УДК 681.3

© С.О. Довгий, О.В. Копійка, П.М. Сіверський, О.М. Трофимчук, О.Г. Лебідь

ЗАБЕЗПЕЧЕННЯ РЕГЛАМЕНТОВАНОГО ЗАХИЩЕНОГО ДИСТАНЦІЙНОГО ДОСТУПУ КОРИСТУВАЧІВ ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ СИСТЕМИ СУПРОВОДЖЕННЯ БЮДЖЕТНОГО ПРОЦЕСУ

У статті розглянуті питання різних варіантів забезпечення регламентованого захищеного дистанційного доступу користувачів інформаційно-аналітичної системи супроводження бюджетного процесу.

Ключові слова: бюджетний процес; бюджетний цикл; інформаційно-комунікаційні технології; інформаційно-аналітичні системи; інформаційне забезпечення; регламентований захищений дистанційний доступ.

Вступ

При розробці інформаційно-аналітичної системи супроводження бюджетного процесу було використано всі переваги інформаційно-комунікаційних технологій (ІКТ):

- єдиний інформаційний простір;
- домінування нових технологічних укладів, що базуються на масовому використанні мережевих інформаційних технологій, перспективних засобів обчислювальної техніки і телекомунікацій;
- зростання ролі інфраструктури (телекомунікаційної, транспортної, інформаційної (Центри обробки даних), організаційної) у системі суспільного виробництва і посилення тенденцій до спільного функціонування в економіці інформаційних і грошових потоків;
- висока значимість проблем забезпечення інформаційної безпеки особистості, суспільства і держави, наявність ефективної системи забезпечення прав громадян і соціальних інститутів на вільне одержання, поширення і використання інформації.

Інформаційна безпека в такому контексті для інформаційних систем державного призначення є дуже важливою складовою.

Мета дослідження – вдосконалити можливості Комітету з питань бюджету Верховної Ради України завдяки забезпеченню регламентованого захищеного дистанційного доступу користувачів інформаційно-аналітичної системи супроводження бюджетного процесу.

Для забезпечення регламентованого доступу при використанні інтелектуальної автоматизованої інформаційно-аналітичної системи супроводження бюджетного процесу було забезпечено наступний порядок обміну даними:

1. Первинна інформація надходить у вигляді різноманітних файлів до Комітету з питань бюджету Верховної Ради України (далі – Комітет) від Міністерства фінансів України (проект Закону України "Про Державний бюджет України", зміни Закону України "Про Державний бюджет України"), Державного казначейства України (фактичне виконання бюджету) та інших державних установ.

2. Відповідно до вимог існуючого законодавства ця інформація повинна надходити з Верховної Ради України по захищених каналах зв'язку до підсистеми "База первинних даних", яка розташована в Інституті телекомунікацій і глобального інформаційного простору НАН України (далі – ІТГІП НАНУ).

3. ІТГІП НАНУ з'єднано з Інститутом кібернетики НАН України (далі ІК НАНУ) за допомогою Академічної мережі обміну даними (АМОД).

4. Інформація з підсистеми "База первинних даних" повинна надходити до суперкомп'ютера в ІК НАНУ через АМОД із забезпеченням існуючих вимог захисту для подальшої обробки та зберігання.

5. З Комітету запити на обробку інформації надходять до ІТГІП НАНУ. В залежності від їх складності та інших вимог можуть бути опрацьовані в ІТГІП НАНУ і передані в Комітет. В разі необхідності розв'язання складних аналітичних задач запити передаються до ІК НАНУ. Отримані після опрацювання на суперкомп'ютері результати надсилаються до Комітету.

Для забезпечення захисту інформації між Верховною Радою України та установами НАН України розроблені такі варіанти заходів із захисту інформації.

Варіант 1

Автономні клієнти ВРУ (не підключені до локальної мережі ВРУ) передають дані до програмно-апаратного комплексу "Бюджет" ІТГІП НАНУ за допомогою бездротового модему каналами зв'язку Оператора, які мають захист за рахунок Оператора (захист від зовнішніх вторгнень), технології побудови мережі (мобільний радіозв'язок) та налаштувань у клієнтів та сервера.

Комплекс "Бюджет" передає структуровані дані для подальшої обробки до суперкомп'ютера в ІК НАНУ через АМОД, яка захищена за рахунок провайдеру Інтернет (захист від зовнішніх вторгнень), технології побудови мережі (оптичне волокно) та налаштувань відповідних маршрутизаторів і фаєрволів.

