей інформації , що її обробляє. Система зазначених заходів, що забезпечує захист інформації, називається комплексною системою захисту інформації.

Але на даний момент при вирішенні технічних проблем захисту інформації, велику загрозу конфіденцільнсті становлять організаційні та комунікаційні проблеми.   
 Ось на приклад: зі зростанням як внутрішнього так і зовнішнього ринку в країні зростає чило програмістів, дизайнерів, архітекторів та багато інших спеціалістів в області інформаційних послуг. Зазвичай такі професії вимгають навіть для навчання сучасні та швидкі комп’ютери але не всі мають можливість придбати професіні машини, які необхідні для їх діяльності. Попит породжує пропозиції тому зараз існують офіси в яких в аренду здатюся робочі місця разом із професійними та не дешевими комплектуючими, які підходять для буд яких, навіть, графічних робіт. За дуже вигідними цінами. Навіть студент може користуватися подібними послугами. Але що робити, якщо необхідно працювати із інформацією яка не підлягає розголошенню, а можливості придбати свій компютер – нема. Нікто не дасть гарантію, ніхто не стане працювати з вашим комп’ютером у час вашої відсутності. Велика кількість людей, а також не усі навість знають один одного – це великий прострір для махінацій різного роду.

Такі самі загрози мають місце навіть державних підприємстваї та службах. Так, зараз більшість програм перейшла на хмарні технології, але навіть і вони не захищені від організаційних проблем, через які злоумисник може здобудти небхідну інформацію, не зважаючі на передові методи аутентифікації та найбезпечніші систмеи передачі данних. Адже усі звикли до комфорту і користуються автозаповненням паролів та форм, записуванням паролів на папірцях – це не пристумо але людський фактор залишає дуже багато можливостей для злодіїв. Адже більшість звикла, що злоумисники десь там – дуже далекою.

Порушення кібербезпеки все частіше зустрічаються в промисловості та уряді, і оборонна промисловість не є винятком. По мірі того, як вартість цих порушень сягає мільярдів гривень, попит на більш жорткий контроль та регулювання кібербезпеки надходить з найвищих рівнів влади.

Протягом останнього десятиліття рівень глобальної кіберзагрози посилювався, піддаючи схожу приватну промисловість та уряд, що посилюється шквалом кібер-атак. Ці вторгнення зростали не лише частотою, але й суворістю, оскільки тепер вони несуть відповідальність за мільярди гривень, що втрачаються щороку. Як державні, так і приватні організації втрачають велику кількість ресурсі від кібератак у всьому світі, привертаючи увагу як засоби масової фнформації, так і політиків. Незважаючи на небажання приватної галузі ділитися новинами про вторгнення в їхні мережі, зараз ми маємо безліч прикладів, що ілюструють діапазон атак, що відбулися.

Зі збільшенням вартості та тяжкості кібератак уряд намагався розробити рішення. Державні та місцеві політичні діячі здійснили безліч акцій, щоб залучити державні та приватні підприємства до укріплення кібербезпеки, охоплюючи низку заходів виконавчої та законодавчої діяльності. Ці заходи, часто зумовлені сприйнятою потребою реагувати на гучні кібер-інциденти, часто є хибними та фрагментарними. Хоча цілеспрямовані, розпорядчі документи, пропонують широкий, але чітко визначений підхід загального уряду до зменшення кібер-ризику, в той час як виконавчі агенції не відповідають адекватному зміцненню державних активів, операцій та інструментів проти атак.

Тим, хто перебуває на оборонній промисловій базі, залишається проходити через складний, багатошаровий набір політичних регламентів, які містять окремі органи влади та конфліктуючі інституційні агенти. Залякуючи навіть найвідоміших підрядників із оборони, це одіозне регуляторне середовище є загрозливим бар'єром для вступу та головним стримуючим фактором для кращих практик кібербезпеки. Представлені резюме регуляторних органів, які безпосередньо відповідають за таке середовище, щоб розмежовувати та демістифікувати нову хвилю кіберрегламентів.

Будь-яке обговорення ефективності реагування політики на кіберзагрози є неповним без перспективи оборонної промислової бази. Часто виступаючи першою лінією оборони та предметом нових та діючих норм, члени цієї групи мають унікальну кваліфікацію для оцінки поточного стану справ. Було розроблено та застосовано інструмент обстеження для виведення перспектив галузі. Були включені запитання щодо вимірювання фінансового впливу відповідності кібер-політиці, визначення найкращих практик кіберзахисту та роз'яснення думки галузі щодо діючих кіберзаконів. [5]

* + - * Понад 25 відсотків професіоналів галузі працюють для фірм, які пережили кібератаку.
      * Промисловість розглядає кібер-атаки з боку зовнішніх суб'єктів як найсерйознішу кіберзагрозу, за якою уважно слідує модель кібератаки від колишнього співробітника.
      * Невеликі компанії використовують заходи безпеки, такі як брандмауер та багатофакторна автентифікація за значно нижчою швидкістю, ніж великі компанії.
      * Дуже мала кількість компаній впевнена у своїй здатності оговтатися від кібератаки протягом 24 годин.
      * 30 відсотків компаній не мають хорошого розуміння витрат, необхідних для відновлення після кібератаки.
      * Малі підприємства на 15 відсотків рідше, ніж великі, погоджуються із твердженням, що “наші працівники добре готові зрозуміти і реагувати на загрози кібербезпеки”.

Посилення комунікацій, правильне зменшення потоку інформації та спрощення діючого режиму кіберрегулювання - це перші кроки, які слід зробити уряду для підвищення операційної безпеки оборонної промисловості. Існує розбіжність між великими, усталеними суб'єктами та меншими підприємствами щодо кіберінформованості, готовності та дотримання вимог. Малому бізнесу потрібні цілеспрямовані урядові комунікації та ресурси, щоб вони залишалися частиною промислового ланцюга поставок. Нова політика також повинна консолідувати регуляторні органи для зменшення навантаження на відповідність промисловості, враховуючи поточний досвід та досвід галузевих партнерів під час розробки та впровадження політики.

В останні роки великі дані стали реальністю: дані збираються безліччю незалежних джерел, а потім їх сплавляють та аналізують для отримання знань. Великі дані відходять від попередніх наборів даних у кількох аспектах, таких як об'єм, різноманітність та швидкість. Великий обсяг даних чинить занадто великий тиск на традиційні структуровані сховища даних, і в результаті з’явилися нові технології. Кількість та різноманітність даних зробили можливим складний аналіз даних. Аналіз даних - це не лише питання опису даних або тестування гіпотез, а й генерування, раніше недоступних, знань із даних.

Хоча в інших умовах та масштабах ризик розкриття інформації вже давно викликає занепокоєння у статистичних та інформатичних спільнотах, і було запропоновано декілька методів обмеження такого ризику. Контроль статистичного розкриття інформації прагне дозволити робити корисні висновки про субпопуляції з набору даних, в той же час зберігаючи конфіденційність осіб, які внесли свої дані. [5]. Для обмеження ризику розкриття інформації щодо випуску мікроданих було запропоновано декілька методів SDC. Загальна особливість у всіх них полягає в тому, що вихідний набір даних зберігається в таємниці і випускається лише модифікована, анонімізована, його версія. В останні роки було запропоновано кілька моделей конфіденційності. Замість того, щоб визначати конкретну трансформацію, яка повинна бути здійснена на початкових даних, моделі конфіденційності визначають умови, яким повинен відповідати набір даних, щоб тримати під контролем ризик розкриття інформації. Моделі конфіденційності зазвичай залежать від одного або декількох параметрів, які визначають, наскільки ризик розкриття інформації прийнятний. Існуючі моделі конфіденційності були здебільшого розроблені з урахуванням єдиного статичного набору даних. Однак для великих даних цього параметра вже не вистачає.

Потенційний ризик для конфіденційності є одним з найбільших недоліків великих даних. Слід враховувати, що великі дані - це збирання якомога більшої кількості даних для отримання знань з них. Більше того, більш ніж часто ці дані свідомо не надаються суб'єктом даних, як правило, споживачем, громадянином, але вони генеруються як побічний продукт якоїсь транзакції, наприклад, перегляд чи купівля предметів в інтернет-магазині, або їх отримує постачальник послуг взамін за якусь безкоштовну послугу, наприклад, безкоштовні акаунти електронної пошти, соціальні мережі, або як природна вимога до якоїсь послуги ,наприклад, GPS-навігаційна система потребує знань про позицію особи, щоб забезпечити її з інформацією про умови руху поблизу.

На даний момент не існує чіткого погляду на найкращу стратегію чи стратегію захисту конфіденційності у великих даних. До появи великих даних такі принципи мали широке застосування у кількох регламентах щодо захисту особистої інформації, що ідентифікується:

* + - * Законність . Згода має бути отримана від суб'єкта, або обробка повинна бути необхідна для договору чи юридичного зобов'язання, життєвих інтересів суб'єкта, суспільних інтересів або законних інтересів процесора, сумісних з правами суб'єкта.
      * Згода, яку дає суб'єкт, повинна бути простою, конкретною, поінформованою та явною.
      * Обмеженнямети . Мета збору даних повинна бути законною та визначеною перед збором.
      * Sddf Необхідність та мінімізація даних . Збирати слід лише ті дані, які потрібні для конкретних цілей. Крім того, дані повинні зберігатися лише стільки, скільки потрібно.
      * Індивідуальні права . Суб'єктам слід надати доступ до даних на них, а також можливість виправити або навіть видалити такі дані (право бути забутими).
      * Інформаційна безпека . Зібрані дані повинні бути захищені від несанкціонованого доступу, обробки, маніпуляції, втрати чи знищення.
      * Прозорість та відкритість . Суб'єкти повинні отримувати інформацію про збір та обробку даних таким чином, щоб вони зрозуміли.
      * Підзвітність . Збірник та обробник даних повинен мати можливість демонструвати відповідність вищезазначеним принципам.
      * Захист даних дизайн та за замовчуванням. Конфіденційність повинна бути вбудована з самого початку, а не додана пізніше.

Без анонімізації між зазначеними принципами та метою великих даних виникає кілька потенційних конфліктів:

* + - * Захист Обмеження мети . Великі дані часто використовуються вдруге для цілей, навіть не відомих під час збору.
      * Згода . Якщо мета збору даних не зрозуміла, згоду не можна отримати.
      * Законність . Без обмеження мети та згоди правомірність сумнівна.
      * Необхідність та мінімізація даних . Великі дані є результатом акумулювання даних для потенційного використання.
      * В Індивідуальні права . Окремі суб'єкти навіть не знають, які дані зберігаються на них, або навіть хто зберігає дані. Тому доступ, виправлення чи стирання даних є для них нездійсненним.
      * Підзвітність . Відповідність не відповідає, а значить, її неможливо продемонструвати.

Враховуючи вищезазначені конфлікти між принципами конфіденційності та великими даними, стверджувалося, щоб уникнути перешкод на технологічному розвитку, захист конфіденційності повинен зосереджуватися лише на використанні даних, які можуть завдати шкоди конфіденційності, а не на зборі даних або навіть допускати саморегуляцію. У протилежному таборі також стверджувалося, що саме збір даних викликає можливі порушення конфіденційності. Дійсно, після збору даних виникає багато потенційних загроз.[6]:

* + - * Порушення даних*.* Це може статися внаслідок агресивного злому або недостатнього вжиття заходів безпеки. Чим більше даних зібрано, тим привабливішими вони стають для зловмисника.
      * Внутрішнє зловживання працівниками.[6]
      * Небажане вторинне використання.
      * Зміни в практиці компанії . Політика, яка заважає компанії брати участь у використанні даних, що шкодять інтересам суб'єктів, може змінитися.
      * Доступ уряду без належних юридичних гарантій.
      * Методи анонімізації - це можливе рішення для подолання конфліктів між принципами конфіденційності та великими даними. Методи анонімізації стикаються з певними труднощами при застосуванні до великих даних. З одного боку, занадто мало анонімізації наприклад, просто де-дентифікація шляхом придушення прямих ідентифікаторів, може бути недостатньою для забезпечення неідентифікованості. Це стає більш проблематичним для великих даних, оскільки кількість та різноманітність даних про людину накопичується, повторна ідентифікація стає більш правдоподібною. З іншого боку, занадто сильна анонімізація може перешкоджати пов'язуванню даних про одну і ту саму окрему тему, або про подібні окремі теми, які надходять із різних джерел, і таким чином, перешкоджати багатьом потенційним перевагам великих даних.

Хоча очевидно, що існує велика напруженість між великими даними та анонімізацією даних, але ми не повинні виключати останніх. Справді, правда, що анонімізація може перешкоджати деякому використанню великих даних (в основному тих, які використовують цільові конкретні особи), але анонімізовані дані все ще дають змогу проводити більшість аналізів, у яких ціллю є достатньо велика громада або все населення.

Хоча очевидно, що існує проблема між великими даними та анонімізацією даних, але ми не повинні виключати останніх. Справді, правда, що анонімізація може перешкоджати деякому використанню великих даних, в основному тих, які використовують цільові конкретні особи, але анонімізовані дані все ще дають змогу проводити більшість аналізів, у яких ціллю є достатньо велика громада або все населення.

Технології SDC, наприклад, глобальне перекодування, придушення, кодування верхнього та нижнього, мікроагрегація, задають перетворення даних, метою яких є обмеження ризику розкриття інформації. Однак загалом вони не визначають жодного механізму для оцінки того, який ризик розкриття інформації залишається у перетворених даних. Однак реальність полягає в тому, що більшість моделей конфіденційності розроблені для захисту єдиного статичного оригінального набору даних, і, таким чином, існує кілька важливих обмежень у їх застосуванні до великих параметрів даних.

Три характеристики, які часто називаються великими даними, - це об'єм, різноманітність та швидкість. Обсяг відноситься до того, що обсяг даних, що підлягають аналізу, великий. Різноманітність стосується того, що великі дані складаються з неоднорідних типів даних, витягнутих та злитих з декількох різних джерел. Під швидкістю розуміється швидкість генерації та обробки даних. Звичайно, не всі перераховані вище властивості повинні узгоджуватися для використання великих іменних даних, але хоча б деякі з них потрібні. Незважаючи на те, що обсяг відображений у назві “великих” даних, зазвичай різноманітність розглядають як найбільш релевантну особливість великих даних.

