МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

**ПРИГАРА Михайло Петрович**

УДК 004.056.5

# ЗАХИЩЕНА СИСТЕМА ТЕХНІЧНОЇ ПІДТРИМКИ ПРОЦЕСІВ ДИСТАНЦІЙНОГО ВОЛЕВИЯВЛЕННЯ

Спеціальність 05.13.21 – «Системи захисту інформації»

**Автореферат**
дисертації на здобуття наукового ступеня
кандидата технічних наук

**Київ 2018**

Дисертацією є рукопис.

Робота виконана на кафедрі програмного забезпечення систем ДВНЗ "Ужгородський національний університет" (УжНУ).

Науковий керівник: кандидат технічних наук, доцент
**Вишняков Володимир Михайлович**,
доцент кафедри кібербезпеки та комп'ютерної інженерії Київського національного університету будівництва і архітектури

Офіційні опоненти: доктор технічних наук, професор
**Шелест Михайло Євгенович**,
професор кафедри кібербезпеки та математичного моделювання Чернігівського національного технологічного університету

кандидат технічних наук
**Цуркан Василь Васильович**,
доцент кафедри кібербезпеки та застосування автоматизованих інформаційних систем і технологій Інституту спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського».

Захист відбудеться «27» червня 2018 р. о $13^{00}$ на засіданні спеціалізованої вченої ради Д.26.062.17 при Національному авіаційному університеті за адресою: 03058, м.Київ, пр. Космонавта Комарова, 1, корп.11, ауд.111.

З дисертацією можна ознайомитись у Науково-технічній бібліотеці Національного авіаційного університету за адресою: 03680, м.Київ, пр. Космонавта Комарова, 1.

Автореферат розісланий «26» травня 2018 р.

В.о. вченого секретаря
спеціалізованої вченої ради
доктор технічних наук, професор  В.В. Козловський

## ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

**Актуальність.** Засоби захисту інформації, що функціонують у складі сучасних систем технічної підтримки процесів дистанційного волевиявлення (надалі - СДВ), не надають упевненості в тому, що специфічні загрози для інформації, виникнення яких підриває довіру громадян до збереження таємниці та об'єктивності результатів волевиявлення, нейтралізовані.

Дистанційне волевиявлення (ДВ) із застосуванням Інтернету надає суттєві переваги щодо зручності, мобільності та економії часу, але стримувальним фактором щодо його впровадження є недовіра спільноти через невпевненість у тому, що результати волевиявлення не будуть викривлені, а таємницю голосів не буде порушено. СДВ упроваджуються в багатьох країнах, але жодна з упроваджених систем не надає беззаперечних гарантій щодо неможливості підробки результатів волевиявлення й абсолютного збереження таємниці голосів. Беззаперечність гарантій полягає у наданні формально обґрунтованих доказів неможливості порушень таємниці голосів та викривленні результатів волевиявлення. Тому наукові дослідження щодо можливості створення захищеної СДВ, де такі гарантії надаються, є актуальними.

**Зв'язок роботи з науковими програмами, планами, темами.** Висвітлені в дисертації наукові результати отримано, здебільшого, у рамках науково-дослідної роботи, яка була виконана Київським національним університетом будівництва і архітектури (КНУБА) на замовлення Державного НДІ автоматизованих систем у будівництві (ДНДІАСБ), що здійснює свою діяльність у сфері створення комп'ютерних систем для потреб будівельної галузі, та „Укртелекому" (Договір про НДР №1036-Х15/80С321-2731). Результати використовуються в навчальному процесі НАУ при викладанні навчальної дисципліни «Стратегії обслуговування телекомунікаційних мереж».

**Мета роботи** - забезпечити беззаперечні гарантії неможливості виникнення порушень цілісності результатів волевиявлення та конфіденційності персональних даних голосуючих за умов повної недовіри до всіх без винятку учасників процесу ДВ, що усуває будь-які підстави для недовіри з боку голосуючих щодо можливості реалізації вказаних порушень.

**Задачі дослідження**

1. Здійснити аналіз характеристик існуючих СДВ з метою виявлення загроз, які підривають довіру громадян до результатів волевиявлення та збереження таємниці голосів, і визначити профіль захищеності інформації, що гарантує відсутність підстав для недовіри щодо точності результатів волевиявлення та/або збереження таємниці голосів.

2. Побудувати **модель СДВ**, що реалізує визначений профіль захищеності інформації під час обробки на сервері за рахунок використання **методу спостереження** в режимі реального часу за станом сервера з боку необмеженого кола будь-яких користувачів Інтернету в умовах недовіри до всіх без винятку осіб, що беруть участь у розробці, створенні та обслуговуванні СДВ.

3. Розробити **метод досконало захищеного обміну даними через Інтернет** між клієнтами та сервером СДВ, що забезпечує формально обґрунтовану неможливість порушень конфіденційності та цілісності даних у каналі зв'язку, із використанням необхідного для цього **методу отримання випадкових бітових послідовностей** в умовах типового клієнтського обладнання доступу до Інтернету без додаткових програмних або апаратних засобів.

4. Створити та протестувати програмне забезпечення, що реалізує розроблену модель та запропоновані методи захисту й спостереження. Оцінити показники якості функціонування цієї моделі.

**Об’єктом дослідження** є процеси захисту та технічної підтримки процедур ДВ з використанням мережі Інтернет.

**Предметом дослідження** є моделі, методи та засоби захищеної системи технічної підтримки процесів ДВ.

**Методи дослідження.** Виявлення «слабких місць» у захисті СДВ здійснено з використанням методів побудови комплексних систем захисту, що знайшли своє відображення у чинних нормативних документах ТЗІ. Розробка методів, що гарантують контрольованість середовища функціонування СДВ, виконана на основі результатів теорії побудови обчислювальних середовищ. Розробка методів забезпечення гарантованої конфіденційності та цілісності даних, що передаються каналами зв’язку, заснована на теорії криптографічних систем, у т.ч. теорії секретного зв’язку К. Шеннона. Синтез джерела дійсно (а не псевдо) випадкових послідовностей здійснено на основі результатів математичного моделювання пакетного трафіка. Статистичні параметри побудованої СДВ оцінювалися з використанням результатів теорії телетрафіка.

**Наукова новизна одержаних результатів**

1. Вперше побудовано **модель СДВ**, у якій за допомогою введення необмеженої кількості користувачів мережі з правами доступу виключно на ознайомлення з усіма файлами і процесами на сервері, але без прав на будь-яку модифікацію, можливе виявлення всіх порушень політики безпеки щодо цілісності результатів волевиявлення та конфіденційності голосів в умовах недовіри до всіх без винятку осіб, що беруть участь у розробці, створенні та обслуговуванні СДВ.

2. Дістав подальший розвиток **метод дистанційного спостереження** за роботою СДВ, використання якого за рахунок виконання визначеної послідовності контрольних дій та за умов повністю відкритого програмного забезпечення, унеможливлює виникнення непомічених порушень прийнятої політики безпеки, що усуває підстави для недовіри до СДВ.

3. Удосконалено **метод захищеного обміну даними через Інтернет**, який завдяки використанню випадкових бітових послідовностей та сумісного застосування шифру Вернама і алгоритму Диффі-Геллмана із параметрами, що забезпечують стійкий захист даних, і завдяки збереженню відстані єдиності згідно з К. Шенноном, формально обґрунтовують неможливість порушення конфіденційності даних у каналі зв’язку.

4. Удосконалено **метод отримання випадкових бітових послідовностей,** який завдяки комбінованому використанню природної нестабільності кварцових резонаторів, що входять до складу типового клієнтського обладнання, та непередбачуваності моментів появи та тривалості переривань, що виникають під час обробки випадкових мережевих запитів, забезпечує можливість коректної реалізації шифру Вернама в сукупності з алгоритмом Диффі-Геллмана. Метод дозволяє на типовому клієнтському обладнанні без додаткових програмних або апаратних засобів реалізувати запропонований удосконалений метод захищеного обміну даними через Інтернет.

**Практичне значення одержаних результатів**

1. Використання побудованої моделі СДВ в сукупності з розробленими методами надає можливість гарантувати відсутність порушень таємниці голосів та істинність результатів волевиявлення під час проведення виборів, конкурсів та опитувань в умовах повної недовіри до всіх без винятку учасників процесу волевиявлення.

2. Використання запропонованого методу дистанційного спостереження за роботою сервера СДВ з боку необмеженої кількості користувачів мережі Інтернет за рахунок усунення підстав для недовіри щодо істинності результатів волевиявлення та збереження таємниці голосів стимулює до участі в масових опитуваннях, виборах та референдумах.

3. Побудована модель СДВ за рахунок можливості приховування інформації про результати особистого волевиявлення від зловмисників усуває доцільність незаконного впливу на виборців методами підкупу, залякування або силового тиску.

4. Результати роботи впроваджено у НАУ, КНУБА, Національному університеті ім. Т.Г. Шевченка та в комп'ютерній мережі Державного науково-дослідного інституту автоматизованих систем в будівництві (Акт впровадження від 19.04.2018 р.), де встановлено відповідне програмне забезпечення для визначення суспільних думок, проведення референдумів, здійснення конкурсних та виборчих процедур.