Автономний клієнт ВРУ подає запит на обробку даних до ІТГІП НАНУ. У свою чергу, ІТГІП НАНУ повертає результат або передає такий запит до суперкомп'ютера. Результат від суперкомп'ютера повертається зворотним шляхом. На автономному клієнті він копіюється на носій інформації та передається клієнту у локальній мережі ВР України.

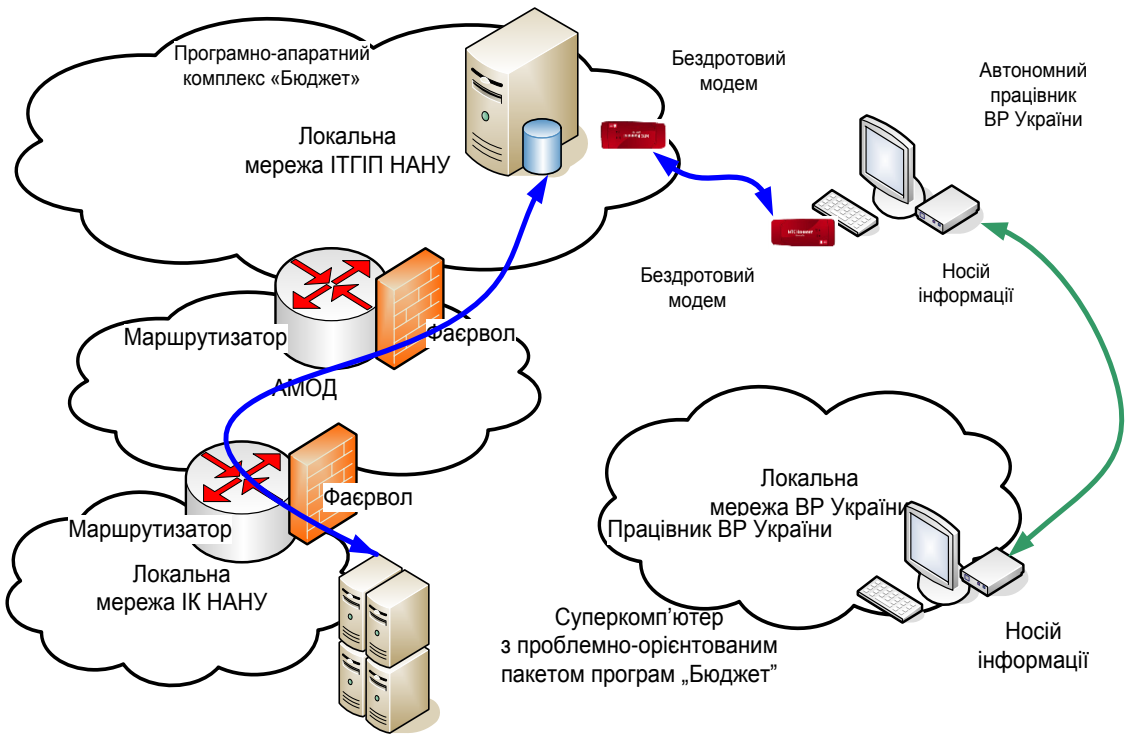

Рис. 1 – 1-й варіант заходів із захисту інформації

Список програмно-апаратних засобів:

Автономний працівник ВР України	Апаратні засоби: Ноутбук чи стаціонарний ПК Бездротовий 3G-модем МТС-Коннект SIM-картка МТС-Коннект Носій інформації (накопичувач на основі flash-пам'яті, оптичний носій, магнітний носій і т.і.) Програмні засоби: Антивірус з функцією запобігання вторгнень з мереж ОС Windows XP або новіша ПЗ Office 2003 Professional або новіше
ІТГІП НАНУ	Апаратні засоби: Фаєрвол * Маршрутизатор (може бути об'єднанимз фаєрволом) *
ІК НАНУ	Апаратні засоби: Фаєрвол * Маршрутизатор (може бути об'єднаним з фаєрволом) *

***** Може бути заміненим програмною реалізацією, встановленою на сервері

Варіант 2

Клієнти ВРУ передають дані до програмно-апаратного комплексу "Бюджет" ІТГІП НАНУ за загальними каналами зв'язку, які мають захист за рахунок провайдерів та налаштувань відповідних маршрутизаторів і фаєрволів.

