снення їх вибору для вирішення відповідних завдань інформаційної безпеки.
Ключові слова: інформаційна безпека, ризик, оцінювання ризиків, аналітико-синтетична кортежна модель, засоби оцінювання ризиків інформаційної безпеки, загроза, вразливість, характеристики ризику.

RESEARCH BASED ON TOOLS INVESTIGATION OF SECURITY RISK ASSESSMENT ACCORDING TO THE INFORMATION SYSTEMS RESOURCES

One of the main stages of integrated systems construction for protecting information resources is risk assessment. Often, specialists of the companies to increase the efficiency of information security pay attention to the choice of adequate tools of information security risks assessment that will meet the relevant requirements. Nowadays there is a wide range of such tools. For their rational choice, a variety of risk assessment tools have been investigated to determine the set of necessary comparative characteristics. According to the mentioned means, taking into account the known analytical-synthetic tuple model of risk characteristics, a tuple is formed, which makes it possible due to the certain parameters, to unify the process of comparative analysis of such means. This will enhance the effectiveness of the choice implementation to solve the corresponding tasks of information security.
Keywords: information security, risk, risk assessment, analytic-synthetic tuple model, tools for information security risk assessment, threat, vulnerability, risk characteristics.

Приставка Филипп Александрович, доктор технических наук, профессор, заведующий кафедрой прикладной математики Национального авиационного университета.
E-mail: chindakor@mail.ru

Приставка Пилип Олександрович, доктор технічних наук, професор, завідувач кафедри прикладної математики Національного авіаційного університету.
Prystavka Philip, Dr Eng, professor, head of applied mathematics department, National Aviation University.

Павленко Петр Николаевич, доктор технических наук, профессор, профессор кафедры средств защиты информации Национального авиационного университета.
E-mail: petrpav@nau.edu.ua
Павленко Петро Миколайович, доктор технічних наук, професор, професор кафедри засобів захисту інформації Національного авіаційного університету.
Pavlenko Petro, Dr Eng, professor, professor of information security means department, National Aviation University.

Казмирчук Светлана Владимировна, кандидат технических наук, доцент, доцент кафедры безопасности информационных технологий Национального авиационного университета.
E-mail: sv.kazmirchuk@gmail.com
Казмірчук Світлана Володимирівна, кандидат технічних наук, доцент, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету.
Kazmirchuk Svitlana, PhD in Eng., Associate Professor of IT-Security Academic Department, National Aviation University.

Коломиец Марина Вячеславовна, студентка Национального авиационного университета.
E-mail: mk160597@mail.ru
Коломієць Марина В'ячеславівна, студентка Національного авіаційного університету.
Kolomiiets Maryna, student, National Aviation University..

DOI: 10.18372/2410-7840.19.11444
УДК 004.056.5

ЗАХИСТ ОПЕРАЦІЙНОГО СЕРЕДОВИЩА СИСТЕМ ІНТЕРНЕТ ГОЛОСУВАННЯ

Володимир Чуприн, Володимир Вишняков, Михайло Пригара

В даній роботі запропоновано метод створення захищеного операційного середовища для сервера системи Інтернет голосування, який усуває причини недовіри суспільства щодо можливих фальсифікацій результатів або розкриття таємниці голосів. Метод базується на концепції ядра безпеки і реалізує профіль захищеності, згідно якому в оперативній пам'яті сервера створюється ділянка, в межах якої доступ до даних має виключно процес підрахунку голосів наперед вибраною відкритою прикладною програмою. Для унеможливлення доступу до цієї ділянки пам'яті для будь-яких інших процесів, використано відкриту операційну систему, у якій функції для такого доступу відсутні. Крім того, створено умови для дистанційного контролю цілісності усіх без винятку файлів і процесів на сервері, а також всіх дій персоналу щодо адміністрування сервера з боку необмеженої кількості контролерів, якими можуть стати будь-які особи. Показано, що запропонований метод в сукупності з відомими методами захисту інформації, надає змогу виявлення всіх можливих

загроз щодо розкриття таємниці голосів та викривлення результатів підрахунку в системах Інтернет голосування. Впровадження даного методу може бути корисним в багатьох сферах, де відбуваються громадські або експертні дистанційні опитування, для унеможливлення викривлення результатів і збереження таємниці голосів за умов недовіри до організаторів та учасників процесу голосування.

Ключові слова: *Інтернет-голосування, технічний захист інформації, збереження таємниці голосів, прозорість системи голосування, забезпечення довіри виборців.*

ПОСТАНОВКА ЗАВДАННЯ. Проблема розробки досконалих систем голосування з використанням мережі Інтернет стає все більш актуальною протягом останніх двох десятиріч, хоч різні прошарки суспільства в різних країнах мають різні уявлення щодо критеріїв досконалості цих систем. В роботах [1-5], поряд з іншим, розглянуто критерії досконалості систем дистанційного голосування. Зокрема, в роботі [1] ці критерії розглянуто у порівнянні систем Інтернет голосування із Інтернет технологіями, що вже знайшли широке застосування у фінансовій та торгівельній сферах. Серед причин відсутності прогресу в галузі Інтернет голосування вказується, що ризики і негативні наслідки від фальсифікацій під час виборів можуть бути набагато значнішими, ніж під час електронної комерції. Стосовно реалій України найбільш детально ці критерії розглянуто в [2-3].

Вимоги до систем Інтернет голосування з позицій ТЗІ сформульовані в багатьох джерелах, наприклад в [2-5], серед яких найбільш узагальнені формулювання надані в роботі [5]:

1. Голосувати можуть тільки ті, хто має на це право.

2. Кожен може проголосувати не більше одного разу.

3. Ніхто не може дізнатись, як проголосував конкретний виборець.

4. Ніхто не може проголосувати замість іншого.

5. Ніхто не може таємно змінити чийсь голос.

6. Кожен голосуючий може перевірити те, що його голос враховано.

Крім цього, в деяких випадках може знадобитись ще й така вимога:

7. Кожен може дізнатись про те, хто проголосував, а хто ні.

Більшість експертів [2] приходять до висновку, що жодна з існуючих систем для голосування через мережу Інтернет в повній мірі не відповідає наведеним вище вимогам.