**Особистий внесок здобувача.** Основні положення й результати дисертаційної роботи, отримані автором самостійно, обмежуються обсягом тих результатів наукової діяльності, які відображені в цій роботі. Із опублікованих у співавторстві робіт у дисертаційній роботі використовуються результати, отримані особисто здобувачем. (Творчий вклад здобувача у роботах із співавторами відображено у розділі «ПУБЛІКАЦІЇ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ»).

**Апробація результатів дисертації.** Результати досліджень дисертаційної роботи доповідались, обговорювались і отримали позитивну оцінку на:

1. IX Міжнародна науково-технічна конференція «Новітні комп'ютерні технології» NOCOTE'2011 (м. Севастополь, 2011).
2. X Міжнародна науково-технічна конференція «Новітні комп'ютерні технології» NOCOTE'2012 (м. Севастополь, 2012).
3. Наукова конференція молодих вчених, аспірантів і студентів КНУБА (м.Київ 2011)
4. 72-га науково-практична конференція КНУБА (м. Київ, 2011).
5. 73-тя науково-практична конференція КНУБА (м. Київ, 2012).
6. 75-та науково-практична конференція КНУБА (м. Київ, 2014).
7. XI Міжнародна науково-технічна конференція «Новітні комп'ютерні технології» NOCOTE'2013 (м. Севастополь, 2013).
8. Міжнародна наукова конференція ICS-2015 «Інформація, комунікація, суспільство 2015» (м.Львів, 2015)
9. 71-ша підсумкова наукова конференція професорсько-викладацького складу ДВНЗ «Ужгородський національний університет» (м. Ужгород, 2017).

**Публікації**. За результатами виконаних досліджень опубліковано 10 наукових робіт, із яких 5 статей у фахових науково-технічних спеціалізованих виданнях та в тезах доповідей на науково-технічних конференціях.

**Структура та обсяг дисертації.** Дисертаційна робота складається зі вступу, чотирьох розділів, висновків по кожному розділу та загальних висновків по роботі в цілому, списку використаних літературних джерел (84 найменування), 2 додатків. Повний обсяг дисертації - 226 сторінок, у тому числі 154 сторінки основного тексту, 28 рисунків, 10 таблиць.

## ОСНОВНА ЧАСТИНА

У **вступі** визначено проблему, що підлягає вирішенню, та обґрунтовано актуальність теми дисертації, сформульовано мету дослідження, визначено коло задач, що вирішуються, вказано на наукову новизну, практичне значення отриманих результатів, наведено дані про їх апробацію та впровадження.

**У першому розділі** здійснено аналіз характеристик існуючих СДВ. Зроблено

висновок, що основна перешкода впровадженню СДВ у практику суспільних відносин - відсутність довіри до забезпечення таємниці волевиявлення та коректного підрахунку його результатів.

Особливістю систем загального голосування є наявність труднощів у формуванні груп організаторів і адміністраторів (менеджерів) СДВ, які були б об'єктивно зацікавлені у достовірності результату підрахунку голосів, оскільки при загальному голосуванні у кожного представника цієї групи може існувати зацікавленість у тому, щоб результат голосування збігався з його власним бажанням. Цим системи загального голосування відрізняються від більшості інших систем, власники яких мають можливість звернутися до послуг об'єктивно незацікавлених менеджерів. У захисті системи загального голосування від фальсифікацій може бути зацікавлено тільки спільноту виборців у цілому, але до кожного окремого громадянина або будь-яких об’єднань громадян є підстави ставитися з недовірою.

Показано, що ця недовіра є наслідком недосконалості методів та засобів ТЗІ, що знайшли застосування в існуючих СДВ. Тому в даній роботі зроблена спроба вирішити проблему недовіри методами, що лежать у сфері ТЗІ.

Здійснено аналіз технологічного циклу функціонування СДВ, який показано на рис.1.


Рис.1. Технологічний цикл функціонування СДВ

На рис.1 прийнято такі скорочення: ПБД ДВ – період заповнення бази даних претендентів на дистанційне волевиявлення; ПП ДВ – період підготовки до дистанційного волевиявлення (завантаження електронних бюлетенів).

У результаті проведеного аналізу визначено інформаційні потоки й об’єкти, що потребують захисту, та виявлено загрози для інформації, відсутність протидії яким підриває довіру до того, що результати волевиявлення будуть об’єктивно відображати волю виборців. Визначення цих загроз, які мають бути включені у відому модель загроз для інформації у структурах типу "клієнт/сервер", надано у табл.1.

Таблиця 1

**Загрози, що впливають на рівень довіри громадян до коректної роботи СДВ**

| № з.п. | Визначення загрози | Наукові завдання з нейтралізації визначених загроз |
|---|---|---|
| 1 | Реєстрація фіктивних виборців | 1. Розробити **модель СДВ**, що гарантує цілісність результатів волевиявлення та збереження таємниці голосів в умовах недовіри до всіх без винятку осіб, що беруть участь у розробці, створенні та обслуговуванні СДВ. |
| 2 | Заміна системного ПЗ сервера на нештатне | |
| 3 | Модифікація штатного системного ПЗ сервера | |
| 4 | Виконання позаштатної команди управління сервером | |

| | | |
|---|---|---|
| 5 | Підробка прикладного ПЗ сервера | 2. Розробити **метод спостереження** в реальному часі за станом сервера і діями адміністратора СДВ з боку необмеженого кола будь-яких користувачів Інтернету, що виключає можливість виникнення непомічених порушень прийнятої політики безпеки та усуває підстави для недовіри до СДВ . |
| 6 | Нелегальна фізична підміна сервера | |
| 7 | Доповнення серверного обладнання нештатними засобами з метою реалізації *MITM* (атаки посередника) | |
| 8 | Підміна результатів голосування у процесі розсилки | |
| 9 | Підробка результату підрахунку голосів | |
| 10 | Примус виборців віддавати свій голос усупереч їх власного бажання | Розробити метод нейтралізації спроб здійснення будь-яких видів тиску на учасників процедур волевиявлення. |
| 11 | Порушення цілісності та (або) конфіденційності інформації при обміні даними через Інтернет | 1. Розробити **метод досконало захищеного обміну даними**, що гарантує цілісність та конфіденційність інформації при обміні даними через Інтернет. 2. Розробити **метод отримання чисто випадкових бітових послідовностей**, засобами виключно типового клієнтського обладнання масового виробництва. |
| 12 | Перехоплення автентифікаційних даних виборців з метою підміни голосуючої особи | |

Примітка: загрози порушення доступності ресурсів СДВ можуть призвести до зриву процедур волевиявлення, але не позначаються на рівні довіри громадян до коректної роботи СДВ.

Побудовано функціональний профіль гарантованого захисту від указаних загроз.

**У другому розділі побудовано модель СДВ**, що відображена в роботі у вигляді кореспондованої сукупності концептуальної моделі захисту інформації в СДВ та логічної моделі взаємодії користувачів із сервером СДВ.

**Основна умова реалізації моделі СДВ** - відкритість програмного забезпечення (ПЗ) сервера включно з ОС та відсутність обмежень щодо процедур контролю. Цій вимозі відповідає ОС *OpenBSD* у мінімальній конфігурації, що показано у табл.2.

Таблиця 2

**Характеристики ОС *OpenBSD* у мінімальній конфігурації**

| **Назва характеристики або команди** | **Значення характеристики** |
|---|---|
| Доступ до вихідних текстів ОС | Повний |
| Захист від несанкціонованого доступу | За певних умов абсолютно досконалий |
| Створення користувача-контролера | Можливо |
| Створення скритих файлів | Неможливо |
| Команда для контролю незмінності ОС | *top* (будуть незмінні 20 *PID*) |
| Команда контролю стану процесів | *ps aux* |
| Створення загроз діями контролера | Неможливо |
| Обмеження прав адміністратора | Можливо |
| Блокування користувача з повними правами | Можливо |

**Розроблено концептуальну модель захисту інформації в СДВ**, що реалізує визначений вище профіль захищеності, яку зображено на рис.2.