Комплекс «Бюджет» передає структуровані дані для подальшої обробки до суперкомп'ютера в ІК НАНУ через АМОД, яка захищена за рахунок провайдеру УарНЕТ (захист від зовнішніх вторгнень), технології побудови мережі (оптичне волокно) та налаштувань відповідних маршрутизаторів і фаєрволів.

Клієнт ВРУ подає запит на обробку даних до ІТГІП НАНУ. У свою чергу, ІТГІП НАНУ повертає результат або передає такий запит до суперкомп'ютера. Результат від суперкомп'ютера повертається зворотним шляхом.

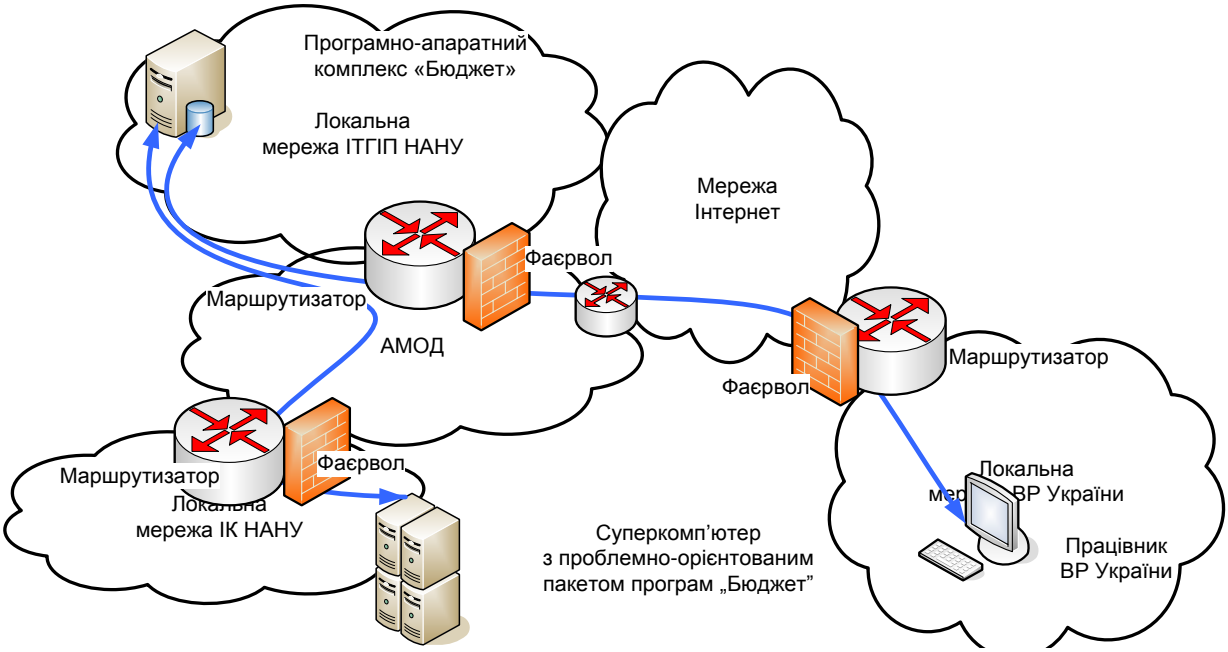

Рис. 2 – 2-й варіант заходів із захисту інформації

Список програмно-апаратних засобів:

Локальна мережа ВР України	Апаратні засоби: Фаєрвол * Маршрутизатор (може бути об'єднаним з фаєрволом) *
ІТГІП НАНУ	Апаратні засоби: Фаєрвол * Маршрутизатор (може бути об'єднаним з фаєрволом) *
ІК НАНУ	Апаратні засоби: Фаєрвол * Маршрутизатор (може бути об'єднаним з фаєрволом) *

* Може бути замінений програмними реалізаціями, встановленими на сервері

Варіант 3

Клієнти ВРУ передають дані до серверу комплексу "Бюджет", на якому встановлено спеціалізоване програмне забезпечення для захисту інформації у каналах загального користування. Цей сервер передає зашифровані дані до програмно-апаратного комплексу "Бюджет" ІТГІП НАНУ за загальними каналами зв'язку, які мають захист за рахунок спеціалізованого програмного забезпечення.