Однією із основних перешкод щодо забезпечення відповідності цим вимогам, як це відмічено у роботах [2-5], є труднощі з отриманням довіри виборців щодо неупередженого підрахунку голосів і збереження таємниці їх волевиявлення. Іншими словами, система голосування має бути побудована таким чином, щоб не залишалось сумнівів щодо відсутності можливості викривлення результатів волевиявлення або розкриття таємниці голосів. У тому числі, що суттєво, і з боку адміністраторів системи, що мають найвищі права доступу до її інформаційних ресурсів. Наявність хоч однієї непрозорої процедури є підставою для недовіри і дискредитації системи. Тільки повна прозорість виконання узгоджених Законом виборчих процедур і контрольованість усіх без виключення шляхів доступу до критичної інформації з боку будь-якої зацікавленої особи, що знаходиться у будь-якому місці, на усіх етапах роботи системи голосування у реальному часі є основною передумовою подолання недовіри виборців. Так що функціональний профіль захищеності інформаційних ресурсів системи дистанційного голосування має включати, поряд з послугами гарантованого захисту від порушень конфіденційності та цілісності, ще й послуги для забезпечення повноцінного громадського контролю. Під повноцінним мається на увазі контроль, проведення якого не залишає жодних сумнівів щодо точності виконання сервером усіх запрограмованих дій.

Враховуючи те, що в діючих нормативних документах, які найбільш наближені до розв'язання подібних задач (НД ТЗІ 2.5-005-99 та НД ТЗІ 2.5-010-03), не надано специфікації щодо дистанційного повноцінного контролю з боку будь-якої кількості зацікавлених осіб, можна вважати актуальною задачу розробки профілю захищеності операційного середовища для систем Інтернет голосування, який з позицій ТЗІ має забезпечувати таке:

1) наявність захищеної ділянки оперативної пам'яті сервера, в якій має здійснюватися процес підрахунку голосів, щоб дані з цієї ділянки були недоступними для усіх процесів, крім єдиного процесу виконання штатної прикладної програми;

2) обмеження функціональності операційної системи тільки тими функціями, які необхідні для проведення голосування, що скорочує можливості здійснення нештатних дій;

3) повноцінний дистанційний контроль цілісності усіх без винятку програмних засобів сервера, включаючи операційну систему, а також безперервний дистанційний громадський контроль за виконанням дій щодо адміністрування сервера,

з боку необмеженої кількості будь-яких зацікавлених осіб.

При цьому слід зауважити, що, як підкреслено у роботі [6], відкритість системи не є перешкодою для захисту від загроз зловмисників, а навпаки, відкриті системи мають більше шансів бути краще захищеними через можливість залучення до участі у їх перевірці і вдосконаленні необмеженої кількості зацікавлених фахівців.

МЕТОЮ даної роботи є розробка методу протидії фальсифікаціям результатів Інтернет голосування шляхом створення захищеного операційного середовища у сервері системи Інтернет голосування, яке забезпечує гарантований захист голосів виборців від розкриття, а результатів підрахунку голосів – від спотворень, за умов повної недовіри до всіх без винятку учасників виборчого процесу, включаючи відповідальних осіб, які виконують функції обслуговування системи голосування на всіх рівнях відповідальності.

ПРОВІДНА ІДЕЯ. Оскільки основною причиною недовіри виборців є відсутність повноцінного контролю з боку суспільства за цілісністю програмних засобів системи голосування, а також за діями персоналу, який обслуговує систему, то в основу розроблюваного методу покладено ідею Брюса Шнайера, яку він навів у завершальному абзаці роботи [6]. Ця ідея на мові оригіналу звучить так: «If we're going to spend money on new voting technology, it makes sense to spend it on technology that makes the problem easier instead of harder», що означає наступне: якщо ми надалі збираємось створювати технології голосування, то краще обрати шлях спрощення замість ускладнення. Враховуючи те, що головним елементом системи Інтернет голосування є сервер, який приймає і підраховує голоси виборців, то зменшення до мінімуму його функціональності є тим фактором, який переводить у практичну площину задачу створення засобів повноцінного контролю системи голосування з боку суспільства. Припускається, що спрощення серверного програмного забезпечення може бути досягнуто за рахунок мінімізації функцій операційної системи, а також шляхом обрання простих і прозорих засобів для створення прикладного програмного забезпечення, які є доступними і зрозумілими якомога ширшому колу програмістів.

ПРИНЦИПИ РЕАЛІЗАЦІЇ МЕТОДУ. Метод організації захищеного операційного середовища для сервера дистанційного голосування через Інтернет (СДВ), що усуває причини недовіри суспільства щодо можливих фальсифікацій результатів виборів, передбачає створення структури операційного середовища, що показана у вигляді кола на рис. 1.