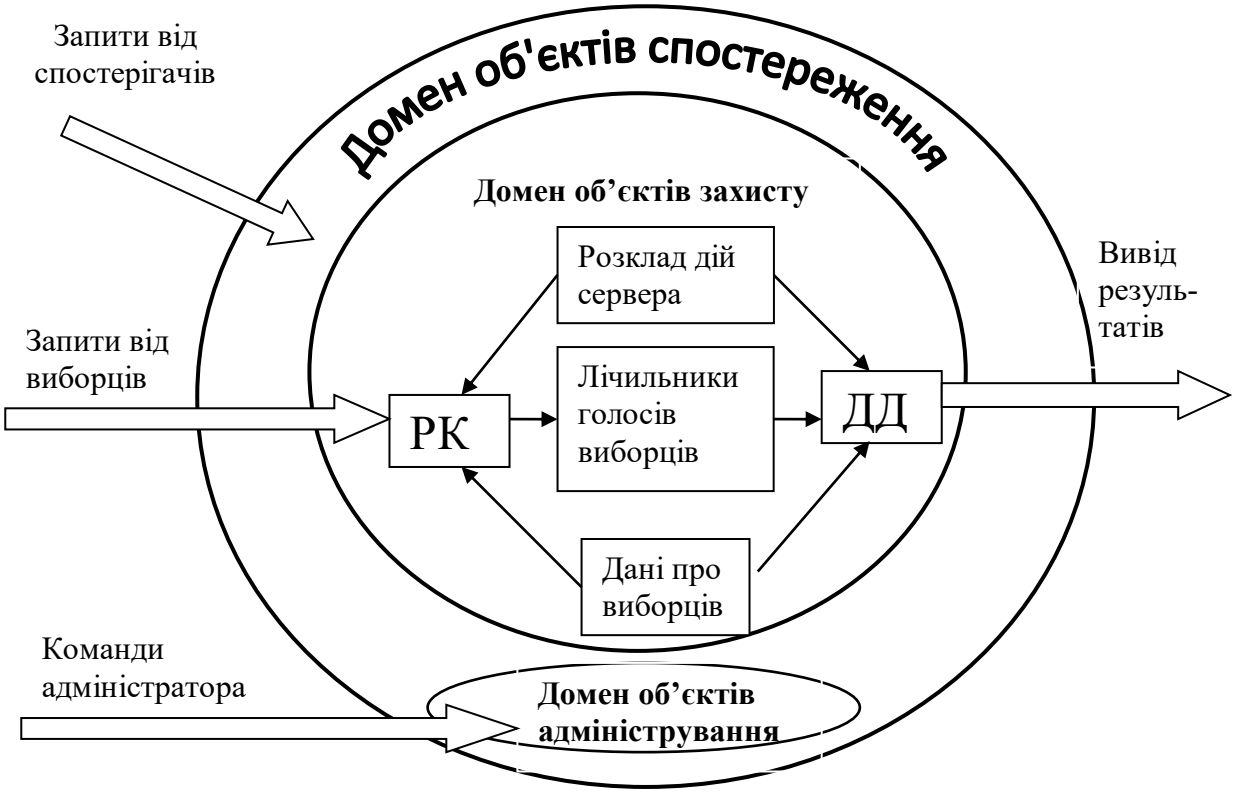


Рис.2. Концептуальна модель захисту інформації в СДВ, де РК – блок розшифровки та контролю запитів, а ДД – блок дозволу доступу до довідок і результатів

Домен об'єктів адміністрування включає всі файли в директорії адміністратора. Домен об'єктів спостереження включає всі файли сервера, а також результати дії команд контролю за роботою сервера. Домен об'єктів захисту включає всі дані, що знаходяться в межах оперативної пам'яті, яка виділена для процесу виконання прикладної програми.

Згідно з даною моделлю функціональність СДВ має забезпечити: 1) логічну ізоляцію процесів прикладної програми від шкідливих проникнень; 2) імпорт даних, що є об'єктами захисту, до обчислювальних процесів прикладної програми; 3) створення умов для використання шифру Вернама для захисту даних, що імпортуються в домен об'єктів захисту; 4) контроль за роботою сервера з боку необмеженого кола будь-яких користувачів Інтернету.

Поверхня внутрішнього шару ізолює множину процесів, що є об'єктами захисту, від інших процесів. Під цією поверхнею діє прикладна програма, яка підтримує виконання запрограмованих процедур волевиявлення. Зовнішній прошарок – це середовище ПЗ сервера, що є відкритим для спостереження з боку широкого кола будь-яких осіб, які мають доступ до Інтернету. Особисті дані голосуючих у зашифрованому вигляді доставляються в оперативну пам'ять прикладної програми через контрольовану точку доступу. Використовуються досконало стійкі шифри для обміну даними та взаємної автентифікації сторін. У прикладній програмі закладені моменти включення та відключення дозволу на обробку запитів від виборців і дозволу на вивід довідок та результатів волевиявлення. Критичні дані перебувають виключно в оперативній пам'яті діючої програми.

**Розроблено логічну модель взаємодії користувачів із сервером СДВ**, яку представлено на рис.3.

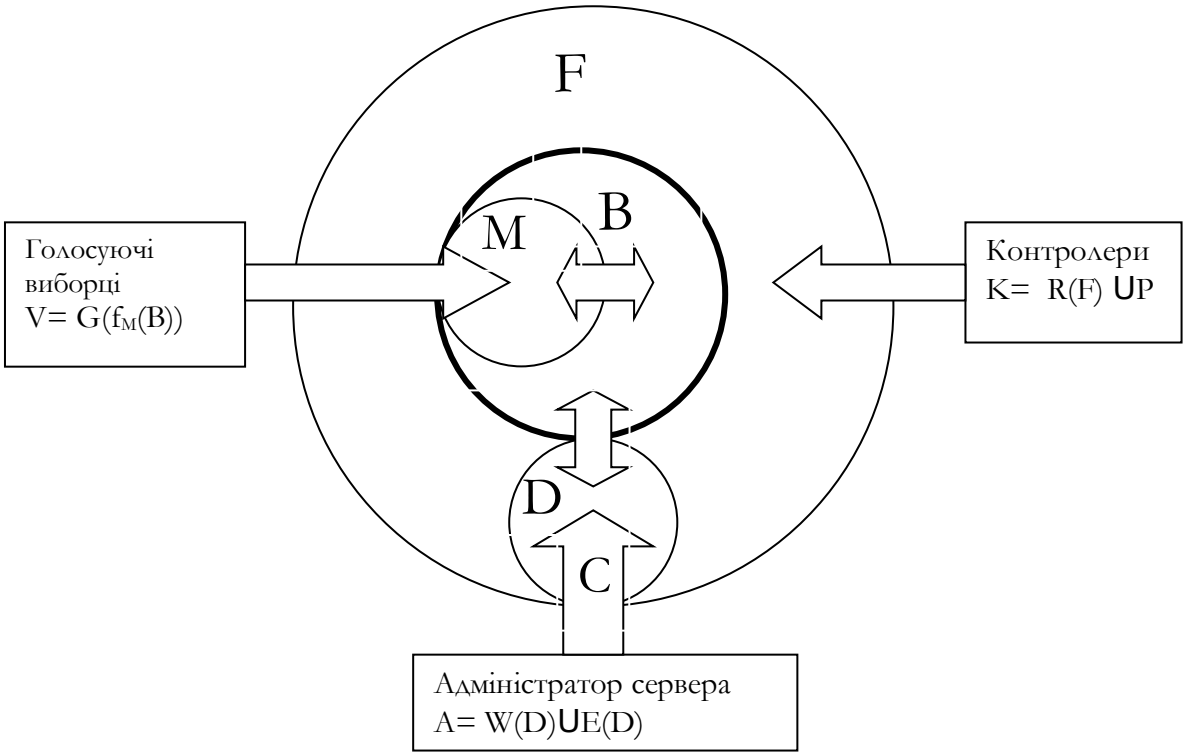


Рис.3. Логічна модель взаємодії користувачів із сервером СДВ

У цій моделі враховуються тільки ті дії користувачів, які сприймаються сервером. Некоректні або помилкові дії не розглядаємо, бо сервер їх не сприймає.

Операційна система сервера (після певних процедур налаштування) дозволяє виконувати користувачам ті, і тільки ті дії, що є елементами множини Q.

$$Q = V \cup A \cup K, \tag{1}$$

де $V$ – множина дій голосуючих виборців;

$A$ – множина можливих (штатних і нештатних) дій адміністратора сервера;

$K$ – множина дій контролюючих осіб.

Множина об'єктів, над якими виконуються дії, складається з наступних множин:

$F$ – множина всіх даних, що розміщені у файловій системі сервера, включаючи файли з програмами, а також з історією команд адміністратора;

$C$ – множина відображень команд адміністратора сервера, причому $C \subset F$, $f : C \to A$, де $f$ – функція відображення;

$D$ – множина файлів у директорії адміністратора, причому $D \subset F$;

$B$ – множина даних в оперативній пам'яті прикладної програми, причому $B \not\subset F$;

$M$ – множина даних для моніторингу звернень виборців, причому $M \subset B$.

Множини дій користувачів над цими об'єктами описують наступні вирази:

$$V = \{G_1(f_M(B)), ..., G_i(f_M(B)), ..., G_n(f_M(B))\}, \tag{2}$$

де $G_i$ – функція, яка відповідає і-вому варіанту запиту виборця до сервера, $i = \overline{1, n}$;

$n$ – кількість варіантів запитів виборця до сервера (наприклад: голосування, отримання довідки про хід голосування тощо);

$f_M$ – функція моніторингу звернень голосуючих виборців до сервера,

$$A = W(D) \cup E(D), \tag{3}$$

де $W$ – функція, яка відповідає множині дій адміністратора (командам запису) для приєднання файлів до множини $D$;

$E$ – функція, яка відповідає діям адміністратора (командам) щодо запуску на виконання файлів (програм) з множини $D$;

$$K = R(F) \cup P, \tag{4}$$

де $R$ – функція, яка відповідає множині дій щодо доступу контролерів для ознайомлення з об'єктами множини $F$, причому $C \subset F$, $D \subset F$;

$P$ – множина дій контролера щодо перевірки статусу процесів на сервері та отримання інших відомостей, які можуть свідчити про порушення політики безпеки.