Комплекс "Бюджет"' передає структуровані дані для подальшої обробки до суперкомп'ютера у ІК НАНУ через АМОД, яка захищена за рахунок провайдеру УарНЕТ (захист від зовнішніх вторгнень), технології побудови мережі (оптичне волокно) та спеціалізованого програмного забезпечення.

Клієнт ВРУ подає запит на обробку даних до ІТГІП НАНУ. У свою чергу, ІТГІП НАНУ повертає результат або передає такий запит до суперкомп'ютера. Результат від суперкомп'ютера повертається зворотним шляхом.

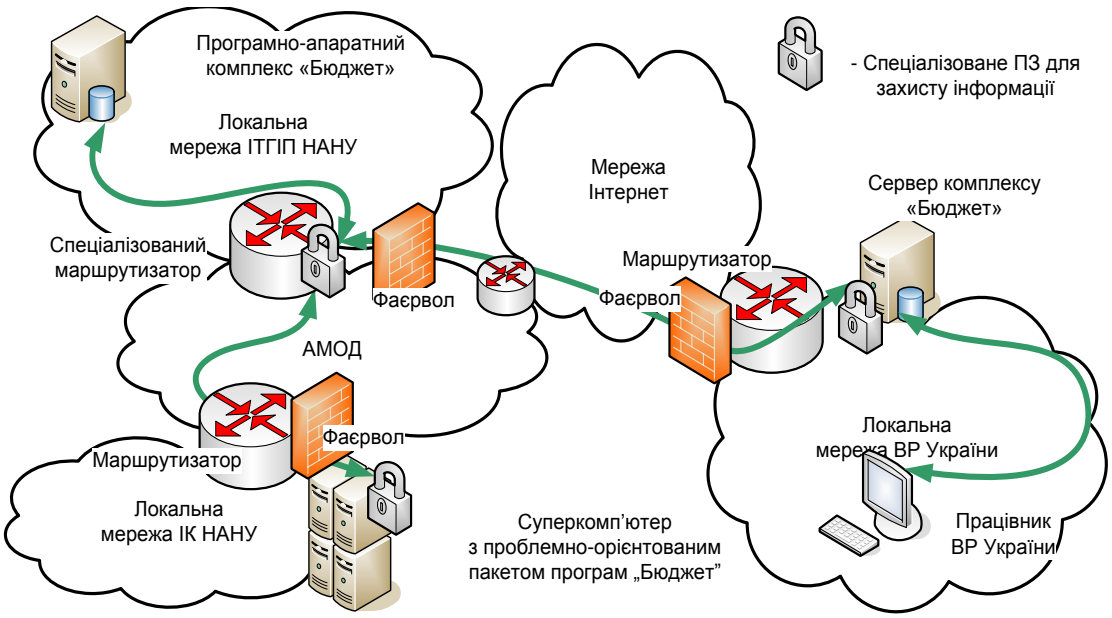

Рис. 3 – 3-й варіант заходів із захисту інформації

Список програмно-апаратних засобів:

Локальна мережа ВР України	Апаратні засоби: Сервер комплексу "Бюджет" Фаєрвол * Маршрутизатор (може бути об'єднаним з фаєрволом) * Програмні засоби: Серверна ОС Windows 2003 Server або новіша СКБД Oracle 11g Антивірус з функцією запобігання вторгнень з мереж Спеціалізоване ПЗ для захисту інформації.

ІТГІП НАНУ	Апаратні засоби: Фаєрвол * Маршрутизатор із вбудованим ПЗ для захисту інформації
ІК НАНУ	Апаратні засоби: Фаєрвол * Маршрутизатор із вбудованим ПЗ для захисту інформації

* Може бути замінений програмними реалізаціями, встановленими на сервері

Варіант 4

Клієнти ВРУ передають дані до серверу комплексу "Бюджет", який за каналами Національної системи конфіденційного зв'язку (через вузол комутації НСКЗ) передає їх до програмно-апаратного комплексу "Бюджет" ІТГІП.

Комплекс "Бюджет" має захист з боку локальної мережі ІТГІП НАНУ від фізичного з'йому інформації за допомогою гальванічного розгалужувача та захист від атак за допомогою комплексної системи захисту інформацій. Задача клієнта передається для подальшої обробки до суперкомп'ютера в ІК НАНУ через АМОД, яка захищена за рахунок провайдеру УарНЕТ (захист від зовнішніх вторгнень), технології побудови мережі (оптичне волокно) та спеціалізованого програмного забезпечення.