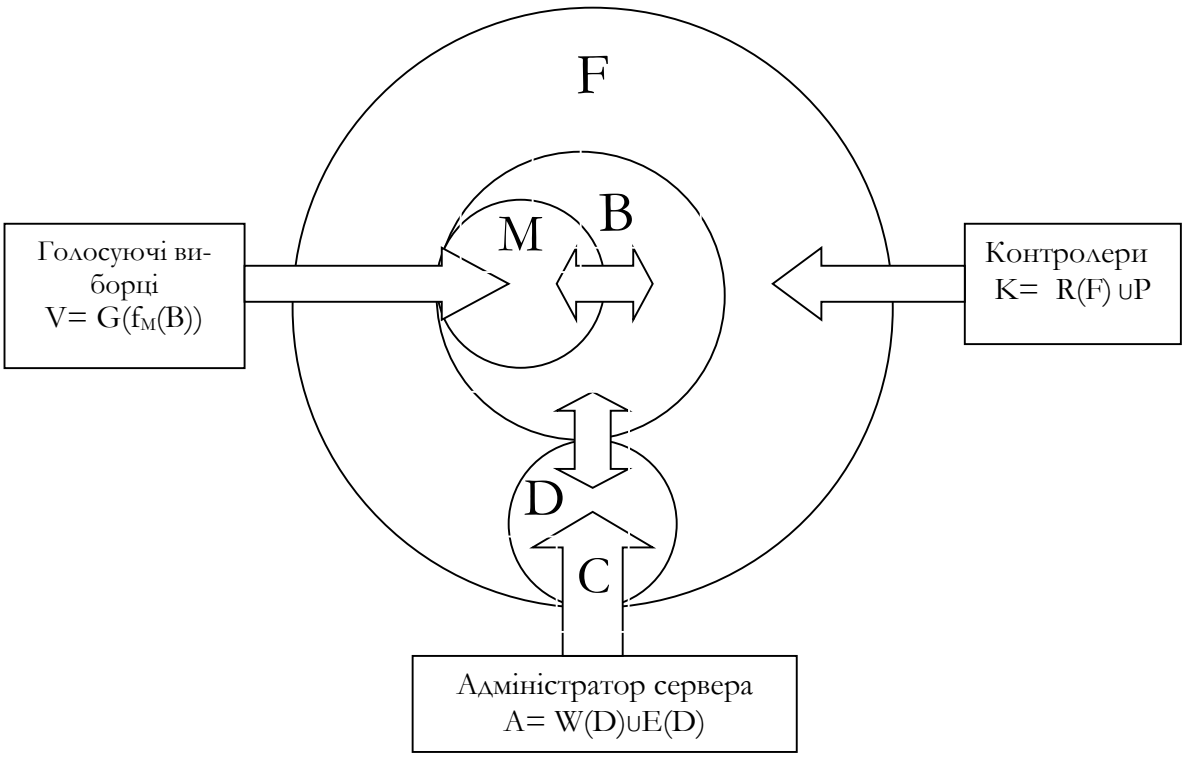

Рис. 1. Структура системи дистанційного голосування, що включає операційне середовище сервера виборчої дільниці та середовище користувачів з різними функціями

Операційна система сервера виборчої дільниці (після певних процедур налаштування) повинна дозволяти виконувати користувачам ті, і тільки ті дії, що є елементами множини Q, де Q являє собою об'єднання множин дій голосуючих виборців, адміністратора сервера та контролерів, які складають повну групу можливих дій користувачів:

$$Q = V \bigcup A \bigcup K, \quad (1)$$

де V – множина дій голосуючих виборців (ця множина у разі потреби може доповнюватись діями осіб для виконання спеціалізованих наперед відомих дій, що повинні бути відображені у заздалегідь відкритій прикладній програмі); A – множина можливих (штатних і нештатних) дій адміністратора сервера; K – множина дій контролюючих осіб.

Слід зауважити, що під терміном дії користувачів, ми розуміємо виключно успішно проведені транзакції щодо їх звернень до сервера.

Повна множина об'єктів, над якими можуть виконуватись дії користувачів складається з наступних множин:

F – множина всіх даних, що розміщенні у файловій системі сервера, включаючи файли з програмами готовими до виконання, а також з історією команд адміністратора;

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

D – множина файлів у тій директорії, до якої має доступ адміністратор, при чому $D \subset F$;

B – множина даних в оперативній пам'яті прикладної програми сервера;

M – множина даних для моніторингу звернень виборців (ці дані використовує прикладна програма для авторизації голосуючих виборців), при чому $M \subset B$ (множина M у разі необхідності може доповнюватись діями осіб для виконання спеціалізованих наперед відомих процедур, що повинні бути відображені у заздалегідь відкритій прикладній програмі).

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

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

де G_i – функція, яка відповідає і-тому 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:

$$A = W(D) \bigcup E(D), \quad (3)$$

де W – функція, яка відповідає множині дій адміністратора (команді запису) для приєднання файлів до множини D; E – функція, яка відповідає діям адміністратора (команді) щодо запуску на виконання файлів (програм) з множини D:

$$K = R(F) \bigcup P, \quad (4)$$

де R – функція, яка відповідає множині дій щодо доступу контролерів для ознайомлення з об'єктами множини F, при чому $C \subset F$, $D \subset F$; P – множина дій контролера (команд) щодо перевірки статусу процесів на сервері та отримання інших відомостей, які можуть свідчити про порушення політики безпеки.

Як бачимо із даної структури СДВ, єдиний користувач, який має можливість виконання небезпечних дій на сервері, це – адміністратор сервера, бо будь-які дії виборців і контролерів не здатні надати їм такі права доступу, які б дозволяли утворити загрозу штатній роботі сервера. Адміністратору дозволено виконувати тільки дві дії, а саме, заносити файли в свою директорію і запускати на виконання файли з цієї директорії. При цьому, будь-яка нештатна дія адміністратора може бути зафіксована контролерами, бо в нього не існує таких дій, які можна було б приховати від контролерів.

МЕХАНІЗМИ РЕАЛІЗАЦІЇ МЕТОДУ

1. Процедура підготовки сервера виборчої дільниці. Встановлення спеціалізованої операційної системи на сервер виконується з компактного диску, образ якого заздалегідь розміщено у вільному доступі разом з усіма текстами програм операційної системи (ОС). Після цього адміністратор сервера створює користувача з правами контролера, а далі, перебуваючи під можливим наглядом контролерів, адміністратор продовжує виконання дій, які передбачені регламентом. Цю послідовність дій разом з діями контролера під час підготовки сервера виборчої дільниці показано на рис. 2.

Після перевірок, що показані на рис. 2, розбіжності будуть виявлені тільки у деяких файлах з даними щодо конкретного налаштування сервера. Оскільки призначення і назви цих файлів є наперед відомими, то контролери можуть впевнитись, що ОС і встановлене програмне забезпечення цілісні на 100%, бо неможливо зробити якусь підробку, залишивши незмінними програмні файли.