Єдиний користувач, який має можливість виконання небезпечних дій на сервері, це адміністратор сервера, бо будь-які дії виборців і контролерів не здатні створити загрозу штатній роботі сервера. Для запобігання небезпечним діям адміністратору дозволено виконувати тільки дві дії: заносити файли у свою директорію і запускати на виконання (тільки один раз) програму з цієї директорії. Водночас не існує таких дій, які можна було б приховати від контролерів.

*Висновок*. Розроблена модель СДВ, представлена у вигляді кореспондованої сукупності концептуальної моделі захисту інформації в СДВ та моделі взаємодії користувачів із сервером СДВ, за умов відкритості ПЗ забезпечує: 1) досконалий захист критичних даних при зберіганні на сервері і при обміні через середовище Інтернет; 2) конфіденційність та неможливість непомічених фальсифікацій за умови повної недовіри до всіх без винятку учасників процесу волевиявлення; 3) можливість застосування методів протидії незаконному впливу на виборців.

**Розроблено метод дистанційного спостереження** в режимі реального часу за станом сервера з боку необмеженого кола користувачів Інтернету з метою протидії загрозам, що пов'язані із можливими зловмисними діями персоналу, який обслуговує СДВ.

***Вимоги щодо функціональності***. Метод має забезпечувати наступну функціональність послуг спостереженості: 1) повну відкритість для спостерігачів програмних засобів СДВ, зокрема операційної системи (ОС); 2) повну контрольованість середовища функціонування цієї системи, зокрема можливість контролю всіх об'єктів, процесів та подій, які в разі відхилення від штатного стану можуть стати причиною викривлення результатів волевиявлення або порушення таємниці голосів; 3) відсутність обмежень у доступі до домену об'єктів спостереження на сервері СДВ у режимі реального часу для будь-яких користувачів Інтернету.

***Сутність методу спостереження.*** Метод передбачає необхідність реалізації послідовності дій адміністраторів та активістів, що показано на рис 4. Як бачимо, у процесі встановлення ОС, створюючи користувача *admin* із обмеженими повноваженнями і блокуючи користувача *root* із повними повноваженнями, адміністратор залишає собі тільки ті можливості управління сервером, які необхідні для виконання штатних функцій. За цих умов на сервері до кінця виборчої кампанії буде тільки один користувач *admin*, який може встановлювати і запускати програми. Решта користувачів з ім'ям *kontrol* не можуть становити загрозу через обмеження їхніх повноважень.

В ОС *OpenBSD* існують команди *top* і *ps aux*, які дозволяють відслідковувати появу всіх без винятку активних процесів.

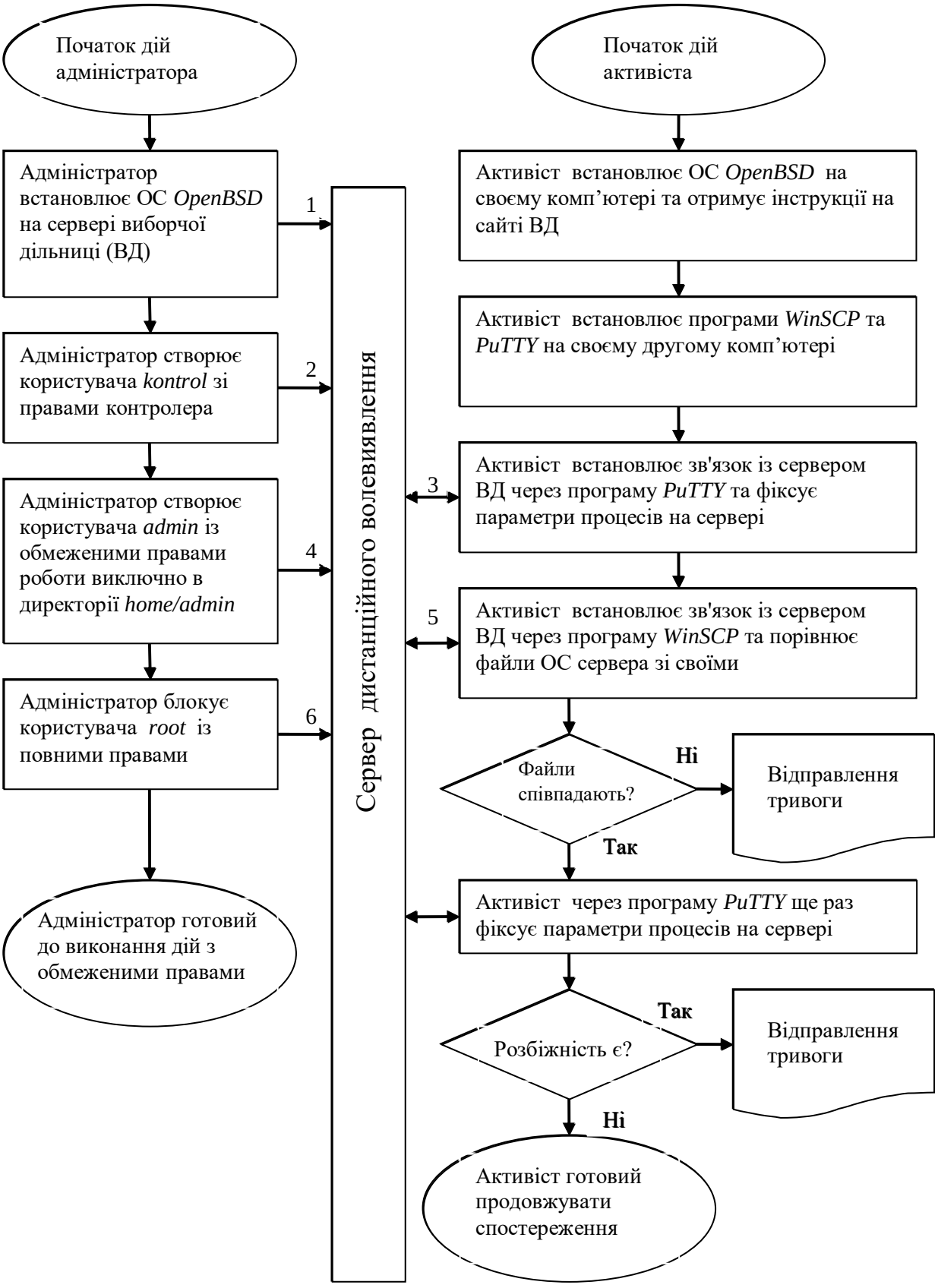


Рис. 4. Метод спостереження за файлами, процесами, подіями та діями адміністратора СДВ

*Процес встановлення ОС* починається із створення на CD *ISO*-образу ОС за допомогою будь-якого комп'ютера, який підключений до Інтернету і має стандартні засоби для створення *ISO*-образів. Після встановлення ОС адміністратор створює користувача із правами контролера (активіста) і робить паузу, щоб контролери за цей час встигли виконати перевірку справжності ОС. Кожен активіст має встановити таку ж ОС на своєму комп'ютері, щоб мати можливість порівнювати між собою файли на сервері і своєму комп'ютері.

*Процес перевірки справжності ОС*. Перевірки, які може виконати активіст для визначення справжності встановленої на сервері ОС, полягають у порівнянні множини характеристик файлів ОС у дисковій файловій системі і множини реакцій на названі нижче команди між двома ОС, які встановлені, з одного боку, на комп'ютері активіста, а з другого – на віддаленому сервері СДВ.

Множина $\boldsymbol{F}$ характеристик кожного з файлів ОС у дисковій системі складається з елементів $\{f_1, ..., f_6\}$, яким відповідають наступні значення: $f_1$ – ім'я файлу; $f_2$ – місце файлу у дереві каталогів; $f_3$ – розмір файлу у байтах; $f_4$ – час останнього корегування файлу; $f_5$ – права доступу до файлу; $f_6$ – повний зміст файлу. Позначимо множину множин характеристик файлів, які підлягають порівнянню, на сервері контролера $\boldsymbol{F}_k = \{ F_{k1}, \dots, F_{kn} \}$, а на віддаленому сервері – $\boldsymbol{F}_s = \{ F_{s1}, \dots, F_{sn} \}$. Оскільки справжність $\boldsymbol{F}_k$ не підлягає сумніву, то перша умова визначення справжності серверної ОС виглядатиме так:

$$F_k \Leftrightarrow F_s . \tag{5}$$

Другою умовою для визначення справжності серверної ОС є коректність результатів перевірки реакцій сервера на команди активіста. Для кожної з команд множина характеристик, за якими оцінюється коректність реакції сервера, буде різна. Повна множина $\boldsymbol{R}$ цих характеристик за всіма командами контролю даної ОС складається з елементів $\{ r_1, ..., r_8\}$, яким відповідають наступні значення:

$r_1$ – *IP*-адреса та *TCP*-порт з'єднання з боку клієнта (команда *netstat*),
$r_2$ – *IP*-адреса та *TCP*-порт з'єднання з боку сервера (команда *netstat*),
$r_3$ – значення часу встановлення з'єднання з точністю до хвилини (команда *ps aux*),
$r_4$ – ідентифікаційні дані користувача (команди *top*, *ps aux*),
$r_5$ – назва команди користувача (команди *top, ps aux*),
$r_6$ – момент початку виконання команди з точністю до хвилини (команда *ps aux*),
$r_7$ – ідентифікатори активних процесів сервера (команди *top, ps aux*),
$r_8$ – моменти початку активних процесів сервера (команди *top, ps aux*).