Щоб модель конфіденційності була корисною в умовах великих даних, вона повинна добре справлятися з обсягом, різноманітністю та швидкістю. Щоб визначити придатність моделі конфіденційності для великих даних, ми розглянемо, наскільки вона задовольняє наступним трьом властивостям:

Композиційність. Модель конфіденційності є композиційною, якщо гарантії конфіденційності моделі зберігаються, можливо, в обмеженій мірі, після неодноразового незалежного застосування моделі конфіденційності. З іншого боку, модель конфіденційності не можна використовувати, якщо кілька незалежних випусків даних, кожен із яких відповідає вимогам моделі конфіденційності, можуть призвести до порушення конфіденційності.

Обчислювальна вартість . Обчислювальна вартість вимірює обсяг роботи, необхідний для перетворення вихідного набору даних у набір даних, що задовольняє вимогам моделі конфіденційності. Раніше ми згадували, що, як правило, існує різноманітна техніка SDC, яка може бути використана для задоволення вимог моделі конфіденційності. Таким чином, обчислювальна вартість залежить від конкретної обраної методики SDC. Оцінюючи вартість моделі конфіденційності, ми розглянемо найбільш поширені підходи.

Пов’язаність. У великих даних інформація про особу збирається з декількох незалежних джерел. Отже, можливість зв’язувати записи, які належать одному і тому ж, або подібному, особі, є головним у створенні великих даних. Зважаючи на захист конфіденційності, дані, зібрані певним джерелом, повинні бути анонімізовані перед випуском. Однак ця незалежна анонімізація може обмежувати можливості злиття даних, тим самим сильно обмежуючи спектр аналізів, які можуть бути виконані на даних, і, отже, знання, які можуть бути отримані з них. Кількість взаємозв'язків, сумісних із моделлю конфіденційності, визначає, чи може аналітик зв’язувати дані незалежно, анонімізовані відповідно до цієї моделі, які відповідають одній і тій же особі. Зауважте, що пов'язуючи записи, що належать одній особі, ми збільшуємо інформацію про цю особу. Це загроза конфіденційності, і, отже, точність зв’язків повинна бути меншою в анонімованих наборах даних, ніж в оригінальних наборах даних.

Усі перераховані вище властивості моделі конфіденційності здаються важливими для ефективної роботи з великими даними. Далі ми детально обговорюємо важливість кожної власності.

Композиційні можливості є важливими для того, щоб гарантії конфіденційності моделі мали значення в контексті великих даних. У великих даних процес збору даних не є централізованим, а розподіляється між декількома джерелами даних. Якщо один із збирачів даних переймається конфіденційністю та вирішує використовувати конкретну модель конфіденційності, гарантії конфіденційності вибраної моделі повинні зберігатися. певною мірою, після злиття даних. Композиційність може бути оцінена між випусками даних, що задовольняють однаковій моделі конфіденційності, між випусками даних, що задовольняють різні моделі конфіденційності, і між випуском даних, що задовольняє модель, конфіденційності, та неанонімованими даними.

Низька обчислювальна вартість також є дуже важливою особливістю моделі конфіденційності, якщо вона повинна залишатися практичною для великих даних, враховуючи, що однією з основних властивостей великих даних є обсяг. тобто великі набори даних. Алгоритми, що мають лінійну або лінійну вартість на розмір набору даних, здаються можливими альтернативами. Алгоритми з квадратичною вартістю або вище не є можливими для великих наборів даних. Кілька простих модифікацій дорогого алгоритму можна зробити більш ефективними. Однією з таких модифікацій є розподіл оригінального набору даних на кілька менших наборів даних та анонімізація кожного з них окремо. Звичайно, розділення може мати наслідки для корисності та конфіденційності отриманих даних; такі наслідки слід аналізувати у кожному конкретному випадку.

Нарешті, важливість зв'язку також є важливою, оскільки великі дані отримуються шляхом сплавлення вхідних даних з різних джерел. Більш точно, можливість аналізу даних про одного і того ж індивіда в різних наборах даних є найважливішим для аналізу даних. Таким чином, щоб бути корисним для великих даних, модель конфіденційності повинна дозволяти анонімним даним деяким чином залишатися взаємозв’язаними.

Хоча анонімізація даних не є всеосяжним рішенням конфіденційності великих даних, наприклад, це може зірвати деякі типи аналізу даних, це, безумовно, може бути корисним інструментом для вирішення вищезгаданих зіткнень. Однак особливі характеристики великих даних, головним чином, вимоги щодо сполучуваності та накопичення даних, зібраних з багатьох джерел, ставлять під сумнів звичайні підход.

## Методи і способи захисту інформації

Зазвичай комп'ютерне обладнання захищене тими ж засобами, які використовуються для захисту іншого цінного або чутливого обладнання, а саме серійних номерів, дверей та замків та сигналізацій. Захист інформації та доступу до системи, з іншого боку, досягається за допомогою інших тактик, деякі з них досить складні.

Заходи безпеки, пов'язані з інформацією про комп’ютер та інформацією про доступ, стосуються чотирьох основних загроз:

* + - * Крадіжка даних, таких як військова таємниця з державних комп'ютерів; вандалізм, включаючи знищення даних комп'ютерним вірусом;
      * шахрайства, такі як працівники банку, що спрямовують кошти на власні рахунки;
      * вторгнення в приватне життя, наприклад, незаконний доступ до захищених особистих фінансових чи медичних даних з великої бази даних.

Найбільш загальним засобом захисту комп'ютерної системи від крадіжок, вандалізму, вторгнення в приватне життя та інших безвідповідальних поведінок є електронний відстеження та реєстрація доступу до різних користувачів комп'ютерної системи та їх використання. Зазвичай це робиться шляхом присвоєння індивідуального паролю кожній особі, яка має доступ до системи. Але обов’язково необхідний системний підхід до системи захисту інформації. Це означає поєднання усіх компонентів інформаційної безпеки: організаційних, фізичних, апаратних, програмних та інших властивостей. Слід використовувати тільки підтверджені та сертифіковані державними станати. При створенні якісної системи захисту інформації вона може автоматично відстежувати використання цих паролів, записуючи такі дані, до яких файлів можна було отримати доступ під певні паролі тощо. Іншим заходом безпеки є збереження даних системи на окремому пристрої або носії, наприклад, магнітній стрічці або дисках, які, як правило, недоступні через комп'ютерну систему. Нарешті, дані часто шифруються, щоб їх можна було розшифрувати лише власниками єдиного ключа шифрування

Реалізація політики безпеки потребує налаштування засобів захисту, управління системою захисту і здійснення контролю функціонування. Саме кібербезпека займається вирішеня проблем захисту інформації.   
Кібербезпека відноситься до профілактичних методів, що застосовуються для захисту інформації від крадіжки, компрометації чи нападу. Це вимагає розуміння потенційних інформаційних загроз, таких як віруси та інший шкідливий код. Стратегії кібербезпеки включають управління особистістю, управління ризиками та управління інцидентами. Кібербезпека - це дуже широка категорія, яка охоплює численні апаратні та програмні технології, і їх можна застосовувати на будь-якому рівні, включаючи особисті, корпоративні чи урядові пристрої чи мережі.

Паролі – це інструмент кібербезпеки, з яким люди стикаються майже щодня. Інші поширені засоби кібербезпеки включають:

* + - * Противірусне програмне забезпечення;
      * програмні виправлення;
      * брандмауери;
      * двофакторна аутентифікація;
      * шифрування.

План кібербезпеки є критично важливим для будь-якої компанії з дуже чутливою інформацією.

Політика безпеки інформаційних технологій  визначає правила та процедури для всіх осіб, які отримують доступ та використовують ресурси та ресурси організації. Ефективна політика безпеки – це модель культури організації, в якій правила та процедури керуються підходом працівників до їх інформації та роботи. Таким чином, ефективна політика безпеки – це унікальний документ для кожної організації, який розробляється з точки зору її людей щодо толерантності до ризиків, того, як вони бачать та цінують свою інформацію, а також наявну в них доступність, яку вони підтримують. З цієї причини багато компаній вважають політику безпеки недоцільною, оскільки її не враховують, як люди організації фактично використовують та обмінюються інформацією між собою та громадськістю.

Завданнями політики інформаційної безпеки є збереження конфіденційності, цілісності та доступності систем та інформації, якими користуються члени організації. Ці три принципи складають :

* Конфіденційність передбачає захист активів від сторонніх осіб
* Цілісність забезпечує модифікацію активів, які здійснюються у визначений та дозволений спосіб
* Доступність - це стан системи, в якому авторизовані користувачі мають постійний доступ до цих ресурсів

Зараз багато компаній призначають головного співробітника служби безпеки або головного працівника інформаційної безпеки для нагляду за їх кібербезпекою.

Завдання управління і контролю зазвичай вирішуються адміністративною групою, склад і розмір якої залежать від конкретних умов. Часто така група працює у складі: адміністратор безпеки, менеджер безпеки та оператори. Система інформаційної безпеки повинна мати певні види власного програмного забезпечення, спираючись на які вона буде здатна виконувати свою цільову функцію.

Усю сукупність технічних засобів поділяють на апаратні й фізичні. Крім того є програмні та організаційні засоби. Тако ж існують такі загальні підходи криптографічних перетворень та методи реалізації інформаційної безпеки:

Аутентифікація:

* + - * Аутентифікація використовується сервером, коли серверу необхідно точно знати, хто отримує доступ до їх інформації чи сайту.
      * аутентифікація використовується клієнтом, коли клієнт повинен знати, що сервер є системою, на яку він претендує.
      * під час аутентифікації користувач або комп'ютер повинні довести свою особу серверу чи клієнту;
      * зазвичай аутентифікація сервером тягне за собою використання імені користувача та пароля. Інші способи аутентифікації можуть бути через картки, сканування сітківки, розпізнавання голосу та відбитки пальців;
      * аутентифікація клієнтом зазвичай включає сервер, який надає клієнту сертифікат, у якому довірена третя сторона, така як Verisign або Thawte, заявляє, що сервер належить до юридичної особи, наприклад, банку, на яку клієнт очікує;
      * зазвичай аутентифікація сервером тягне за собою використання імені користувача та пароля. Інші способи аутентифікації можуть бути через картки, сканування сітківки, розпізнавання голосу та відбитки пальців.

Хешування — це ділення на блоки повідомлення, які, як правило, можуть бути представлені у вигляді масивів, на підмножини, що володіють певними властивостями. Такі властивості зазвичай описуються хеш-функцією, та називаються хеш-адресою. Для виконання зворотнього процесу використовують хеш-таблиці. Такі структури забезпечують швидкий та безпомилковий доступ до елементу таблиці за хеш-адресою. У ідеальних умовах, зазвичай, використовуючи ключ за одне звернення отримується доступ до елементу, але для цього хеш-адреса має бути унікальною. У той самий час, в реальних ситуаціях зазвичай трапляється так, що за однаковою хеш-адресою можуть знаходитися декілька елементів, а тому, для реалізації алгоритму, доводиться використовувати компроміси. Також хешування перетворює у бітовий рядок фіксованої довжини вхідне повідомлення, зазвичай використовуючи певну маску.

Найчастіше використовується автентифiкацiя за допомогою пароля. Вона полягає у введеннi користувачем секретної фрази, що вiдповiдає його попередньто визначено iдентифiкатору. Зазначена iнформацiя порiвнюється з еталонним паролем, що зберiгається у спецiальнiй базi даних, яка зповинна бути захищенною – через використання криптографічні перетворення, у результатi чого приймається рiшення про особистiсть користувача та надання доступу до iнформацiйних ресурсiв, після звірки із талицею розподілення прав доступу. Така автентифiкацiя вирiзняється своєю простотою та звичнiстю, проте має суттєвi недолiки через уразливiсть методiв обробки паролiв для їх зберiгання.

Організаційні засоби регламентують методи та кроки які запобігають витоку інформації та унеможливлюють несанкціонований доступ до конфіденційної інформації .

Законодавчі засоби захисту визначаються законодавчими актами України, якими регламентуються засоби та правила використання криптографічних перетворень, фізичних та програмних.

### Цифрові сертифікати

Цифровий сертифікат – також відомий як сертифікат відкритого ключа, використовується для криптографічного зв’язку права власності на відкритий ключ із суб’єктом, який його володіє. Цифрові сертифікати призначені для обміну відкритими ключами, які використовуються для шифрування та автентифікації. Цифрові сертифікати включають сертифікований відкритий ключ, що ідентифікує інформацію про особу, яка володіє відкритим ключем, метадані, що стосуються цифрового сертифіката, та цифровий підпис відкритого ключа, створений емітентом сертифіката.Поширення, автентифікація та відкликання цифрових сертифікатів є головними цілями інфраструктури відкритих ключів, системи, за допомогою якої публічні ключі поширюються та аутентифікуються. Цифровий сертифікат - цифровий документ, що підтверджує відповідність між відкритим, публічним, ключем і інформацією, що ідентифікує власника ключа.

[Криптографія відкритого ключа](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://searchsecurity.techtarget.com/definition/asymmetric-cryptography&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhhJ_ebkwhcMGmIZPhZ5amZkANladQ) залежить від пар ключів: один [приватний ключ,](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://searchsecurity.techtarget.com/definition/private-key&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhgfa49wjGGCI50uQv5n0XCAuM64uQ) який повинен утримувати власник і використовується для підписання та розшифрування, і один відкритий ключ, який може використовуватися для шифрування даних, що надсилаються власнику відкритого ключа, або автентифікації власників сертифікатів підписані дані. Цифровий сертифікат дає змогу суб'єктам господарювання ділитися відкритим ключем таким чином, щоб їх можна було аутентифікувати.

Цифрові сертифікати використовуються у функціях криптографії відкритого ключа; вони найчастіше використовуються для ініціалізації захищених [SSL-](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://searchsecurity.techtarget.com/definition/Secure-Sockets-Layer-SSL&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhjwZYfn75tZyp2jzrSemZdW6i4cWQ) з'єднань між веб-браузерами та веб-серверами. Цифрові сертифікати також використовуються для обміну ключами, які використовуються для шифрування відкритих ключів та аутентифікації цифрових підписів.