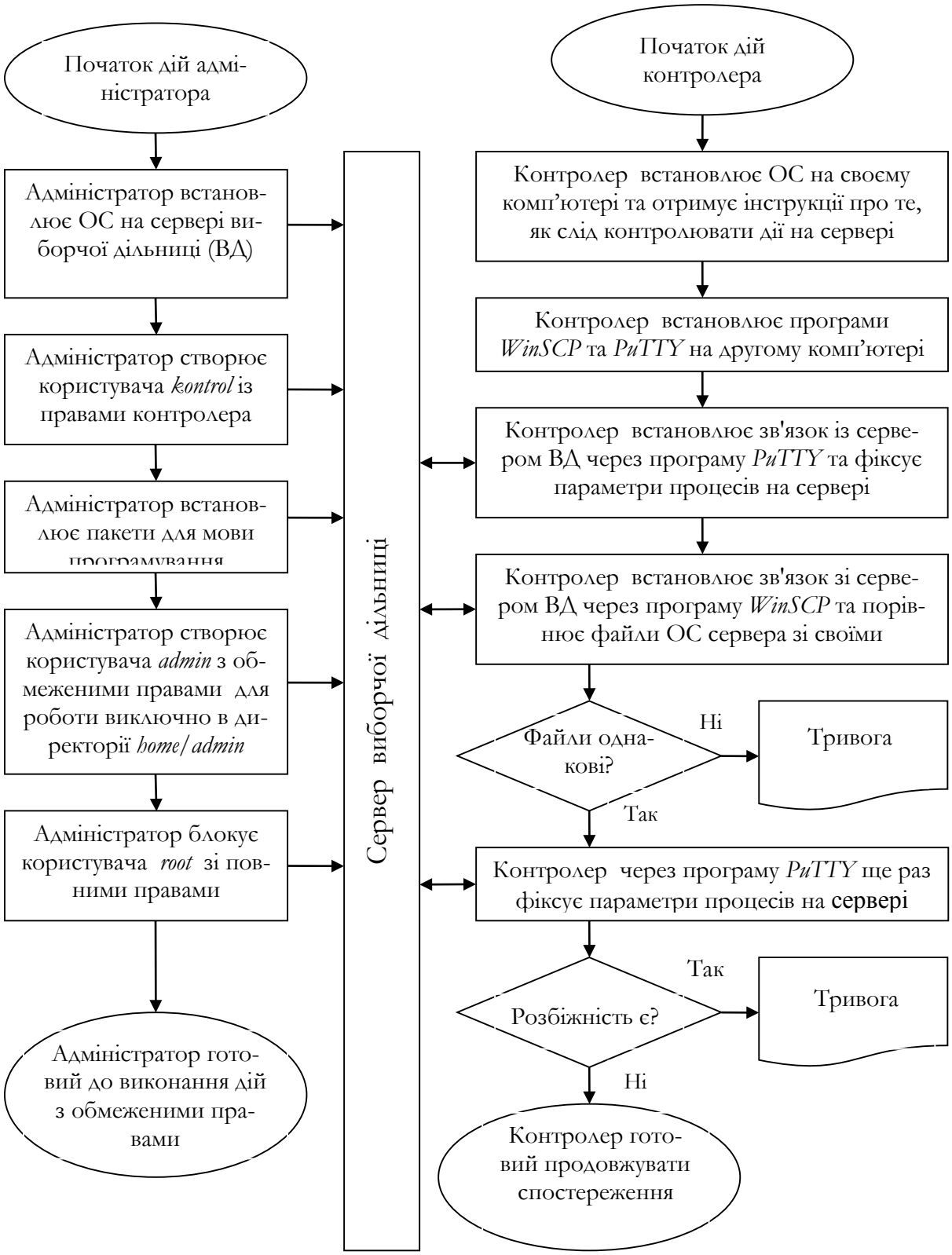

Рис. 2. Процедура підготовки сервера виборчої дільниці

2. Підготовчі дії для дистанційного голосування. Реєстрація виборця для дистанційного голосування (ДГ) потребує (як мінімум один раз) його особистої присутності. В Україні це може відбуватись в одному з 756 відділів ведення Державного реєстру виборців (ДРВ) [7]. При цьому повинні бути виконані наступні дії:

1. Занесення відомостей про особу виборця у розділ спеціальної бази даних (БД) для ДГ по конкретній виборчій дільниці. Ці відомості можуть бути отримані з ДРВ.

2. Занесення у БД даних для ідентифікації і автентифікації особи виборця. Це можуть бути еле-

ктронна пошта, номер мобільного телефону, пароль та/або щось інше, включаючи біометричні, ознаки, наприклад, зразок голосу.

Кожному голосуванню передує уточнення списків тривалістю один-два місяці. В цей період слід завантажити на сервер прикладне ПЗ, склад якого показано у табл. 1, а також занести остаточне рішення кожного виборця про те, чи має він намір скористатись методом ДГ під час даного голосування. Дані про це рішення на сервер ВД надходять у вигляді власноручно введеного виборцем паролю для голосування. Цей пароль виборець повинен ввести після підтвердження своєї особи власною присутністю (наприклад, у відділі ДРВ) або дистанційно з використанням особистої ознаки (наприклад, зразку голосу).

Таблиця 1

Файли прикладного програмного забезпечення

Ім'я файлу	Зміст файлу	Призначення
SVD.js	Серверна програми на мові *JavaScript*в, яка є готовою для безпосереднього виконання	Управління роботою сервера виборчої дільниці протягом усього періоду виборчого процесу
CPW.html	Текст клієнтського модулю на мові HTML з програмою обміну даними з сервером на мові *JavaScript* для періоду введення паролів	Реалізація досконало захищеного діалогу між виборцем і серверною програмою в період введення паролів для голосування
vyborci.dbt	Відомості про виборців, які зареєстровані для ДГ на даній виборчій дільниці. Дані, які потребують захисту зберігаються у зашифрованому вигляді	Занесення значень у масиви даних серверної програми для процедур ідентифікації та автентифікації виборців, а також для заповнення довідок про хід та результати голосування
anketa.html	Текст клієнтського модулю на мові HTML з виборчими бюлетенями і програмою обміну даними з сервером на мові *JavaScript* в період голосування, а також для отримання довідок про хід та результати голосування	Реалізація досконало захищеного діалогу між виборцем і серверною програмою в період голосування, а також надання можливості клієнтам отримувати відкриті довідки про хід та результати голосування

Період введення паролів показано на часовій діаграмі роботи сервера, яка представлена на рис. 3.