Позначимо множину значень характеристик, які підлягають перевірці, на боці контролера $\boldsymbol{R}_k = \{ r_{k1}, \dots, r_{km} \}$, а на віддаленому сервері – $\boldsymbol{R}_s = \{ r_{s1}, \dots, r_{sm} \}$. Умова визначення справжності серверної ОС щодо цих характеристик виглядає так:

$$R_k \Leftrightarrow R_s . \tag{6}$$

Рішення про справжність серверної ОС прийматиметься тільки в разі істинності наступного предикату:

$$\left(F_k \Leftrightarrow F_s\right) \wedge \left(R_k \Leftrightarrow R_s\right). \tag{7}$$

*Перевірка цілісності даних про результати волевиявлення.* Структура системи, яку можуть створити зловмисники, щоб непомітно для активістів порушити цілісність даних про результати волевиявлення, показана на рис. 5.

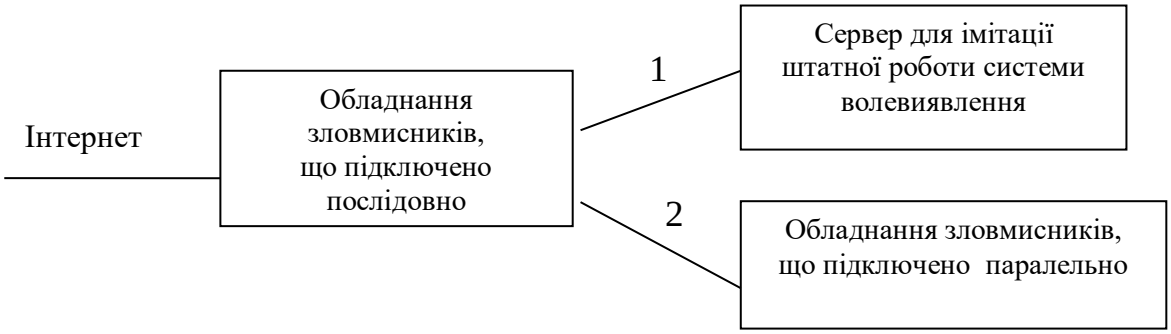


Рис. 5. Схема здійснення спроб підробки результатів волевиявлення

Для забезпечення непомітності слід встановити на окремому комп'ютері штатну ОС, яка буде надавати правильні відповіді на всі запити активістів. Для фальсифікацій встановлюється додаткове обладнання, яке може підключатись паралельно та послідовно зі штатним сервером. Задача обладнання, підключеного послідовно, полягає в розподілі звернень від користувачів на два потоки: у потік, що позначений цифрою 1, відправляти звернення контролерів; у потік, що позначений цифрою 2, відправляти звернення виборців. Для зловмисників відрізняти звернення активістів, які завжди відправляються на *TCP* порт 22, від звернень виборців не є складним. Якщо не вжити контрзаходів, то через дану схему активісти будуть перевіряти «фальшивий» сервер, на якому все буде точно відповідати штатному сценарію у той час, як виборці голосуватимуть на паралельному комп'ютері із підробленою серверною програмою. Однак «слабке місце» такого задуму зловмисників полягає в тому, що протокол *TCP* не дозволяє встановлювати з'єднання одразу з двома серверами, особливо в захищеному режимі. Отже, виявлення факту реалізації даної загрози потребує перевірки потоку даних до сервера за допомогою команди *netstat –p tcp.* При цьому можливі такі два варіанти:

1) Активіст під час уведення виборцями паролів для голосування не виявив на сервері відповідних потоків даних від виборців. Це одразу свідчить про факт реалізації даної загрози.

2) Активіст виявив, що реакція сервера під час уведення виборцями паролів для голосування відрізняється від нормальної. Це означає, що зловмисники роблять спробу імітації запитів виборців до сервера, але якщо паролі виборців надійно захищені, то успішність підробки цього процесу не є можливою.

*Висновок.* Розроблений метод базується на спостереженні за станом активних процесів (діючих програм) і всіх файлів на сервері з боку необмеженої кількості будь-яких осіб із будь-яких вузлів Інтернету. Даний метод унеможливлює створення непомічених загроз на сервері за умов використання відкритого ПЗ. Метод створює умови, за яких будь-яке зловживання щодо роботи сервера не може залишитись непоміченим.

**У третьому розділі розроблено метод досконало захищеного обміну даними через Інтернет** між клієнтами та сервером СДВ у класі симетричних систем із використанням ендоморфного шифру. Спочатку здійснюється генерування випадкових бітових послідовностей як на боці клієнта, так і на сервері та виконується обмін ключами за

алгоритмом Диффі-Геллмана. А потім здійснюється обмін конфіденційною інформацією через відкритий канал шляхом використання шифру Вернама.

У роботі конкретизовано діапазони оптимальних значень параметрів цих криптографічних методів, визначено обмежувальні умови застосування та розроблено засоби забезпечення виконання цих умов. Розробка методу передбачала необхідність визначення:

1) тривалості обслуговування запитів клієнтів для різних значень якості обслуговування (що визначається у даному випадку ймовірною тривалістю очікування у черзі до сервера);

2) довжини ключів шифру, що безпосередньо пов'язано з вибором методу шифрування та визначенням кількості конфіденційних даних, які мають бути передані через канал протягом одного сеансу зв'язку;

3) параметрів алгоритму Диффі-Геллмана, зокрема варіанту мультиплікативної групи для реалізації цього алгоритму, за яких злом системи захисту є гарантовано неможливим;

4) методу отримання випадкових бітових послідовностей, реалізація котрого є необхідною умовою коректного функціонування досконало секретної системи та коректної реалізації алгоритму Диффі-Геллмана.

Розроблений протокол, що реалізує метод - надбудова над стандартним протоколом прикладного рівня *HTTP*. Схема обміну даними між виборцем і сервером, що здійснюється з використанням цього протоколу, зображена на рис. 6.

| Комп'ютер виборця | | Сервер виборчої дільниці |
|---|---|---|
| | 1. *http*://<адреса сервера>/*anketa.html* → | |
| | ← 2. *anketa.html* - програма для клієнта | |
| | 3. *http*://<адреса сервера>/*Q*0<Значення $A = X^N$ > → | |
| | ← 4. *Nnn*<Значення $B = X^M$ > | |
| | 5. *http*://<адреса сервера>/*Q*1*Nnn* <ID, PW, NR > → | |
| | ← 6. *S* або *En* (*n* - номер помилки) | |
| | 7. *http*://<адреса сервера>/*Q*2*Nnn* <голос > → | |
| | ← 8. *En* (*n* - номер помилки) | |

Рис.6. Метод захищеного обміну даними через Інтернет

В якості основного параметра ефективності захисту при використанні шифру Вернама розглядають так звану відстань єдиності. Якщо вважати, що шифр – це сукупність множини відкритих текстів *X*, множини ключів *K*, множини криптограм *Y*, ключі шифру є рівно ймовірними, а передані тексти осмисленими, то натуральне число $L_0$, для якого очікувана кількість фальшивих ключів дорівнює нулю, визначає відстань єдиності. При сумарній довжині переданих через канал даних, меншій або рівній $L_0$, істинний ключ шифру може бути лише один. Нехай осмислені тексти повідомлень у сумі впродовж одного сеансу зв'язку мають довжину *L*, записані природною мовою з надлишковістю *D* в абетці *A* та складаються із *m* букв.

Відповідно до теореми про оцінку середньої кількості ключів, маємо:

$$| K| / ( k_L + 1) \le m^{LD}, \qquad (8)$$

де $k_L$ – кількість різних фальшивих ключів для розшифрування тексту довжиною *L*.

При $k_L = 0$ маємо

$$|K| \leq m^{LD}. \tag{9}$$

Після відомих із математичних основ криптоаналізу перетворень отримуємо

$$L \geq \log_2|K| / D \log_2 m. \tag{10}$$

Нехай знаки відкритого тексту, криптограми і ключа шифру отримують свої значення з кільця залишків $Z_m$, а довжини ключа і криптограми дорівнюють довжині $n$ відкритого тексту. Тоді рівняння шифрування можливо представити як

$$y_i \equiv (x_i + k_i) \bmod m_i , \quad i = 1, 2, \ldots , n . \tag{11}$$

Рівняння (11) визначає процедуру шифрування $n$-грами відкритого тексту $(x_1, x_2, \ , x_n)$ на ключі (гамі) $(k_1, k_2, \ldots , k_n)$, у результаті якої утворюється криптограма $(y_1, y_2, \ldots , y_n)$.