Цифрові сертифікати використовуються всіма основними веб-браузерами та веб-серверами, щоб гарантувати, що опублікований вміст не змінювався жодними несанкціонованими учасниками, та для обміну ключами для шифрування та розшифрування веб-контенту. Цифрові сертифікати також використовуються в інших контекстах, як в Інтернеті, так і в режимі офлайн, для забезпечення криптографічної безпеки та конфіденційності даних.

Хоча суб'єкт господарювання може створити власну PKI та видавати свої цифрові сертифікати - а в деяких випадках такий підхід може бути розумним, наприклад, коли організація підтримує власну PKI для видачі сертифікатів для власного внутрішнього використання.

Криптографія відкритого ключа дозволяє виконувати ряд різних функцій, включаючи як шифрування, так і автентифікацію. Цифровий підпис – це ще одна з тих функцій, яку вмикає криптографія відкритого ключа, цифрові підписи генеруються за допомогою алгоритмів підпису даних, в результаті чого одержувач може безпомирно підтвердити, що дані підписав власник певного відкритого ключа.

Цифрові підписи створюються шляхом [хешування](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://searchsqlserver.techtarget.com/definition/hashing&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhjHC4TOHkTjQOx2MRNrJ8104k2RGw) даних, що підписуються, одностороннім криптографічним хешем. Потім результат шифрується приватним ключем підписувача. Цифровий підпис містить цей зашифрований хеш, який можна автентифікувати, перевірити,лише за допомогою відкритого ключа відправника для дешифрування цифрового підпису та запуску того самого алгоритму одностороннього хешування на вміст, який був підписаний. Потім два хеші можна порівняти, і якщо вони збігаються, це доводить, що дані не змінилися з моменту їх підписання – і що відправник є власником пари відкритих ключів, яка використовується для його підписання.

Загалом, цифровий підпис може залежати від розповсюдження відкритого ключа у вигляді цифрового сертифіката – але це не обов'язково, щоб публічний ключ був переданий у цій формі. Однак самі цифрові сертифікати підписуються цифровим шляхом, і їм не слід довіряти, якщо підпис не можна перевірити.

Існує три різні типи цифрових сертифікатів, які використовуються веб-серверами та веб-браузерами для аутентифікації через Інтернет. Ці цифрові сертифікати використовуються для прив'язки веб-сервера домену до особи або організації, яка належить домену.

Ці сертифікати зазвичай називають [сертифікатами SSL,](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://searchsecurity.techtarget.com/definition/SSL-certificate-Secure-Sockets-Layer-certificate&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhiwBayUG8gxJiLuQeD9EyjqcI4cYQ) навіть незважаючи на те, що протокол SSL був замінений [протоколом безпеки рівня транспортного рівня](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://searchsecurity.techtarget.com/definition/Transport-Layer-Security-TLS&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhh5r43V_L0XQX_JV0T-RcTM7FJwEQ) TLS.

* + - * Сертифікати, підтверджені доменом DV SSL, надають найменший рівень впевненості щодо власника сертифіката. Заявники на сертифікати DV SSL повинні лише продемонструвати, що вони мають право використовувати доменне ім’я. Хоча ці сертифікати можуть гарантувати, що дані надсилаються та отримуються власником сертифіката, вони не дають гарантій того, хто це суб'єкт господарювання.
      * Сертифіковані організацією сертифікати SSL надають додаткові гарантії щодо власника сертифіката; на додаток до підтвердження того, що заявник має право користуватися доменом, заявники SSL сертифікати проходять додаткове підтвердження своєї власності на домен.
      * В Сертифікати з розширеною валідацією SSL видаються лише після того, як заявник зможе довести свою особу на задоволення. Процес перевірки включає перевірку існування суб'єкта господарювання, який подає заявку на отримання сертифіката, перевірку відповідності особи офіційним записам, перевірку того, що суб'єкт господарювання уповноважений використовувати домен, і підтвердження того, що власник домену уповноважив видачу сертифіката.

Ці типи сертифікатів SSL доступні у для веб-доменів, хоча точні методи та критерії для цих сертифікатів розвиваються, коли галузь адаптується до нових умов та застосувань.

Окрім SSL-сертифікатів, існують і інші типи цифрових сертифікатів, які використовуються для інших цілей. Вони такі:

* + - * Свідоцтва про підписання коду можуть видаватися організаціям або особам, які публікують програмне забезпечення. Ці сертифікати використовуються для обміну відкритими ключами, які підписують програмний код, включаючи патчі та оновлення програмного забезпечення. Сертифікати підпису коду засвідчують справжність підписаного коду.

Клієнтські сертифікати, які також називаються цифровим ідентифікатором, видаються особам, щоб прив’язати свою особу до відкритого ключа в сертифікаті. Особи можуть використовувати ці сертифікати для цифрового підпису повідомлень чи інших даних; люди також можуть використовувати свої приватні ключі для шифрування даних, які одержувачі можуть розшифрувати за допомогою відкритого ключа в сертифікаті клієнта.

Цифровий сертифікат зазвичай супроводжує певне повідомлення. Його використання необхідно для засвідчення справжності електронного ключа, який використовується. Існуючі моделі організації інфраструктур сертифікаті: централізована інфраструктура відкритих ключів, під назвою - PKI та децентралізована. Централізована модель застосовує кореневі центри сертифікації, підпису яких зобов'язан довіряти кожен користувач.

У той самий час – децентралізованій моделі кожен користувач самостійно вибирає, яким сертифікатам він довіряє й у якій степені. Довірені сертифікати мають важливе значення в сучасному бізнес-кліматі, але це не означає, що до них легко підійти. Ризики для сертифікаційних служб багато, безумовно, але цей трискладовий технічний посібник розроблений для того, щоб зрозуміти виклики, а потім запропонувати поради щодо того, як професіонали infosec можуть збільшити безпеку довірених сертифікаційних органів на їхньому підприємстві. Він відкривається оглядом нещодавнього дослідження щодо експертного сприйняття ризиків безпеки та де лежать ключові небезпеки, які можуть піддавати бізнес порушенням. Він досліджує загальну тему підвищення безпеки, але також поглинається в конкретні проблеми безпеки, включаючи ризики безпеки, притаманні мобільним сертифікатам. Серед розглянутих у цій публікації потенційних підходів до підвищення безпеки АС є переваги послуг підписки на сертифікати SSL.

Зазвичай використовується стандарт сертифікатів X.509 (\*.CER) в якому у міститься відкритий ключ за підписом центра сертифікації.

Цифрові сертифікати в основному служать двом цілям:

— Встановити особу власника;

— зробити доступним первинний ключ власника.

Кількість цифрових сертифікатів, необхідних для роботи в сучасному підключеному світі, продовжує зростати, і це змушує організації повторно оцінювати, як вони керують життєвим циклом своїх сертифікатів. Якщо сертифікати, видані з внутрішнього сертифікаційного органу - [CA](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://searchsecurity.techtarget.com/definition/certificate-authority&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhjFgrxffcqD1k7T2yEtqQ3Z4yA8Jg) , не ретельно керуються, вони можуть швидко поставити організацію під загрозу перебоїв у роботі системи через пропущені оновлення та порушення даних через компроміс або неправильне використання. Сертифікати, особливо ті, які використовуються для публічних служб, які залишаються без нагляду і не керуються, можуть закінчуватися або замінюватися неправдивими або недійсними сертифікатами. Ці ситуації можуть призвести до повідомлень про помилки, які підривають довіру клієнтів, простої до служби або хакери, що атакують служби та їх користувачів.

Усі цифрові сертифікати випускається повноважною організацією – так званим джерелом сертифікатів – CA. Цифрові сертифікати діють обмежений час. Після закінчення терміну дії сертифіката необхідно його замінити на інший.

Сертифікати складаються із:

* Серійний номер сертифіката, який зареєстрований у джерелі що його видала;
* цифрового підпис;
* ім'я центра сертифікації, який засвідчує підпис власника;
* термін придатності;
* ім'я власника сертифіката;
* відкрити ключі власника сертифікату, їх може бути декілька.
* електронний цифровий підпис, який згенеровано з використанням таємного ключа центра сертифікації, ним підписується результат хешування всієї інформації, що зберігається в сертифікаті.

## Аналіз стійкості обраного методу шифрування

AES-256 - це стандартизована специфікація шифрування. Його використовують у всьому світі всі, від корпорацій, до державних підприємств та уряду. Найбільший розмір ключа - 256 біт. Це означає, що ключ, що перетворює зашифровані дані в незашифровані дані, є рядком 256.

З кожним символом, що має дві можливості 1 або 0, існує 2 у стеню 256 можливих комбінацій. Зазвичай лише 50% з них потребують вгаування, щоб отримати правильний ключ, тому лише 2 у ступеню 255 варіантів потрібно перебрати.

Роблячи щоденні, повторювані обчислення, такі як брутфорс – перебір можливих варіатів чи майнінг біткойна, GPU краще підходить, ніж процесор. Графічний процесор високого класу зазвичай може робити близько 2 мільярдів обчислень в секунду, тобто 2 гігафлопи.

Використовуючи мільярд таких графічних процесорів, з'єднаючи це все в паралельну комп'ютерну систему. Разом вони могли обчислювати 2 000 000 000 000 000 000 - 2 квінтільйона ключів в секунду.[24]

Так як в році 31 556 952 секунд – через множення дістанемо кількість ключів за рік - 10 септиліон, тобто 10 йоттафлопсключів в рік.

Тепер ділимо кількість можливих ключів AES-256 на отриманий результат та дістанемо час за яский такий шифр можливо зламати - 9.1732631e50 це більш ніж у 10 разів більше за вік нашої сонячної системи. [24]

Входячи з цього можна зробити висновок, що така система шифрування може бути зламана тыльки комбінованими атаками. Тобто використовуючи, як людський фактор, так і аналіз дій, уподобань, та всієї доступної інформації о господарях зашифрованої інформації, для суттевого зменщення кількості можливих варіацій паролей.

## Висновки по розділу

Було проаналізовано уразливості iнформацiйних систем. Проведений аналіз уразливості інформаційно-комунікаційних систем показав, що існує значна кількість загроз які можуть привести до нанесення збитків при передачі інформації. Інформаційна безпека передачі даних в значній мірі залежить від реалізованого протоколу передачі даних, механізму передачі даних в мережі та комутаційного обладнання, що використовується в мережі. Але головну роль відіграє правильна політика безпеки яка включає нормативні постонви що до організаційного процеси.

Надзвичайно важливо виконувати огранізаційно-технічні заходи щодо зберігання ключв доступу та паролів, не зважаючи на фізичний рівень безпеки. Пароль – секретна фраза користувача, що використовується для його автентифiкацiї та отримання доступу до сервiсу. Вiн вимагає не менш надiйного методу обробки та зберiгання зi сторони серверу автентифiкацiї для унеможливлення розсекречення та, вiдповiдно, незаконного доступу до облiкового запису, ніж на стороні користувача.

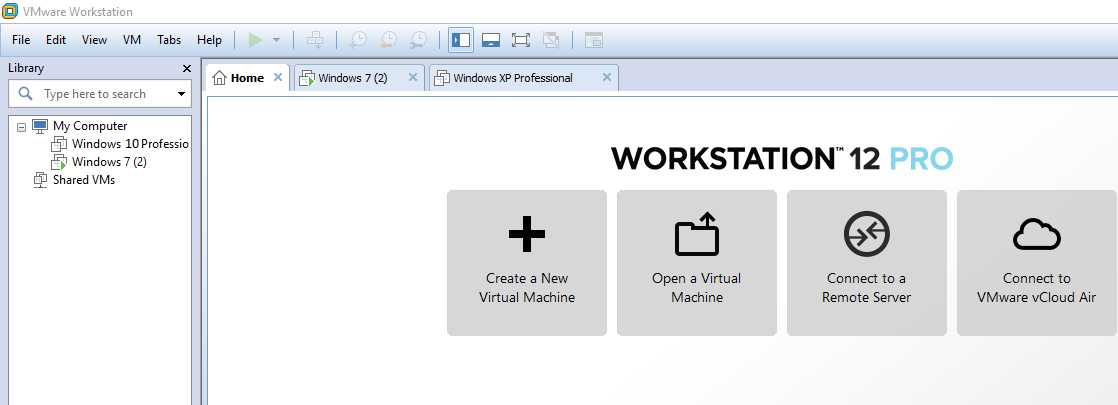
# РОЗДІЛ 3

# ЗАХИСТ ІНФОРМАЦІЇ НА ОСНОВІ РОЗРОБЛЕНОЇ МЕТОДОЛОГІЇ

## Створення середовища для виконання дипломної роботи

У першу чергу, було підготовлено середовище для виконання даної роботи: віртуальну машину див. рис.3.1. з двома операційними системами: Windows 10 і Windows 7, а також сам персональний комп’ютер (ПК).

На ОС Windows 10 ми будемо реалізовувати проект, на Windows 7 – перевіримо сумістність продукта, адже за статистикою – майже 27% усіх користувачів операційних систем використовують Windows 7, див. рис 3.2..

Рис.3.1. Віртуальна машина VMware Workstation

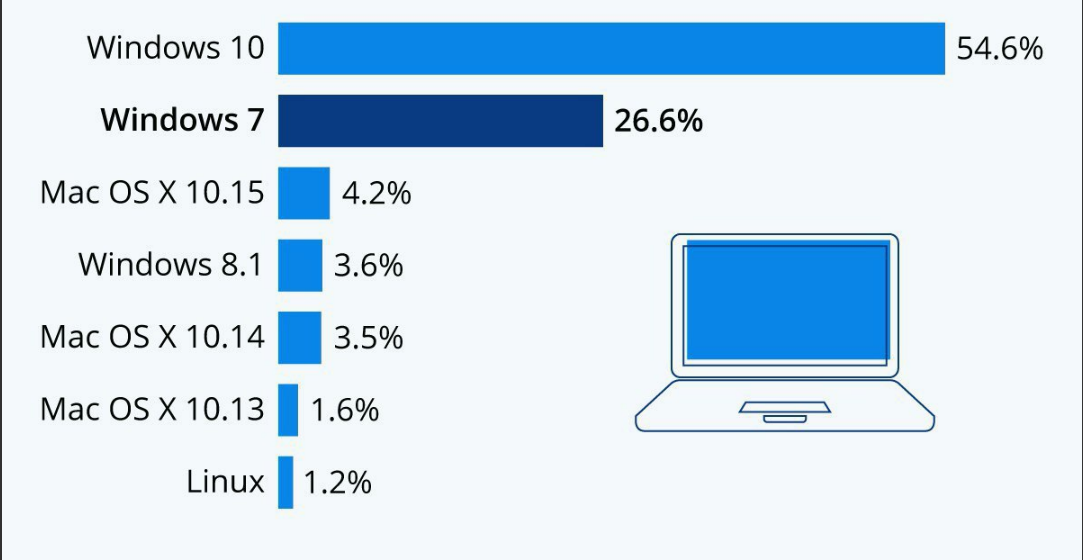


Рис.3.2. Популярність операційних систем

Для розгорнення декількох операційних систем на одній машині та їх адміністрування було використано гіпервізор, монітор віртуальної машини - VMware Workstation.