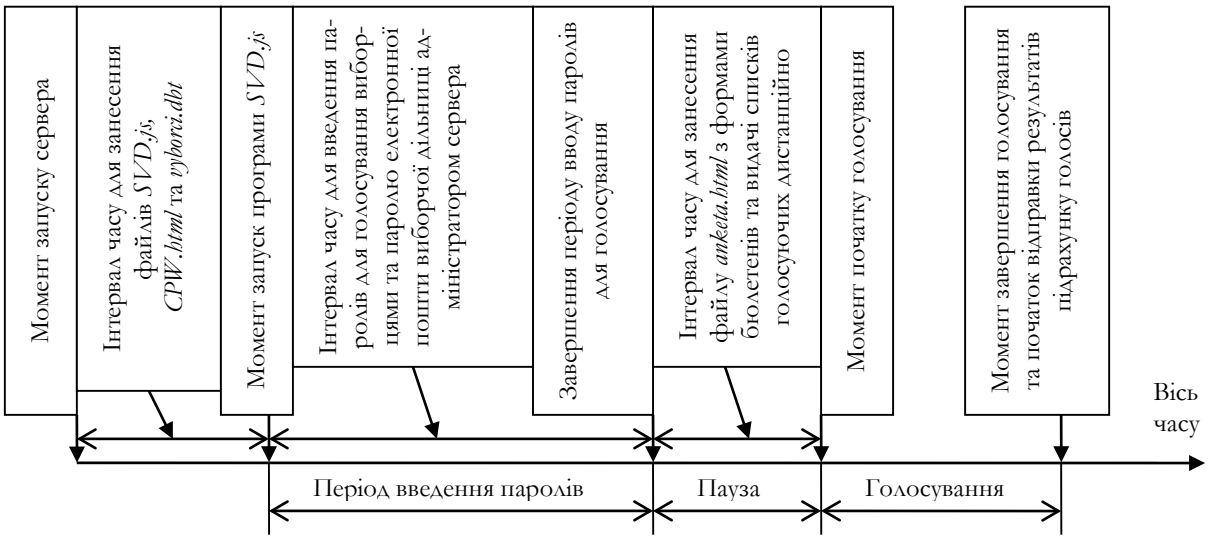

Рис. 3. Часова діаграма роботи сервера виборчої дільниці

3. Механізми створення захищеного операційного середовища. Прикладна серверна програма одразу після запуску (з файлу *SVD.js*) виділяє ділянку оперативної пам'яті для розміщення значень усіх своїх змінних і масивів даних про виборців. Усі функції цієї програми діють таким чином, щоб критичні дані з цієї ділянки пам'яті ніяк і ніколи не потрапили за її межі. Саме ця ділянка пам'яті і є основою для побудови захищеного операційного середовища або ядра безпеки, доступ до якого відбувається тільки через досконало захищені канали зв'язку зі штатними клієнтами. В усіх відомих ОС, які призначені для одночасного розв'язання багатьох задач, для кожної задачі також виділяється окрема ділянка пам'яті, але для того, щоб перетворити таку ділянку у захищене опера-

ційне середовище необхідно гарантувати, що ніяким чином дані з цієї ділянки не зможуть бути прочитані іншою програмою. Приймаючи до уваги той факт, що існує можливість створення і запуску на паралельне виконання програм, які зможуть отримати доступ до вказаної ділянки пам'яті, необхідно забезпечити захист від можливої дії таких програм. Для реалізації такого захисту в даній роботі пропонується на рівні ОС заборонити виконання будь-яких програм, крім тих, які є штатними і перевіреними на безпечність. Для недопущення можливості запуску на виконання позаштатних програм запропоновано ввести користувачів з повноваженнями контролерів, які мають можливість перевіряти всі файли і процеси на сервері, а також всі команди адміністрування. Оскільки ніяка позаштатна програма на сервері не може перейти до стадії виконання без команди користувача, то пропонується в ОС передбачити наступне:

– файл з даними про введення та видалення користувачів;

– файли з історією команд кожного користувача;

– неможливість знищення або модифікації цих файлів.

Наявність цих файлів спрощує процедуру контролю і надає доказову базу щодо наявності чи відсутності порушень політики безпеки з боку користувачів.

4. Побудова досконало захищених каналів зв'язку. Наявність відомих методів криптографічного захисту не залишає сумнівів в можливості побудови досконало захищених каналів для обміну даними між клієнтськими пристроями виборців і ядром безпеки сервера. Реалізація методів досконалого захисту накладає жорсткі умови на процеси генерування випадкових чисел, що докладно розглянуто в роботі [8] на прикладі системи Інтернет голосування. Досконалим будемо називати такий захист, витрати часу на подолання якого перевищують межі реальності. Зауважимо, що, як доведено в роботі [9], абсолютний захист забезпечує алгоритм Вернама, але для реалізації цього алгоритму у чистому вигляді необхідно мати додатковий абсолютно захищений канал для обміну ключовою інформацією. Всі інші відомі нам алгоритми не гарантують абсолютного захисту, але можливо підібрати до них такі параметри, щоб час на розкриття інформації в сучасних умовах обчислювався сотнями, або навіть мільярдами років. Такий захист будемо називати досконалим, хоч він в практичному розумінні може не поступатись абсолютному.

АНАЛІЗ ЗАХИЩЕНОСТІ КРИТИЧНОЇ ІНФОРМАЦІЇ. Перелік загроз, які можуть порушити таємницю голосів виборців або вплинути на вірність підрахунку, в залежності від місця знаходження порушника разом з методами протидії представлено у вигляді табл. 2 і табл. 3.

Оскільки для кожного сеансу зв'язку створюється окремий досконало захищений канал за принципом *End-to-End*, то реалізувати загрози 1-3, що наведені у табл. 2, не уявляється можливим, а у разі підміни результатів ДГ (див. табл. 2 п. 4) по виборчій дільниці, виборці можуть легко це виявити, отримавши довідку про результати безпосередньо з ядра безпеки сервера по досконало захищеному каналу.

Протидія загрозам, що наведені у табл. 3, шляхом порівняння файлів і контролем за виконанням команд адміністрування, дозволяє виявити і документально підтвердити будь-яку спробу реалізації загроз 1, 2, 4 та 5 з боку персоналу, що обслуговує сервер. Фізична заміна сервера не може залишитись непоміченою, бо при цьому змінюються ідентифікатори всіх процесів, які система призначає від генератора випадкових чисел. Найбільш складною для виявлення є загроза типу атаки посередника за принципом *MITM* (*Man in the middle*). Для цього зловмисники можуть скористатись тим, що запити контролерів відправляються на *TCP* порт 22, а запити виборців на інший *TCP* порт, наприклад, 8000. Схему підключення обладнання для реалізації такої загрози показано на рис. 4, де за допомогою обладнання, що підключено послідовно, потік запитів від контролерів, який позначено цифрою 1, відправляють на сервер зі штатним програмним забезпеченням, а потік запитів від виборців, який позначено цифрою 2, відправляють на позаштатний сервер.

Таблиця 2

Загрози, які можуть бути реалізовані поза сервером виборчої дільниці

Опис загрози	Метод протидії
1. Перехоплення даних під час передавання	Створення досконало захищених каналів
2. Заміна даних під час передавання	Використання протоколів, які досконало захищають цілісність даних
3. Проникнення до серверу через засоби дистанційного доступу	Відсутність можливості проникнення до серверу з правами повного доступу
4. Заміна даних про результат голосування	Порівняння даних з довідками, отриманими через досконало захищений канал

Таблиця 3

Загрози, які можуть бути реалізовані персоналом, що обслуговує сервер виборчої дільниці

Опис загрози	Метод протидії
1. Фальсифікація операційної системи	Порівняння файлів ОС зі штатними
2. Виконання позаштатної команди управління	Контроль введення команд управління
3. Фізична заміна сервера	Контроль параметрів процесів ОС
4. Фальсифікація прикладного ПЗ	Порівняння текстів ПЗ зі штатними
5. Несвоєчасне виконання штатних дій	Перевірка дій за регламентом
6. Підключення позаштатних засобів з метою реалізації атаки посередника	Контроль характеристик трафіку