**Розроблено метод отримання випадкових бітових послідовностей**, реалізація котрого може бути здійснена штатними засобами будь-якого клієнтського комп'ютеризованого обладнання масового виробництва. Актуальність цієї розробки пов'язана із використанням шифру Вернама. Отож усі можливі спроби зламу цього шифру будуть пов'язані зі спробами компрометації методу отримання випадкових послідовностей. З іншого боку, для програмної реалізації алгоритму Диффі-Геллмана також необхідно отримувати випадкові бітові послідовності. До того ж швидкість генерування цих послідовностей має бути узгоджена із швидкістю знаходження степеня над полем $GF(2^n)$, де $n$ - безпечне просте число ($SPN$), що може дорівнювати числам 503, 563, 587, 719, …, які відповідають виразу $2p+1$, де $p$ - просте число.

Для генерації дійсно випадкових чисел запропоновано використати таке природне явище, як нестабільність частоти кварцових резонаторів, що є невід'ємними частинами будь-якого комп'ютера масового виробництва. Усі ці комп'ютери комплектуються двома незалежними кварцовими резонаторами, один із яких має частоту 32,768 кГц і використовується в якості таймера, а другий - з частотою не менше ніж 14318,18 кГц, – для формування тактових сигналів процесора. Обидва резонатори мають нестабільність від 10 до 100 *ppm* (або від $10^{-5}$ до $10^{-4}$ ), не є синхронізовані між собою. Причиною цієї нестабільності є фазовий білий шум, обумовлений впливом іонізації та нейтронних потоків зовнішнього середовища. Сутність запропонованого методу пояснює рис. 7.

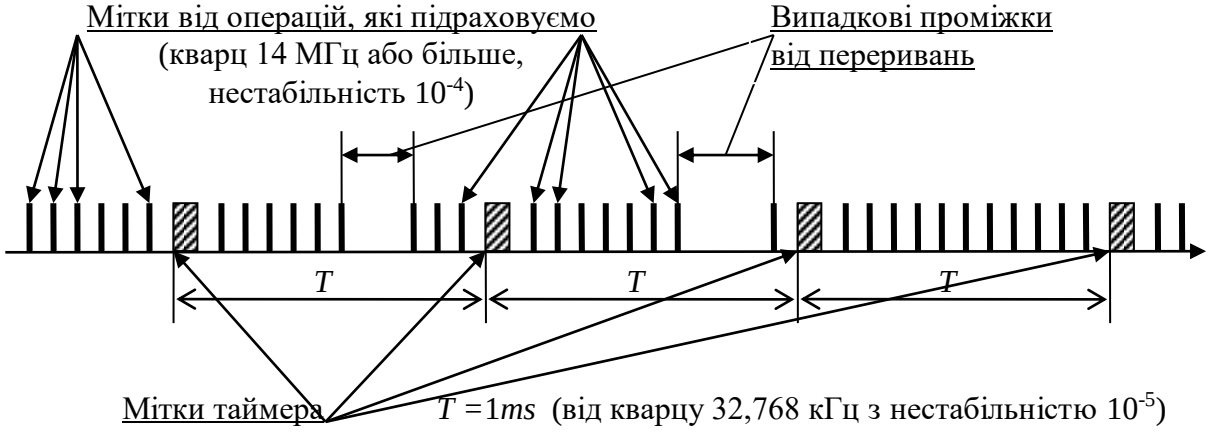


Рис.7. Метод отримання випадкових бітових послідовностей

Кількість нарахованих операцій, що виконуються процесором комп'ютера в інтервалах тривалістю *T*, може змінюватись від сотень до тисяч. Випадковий характер цієї кількості підсилюється наявністю випадкових проміжків від переривань процесу підрахунку. Моменти появи і тривалість цих переривань є непередбачуваними, бо вони обумовлені запитами з мережі Інтернет. Відомо, що потік цих запитів має фрактальний характер, функція розподілу котрого не є відомою. Зокрема в якості моделі потоку запитів розглянуто напівнескінчений відрізок стаціонарного випадкового процесу *X* дискретного аргументу (часу) *t=0,1,...,k, ...* , тобто часовий ряд $\{X_k;\ k = 0;1;2;...\}$, де *k* - поточний номер часового інтервалу усереднення процесу *X*. Тоді точкове значення *k*-го відліку часового ряду $\{X_k^{(\tau)};\ k= 0;1;2;\ \ldots\}$ при моделюванні потоку запитів інтерпретується як кількість запитів $x_k^{\tau}$ , що надійшли у вузол обробки даних протягом *k*-го інтервалу часу тривалістю *τ*. Тобто, у даному випадку $\tau$ - це інтервал усереднення запитів у потоці. Якщо ряд $\{X_k^{(\tau)};\ k= 0;1;2;\ \ldots\}$ унормувати відносно τ, то отримаємо ряд $\{I_k^{(\tau)};\ k= 0;1;2;\ \ldots\}$, в якому *k* -й компонент визначає поточну інтенсивність запитів на *k* -ому кроці його усереднення. Кількість запитів, що надійшли у вузол обробки даних протягом *k*-го інтервалу часу тривалістю *τ*, дорівнює максимально можливому значенню індексу $i_{max}$ , що задовольняє нерівності

$$\tau \geq sum\ \Delta\tau_{k,i} = \Delta\tau_{k,1} + \Delta\tau_{k,2} + \ldots + \Delta\tau_{k,imax}, \qquad (12)$$

де $\Delta\tau_{k,i}$ - проміжок часу між сусідніми запитами у потоці, *i = 0,1,2, …* - поточний номер цього проміжку, а *k* - поточний номер часового інтервалу усереднення процесу $\{X_k^{(\tau)};\ k= 0;1;2;\ \ldots\}$.

Отже, *k*-й компонент ряду $\{I_k^{(\tau)};\ k= 0;1;2;\ \ldots\}$, що визначає поточну інтенсивність запитів на *k*-ому кроці його усереднення, визначено як

$$I_k^{(\tau)} = x_k^{\tau}/\tau. \qquad (13)$$

Використання частотного методу криптоаналізу втрачає сенс, якщо упевнитись, що потік запитів має ознаки фрактального процесу. Таку упевненість отримуємо шляхом оцінювання значень параметра Херста за індексом дисперсії. IDC визначається як відношення дисперсії кількості оброблених запитів на заданому часовому інтервалі *T* до математичного очікування цієї величини:

$$F(T) = \frac{Var[N(T)]}{E[N(T)]}, \text{ де } N(T) - \text{кількість запитів на інтервалі } T. \qquad (14)$$

Для самоподібних процесів натуральний логарифм *F(T)*-1 як функція від натурального логарифма інтервалу *T* лінійно зростає, оскільки:

$$\ln[F(T)-1] = (2H-1)\ln T + y, \text{де } y = \ln\left[\frac{2K}{\alpha(1-\alpha)} M_{\Gamma}(\alpha) B^{-\alpha/2}\right],\ M_{\Gamma}(x) = \frac{\Gamma(1+x/2)\Gamma(1-x)}{\Gamma(1-x/2)}. \qquad (15)$$

Оцінювання параметру Херста може бути здійснено по кутовому коефіцієнту нахилу цієї прямої лінії.

**Запропоновано метод протидії загрозам, що пов'язані з моральним або іншим тиском** на суб'єктів процесу ДВ. Головна ідея, яку покладено в розробку методу: система

має надавати виборцю абсолютно ідентичні повідомлення в разі голосування як із правильним паролем, так і з деякою множиною неправильних паролів, наприклад, тих, що мають ту ж саму довжину, що й правильний пароль . При цьому зараховується тільки один результат із правильним паролем. Логічна схема реалізації методу є очевидною і не потребує додаткових пояснень. Метод забезпечує можливість усунення будь-якого впливу на власне рішення виборця з боку інших осіб шляхом забезпечення імітації процесу голосування з метою уведення в оману зловмисника.

**У четвертому розділі** для підтвердження можливостей досягнення результатів, отриманих під час роботи, проведено натурне моделювання усіх засобів СДВ, у складі якої функціонує розроблена система ТЗІ. Для моделювання обрано типову організаційно-технічну модель проведення загальнонаціональних виборів в Україні, принципи її функціонування сформульовано у вигляді технічних вимог. З метою мінімізації затримки під час обслуговування виборців передбачено можливість на сервері підтримки діалогу зі ста виборцями одночасно. Таку кількість виборців для одночасного обслуговування обрано виходячи з експериментальної оцінки відношення сумарної тривалості пауз $P_i$, які виникають між інтервалами $\tau_j$, що відповідають часу обробки запитів від одного виборця, до суми цих інтервалів, а саме:

$$K = \frac{\sum_{i=1}^{w} P_i}{\sum_{j=1}^{v} \tau_j}, \qquad (16)$$

де $K$ – оцінка кількості виборців, які можуть одночасно обслуговуватись сервером;
$w$ – кількість пауз між періодами обслуговування запитів від одного виборця;
$v$ – кількість інтервалів часу на обслуговування запитів одного виборця.

Часову діаграму процесу обслуговування виборця сервером показано на рис. 8.