Гіпервізор, або монітор віртуальної машини, - це програмне забезпечення , програмне забезпечення або апаратне забезпечення комп'ютера, яке створює та запускає віртуальні машини . Комп'ютер, на якому гіпервізор працює на одній або декількох віртуальних машинах, називається хост-машиною, а кожна віртуальна машина називається гостьовою машиною. Гіпервізор представляє гостьовим операційним системам віртуальну операційну платформу та керує виконанням гостьових операційних систем. Кілька екземплярів різних операційних систем можуть мати спільний доступ до віртуалізованих апаратних ресурсів: наприклад, екземпляри Linux , Windows та macOS можуть працювати на одній фізичній машині x86. Це контрастує з віртуалізацією на рівні операційної системи , де всі екземпляри, зазвичай їх називають контейнерами, повинні мати одне ядро, хоча гостьові операційні системи можуть відрізнятися в просторі користувачів, наприклад, різні дистрибутиви Linux з тим же ядром.

Використання технології гіпервізора [зловмисними програмами](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://en.m.wikipedia.org/wiki/Malware&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhi9RjnSoCKqLuX1ksUwvy52lPJJGw) та [руткітами, що](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://en.m.wikipedia.org/wiki/Rootkit&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhjFVyhzulDXwU__wMMEukCOAN1Rwg) встановлюють себе як гіпервізор нижче операційної системи, відомий як [гіперджекгінг](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://en.m.wikipedia.org/wiki/Hyperjacking&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhjNFYxG08S6-L9ubSd8BEJIVyJBHg) , може ускладнити їх виявлення, оскільки зловмисне програмне забезпечення може перехопити будь-які операції операційної системи, наприклад, хтось вводить пароль, без програмне забезпечення проти зловмисного програмного забезпечення обов'язково виявляє його, оскільки зловмисне програмне забезпечення працює нижче всієї операційної системи. Втілення цієї концепції нібито відбулося в лабораторному [руткіті SubVirt](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://en.m.wikipedia.org/w/index.php%3Ftitle%3DSubVirt%26action%3Dedit%26redlink%3D1&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhiz4ZtXystSfBS3gA0pyur-0XtsoA) розробленому спільно дослідниками з [Microsoft](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://en.m.wikipedia.org/wiki/Microsoft&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhixwHvWqNcbr2FLpGBxKEZgK-zl9w).

 Віртуальні машини базуються на [комп'ютерній архітектурі](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://en.m.wikipedia.org/wiki/Computer_architectures&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhg6mYOf-tpl8V-OjyAvXSn-H1hzVw) та забезпечують функціональність фізичного комп'ютера. Їх реалізація може включати спеціалізоване обладнання, програмне забезпечення або їх комбінацію.

Існують різні види віртуальних машин, кожна з яких має різні функції:

* [**Системні віртуальні машини**](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://en.m.wikipedia.org/wiki/System_virtual_machine&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhhVnOxxJ8okBhAE_WietbsXQW0rug), їх також називають [повноцінними віртуалізаційними](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://en.m.wikipedia.org/wiki/Full_virtualization&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhhK5uFQHIS3pXSTqrr2nsHewg5M7Q) [**машинами**](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://en.m.wikipedia.org/wiki/System_virtual_machine&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhhVnOxxJ8okBhAE_WietbsXQW0rug), забезпечують заміну справжньої машини. Вони забезпечують функціонал, необхідний для виконання цілих [операційних систем](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://en.m.wikipedia.org/wiki/Operating_system&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhh7NYyEMxwMn4rjj_n0Me5urh1Jyg) . [Гіпервізор](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://en.m.wikipedia.org/wiki/Hypervisor&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhhbVzDJnhOo4U_cEsrnPBhsLanBug) використовує власні служби для спільного використання та управління апаратними засобами, дозволяючи для різних середовищ, ізольованих один від одного, але існувати на одній фізичній машині. Сучасні гіпервізори використовують [апаратну віртуалізацію](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://en.m.wikipedia.org/wiki/Hardware-assisted_virtualization&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhjPx1j5M3aXXWWGXCl5NCpl-IlJrQ) , специфічну для віртуалізації апаратуру, головним чином з хост-процесорів.
* Віртуальні машини призначені для виконання комп'ютерних програм у незалежному від платформи середовищі.

Існують декілька методів віртуалізації:

* У віртуалізації за допомогою апаратного забезпечення апаратне забезпечення забезпечує архітектурну підтримку, яка полегшує побудову монітора віртуальної машини та дозволяє гостям ОС працювати ізольовано.
* А У віртуалізації на рівні операційної системи фізичний сервер віртуалізується на рівні операційної системи, що дозволяє на одному фізичному сервері працювати декілька ізольованих і захищених віртуалізованих серверів. Середовища "гостьової" операційної системи поділяють той же запущений екземпляр операційної системи, що і хост-система. Таким чином, те саме [ядро операційної системи](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://en.m.wikipedia.org/wiki/Operating_system_kernel&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhjWbACoYtYqAjvpaCbde5RWE_IltA) також використовується для реалізації середовищ "гостьових", а програми, що працюють в заданому "гостьовому" середовищі, розглядають його як окрему систему.

VMware Workstation - це розміщений [гіпервізор,](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://en.m.wikipedia.org/wiki/Hypervisor&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhhbVzDJnhOo4U_cEsrnPBhsLanBug) який працює на [x64](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://en.m.wikipedia.org/wiki/X64&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhj5VJnM-_P8_zQwPzHSJlPper7n-A) версіях операційних систем Windows та Linux, доступна версія [x86](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://en.m.wikipedia.org/wiki/X86&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhg7PQN36fSVkDn-ww_MHVfnUTkIxA) попередніх версій, він дозволяє користувачам налаштовувати [віртуальні машини](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://en.m.wikipedia.org/wiki/Virtual_machine&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhj_XYd9GKihUYULq02Vh1Mzzesi_Q) – VM на одній фізичній машині та використовувати їх одночасно разом із фактичною машиною. Кожна віртуальна машина може виконувати власну [операційну систему](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://en.m.wikipedia.org/wiki/Operating_system&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhh7NYyEMxwMn4rjj_n0Me5urh1Jyg), включаючи версії [Microsoft Windows](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://en.m.wikipedia.org/wiki/Microsoft_Windows&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhi4cCxG9CZ8DgHj1RflsslgP_hfqw) , [Linux](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://en.m.wikipedia.org/wiki/Linux&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhiNUmM2tI-faCqhWeZ7Y13LbfXHbQ) , [BSD](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://en.m.wikipedia.org/wiki/BSD&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhhfPs8RGUYrg_DhQNvoDN5ukHgveg) та [MS-DOS](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://en.m.wikipedia.org/wiki/MS-DOS&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhgGbEPs7riHA_6sfN5Uu4ow2FXbhw) . Робоча станція VMware розроблена [VMware, Inc.](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://en.m.wikipedia.org/wiki/VMware,_Inc.&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhj5zOASU_0wuOuCDvS8Spt0VNx87w) , підрозділом [Dell Technologies](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://en.m.wikipedia.org/wiki/Dell_Technologies&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhj_-D1_S-CbNE91E1Am4wikMzFHyA) . Існує безкоштовна версія VMware Workstation Player для некомерційного використання. Для використання фірмових операційних систем, таких як Windows, потрібна ліцензія на операційні системи. Готові віртуальні віртуальні машини Linux, створені для різних цілей, доступні без ліцензії.

VMware Workstation підтримує [з'єднання](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://en.m.wikipedia.org/wiki/Bridging_(networking)&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhgt0UAgcwmS2JR-edkNat6qLMxw1g) існуючих [адаптерів](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://en.m.wikipedia.org/wiki/Network_adapter&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhg-KkKCJyeMYd0ZBmbDpjO9yzGpVw) хост- [мережі](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://en.m.wikipedia.org/wiki/Network_adapter&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhg-KkKCJyeMYd0ZBmbDpjO9yzGpVw) та обмін фізичними [дисководами](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://en.m.wikipedia.org/wiki/Disk_drive&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhjcuzW4lgacwZWJYh1crEG2U21NLg) та [USB-](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://en.m.wikipedia.org/wiki/Universal_Serial_Bus&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhgKfMXmib74znK2zhb31NOIr0H6Ig) пристроями з віртуальною машиною. Він може імітувати дискові накопичувачі. Файл [зображень ISO](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://en.m.wikipedia.org/wiki/ISO_image&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhisMZ54MXrc3dPyljebourg2reW5g) може бути [змонтований](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://en.m.wikipedia.org/wiki/Mount_(computing)&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhgeb9I6zOlXJ-s2a1-m1Fd0rVjVew) у вигляді віртуального [оптичного дисковода](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://en.m.wikipedia.org/wiki/Optical_disc_drive&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhgMaDhOHdW2L6sXGpgNLJMLiu3s-g) , а віртуальні [жорсткі диски](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://en.m.wikipedia.org/wiki/Hard_disk_drive&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhgANMgrm3qwZFqy2pkmBls8kO0GFg) реалізовані у [форматі .vmdk](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://en.m.wikipedia.org/wiki/.vmdk&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhg6sniw5RvfosrApRuNQPxagnNJvA).

VMware Workstation Pro може в будь-який момент зберегти стан віртуальної машини. Після чого, пізніше відновити, фактично повернувши віртуальну машину до збереженого стану, як вона була, і звільнитись від будь-яких помилок.

VMware Workstation включає можливість групування декількох віртуальних машин у папці інвентаризації. Потім машини в такій папці можуть бути включені та вимкнені як єдиний об'єкт, корисний для тестування складних середовищ клієнт-сервер.

### Visual Studio - інтегроване середовище розробки ПЗ.

Microsoft Visual Studio - це [інтегроване середовище розробки](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://en.m.wikipedia.org/wiki/Integrated_development_environment&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhh37RHMkiFPLUKfaDMd4o96_diAFg) – IDE, від [Microsoft](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://en.m.wikipedia.org/wiki/Microsoft&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhixwHvWqNcbr2FLpGBxKEZgK-zl9w) . Інтегроване середовище розробки  - це [програмне забезпечення,](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://en.m.wikipedia.org/wiki/Application_software&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhjKXRwQ7MkdjlgrFn2T0U5wsJvpPg) яке надає комплексні засоби [комп'ютерним програмістам](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://en.m.wikipedia.org/wiki/Computer_programmer&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhgdv5q_zZACpTM7Tl3j1ynLGsNAUg) для [розробки програмного забезпечення](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://en.m.wikipedia.org/wiki/Software_development&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhheqqYRevs8OTwBsPPDobYXy4pC_A) . Він використовується для розробки [комп’ютерних програм](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://en.m.wikipedia.org/wiki/Computer_program&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhhFGXvG965O3gfrlKodJ6aJdHrq2A) , а також [веб-сайтів](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://en.m.wikipedia.org/wiki/Web_site&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhibr5rWrdefyGnWY6RyFL9OIbFQLQ) , [веб-додатків](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://en.m.wikipedia.org/wiki/Web_app&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhhWroFFZImjnLzg113PT3PhLuJnnw) , [веб-служб](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://en.m.wikipedia.org/wiki/Web_service&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhgrvTd4oSHZxdPhmkNnnCJ0yesVGA) та [мобільних додатків](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://en.m.wikipedia.org/wiki/Mobile_app&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhi8PpODYdHMR1wvUodSihgMPK9nCg) . Visual Studio використовує платформи Microsoft для розробки програмного забезпечення, такі як [API Windows](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://en.m.wikipedia.org/wiki/Windows_API&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhh4FOoaWOiHwobaKzjR8Bvtc2qQPg) , [Windows Forms](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://en.m.wikipedia.org/wiki/Windows_Forms&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhiTFcZT0DDrW2B50ccVo4uEI1IBFQ) , [Foundation Presentation Foundation](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://en.m.wikipedia.org/wiki/Windows_Presentation_Foundation&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhi5eqX38jr8YQbdg3djSVUd-xJHBA) , [Windows Store](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://en.m.wikipedia.org/wiki/Windows_Store&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhjvK9AU6c_QiBWPNOkSQkKnYqcBzg) та [Microsoft Silverlight](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://en.m.wikipedia.org/wiki/Microsoft_Silverlight&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhgKMmzkdpmKUdMz-Y0OlI_hl2SdEQ) . Він може створювати як [власний код, так](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://en.m.wikipedia.org/wiki/Machine_code&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhhlKj-8RiciDrbjuQZ_Rpb4nyJdKw) і [керований код](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://en.m.wikipedia.org/wiki/Managed_code&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhgjCgNxRWUremtcDHUXF_EGcMEW9g) .

У Visual Studio є в наявності редакор коду, який підтримує підсвічування синтаксису та завершення коду за допомогою підказок для змінних, функцій, методів, циклів та запитів така функція підтримується для XML а також для всіх мов проограмування, що підтримуються IDE Автозаповнення пропозицій відображається у вільному списку списку над вікном редактора коду, поблизу курсору редагування.

Редактор коду Visual Studio також підтримує налаштування закладок у коді для швидкої навігації. Інші навігаційні засоби включають збір блоків коду та поступовий пошук , на додаток до звичайного пошуку тексту та пошуку в регулярних виразах . Редактор коду також включає буфер обміну для багатьох предметів та список завдань. Редактор коду підтримує фрагменти коду, які зберігаються в шаблонах для повторюваного коду і можуть бути вставлені в код і налаштовані під проект, над яким працює. Також вбудований інструмент управління фрагментами коду. Ці інструменти з'являються у вигляді плаваючих вікон, які можна встановити для автоматичного приховування, коли вони не використовуються або стикуються на стороні екрана.