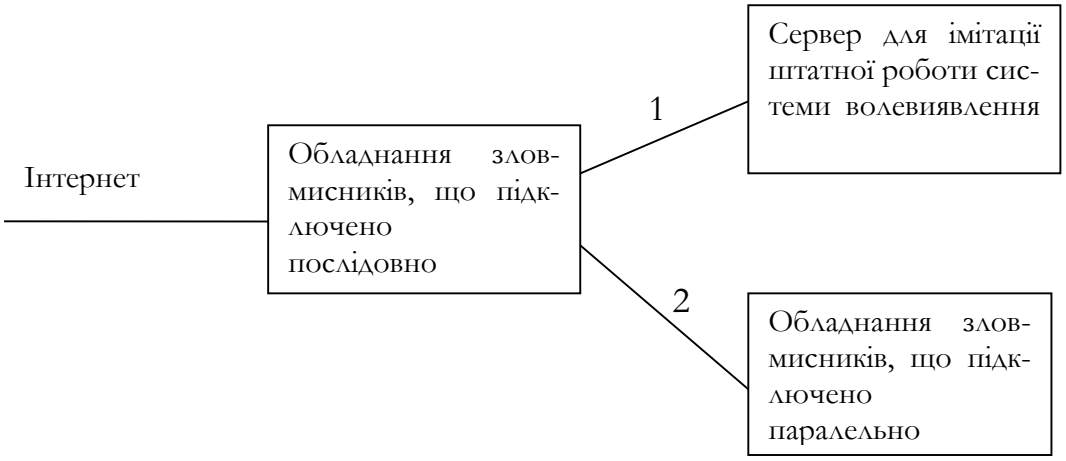

Рис. 4. Схема підключення обладнання для здійснення атаки посередника

Задум зловмисників щодо реалізації даної загрози полягає в тому, щоб контролери перевіряли сервер, де все програмне забезпечення є штатним, а запити виборців потрапляли б на сервер з підробленою програмою, яка може змінювати результати голосування та розкривати таємницю голосів. Невдача такого задуму для зловмисників полягає в тому, що протокол *TCP* не дозволяє встановлювати з'єднання одразу з двома серверами, а потік, що позначений цифрою 1, зловмисники не можуть розшифрувати і підробляти, бо для цього їм потрібно встановлювати нештатні програмні засоби на штатний сервер, що неможливо замаскувати від контролерів. Розкриття даної загрози потребує перевірки *TCP* пакетів, що прямують до сервера та від сервера за допомогою команд *netstat –p tcp* та *tcpdump*. Можливі два наступні варіанти реалізації даної загрози:

1. Зловмисники відправляють запити виборців тільки на позаштатний сервер. При цьому для виявлення загрози достатньо відправити на *TCP* порт 8000 будь-який запит і перевірити його на сервері командою *netstat*. У разі відсутності пакету на сервері, загроза є.

2. Зловмисники відправляють запити виборців одночасно на штатний сервер і на свій позаштатний. При цьому для виявлення загрози треба відправити на *TCP* порт 8000 будь-який запит і порівняти параметр *Sequence Number* у заголовку *TCP* пакета, що надійшов у відповіді на цей запит, з тим значенням, що отримано за допомогою команди *tcpdump*. Якщо вони не співпадають, то загроза є. Неможливість непоміченого проникнення зловмисників на штатний сервер є запорукою можливості створення умов для виявлення атак посередника.

Таким чином, завдяки запропонованому в даній роботі методу створення захищеного операційного середовища на сервері виборчої дільниці, вдається подолати усі можливі загрози щодо порушення таємниці голосів виборців та щодо точності отримання результатів голосування, які описані у табл. 2 та табл. 3.

Слід зауважити, що завдяки досконалому захисту від будь-якого нештатного втручання в процес зарахування голосів виборців стає неможливим помилкове зарахування голосів, бо у вивірених комп'ютерних програмах, подібні помилки, за умов нормального завершення транзакції, є неприпустимими. Тому, вище вказана вимога по те, щоб кожен голосуючий міг перевіряти як враховано його голос, в даних умовах втрачає сенс, бо замість цього зроблена перевірка, яка не допускає такого явища, як невірне зарахування голосів, а захищатись від того, що неможливо, не має потреби. Є й застарілі вимоги до систем електронного голосування, які явно втратили актуальність. До них можна віднести, наприклад, ви-

могу, яка в роботі [2] сформульована так: «для полегшення перерахунку голосів у разі конфліктної ситуації може передбачатися процедура роздрукування голосів». По-перше, роздруковані комп'ютерною програмою голоси за кількістю не можуть відрізнятись від значень, які видані програмою, а, по-друге, перерахунок папірців ніяк не може бути точніше або легше за комп'ютерний.

ЕКСПЕРИМЕНТАЛЬНІ ДОСЛІДЖЕННЯ ЗАПРОПОНОВАНОГО МЕТОДУ. Головною метою проведення експерименту було визначення витрат серверного часу на обслуговування клієнтів за умов створення для кожного з них досконало захищеного каналу зв'язку. Крім того, треба було оцінити трудомісткість контролю цілісності програмних засобів сервера, включаючи ОС, і контролювання дій адміністратора. Також треба було оцінити складність та прозорість прикладного програмного забезпечення.

Для експерименту було обрано, як найбільш відповідну за критеріями максимальної захищеності і мінімальної функціональності, ОС *OpenBSD* у мінімальній конфігурації. Для розробки прикладного ПЗ було обрано широко розповсюджену мову *JavaScript*, як для серверної програми, так і для клієнтських програм, вбудованих в *HTML* документи.

Експерименти було проведено на серверному обладнанні Інтернет вузлу Державного науково-дослідного інституту автоматизованих систем в будівництві на задачах опитування студентів трьох ВУЗів України НАУ, НТУУ «КПІ» і КНУБА та продемонстровано на 4-й Міжнародній науковій конференції «Інформація, комунікація, суспільство 2015» [10]. Форму бюлетеня для цього опитування показано на рис. 5.

З варіантом даної програми, що був створений для опитування студентів КНУ ім. Т.Г. Шевченка можна ознайомитись за посиланням: http://fit.univ.kiev.ua/archives/3246).

В результаті проведених експериментів визначено, що витрати серверного часу на обслуговування кожного запиту виборця складають від 2 до 4 секунд, де близько 90% витрачається на криптографічні перетворення, які докладно описано в роботі [7]. Це означає, що обслуговування виборців однієї дільниці, кількість яких не може перевищувати 2500, буде займати не більше трьох годин, що цілком задовольняє вимогам виборчої системи України. Для повної перевірки цілісності програмного забезпечення сервера з використанням засобів автоматизації потрібно не більше години. Тексти програм, як серверного *SVD.js*, так і клієнтського *anketa.html* модулів, мають приблизно по 600 рядків на широко розповсюдженій комп'ютерній мові, що свідчить про їх простоту і можливість легкої перевірки.