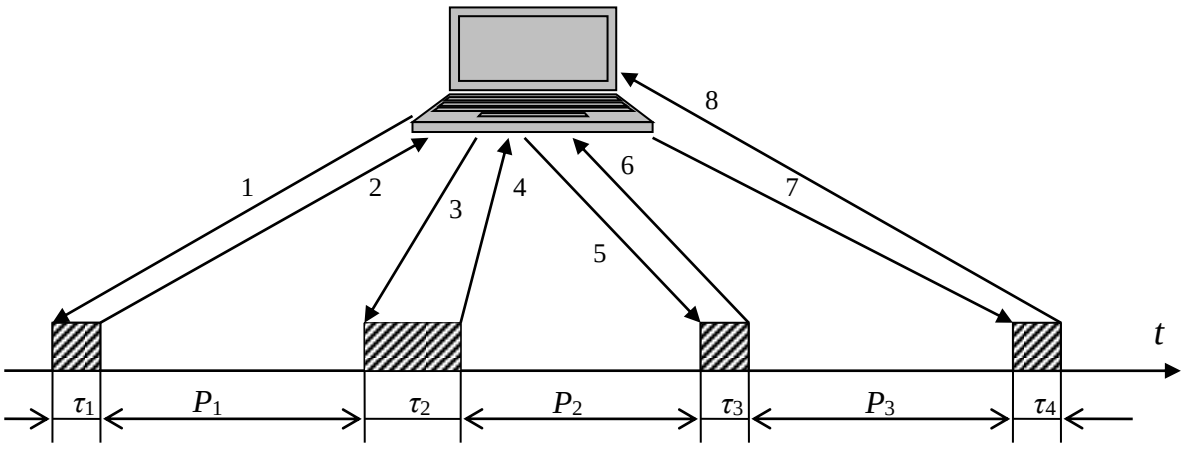


Рис. 8. Часова діаграма процесу обслуговування виборця під час голосування

Через те що сумарна тривалість пауз під час обслуговування запитів виборця приблизно у 100 разів більша за суму періодів обробки цих запитів, а серверна програма у періоди пауз може обслуговувати запити від інших виборців (до 99), час очікування для клієнтів у більшості випадків не перевищує 2-3 секунди.

Розкрито програмні механізми реалізації всіх запропонованих методів захисту та надано відповідні фрагменти комп'ютерних програм на мові *JavaScript*.

# ВИСНОВКИ

У дисертаційній роботі, відповідно до поставленої мети, розв’язано актуальну науково-технічну задачу гарантування неможливості виникнення порушень цілісності результатів та конфіденційності персональних даних в системах дистанційного волевиявлення, що усуває будь-які підстави для недовіри з боку голосуючих щодо можливості реалізації вказаних порушень.

У процесі виконання дисертаційної роботи отримані такі основні результати:

1. Здійснено аналіз характеристик існуючих СДВ. Показано, що основний недолік цих систем - відсутність дієвих механізмів контролю функціонування СДВ із боку суспільства. Через це не може буде забезпечена довіра людей щодо збереження таємниці голосів та результатів волевиявлення. Виявлено «слабкі місця» у захисті існуючих СДВ, зокрема виявлено загрози, відсутність протидії яким підриває довіру громадян до СДВ. Визначено профіль захищеності інформації, що забезпечує беззаперечні гарантії неможливості порушень таємниці голосів та результатів волевиявлення.

2. Побудовано модель захищеної СДВ у вигляді кореспондованої сукупності концептуальної моделі захисту інформації в СДВ та моделі взаємодії користувачів із сервером СДВ. Згідно з цією моделлю за допомогою засобів ОС сервера здійснюється логічна ізоляція процесів прикладної програми, досконало стійкий захист даних виборців в каналі доступу до критичних даних прикладної програми та безперервний контроль усіх ресурсів сервера (файлів та процесів) з боку необмеженого кола осіб. Модель реалізує визначений профіль захищеності засобами типового комп’ютерного обладнання з гарантованістю на рівні Г7 в умовах повної недовіри до всіх без винятків учасників процесу волевиявлення.

3. Запропоновано метод дистанційного спостереження за файлами, процесами, подіями на сервері СДВ з метою протидії загрозам штатній роботі сервера СДВ. Метод базується на спостереженні за станом активних процесів (діючих програм) і всіх файлів на сервері з боку необмеженої кількості будь-яких користувачів Інтернету за умов повної відкритості ПЗ і наперед відомого розкладу дій адміністратора. Даний метод унеможливлює створення непомічених загроз на сервері.

4. Розроблено метод досконало захищеного обміну даними через Інтернет між клієнтами та сервером ДВ, що забезпечує стійкий захист даних від порушень конфіденційності та цілісності. Доведено, що для забезпечення гарантованої захищеності обміну даними через Інтернет доцільно використати досконало стійкий шифр Вернама. Визначено умови забезпечення режиму досконалої стійкості цього шифру. Для захисту ключової інформації застосовано алгоритм Диффі-Геллмана. Для реалізації алгоритму обрано мультиплікативну групу над полями Галуа $GF(2^n)$, де $n$ – безпечне просте число (*SPN*), що може дорівнювати числам 503, 563, 587, 719, які відповідають виразу $2p+1$, де $p$ - просте число.

5. Розроблено метод отримання випадкових бітових послідовностей. Для отримання дійсно випадкових бітових послідовностей запропоновано використати: 1) випадковий та статистично не прогнозований характер потоку запитів до комп’ютера, що включений у мережу Інтернет; 2) випадковий характер нестабільності частоти кварцових резонаторів, що є у складі комп’ютера. Метод дозволяє забезпечити: 1) коректне функціонування досконало стійкої системи захисту, що реалізована з використанням шифру Вернама; 2) коректну реалізацію алгоритму Диффі-Геллмана. Реалізація методу може бути здійснена засобами типового комп’ютера, що важливо для широкого впровадження СДВ.

6. Запропоновано метод протидії загрозам, що пов'язані із силовим або психологічним впливом на виборців. Сутність цього методу полягає у наданні технічної можливості виборцям у разі необхідності імітувати процес волевиявлення та приховувати інформацію, яка потрібна зловмиснику, що робить недоцільною реалізацію подібних загроз.

7. Проведено комп'ютерне моделювання роботи СДВ згідно із запропонованою моделлю, побудованою з використанням розроблених методів ТЗІ. Показано, що за підтримки одночасного діалогу із 100 користувачами час очікування відповіді сервера не перевищує 2-3 секунди.

8. Надана оцінка часу очікування обслуговування запитів клієнтів до сервера. Показано, що збільшення інтервалу обслуговування клієнта на величину більшу ніж 6с , призводить до того, що кожний п'ятий клієнт буде очікувати своєї черги до сервера від 7с до 14с, а кожний сімнадцятий – від 14с до 21с.

9. Представлені результати забезпечують досягнення мети дослідження - забезпечити беззаперечні гарантії неможливості виникнення порушень конфіденційності персональних даних користувачів та результатів їхньої обробки в СДВ в умовах повної недовіри до всіх без винятку учасників процесу волевиявлення.

## ПУБЛІКАЦІЇ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. В.М. Вишняков, М.П. Пригара, О.В. Воронін, «Відкрита система таємного голосування», Управління розвитком складних систем, 2014, №20, С. 110 – 115. http://urss.knuba.edu.ua/files/zbirnyk-20/22.pdf *Особистий внесок здобувача: здобувачу належить провідна ідея формування відкритих систем із загальним контролем.*

2. С.В. Бронин, Пригара М. П, «Подбор оптимального набора строительных обьектов при планировании инвестиционной деятельности в строительстве», «Будівельне виробництво» No 55 2013р. http://ndibv.kiev.ua/wp-content/uploads/2016/04/ЗМІСТ-_Будівельне-виробництво_-№55-2013р.-.pdf *Особистий внесок здобувача: здобувачу належить адаптація економічних методів планування інвестиційної діяльності для будь-яких об'єктів на прикладі будівництва.*

3. В.М. Чуприн, В.М.Вишняков, М.П. Пригара, «Генерування випадкових чисел штатними засобами хостів мережі Інтернет», Захист інформації. – 2016. – Т. 18, №4 – С. 323-335. *Особистий внесок здобувача: здобувачу належить провідна ідея формування дійсно випадкових чисел.*

4. В.М. Чуприн, В.М. Вишняков, М.П. Пригара, «Метод протидії незаконному впливу на виборців у системі Інтернет голосування», Безпека інформації. – 2017. – Т. 23, №1 – С. 7-14. *Особистий внесок здобувача:здобувачу розробка методу емуляції правильної роботи системи при ознаках впливу на виборця.*

5. В.М. Чуприн, В.М.Вишняков, М.П. Пригара, «Захист операційного середовища систем інтернет голосування», ЗАХИСТ ІНФОРМАЦІЇ. – Т. 19, №1 – С. 56-66. *Особистий внесок здобувача: здобувачу належить провідна ідея ізольованого ядра безпеки.*

6. М. П. Пригара, «Використання метода Форда-Фалкерсона для визначення перевантажених маршрутів та ресурсів комп'ютерних мереж», Новітні комп'ютерні технології. – Кривий Ріг : ДВНЗ «Криворізький національний університет», 2013. – Випуск XI. – С. 185-187.