Visual Studio має компіляцію фоновому режим. .Коли код пишеться, Visual Studio компілює його у фоновому режимі, щоб надати зворотній зв'язок про синтаксис та помилки компіляції, які позначені червоним хвилястим підкресленням. Попередження позначені зеленим підкресленням. Фонова компіляція не генерує виконуваний код, оскільки для нього потрібен інший компілятор, ніж той, який використовується для створення виконуваного коду.

На данний час Visual Studio підтримує : HTML / XHTML, JavaScript, XML / XSLT ,CSS, Python і Ruby. Також має вбудновані мови програмування:

* C / C ++ ;
* C # ;
* F # ;
* VB.NET.

## Обрані алгоритми шифрування

### Алгоритм AES

AES - симетричний шифр. Це означає, що той самий ключ, який використовується для шифрування даних, використовується для його розшифровки.

Асиметричні системи шифрування вирішують цю проблему, захищаючи дані за допомогою відкритого ключа, який доступний для всіх. Розшифрувати його може лише призначений одержувач, який має правильний приватний ключ. Такий підхід робить асиметричне шифрування набагато кращим при забезпеченні безпеки даних у дорозі, оскільки відправник не повинен знати приватний ключ одержувача. Хороший приклад - шифрування RSA, яке використовується для захисту обміну ключами TLS, необхідного під час підключення до захищеного веб-сайту HTTPS.

Таким чином, симетричні шифри на зразок AES набагато краще забезпечують захист даних у спокої - наприклад, коли вони зберігаються на вашому жорсткому диску. Для цього вони перевершують асиметричні шифри, оскільки:

* Вони вимагають значно меншої обчислювальної потужності. Це робить шифрування та дешифрування даних із симетричним шифруванням набагато швидше, ніж при асиметричному шифруванні. В перспективі, симетричні шифри, як правило, цитуються як приблизно "в 1000 разів швидше", ніж асиметричні.
* А оскільки вони швидші, симетричні шифри набагато корисніші для масового шифрування великої кількості даних. Асиметричні шифри, такі як RSA, реально використовуються лише для шифрування невеликої кількості даних, наприклад ключів, що використовуються для захисту симетричного шифрування ключа.

AES широко вважається найбільш захищеним симетричним шифром шифруваного ключа, який ще був винайдений. Існують і інші симетричні ключові шифри, які вважаються високобезпечними, такі як Twofish, який був спільно винайдений відомим криптографом Брюсом Шнайєром.

Через широке поширення AES більшість виробників процесорів тепер інтегрували інструкцію AES у свої процесори. Поліпшення обладнання покращує продуктивність AES на багатьох пристроях, а також підвищує їх стійкість до атак.

Атаки [бічних каналів](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://en.wikipedia.org/wiki/Side-channel_attack&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhj5pDrOtANX817aCamJnCkI_s4L1g) шукають підказки з комп'ютерної системи, що реалізує шифрування AES, щоб дізнатися додаткову інформацію. Це може бути корисно для зменшення кількості можливих комбінацій, необхідних для грубої сили АЕС.

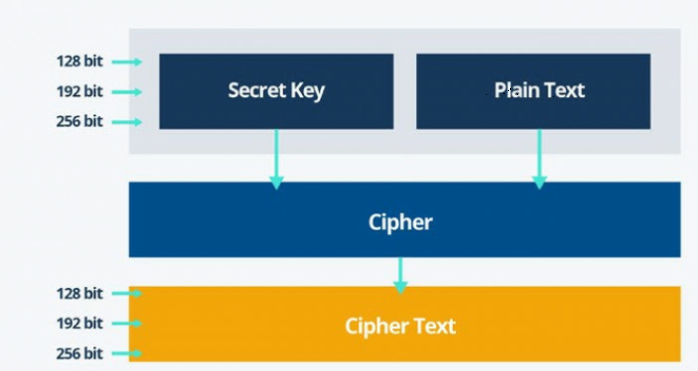
Ці атаки використовують інформацію про час - скільки часу комп'ютер займає для обчислень, електромагнітні витоки.

Правильно реалізований AES пом'якшує атаки бічних каналів, запобігаючи можливі шляхи витікання даних, саме там допомагає використання апаратного набору інструкцій AES, та за допомогою методів рандомізації для усунення зв’язку між захищеними шифром даними та будь-якими протікаючими даними які можна було зібрати за допомогою атаки бічного каналу.

Шифрування AES є настільки ж безпечним, як і його ключ. Ці ключі незмінно захищені самими паролями, і всі ми знаємо, наскільки [страшні](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://en.wikipedia.org/wiki/List_of_the_most_common_passwords&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhgMBsw6S-oLAdgvpHCDrm8yla2N_Q) нам люди при використанні захищених паролів. Кейлоггери, запроваджені вірусами, атаками соціального інжинірингу тощо, також можуть бути ефективними способами компрометувати паролі, які захищають ключі AES. Тому у програмі запроваджено візуалізацію міцності паролю, а також було представлено психолгічний фактор – унеможливлення створення бази даних без введення паролю.

Використання [менеджерів паролів](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://proprivacy.com/password-manager/guides/keepass-password-manager&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhiqk_FeIDdqeFn54chWL4UCKA9BYQ) значною мірою пом'якшує цю проблему, як і використання двосторонніх брандмауерів, хорошого антивірусного програмного забезпечення та підвищення обізнаності з питань безпеки.

Алгоритм шифрування AES шифрує та розшифровує дані блоками з 128 біт. Це можна зробити за допомогою 128-бітних, 192-бітних або 256-бітних ключів. AES, що використовує 128-бітні ключі, часто називають AES-128 тощо.

  
Рис. 3.3. Схема шифрування AES

Cпрощений огляд процесу AES зображено на рис. 3.3., що предтавлений вишче:

* Plain text це конфіденційні дані, які необхідно шифрувати;
* Secret Key це128-бітова, 192-бітова або 256-бітна змінна, хеш, створений алгоритмом;
* Chipher – шифрування;
* Chipher Text – зашифрований текст.

Фактичний шифр AES потім виконує ряд математичних перетворень, використовуючи простий текст і секретний ключ як вихідну точку. За таким алгоритмом:

* Розширення ключа. При цьому використовується оригінальний секретний ключ для отримання серії нових, використовуючи алгоритм розкладу ключів Rijndael.
* Змішування. Кожну ітерацію ключ поєднується з простим текстом за допомогою [алгоритму](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://proprivacy.com/vpn/guides/openvpn-scramble-xor-obfuscation&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhhidPdWsHieiSK7tb7EvsdHIkTHCg) додавання [XOR](https://translate.googleusercontent.com/translate_c?depth=1&hl=ru&rurl=translate.google.com&sl=en&sp=nmt4&tl=uk&u=https://proprivacy.com/vpn/guides/openvpn-scramble-xor-obfuscation&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265,15700271&usg=ALkJrhhidPdWsHieiSK7tb7EvsdHIkTHCg) див рис. 3.4..

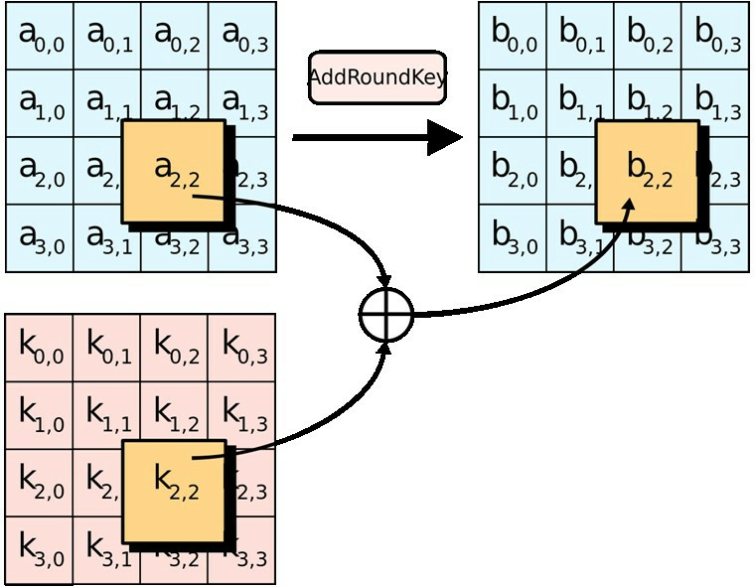


Рис. 3.4. Змішування алгоритма AES

* Заміна отриманих даних за допомогою таблиці заміщення. Цей крок в принципі дуже схожий, але декылько набагато складніший на практиці, із замінними шифрами, наприклад, Цезаря. Детальніше див. рис. 3.5..

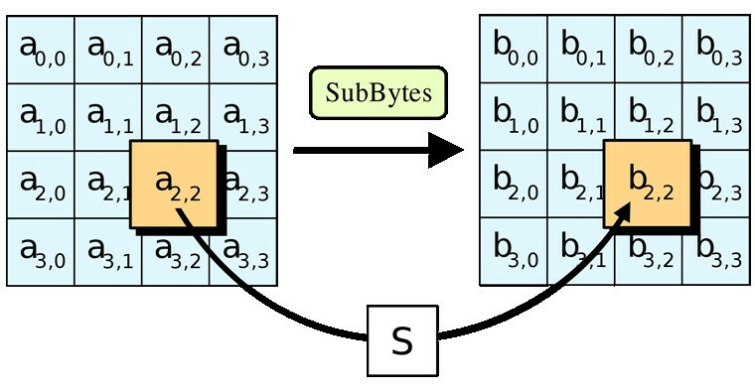


Рис. 3.5. Алгоритм заміни

* Змішування рядків, у яких кожен байт у стовпці 4 x 4 з шістнадцяти байтів, що складає 128-бітний блок, переміщується праворуч, див. рив. 3.5..

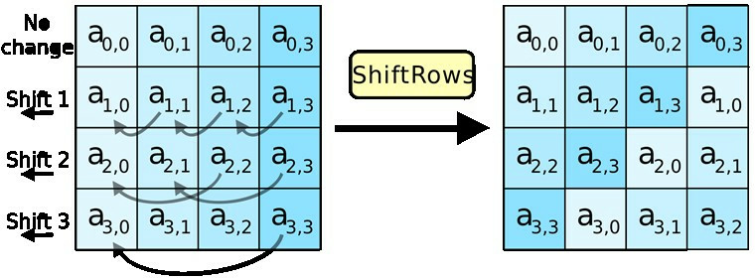
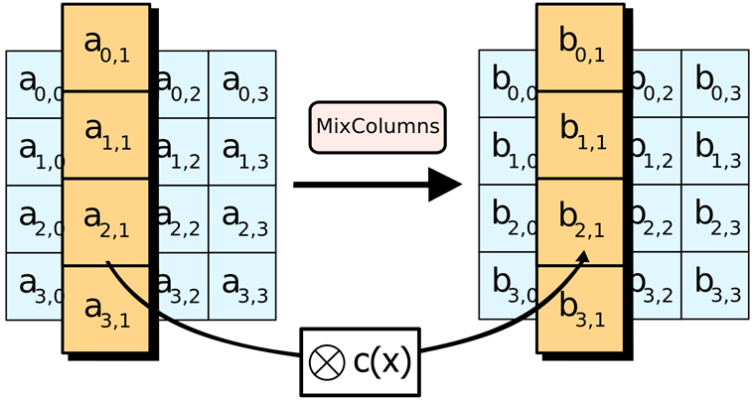


Рис. 3.5. Алгорим змішування рядків

* Змішування стопців. До кожного стовпця застосовується подальший алгоритм, див. рис 3.6..

  
Рис. 3.6. Алгоритм змішування стовпців

Процес повторюється кілька разів, причому кожне повторення називається раундом. Кожен раунд повторно шифрується за допомогою одного із отриманих ключів підчас розширення ключа.

Кількість проведених раундів залежить від використовуваної довжини ключа. AES-128 використовує десять раундів, AES-192 використовує дванадцять раундів, а AES-256 використовує чотирнадцять раундів.

Розшифрувати AES досить просто – для цього необхідно перепройти всі вищезазначені кроки, починаючи з кінця. Звичайно потрібно мати оригінальний секретний ключ.

AES можна використовувати з 126-бітним, 192-бітним або 256-бітним розмірами ключів. Найбільш грубий спосіб вимірювання надійності шифру - це розмір його ключа. Чим більше ключ, тим більше можливих комбінацій.

### Алгоритм ChaCha20

Існують декілька основних причин через які інколи замість ChaCha20 віддають превагу AES:

* Процесор без спеціальних інструкцій ChaCha20, як правило, швидше, ніж AES. Причиною цього є той факт, що ChaCha20 заснований на ARX – Addition-Rotation-XOR, що є зручними для процесора інструкціями, тоді як AES використовує бінарні поля для обчислень Sbox та Mixcolumn, які, як правило, реалізуються як таблиця пошуку для того, щоб бути більш ефективний.
* Той факт, що AES використовує таблицю пошуку з індексом, отриманим із секрету, робить загальні реалізації вразливими до атак таймінгу. ChaCha20 не вразливий до таких атак.

### Створення ключів

Усі ключі перетворюються за допомогою алгоритмів Argon 2 чи AES. Саме такий підхід дозволяє підвичити надійність. Алгоритм Argon2 працює за наступним принципом:

— Проводиться хешування пароля з використанням хеш-функції Blake2b;

— Результат хеширования записується в блоки пам'яті;

— Блоки пам'яті перетворюються з використанням функції стиснен G;

— В результаті роботи алгоритму генерується ключ.