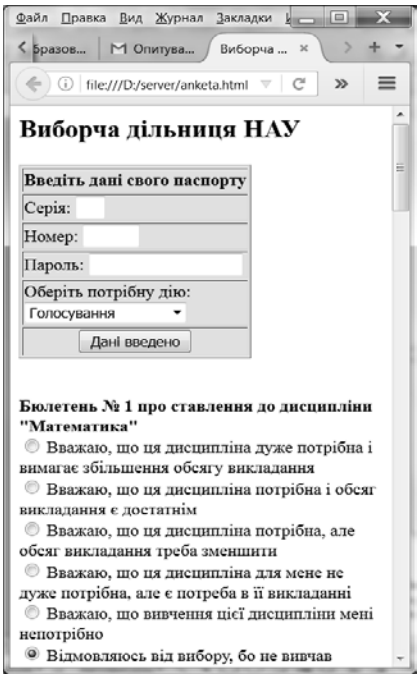

Рис. 5. Форма бюлетеня під час опитування студентів Національного авіаційного університету

ВИСНОВКИ

1. Запропоновано метод створення захищеного операційного середовища для сервера системи Інтернет голосування, який усуває причини недовіри суспільства щодо можливих фальсифікацій результатів виборів або розкриття таємниці їх голосів. Метод базується на концепції ядра безпеки і реалізує профіль захищеності, згідно якому в оперативній пам'яті сервера створюється ділянка, у якій доступ до даних має виключно процес підрахунку голосів наперед вивіреною відкритою прикладною програмою. Для унеможливлення доступу до цієї ділянки будь-яким іншим процесам використано відкриту операційну систему, у якій функцій для такого доступу немає. Крім того, створено умови для дистанційного контролю цілісності усіх без винятку файлів і процесів на сервері, а також всіх дій персоналу щодо адміністрування сервера з боку необмеженої кількості контролерів, якими можуть стати будь-які зацікавлені особи.

2. Визначено повну сукупність загроз, реалізація котрих може стати причиною розкриття таємниці голосів та фальсифікації результатів волевиявлення. У рамках прийнятої моделі ядра безпеки розроблено механізми протидії цим загрозам. Показано, що запропонований в цій роботі метод в сукупності з відомими методами захисту інформації, надає змогу виявлення всіх без винятку можли-

вих загроз щодо розкриття таємниці голосів та викривлення результатів підрахунку в системах Інтернет голосування.

3. Проведено експериментальні дослідження, які підтверджують технічну можливість реалізації запропонованого методу в системі Інтернет голосування для України. Зокрема, витрати серверного часу на обслуговування кожного запиту виборця складають від 2 до 4 секунд, з яких близько 90% витрачається на криптографічні перетворення. Обслуговування виборців однієї дільниці, кількість яких згідно законодавства України не може перевищувати 2500 осіб, буде займати не більше трьох годин. Кожен виборець має можливість з будь-якого термінального вузлу Інтернет перевірити в режимі реального часу цілісність програмного забезпечення сервера. Для такої перевірки потрібно не більше однієї години.

4. Даний метод може бути використаний для створення систем дистанційного голосування через Інтернет в багатьох сферах для будь-яких громадських та експертних дистанційних опитувань, для проведення різного роду конкурсів, тендерів, експертиз тощо – всюди, де існують сумніви щодо збереження таємниці волевиявлення і необхідно усунути можливість зловживань під час проведення голосування.

ЛІТЕРАТУРА

[1]. Jefferson D. If I Can Shop and Bank Online, Why Can't I Vote Online? Access mode: World Wide Web. – URL: https:// www. verifiedvoting. org/ resources/ internet-voting/ vote-online.

[2]. Савчук О. Системи електронних виборів: процедури голосування та матеріально-технічні засоби. Міжнародний досвід. Режим доступу: World Wide Web. – URL: http://euinfocenter.rada.gov.ua/uploads/documents/28966.pdf.

[3]. Судрієтт Р.У. Технології голосування: життєво важливий інструмент для учасників виборів // Вісник Центральної виборчої комісії. – 2013. – № 3 (27) – С. 27-29. Режим доступу: World Wide Web. – URL: http:// www.cvk. gov.ua/ visnyk/ pdf/2013_3/ Visnik_3_2013_st_11.pdf.

[4]. Lessons from the EVOTE 2014 Internation Conferens Access mode: World Wide Web. – URL: http://e-lected.blogspot.com/search?updated-min= 2014-01-01T00:00:00-08:00&updated-max=2015-01-01T00:00:00-08:00&max-results=50.

[5]. Шнайер Б. Прикладная криптография. 2-е издание. Протоколы, алгоритмы и исходные тексты на языке Си. – М.: Триумф, 2002. – С. 94-95

[6]. Schneier B. What's Wrong With Electronic Voting Machines? Access mode: World Wide Web. – URL: https://www.schneier.com/essays/archives/2004/11/ whats_wrong_with_ele.html

[7]. Вишняков В.М. Відкрита система таємного голосування / В.М. Вишняков, М.П. Пригара, О.В. Воронін // Управління розвитком складних систем. Збірник наукових праць. – 2014. – Вип. 20. – С. 110 - 115. Режим доступу: World Wide Web. – URL: http://urss.knuba.edu.ua/files/zbirnyk-20/22.pdf

[8]. Чуприн В.М. Генерування випадкових чисел штатними засобами хостів мережі Інтернет./ В.М. Чуприн, В.М.Вишняков, М.П. Пригара // Захист інформації. – 2016. – Т. 18, №4 – С. 323-335. Режим доступу: World Wide Web. – URL: http://jrnl.nau.edu.ua/index.php/ZI/article/view/11085/14800

[9]. Shannon C.E. The Communication Theory of Secrecy Systems / C.E. Shannon // Bell System Technical Journal. – 1949 – v.28, n.4 – C.654-715.