7.М.П. Пригара, «МЕТОДИ ОПТИМАЛЬНОГО ВИБОРУ РІВНЯ ЗАХИСТУ КОМП'ЮТЕРНИХ СИСТЕМ», Наукова конференція молодих вчених, аспірантів і студентів КНУБА: тези доповідей. – в 2-х частинах. – Ч.1. – К.: КНУБА, 2011. – 212 с. http://science.knuba.edu.ua/source/archive/molodi_vcheni/molodi_vcheni_tezy_2011-1.pdf

8.М.П. Пригара, Т.О. Чайковська, «ПАТТЕРН «COMPOSITE», Збірник тез студентських доповідей : КНУБА, 2012.-222 с. http://science.knuba.edu.ua/source/archive/npk/npk_tezy_2012.pdf

9.В. М. Вишняков, М. П. Пригара, Д. М. Тарасюк, «Багаторівневий захист даних в системах розв'язання складних задач на суперкомп'ютері», НОВІТНІ КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ Матеріали IX Міжнародної науково-технічної конференції NOCOTE'2011 - Київ–Севастополь, 13–16 вересня 2011 р. – К. : Мін- регіон України. С. – 36-38.

10. В.М. Вишняков, М.П Пригара, «Забезпечення свободи волевиявлення в системі Інтернет-голосування (ІГ)», Матеріали 4-ї Міжнародної наукової конферен- ції ICS-2015 «Інформація, комунікація, суспільство 2015» , С. 124 – 125. Режим доступу: World Wide Web. – URL: http://ena.lp.edu.ua: 8080/xmlui/bitstream/ handle/ntb/33187/055-124-125.pdf? sequence= 1&is Allowed=y

## АНОТАЦІЯ

**Пригара М.П. Захищена система технічної підтримки процесів дистанційного волевиявлення.** – Рукопис.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – «Системи захисту інформації». – Національний авіаційний університет, Київ, 2018.

Дисертаційна робота присвячена технічному захисту інформації (ТЗІ) у рамках системи дистанційного волевиявлення (СДВ), що гарантує збереження таємниці голосів та забезпечує свободу волевиявлення в умовах адміністративного тиску. Виявлено «слабкі місця» у захисті існуючих СДВ, зокрема специфічні загрози для інформації, відсутність протидії котрим підриває довіру громадян до її «чесної» роботи. Визначено можливості та шляхи нейтралізації цих «слабких місць».

Побудовано модель СДВ, у якій завдяки введенню необмеженої кількості користувачів з правами доступу на ознайомлення з усіма файлами і процесами на сервері, але без права на будь-яку модифікацію, забезпечена можливість виявлення всіх порушень політики безпеки щодо цілісності результатів волевиявлення та конфіденційності голосів в умовах недовіри до всіх без винятку осіб, що беруть участь у розробці, створенні та обслуговуванні СДВ. Запропоновано удосконалений метод захищеного обміну даними через Інтернет, який завдяки використанню випадкових бітових послідовностей та сумісного застосування шифру Вернама і алгоритму Диффі-Геллмана з параметрами, що гарантують стійкий захист даних, і завдяки збереженню відстані єдиності згідно з К. Шенноном, забезпечують формально обґрунтовану неможливість порушення конфіденційності даних в каналі зв'язку.

**Ключові слова:** системи дистанційного волевиявлення, технічний захист інформації, гарантована контрольованість програмного середовища, досконала стійкість щодо порушень конфіденційності та цілісності даних.

## АННОТАЦИЯ

**Пригара М.П. Защищенная система технической поддержки процессов дистанционного волеизъявления.** – Рукопись.

Диссертация на соискание ученой степени кандидата технических наук по специальности 05.13.21 – «Системы защиты информации». – Национальный авиационный университет, Киев, 2018.

Диссертационная работа посвящена созданию системы технической защиты информации (ТЗИ) в рамках системы дистанционного волеизъявления (СДВ), которая гарантирует сохранение тайны голосования и свободы волеизъявления в условиях

возможного административного давления. Выявлены "слабые места" в защите существующих СДВ, в частности специфические угрозы для информации, отсутствие противодействия которым подрывает доверие граждан к работе СДВ. Определены возможности и пути нейтрализации этих "слабых мест".

Построены модели процессов с учётом всех возможных вариантов уязвления информации для каждого этапа избирательной кампании, предложены методы противодействия угрозам, которые могут исказить информацию в результате такого нападения.

Впервые предложен метод противодействия угрозам штатной работе сервера, который основан на наблюдении за состоянием активных процессов (действующих программ) и всех файлов на сервере со стороны неограниченного числа заинтересованных лиц, в т.ч. общественных контролеров, при условии полной открытости всех программных средств и публикации расписания действий персонала, администрирующего сервер. Данный метод делает невозможным создание незамеченных угроз на сервере СДВ, если используется исключительно открытое ПО, состав и спецификации которого опубликованы заранее и, следовательно, являются известными широкой общественности. Метод создает условия, при которых любое злоупотребление, связанное с работой сервера, не может остаться незамеченным. Любая попытка воспользоваться нештатной программой или подменить сам сервер будет зафиксирована и документирована любым заинтересованным лицом независимо от его статуса или роли в избирательном процессе.

Представлена оценка необходимой длительности обслуживания запроса клиента в зависимости от значения допустимой длительности ожидания клиентов в очередях к серверу. Показано, что увеличение интервала обслуживания клиента на величину больше, чем 6с, приводит к тому, что каждый пятый избиратель будет ожидать своей очереди к серверу от 7с к 14с, а каждый семнадцатый - от 14с к 21с.

Доказано, что для обеспечения гарантированной защиты обмена данными через Интернет в СДВ целесообразно использовать шифр Вернама, корректность применения которого предусматривает необходимость разработки метода получения случайных битовых последовательностей. Определены условия обеспечения режима совершенной стойкости при обмене данными через Интернет. Определена необходимая длина ключевой последовательности для шифра Вернама.

Для обеспечения защиты ключевой информации при дистанционном доступе избирателя к серверу через сеть Интернет применен алгоритм Диффи-Хеллмана. Определены необходимые значения параметров этого алгоритма, при которых потенциально возможные затраты компьютерного времени на решение задачи дискретного логарифмирования превышают длительность избирательной кампании. В частности, избрана для реализации мультипликативная группа над полями Галуа GF ($2^n$), где n - безопасное простое число (SPN), которое может принимать значения 503, 563, 587, 719, определяемые из выражения $2p+1$, где $p$ - простое число.

Усовершенствован метод получения действительно (а не псевдо) случайных битовых последовательностей с использованием такого природного явления как нестабильность частоты кварцевых резонаторов, которые являются неотъемлемыми частями любого компьютера. Реализация метода является необходимым условием корректного функционирования стойкой системы защиты, которая реализована с использованием шифра Вернама, а также необходимым условием корректной реализации алгоритма Диффи-Хелмана.

Предложен метод противодействия угрозам, которые связаны с силовым или психологическим давлением на избирателей во время голосования, которые могут

искажать подлинность результатов голосования. Сущность метода заключается в полном сокрытии информации, которая нужна злоумышленнику, что делает нецелесообразным реализацию подобных угроз и позволяет избирателям реализовать свое право на свободное волеизъявление.

Для практического подтверждения результатов, полученных в работе, проведено компьютерное моделирование всех средств СДВ, в т.ч. средств защиты информации, в условиях, которые моделируют процесс общенациональных выборов в Украине. Экспериментальным путем доказано, что комплекс программно-технических средств, созданный на основе предложенных в работе методов, способен противостоять угрозам информации, реализация которых вызывает недоверие граждан к существующим системам дистанционного волеизъявления.

**Ключевые слова**: системы дистанционного волеизъявления, техническая защита информации, гарантированная контролируемость программной среды, совершенная стойкость системы противодействия нарушениям конфиденциальности и целостности данных.

## ABSTRACT

**Prygara M. Secure system of technical support of processes of remote expression of will.** – Manuscript.

Thesis for a Candidate of Technical Sciences degree in specialty 05.13.21 – «Information Security Systems». – National Aviation University, Kyiv, 2018.

The dissertation is devoted to the technical protection of information within the remote voting system (RVS), which guarantees secrecy of votes and ensures freedom of expression of will in conditions of administrative pressure. "Weaknesses" are identified in the protection of existing RVS, including specific threats to information, the lack of counteraction which undermines the trust of citizens in its "honest" work. The possibilities and ways of neutralizing these "weaknesses" are determined.

The model of the RVS was constructed, which, by introducing an unlimited number of users with access rights to reviewing all files and processes on the server, but without the right of any modification, was able to detect all violations of the security policy regarding the integrity of the results of the expression of will and the confidentiality of votes in conditions of distrust to all, without exception, persons involved in the development, creation and servicing of the RVS. An improved method of secure data exchange over the Internet is proposed, which, due to the use of random bit sequences and the coherent application of the Vername cipher and the Diffie-Hellman algorithm with parameters that guarantee the stable data protection, and, due to the preservation of the distance of unity according to K. Shannon, provide a formally grounded impossibility of violation confidentiality of data in the communication channel.

**Keywords:** controlled from distance voting systems over the Internet, technical priv, methods of providing of the assured testability of software environment, confidentiality and integrity of data that is passed by communication channels.