### Інтерфейс програми

Головне вікно дипломного проекту виглядає, як на рис. 3.7.:

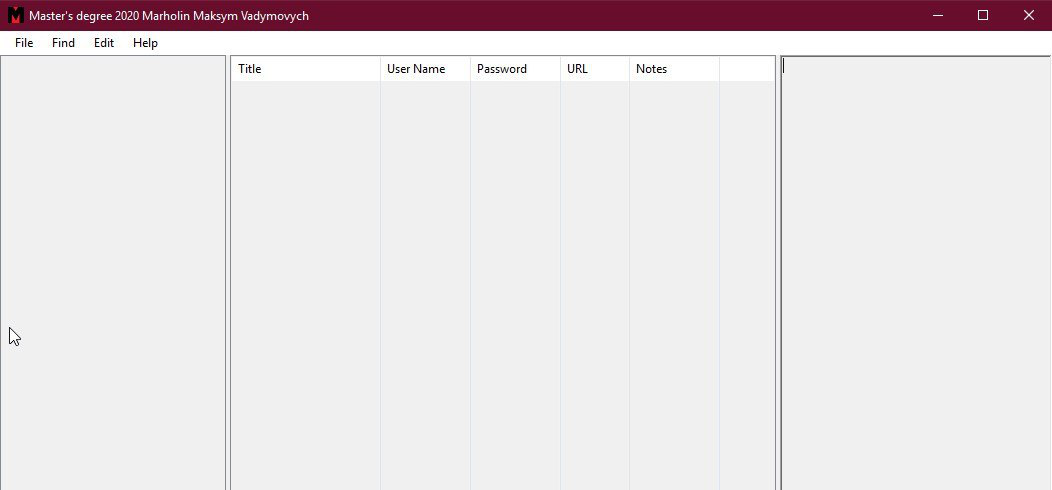


Рис.3.7. Головне вікно прошрами

У меню, яке знаходиться зліва у горі знаходяться випадаючі списки . File – меню редагування та створення нових баз даних, Find – пошук у проекті, Edit – редагування збереженої інформації у базі, створення нових записів, редагування груп, Help – відомості о проекті. Нижче наведені рис. 3.7, 3.8, 3.9, 3.10 із розгорнутими меню. Вони максимально інформативні та прості у розумінні, тож користувач зможе швидко з усім розібратися.

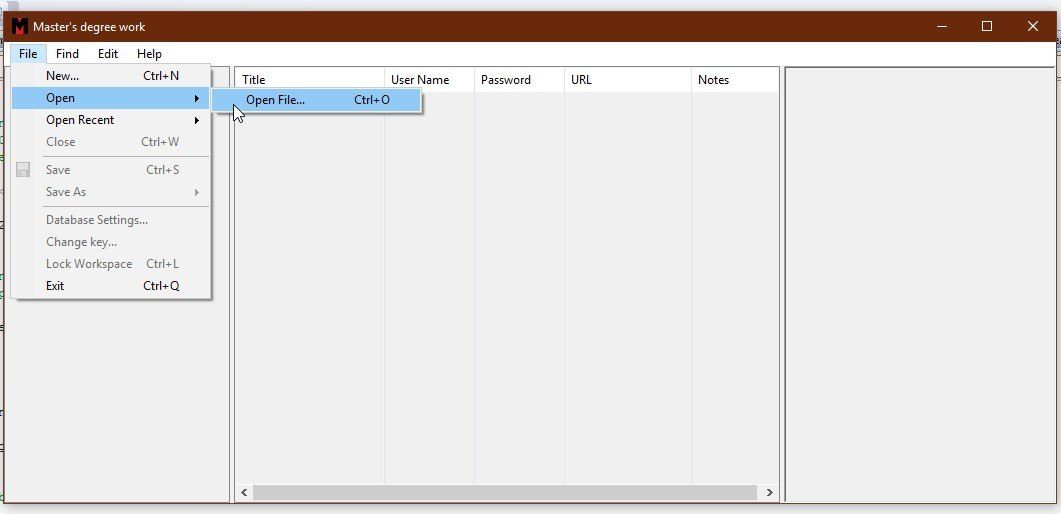


Рис. 3.7 File

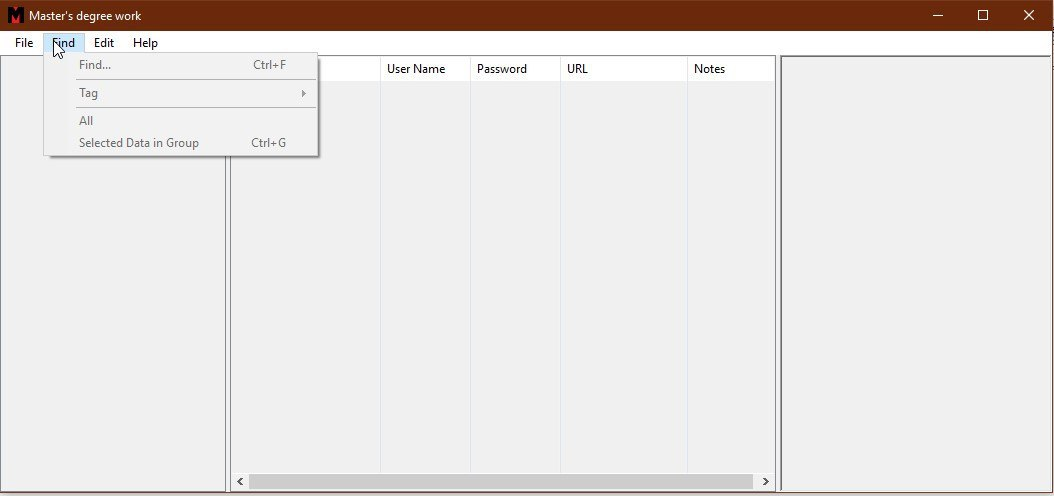


Рис. 3.8. Find

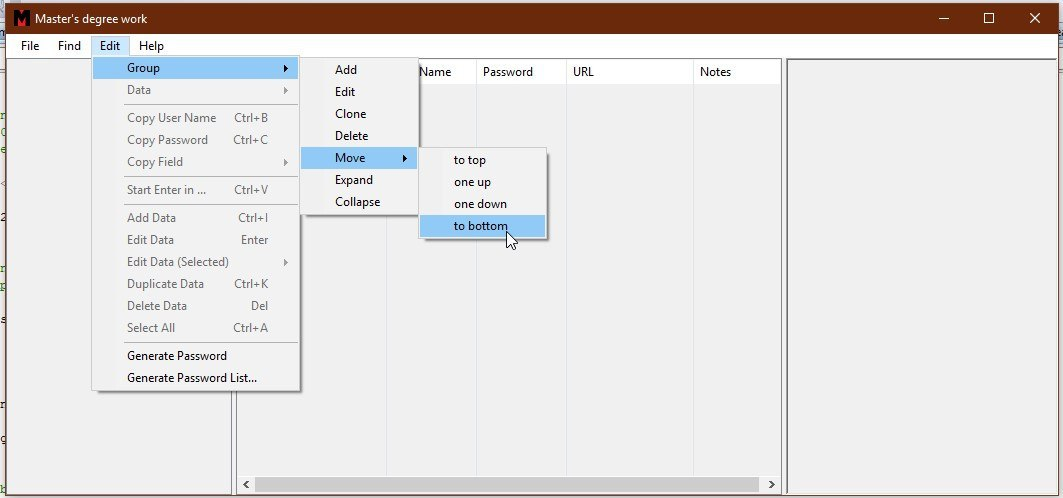


Рис. 3.9. Edit

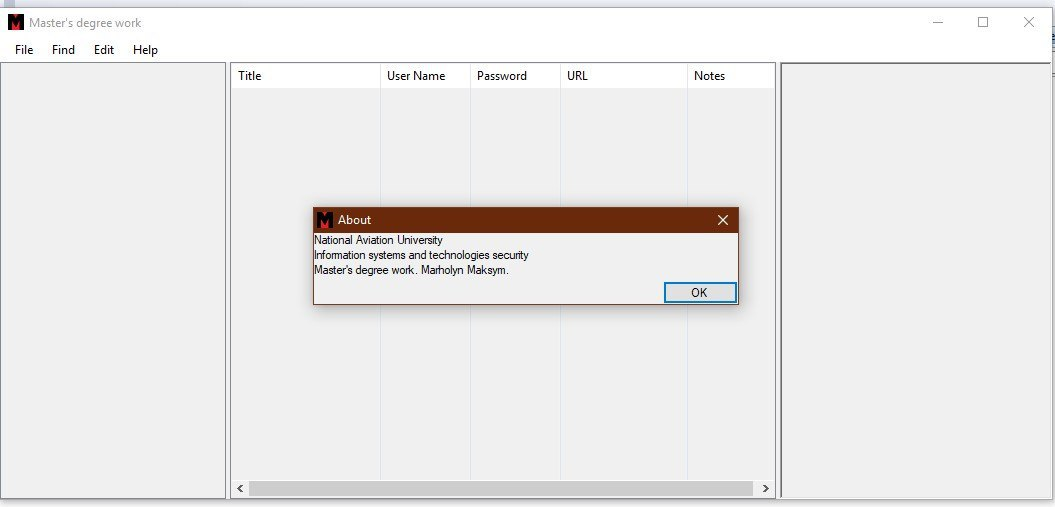


Рис 3.10. About

При створенні нової бази даних через меню File -> New відкривається вікно зберігання, де необхідно вказати шлях по якому зберігатись файл, як зображено на рис. 3.11.

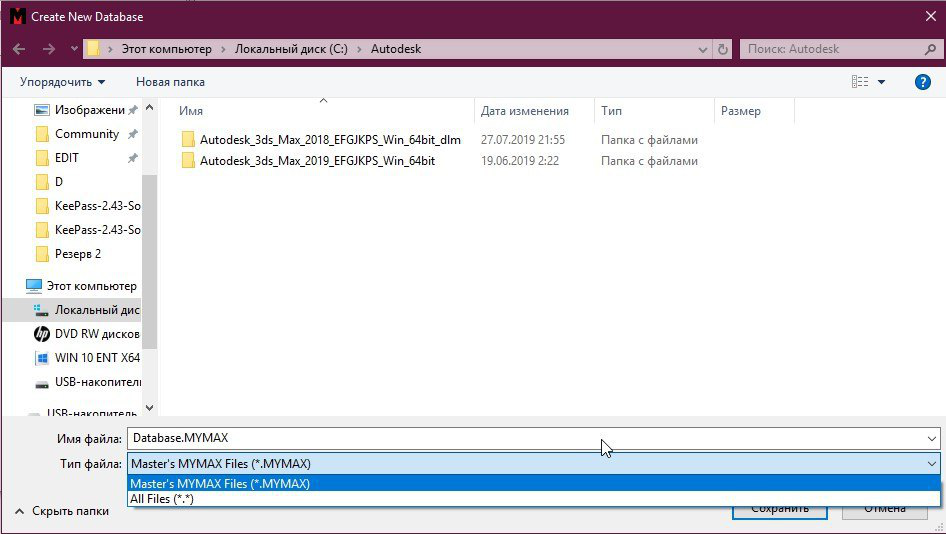


Рис. 3.11. New

Усі файли проекту мають розширення MYMAX. Після вибору місця зберігання проекту необхідно вказати пароль та обрати назву бази даних – рис. 3.12. Також користувач має можливість інтерактивно змінювати ступінь безпеки за яким шифруються файли, але усе залежить від швидкодії машини на якій запускається проект – на слабкому комп’ютері відкриття та редагування складних алгоритмів займає більше часу.

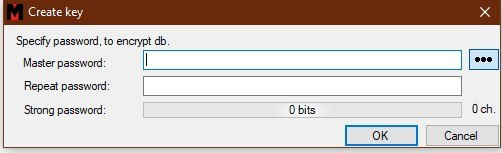


Рис 3.12. Pass

Стійкість алгоритму залежить від надійності ключа шифрування, саме тому було введено перевірку надійності паролю, у строчці “Strong Password”, як зображено на рис. 3.13.:

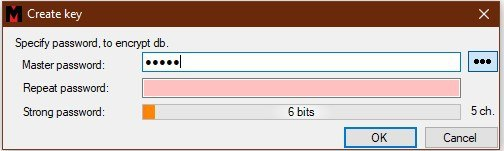


Рис 3.13. Strong Password

Стійкість пароля не э лінійною, наприклад – шість цифр та одна літері не теж саме ніж сім цифр. Це зображено на рис. 3.14.:

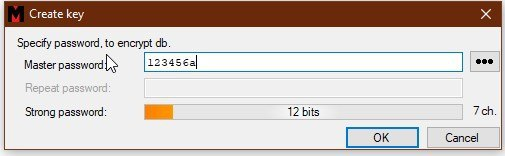


Рис. 3.14. Bits

Після вибору та введення пароля відкривається наступне вікно, яке надає можливість скорегувати політику безпеки та спосіб захисту програми. Дуже важливо щоб користувач заздалегідь знав за що відповідає та чи інша функція. Тому зад для швидкої адаптації нових користувачів було впроваджено, на першій сторінці, опис усіх можливостей у створенні політик безпеки. Перша вкладника зображена на рис. 3.15.:

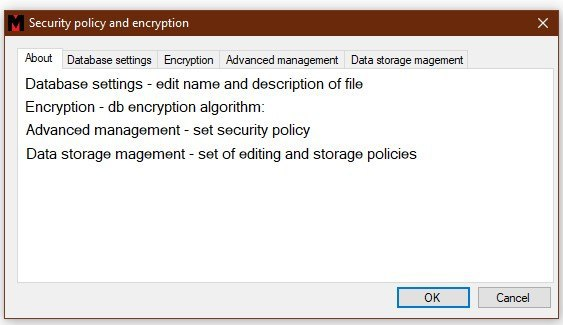


Рис. 3.15. About Security policy

У наступній вкладинці “Database settings” знаходиться меню редагування основних даних захищеної бази даних. У ній є можливість створити опис, надати назву але це не є обов’язковим. Користувач може пропустити цей пункт меню і перейти до створення методології шифрування. На рис. 3.16. відображене меню введення опису та назви нової бази даних.

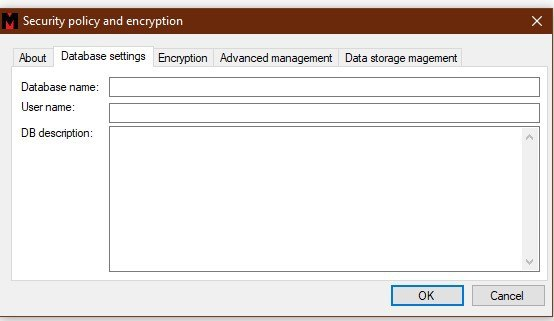


Рис. 3.16. Database settings

У вкладинці ”Encryption” рис. 3.17. користувач має можливість обрати алгоритм шифрування, стійкість та надійність методів захисту бази даних, які можливо гнучко скоректувати залежно від стандартів інформаційної безпеки яким необхідно слідувати. Але як правило не усі комп’ютери однаково швидко виконують криптографічні перетворення. Існують різні комп’ютери для різних типів задач, адже якщо заплановано використовувати машину для тільки у браузері для друкування та перегляду інтернет сторінок – то усі обчислення відбуваються не на стороні клієнта, а на хмарному сервері, отже і комп’ютер не повинен бути із великою обчислювальною спроможністю, для такого типу задач . З іншої сторони, якщо комп’ютер призначений для створення та редагування 3D – графіки, розробки складних креслень, обрахування інженерних формул та обрахування складних математичних, фізичних формул – то комп’ютер повинен мати спроможність обраховувати такі данні швидко . Адже час це гроші. Саме тому виникають дуже великі прірви між різними типами комп’ютерів. Тому дуже важливо мати змогу гнучко редагувати та створювати необхідні політики безпеки у середині програми, та мати інструменти для аналізу криптографічних перетворень на тій чи іншій машині. То що завжди є залежність від часу та надійності шифрування. На різних машинах на одну секунду може обрахуватись різна кількість ітерацій шифрування.