[10]. Вишняков В.М., Пригара М.П. Забезпечення свободи волевиявлення в системі Інтернет-голосування (ІГ). Матеріали 4-ї Міжнародної наукової конференції 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&isAllowed=y

REFERENCES

[1]. Jefferson D. If I Can Shop and Bank Online, Why Can't I Vote Online? Access mode: World Wide Web. – URL: https:// www. verifiedvoting. org/ resources/ internet-voting/vote-online

[2]. Savtchuk O. Systems electronic voting: procedures, material and technical means. International experience. Access mode: World Wide Web. – URL: http://euinfocenter.rada.gov.ua/uploads/documents/ 28966.pdf

[3]. Sudriett R.U. 'Technologies voting vital tool for election participants', Bulletin of the Central Election Commission. – 2013. – n. 3 (27) – pp. 27-29. Access mode: World Wide Web. – URL: http://www.cvk.gov.ua/visnyk/pdf/ 2013_3/Visnik_3_2013_st_11.pdf

[4]. Lessons from the EVOTE 2014 Internation Conference Access mode: World Wide Web. – URL: http://e-lected.blogspot.com/search?updated-min= 2014-01-01T00:00:00-08:00&updated-max=2015-01-01T00:00:00-08:00&max-results=50

[5]. Schneier B. Applied Cryptography. 2 edition. Protocols, algorithms and source code in the language of Си. – Moscow: Triumph, 2002. – pp. 94-100.

[6]. Schneier B. What's Wrong With Electronic Voting Machines? Access mode: World Wide Web. – URL: https://www.schneier.com/essays/archives/2004/11/ whats_wrong_with_ele.html

[7]. Vyshniakov V.M., Prygara M.P., Voronin O.V. 'Open secret ballot system', Managing the development of complex systems, vol. 20, pp. 110-115. Access mode: World Wide Web. – URL: http://urss.knuba.edu.ua/files/zbirnyk-20/22.pdf

[8]. Chupryn V.M., Vyshniakov V.M., Prygara M.P. 'Method of generation of casual numbers on the basis of the use of apparatus of the computer plugged in the Internet', Ukrainian Information Security Research Journal, vol. 18, pp. 323-335. Access mode: World Wide Web. –

URL: http:// jrnl. nau. edu. ua/ index. php/ ZI/ article/ view/11085/14800

[9]. Shannon C.E. The Communication Theory of Secrecy Systems / C.E. Shannon // Bell System Technical Journal. – 1949 – v.28, n.4 – pp.654-715.

[10]. Vyshniakov V.M., Prygara M.P. 'Ensuring freedom of expression on the Internet voting (IV)', Materials of the 4th International Conference ICS-2015 'Information, communication, society 2015' , pp. 124 – 125. Access mode: World Wide Web. – URL: http://ena.lp.edu.ua:8080/ xmlui/ bitstream/ handle/ ntb/ 33187/ 055-124-125.pdf?sequence=1&isAllowed=y

ЗАЩИТА ОПЕРАЦИОННОЙ СРЕДЫ СИСТЕМ ИНТЕРНЕТ ГОЛОСОВАНИЯ

В данной работе предложен метод создания защищенной операционной среды для сервера системы Интернет голосования, который устраняет причины недоверия общества относительно возможных фальсификаций результатов или раскрытия тайны голосов. Метод основан на концепции ядра безопасности и реализует профиль защиты, согласно которому в оперативной памяти сервера создается участок, где исключительный доступ к данным имеет процесс подсчета голосов заранее выверенной открытой прикладной программы. Для предотвращения доступа к этому участку каких-либо иных процессов, используется открытая операционная система, в которой отсутствуют функции для такого доступа. Кроме того, созданы условия для дистанционного контроля целостности всех без исключения файлов и процессов на сервере, а также всех действий персонала по администрированию сервера со стороны неограниченного количества контроллеров, которыми могут стать любые заинтересованные лица. Показано, что предложенный метод в совокупности с известными методами защиты информации, передаваемой по открытым каналам, дает возможность выявления всех без исключения возможных угроз по раскрытию тайны голосов и искажения результатов подсчета в системах Интернет голосования. Внедрение данного метода может быть полезным во многих сферах для любых общественных и экспертных дистанционных опросов, где требуются точность подсчета и сохранение тайны голосов в условиях полного недоверия ко всем без исключения участникам избирательного процесса.

Ключевые слова: Интернет-голосование, техническая защита информации, сохранение тайны голосов, прозрачность системы голосования, обеспечение доверия избирателей.

PROTECT THE OPERATING ENVIRONMENT INTERNET VOTING SYSTEMS

In this paper we propose a method of creating a secure operating environment for Internet voting system server, which eliminates the causes of public distrust about the possible falsification of results or disclosure of the secrets of the vote. The method is based on the concept of the security kernel. Portion of memory is allocated in the server, where exclusive access to the data of the vote counting process has previously verified open application. To prevent access to this memory portion of any other processes is used an open operating system, which does not have functions for such access. Furthermore, conditions have been created for the remote monitoring of the integrity of any and all files and processes on the server, as well as all of the personnel server administration from an unlimited number of controllers that can become any person concerned. It is shown that the proposed method in conjunction with known methods of protecting information transmitted via open channels, it makes it possible to identify any and all possible threats to disclose the secrets of the vote counting and distortion of the results of Internet voting systems. The introduction of this method can be useful in many areas for all public and expert remote surveys that require counting accuracy and secrecy of the vote in full confidence to any and all participants in the electoral process.

Keywords: Internet voting, technical protection of information, secrecy of votes, the voting system transparency, ensuring voter confidence.

Чуприн Володимир Михайлович, кандидат технічних наук, професор кафедри телекомунікаційних систем Національного авіаційного університету.
E-mail: vladimir@ndiasb.kiev.ua

Чуприн Владимир Михайлович, кандидат технических наук, профессор кафедры телекоммуникационных систем Национального авиационного университета.

Chupryn Volodymyr, PhD in engineering, professor, Department of Telecommunication Systems, National Aviation University.

Вишняков Володимир Михайлович, кандидат технічних наук, доцент, доцент кафедри телекомунікаційних систем Національного авіаційного університету.
E-mail: volodymyr.vyshniakov@gmail.com

Вышняков Владимир Михайлович, кандидат технических наук, доцент, доцент кафедры телекоммуникационных систем Национального авиационного университета.

Vyshniakov Volodymyr, PhD in engineering, associate professor, Department of Telecommunication Systems, National Aviation University.

Пригара Михайло Петрович, аспірант кафедри інформаційних технологій Київського національного університету будівництва і архітектури.
E-mail: misha_prigara@ukr.net

Пригара Михаил Петрович, аспирант кафедры информационных технологий Киевского национального университета строительства и архитектуры.

Prygara Mykhailo, graduate student of Department of Information Technologies, Kyiv National University of Construction and Architecture.