На вкладниці ”Encryption” користувач задає метод шифрування – AES чи ChaCha20. Для більшої надійності використовуються 256 ключі. Вони відрізняються кількістю ітерацій. У меню “Key Settings” відбувається збільшення введеного ключа за допомогою функцій девіації. Завдяки гнучкій функції редагування кількості ітерацій функції девіації програма надає можливість користвачу налаштувати максимально допустиме значення, опираючись на ресурси комп’ютера. Здебільшого користувач не знаю на що спроможна його машина, тому, на перший погляд такий підхід нічого не поліпшує. Але навіть навпаки – користувач може ввести завелике значення ітерацій, для його обчислювальної техніки, у наслідок чого шифрування займатиме забагато часу. Саме тому було розроблено та інтегровано в інтерфейс інтерактивний помічник. Завдяки кнопкам “Check algorithm speed”, рис. 3.18., користувач може перевірити скільки займає обрахування зазначеної кількості ітерацій. Але знову ж таки постає проблема підбору максимально ефективного значення ітерацій функції девіації. Тому, опираючись на швидкодію комп’ютера, на якому програма була запущена, інтерактивний помічник, має змогу визначити найбільш прийнятне значення ітерацій алгоритму. За оптимальне значення часу на обрахування функції було обрано стандарт в одну секунду . Для активації автоматичного обрахування та встановлення кількості ітерацій необхідно натиснути на кнопку “Set max speed”, рис. 3.19..

Також можливо використовувати додаткове перетворення Argon2, що працює за таким алгоритмом:

— Хешує пароль пароль ;

— Результат хешування записується блоками в пам’ять ;

— Блоки памяті перетворюються за допомогою функції стиснення ;

— В результаті роботи генерується ключ.

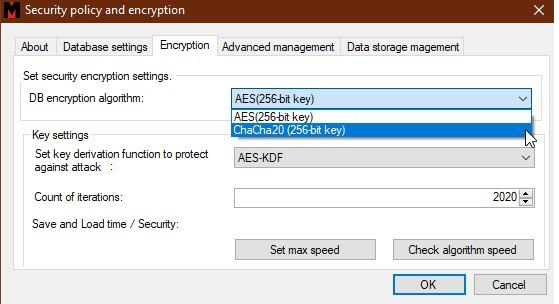


Рис. 3.17. Encryption

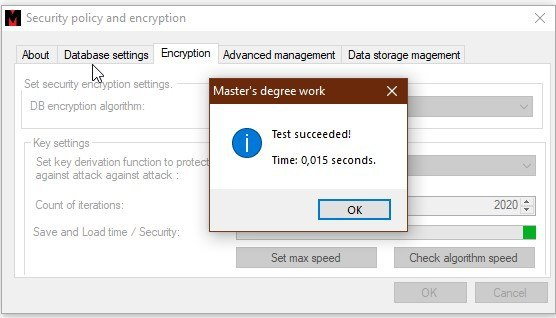


Рис 3.18. Check algorithm speed



Рис. 3.19. Set max speed

Вкладинка “Advanced magement” надає можливість встановлювати політику безпеки. Вона передбачає зміну пароля через встановлений проміжок часу у днях. Є дві опції за якими можливо нагадати користувачу о необхідності зміни пароля та примусово змінити його. Без цих опцій політика безпеки стає вразлива, так як виростає вірогідність, що пароль до бази даних стане відомий третім особам, рис. 3.20..

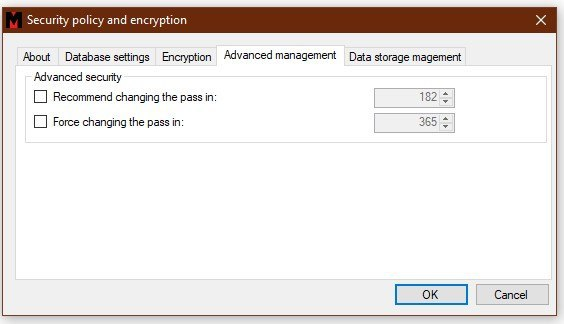


Рис. 3.20. Advanced magement

Для зручності редагування даних є можливість зберігати видалені файли у окремій групі, так званій “корзині”, користувачі ос Windows звикли до безпечного видалення даних через “корзину”, тому така функція реалізована у вкладниці “Data storage”, рис. 3.21.:

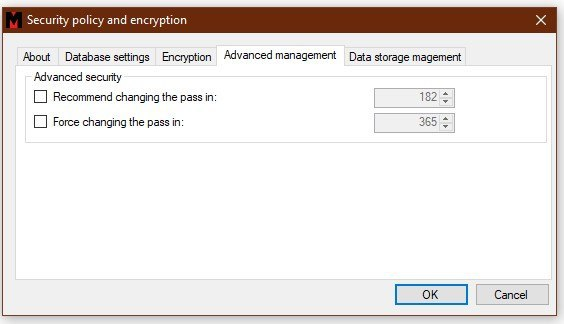


Рис. 3.21. Data storage

При завершенні створення початкового фалу проекта стануть активні вікна редагування бази даних. Поле ліворуч відповідає за створення та редагування груп, вони створенні для зручності використання програми. Поле по центру відповідає за редагування даних та створення нових записів. Можливо не тільки зберігати конфіденційні паролі та логіни, але й помітки з посиланнями, які теж потрібно захистити – рис. 3.22.

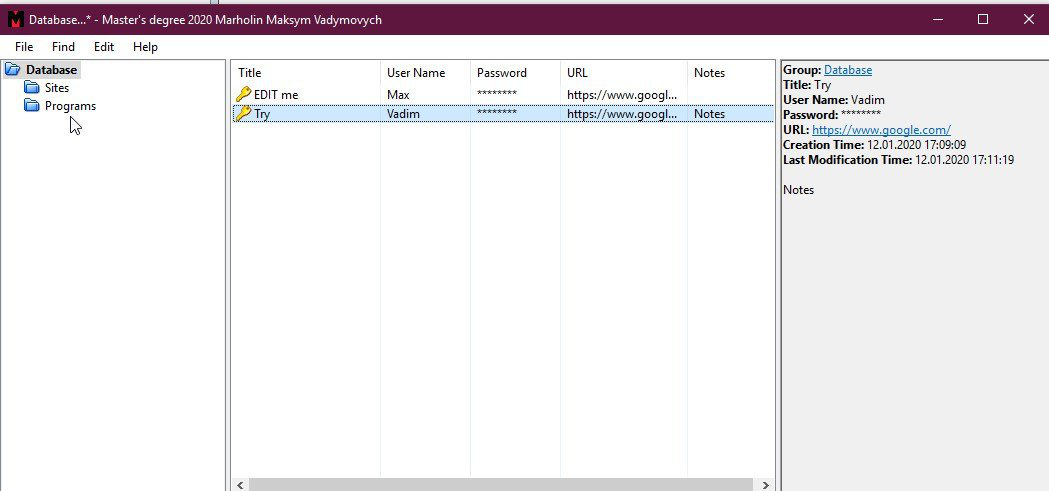


Рис. 3.22. Main window

Основна нововведення – можливість заповнювати пароль без його копіювання у буфер обміну. Реалізована функція автоматичного друкування з вікна програми у обрану програму чи ресурс. У меню ця функція називається «Start Enter in …» . приклад роботи цього методу зображено на рис.3.15. та 3.16..

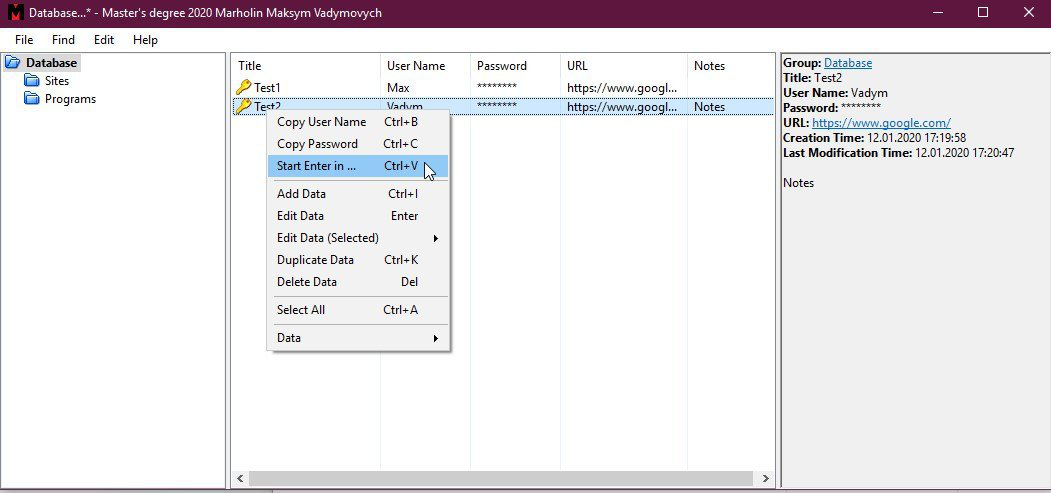


Рис. 3.15. Start Enter in…

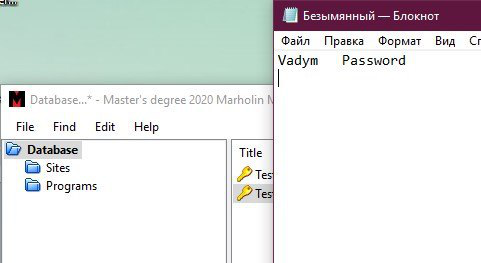


Рис 3.16 Result

## Оцінка ефективності

В реалізованому проеті вбудована функція оцінки ефектиіності захисту данних, див. рис. 3.12. В залежності від введеного паролю інтерактивно повідомлює що до надійності, виводить інформацію щодо його бітності та уількості символів.

Функція автоматичного введення екномить не тільки час на копіювання чи набір паролей але й гарантує, що інофрмацію жоден злоумисник не зможе запамятати та відтворити. Критерії оцінки етапу проектування та експлуатації вказані в табл.3.1 та 3.2.

*Таблиця 3.1*

Критерії оцінки ефективності на етапі проектування

|  |  |  |
| --- | --- | --- |
| Критерії етапу проектування | | |
| Складність | Коректність | Трудоємність |
| — Аналіз проблем захищеності сучасних інформаційних систем;  — пошук та дослідження існуючих рішень в сферах запобігання витоку персональних та конфіденційних даних; — вибір методології для розробки пз;  — розробка алгоритмів та логіки на яких буде реалізован програмне забезпечення; | — Відповідність до існуючих нормативно правових актах інформаційної безпеки;  — Реалізація усіх засад обраних методів захисту інформацї. | — Вивчення сучасних методів та роботи з обраним середовищем розробки програмного забезпечення.  — Оновлення зань нормативно правових актах інформаційної безпеки України. |

*Таблиця 3.2*

Критерії оцінки ефективності на етапі експлуатації

|  |  |  |
| --- | --- | --- |
| Критерії етапу експлуатації | | |
| Складність | Коректність | Трудоємність |
| — Розуміння інтерфейсу програмної реалізації | — Коректність вооду даних для зберігання та захисту у програмі. | — Звикання до необхідності використовувати новий програмний засіб інформаційної безпеки. |

## Висновки по розділу

Був розроблений прогрмний продукт, який дозволяє зберігати конфіденційні записи, логіни та паролі, сортувати , редагувати та все це у дуже простому та зручному інфтерфейсі. А саме головне безпечному. Якщо ми подивимося на сучасні програмні засоби для сзерігання ключів доступу до різноманітних ресурсів то їх об'єднує декілька особливостей. А саме в більшості вони вбудовані в конкретні програмні рішення – такі як бразури , та спецілізовані програми, в них наявні функції запамятовування паролів та логінів для подальшого швидкох аутентифікації. В інших використуваються копіювання всюго паролю до буфера обміну через засоби Window. Але такі рішення не підходять для випадків коли за однуєю машиною працюють чи мають до неї фізичний доступ декілька користувачів або при заходженні компютера у публіних місцях, коли кожен може залогінитися під чужим зебереженим паролем. Це не припустимо, особливо у час інформаційної війни коли конфіденційна інформація може коштувати не лише грошей, а й навіть життя.

Тому, проаналізувавши методи на ситуації мною було розроблено продук який вдосконалює теперішні рішення в області зберігання конфіденційної та персональної інформації. Оновним нововведення стало автоматичне друкування через віртуальну клавіатуру збережених та зашифрованних данних, відтепер не потрібно користуватися буфером обміну, чи переписувати пароль в ручну. Достатньо натисну одну клавішу і программа сама впише логін і пароль. Також для підтримки старих моделей компютерів, а такой ідввищення ступіня азахисту – користувачу відтепер буде надаватись вибір – звичайне швидке шифрування, яке не займає багато часу чи обрати надійність та пожертвувати часом на відкриття, редагування та зберігання зшифрованих файлів. На мою думку подібні рішення варто інтегрувати у операційні сисмеми для підвищення інформаційної безпеки. Розроблений продукт підтримує найпопулярніші операційні системи - Windows 10 та Windows 7.

# СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ ВИКОРИСТАНИХ ДЖЕРЕЛ

* 1. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» ( Відомості Верховної Ради України (ВВР), 1994, N 31, ст.286 ).
  2. Закон України «Про основні засади забезпечення кібербезпеки України» (Відомості Верховної Ради (ВВР), 2017, № 45, ст.403).
  3. Державний стандарт України «Захист інформації. Технічний захист. Інформації. Основні положення». Чинний від 01.01.1997 р.
  4. НД ТЗІ 2.5-010-03 «Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу».
  5. Hundepool A, Domingo-Ferrer J, Franconi L, Giessing S, Nordholt ES, Spicer K, de Wolf P-P – 2019 – Statistical disclosure control. Wiley, New York
  6. Brookman J, Hans GS – Why collection matters: surveillance as a de facto privacy harm. In: Big data and privacy: making ends meet. The center for internet and society – 2019 – Stanford Law School.

1. Закон України «Про Національну систему конфіденційного зв'язку» » // Відомості Верховної Ради України (ВВР) – 2002. – №22. ст.816 (остання редакція від 19.04.2014).
2. Закон України «Про захист інформації в Інформаційно-телекомунікаційних системах» » // Відомості Верховної Ради України (ВВР) – 1994. – №31. ст.286 (остання редакція від 27.03.2014).
3. Захист інформації. Технічний захист інформації. Основні положення: ДСТУ 3396.0-96. – [Чинний від 01.01.1997]. – Держспоживстандарт України, 2006, №4233, 18 с. – (Національні стандарти України).
4. Захист інформації. Технічний захист інформації. Порядок проведення робіт: ДСТУ 3396.1-96. – [Чинний від 01.07.1997]. – Держспоживстандарт України, 2007, №4233, 18 с. – (Національні стандарти України).
5. Захист інформації. Технічний захист інформації. Терміни та визначення: ДСТУ 3396.2-97. – [Чинний від 01.01.1998]. – Держспоживстандарт України, 2007, №4233, 32 с. – (Національні стандарти України).
6. Конституція України від 28.06.1996 №254к/96-ВР – 1996. №30. – С.141.(остання редакція від 20.04.2018).
7. Леинванд Аллан, Пински Брюс. Конфигурирование маршрутизаторов Cisco, 2-е изд. : Пер. с англ. - М.: Издательский дом «Вильямс», 2001. – 368 с.
8. Мультикаст в GNS3: [Електронний ресурс]. – Режим доступу до статті:<http://habrahabr.ru/post/215883/> - дата доступу: 10.12.2019.
9. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу. – 1999. – №22. – С.20(із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 №806).
10. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу. – 1999. – №22.
11. НД ТЗІ 1.1-005-07 Захист інформації на об’єктах інформаційної діяльності. – 2007. – №232. – С.6(із змінами згідно наказу Адміністрації Держспецзв'язку від 03.11.2011 №93/ДСК).
12. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі. – 2000. – №53. – С.32(із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 №806).
13. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу. – 1999. – №22. – С.74(із змінами згідно наказу Адміністрації Держспецзв'язку від 15.10.2008 №172).
14. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 3-е изд. / В. Г. Олифер, Н. А. Олифер. - СПб.: Питер, 2006.- 958 с.
15. Положення про технічний захист інформації в Україні, затверджене Указом Президента України. – 2000. – №1229/99 – с. 5 (із змінами від 11.04.20018).
16. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах (Правила № 373). – 2006. – №373 – с. 10 (із змінами від 07.09.2018).
17. 6th International Conference on Cyber Security: [Електронний ресурс]. – Режим доступу до статті: https://www.researchgate.net/publication/324413927 - дата доступу: 02.12.2019.
18. From Cyber-Bombs to Political fallout: threat Representations with an impact in Cyber-Security Discourse. International Studies Review: [Електронний ресурс]. – Режим доступу до статті: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2200862>- дата доступу: 02.12.2019.
19. Cyber Security is a Board Level Issue: [Електронний ресурс]. – Режим доступу до статті: https://www.crowdstrike.com/blog/why-cybersecurity-should-be-a-board-level-discussion/- дата доступу: 02.12.2019.
20. Cybersecurity: A Pre-history: [Електронний ресурс]. – Режим доступу до статті: https://www.tandfonline.com/doi/abs/10.1080/02684527.2012.708530 - дата доступу: 01.12.2019.
21. Cybersecurity Risks Detection and Prevention : [Електронний ресурс]. – Режим доступу до статті: <https://www.semanticscholar.org/paper/Cybersecurity-Risks-Detection-and-Prevention-Wally/8db541717b4a098fe4ed962f9ce765011a03d72c> - дата доступу: 01.12.2019.
22. An Investigation on Cyber Security Threats and Security Models: [Електронний ресурс]. – Режим доступу до статті: <https://www.semanticscholar.org/paper/An-Investigation-on-Cyber-Security-Threats-and-Thakur-Qiu/26534add8408c3b1517777026cc3d19430a8727a> - дата доступу: 01.12.2019.
23. Implementation of efficient AES encryption: [Електронний ресурс]. – Режим доступу до статті: [https://www.researchgate.net/publication/308866491\_FPGA\_ implementation\_of\_efficient\_AES\_encryption](https://www.researchgate.net/publication/308866491_FPGA_%20implementation_of_efficient_AES_encryption) - дата доступу: 10.11.2019.
24. Various Schemes for Database Encryption: [Електронний ресурс]. – Режим доступу до статті: <https://www.ripublication.com/ijaer17/ijaerv12n19_104.pdf> - дата доступу: 10.12.2019.
25. Keeping a Secret. Technology Review: [Електронний ресурс]. – Режим доступу до статті: [https://books.google.com.ua/ books?id=NlZFAQAAMAAJ&pg =PA32&lpg=PA32&dq=Keeping+a+Secret.+Technology+Review&source=bl&ots=Nq\_34Phezp&sig=ACfU3U2epdtKODf02lYLzATK1GKv9stleg&hl=ru&sa=X&ved=2ahUKEwi5mN3Cvo\_nAhVroosKHabzA-QQ6AEwBXoECAoQAQ# v=onepage&q=Keeping%20 a%20Secret.%20Technology%20Review&f=false](https://books.google.com.ua/%20books?id=NlZFAQAAMAAJ&pg%20=PA32&lpg=PA32&dq=Keeping+a+Secret.+Technology+Review&source=bl&ots=Nq_34Phezp&sig=ACfU3U2epdtKODf02lYLzATK1GKv9stleg&hl=ru&sa=X&ved=2ahUKEwi5mN3Cvo_nAhVroosKHabzA-QQ6AEwBXoECAoQAQ# v=onepage&q=Keeping%20 a%20Secret.%20Technology%20Review&f=false) - дата доступу: 20.12.2019.
26. Secure group key establishmentrevisited: [Електронний ресурс]. – Режим доступу до статті: <https://eprint.iacr.org/2005/395.pdf> - дата доступу: 10.12.2019.

# *Додаток А*

Код програми

private byte[] FileEn()

{

byte[] myHDR;

using(ZapomnoryStream mylsn= new ZapomnoryStream())

{

ZapomnMy.Write(ms, ZapomnMy.UInt32ToBytes(FSign1));

ZapomnMy.Write(ms, ZapomnMy.UInt32ToBytes(FileSignature2));

ZapomnMy.Write(ms, ZapomnMy.UInt32ToBytes(m\_uFileVersion));

WriHField(ms, MYMAXHDRFieldID.CipherID,

m\_pwDatabase.DataCipherUuid.UuidBytes);

int nCprID = (int)m\_pwDatabase.Compression;

WriHField(ms, MYMAXHDRFieldID.CompressionFlags,

ZapomnMy.UInt32ToBytes((uint)nCprID));

WriHField(ms, MYMAXHDRFieldID.MasterSeed, m\_myMasterSeed);

if(m\_uFileVersion < FileVersion32\_4)

{

Debug.Assert(m\_pwDatabase.KdfParameters.KdfUuid.Equals(

(new AesKdf()).Uuid));

WriHField(ms, MYMAXHDRFieldID.TransformSeed,

m\_pwDatabase.KdfParameters.GetByteArray(AesKdf.ParamSeed));

WriHField(ms, MYMAXHDRFieldID.TransformRounds,

ZapomnMy.UInt64ToBytes(m\_pwDatabase.KdfParameters.GetUInt64(

AesKdf.ParamRounds, PwDefs.DefaultKeyEncryptionRounds)));

}

else

WriHField(ms, MYMAXHDRFieldID.KdfParameters,

KdfParameters.SerExt(m\_pwDatabase.KdfParameters));

if(m\_myEncryptionIV.Length > 0)

WriHField(ms, MYMAXHDRFieldID.EncryptionIV, m\_myEncryptionIV);

if(m\_uFileVersion < FileVersion32\_4)

{

WriHField(ms, MYMAXHDRFieldID.InmRandomStreamKey,

m\_myInmRandomStreamKey);

WriHField(ms, MYMAXHDRFieldID.StreamStartBytes,

m\_myStreamStartBytes);

int nIrsID = (int)m\_craInmRandomStream;

WriHField(ms, MYMAXHDRFieldID.InmRandomStreamID,

ZapomnMy.Int32ToBytes(nIrsID));

}

if(m\_pwDatabase.PublicCustomData.Count > 0)

WriHField(ms, MYMAXHDRFieldID.PublicCustomData,

VariantDictionary.Ser(m\_pwDatabase.PublicCustomData));

WriHField(ms, MYMAXHDRFieldID.EndOfHDR, new byte[] {

(byte)'\r', (byte)'\n', (byte)'\r', (byte)'\n' });

myHDR = ms.ToArray();

}

return myHDR;

}

private void WriHField(Stream s, MYMAXHFID kdbID,

byte[] myData)

{

s.WriteByte((byte)kdbID);

byte[] my = (myData ?? ZapomnMy.EmptyByteArray);

int myln = my.Length;

if( { Debug.Assert(false); throw new OutOfZapomnoryException(); }

{

if(myln > (int)ushort.MaxValue)

{

Debug.Assert(false);

throw new ArgumentOutOfRangeException("myData");

}

ZapomnMy.Write(s, ZapomnMy.UInt16ToBytes((ushort)myln));

}

else ZapomnMy.Write(s, ZapomnMy.Int32ToBytes(myln));

ZapomnMy.Write(s, my);

}

private void WHDR(Stream s)

{

int nIrsID = (int)m\_craInmRandomStream;

WriteField(s, MYMAXFile.InmRandomStreamID,

ZapomnMy.Int32ToBytes(nIrsID), null);

WriteField(s, MYMAXFile.InmRandomStreamKey,

m\_myInmRandomStreamKey, null);

ProtectedBinary[] vBin = m\_mysBinaries.ToArray();

for(int i = 0; i < vBin.Length; ++i)

{

Protmy = vBin[i];

if(my == null) throw new Exception();

MYMAXBinaryFlags f = MYMAXBinaryFlags.None;

if(my.IsOk) f |= MYMAXBinaryFlags.Protected;

byte[] myFlags = new byte[1] { (byte)f };

byte[] myData = my.ReadData();

WriteField(s, MYMAXFile.Binary,

myFlags, myData);

if(my.IsOk) ZapomnMy.ZeroByteArray(myData);

}

if(value.IsProt)

{

MemUtil.ZeroByteArray(myrowl);

MemUtil.ZeroByteArray(myCmp);

}

}

else

{

byte[] myrowl = value.ReadData();

m\_xmlWriter.WriteBase64(myrowl, 0, myrowl.Length);

if(value.IsProt) MemUtil.ZeroByteArray(myrowl);

}

}

}

private void WriteObject(string name, myramgroopDeletedObject value)

{

Debug.Assert(name != null);

Debug.Assert(value != null); if(value == null) throw new ArgumentNullException("value");

m\_xmlWriter.WriteStartElement(name);

WriteObject(ElemUuid, value.Uuid);

WriteObject(ElemDeletionTime, value.DeletionTime);

m\_xmlWriter.WrT();

}

private void WriteBinPool()

{

m\_xmlWriter.WriteStartElement(ElemBinaries);

ProtBinary[] v = m\_mysBinaries.ToArray();

for(int i = 0; i < v.Length; ++i)

{

m\_xmlWriter.WriteStartElement(ElemBinary);

m\_xmlWriter.WriteAttributeString(AttrId,

i.ToString(NumberFormatInfo.InvariantInfo));

SubWriteValue(v[i]);

m\_xmlWriter.WrT();

}

m\_xmlWriter.WrT();

}

public static bool WriteDatas(Stream mymrOutput, myramgroopData[] vDatas)

{

return WriteDatas(mymrOutput, null, vDatas);

}

public static bool WriteDatas(Stream mymrOutput, myramgroopDatabase okContext,

myramgroopData[] vDatas)

{

if(mymrOutput == null) { Debug.Assert(false); return false; }

if(vDatas == null) { Debug.Assert(false); return false; }

// MYMAXFile f = new MYMAXFile(pwDatabase);

f.m\_format = MYMAXFormat.PlainXml;

XmlTextWritermyform = null;

try {myform = new XmlTextWriter(mymrOutput, StrUtil.Utf8); }

catch(Exception) { Debug.Assert(false); return false; }

if(myentry== null) { Debug.Assert(false); return false; }

f.m\_xmlWriter =myform;

myform.Formatting = Formatting.Indented;

myform.IndentChar = '\t';

myform.Indentation = 1;

myform.WriteStartDocument(true);

myform.WriteStartElement(ElemRoot);

foreach(myramgroopData pe in vDatas)

f.WriteData(pe, false);

myform.WrT();

myform.WriteEndDocument();

myform.Flush();

myform.Close();

return true; \*/

myramgroopDatabase ok = new myramgroopDatabase();

ok.New(new IOConnectionInfo(), new CompositeKey());

myramgroopGroupmywritt = ok.RootGroup;

if(pg == null) { Debug.Assert(false); return false; }

foreach(myramgroopData pe in vDatas)

{

myramgroopUuid pu = pe.CustomIconUuid;

if(!myentr.Equals(myramgroopUuid.Zero) && (ok.GetCustomIconIndex(pu) < 0))

{

int i = -1;

if(okContext != null) i = okContext.GetCustomIconIndex(pu);

if(i >= 0)

{

myramgroopCustomIcon ci = okContext.CustomIcons[i];

ok.CustomIcons.Add(ci);

}

else { Debug.Assert(okContext == null); }

}

myramgroopData peCopy = pe.CloneDeep();

mywritt.AddData(peCopy, true);

}

MYMAXFile f = new MYMAXFile(ok);

f.Save(mymrOutput, null, MYMAXFormat.PlainXml, null);

return true;

}