Клієнт ВРУ подає запит на обробку даних до ІТГІП НАНУ. У свою чергу, ІТГІП НАНУ повертає результат або передає такий запит до суперкомп'ютера. Результат від суперкомп'ютера повертається зворотним шляхом.

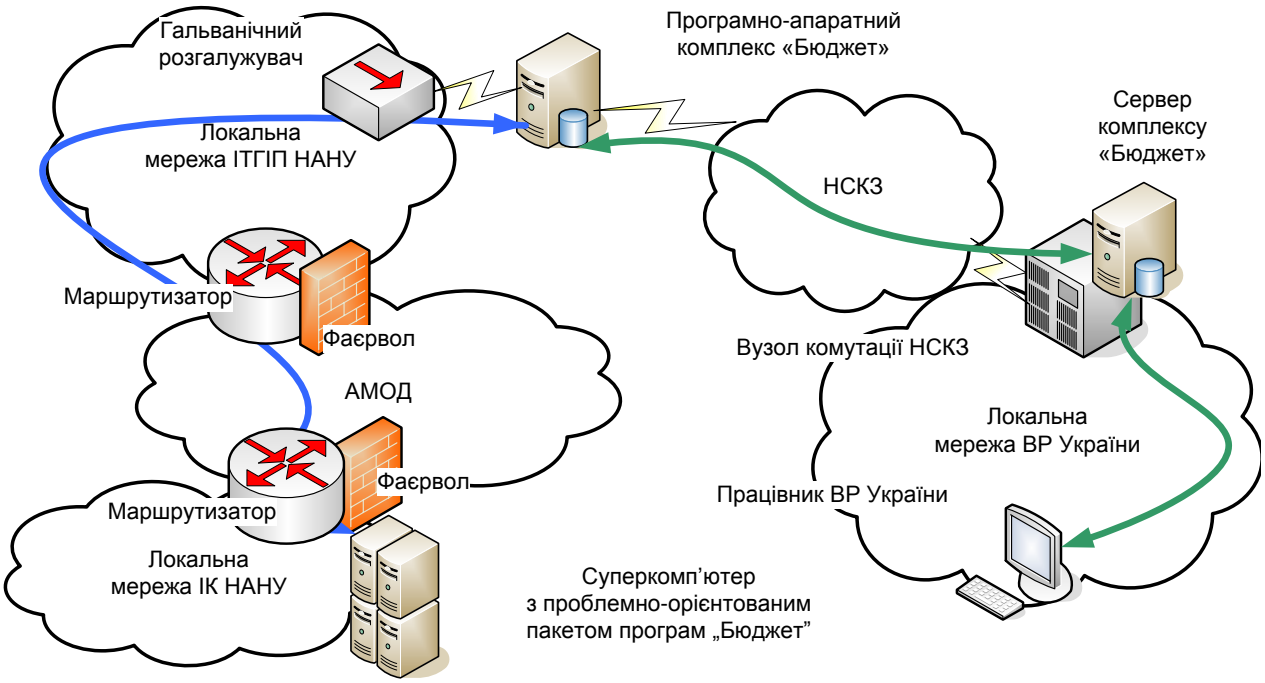

Рис. 4 – 4-й варіант заходів із захисту інформації

Список програмно-апаратних засобів:

Локальна мережа ВР України	Апаратні засоби: 1. Сервер комплексу "Бюджет" 2. Комплекс передачі інформації НСКЗ (вузол комутації та мережа) Програмні засоби: 1. Серверна ОС Windows 2003 Server або новіша 2. СКБД Oracle 11g 3. Антивірус з функцією запобігання вторгнень з мереж
ІТГІП НАНУ	Апаратні засоби: 1) Гальванічний розгалужувач 2) Фаєрвол * 3) Маршрутизатор * Програмні засоби: • Комплексна система захисту інформації
ІК НАНУ	Апаратні засоби: 1. Фаєрвол * 2. Маршрутизатор із вбудованим ПЗ для захисту інформації

* Може бути замінений програмними реалізаціями, встановленими на сервері

На рис. 5 наведено варіант забезпечення роботи з системою віддалених користувачів.

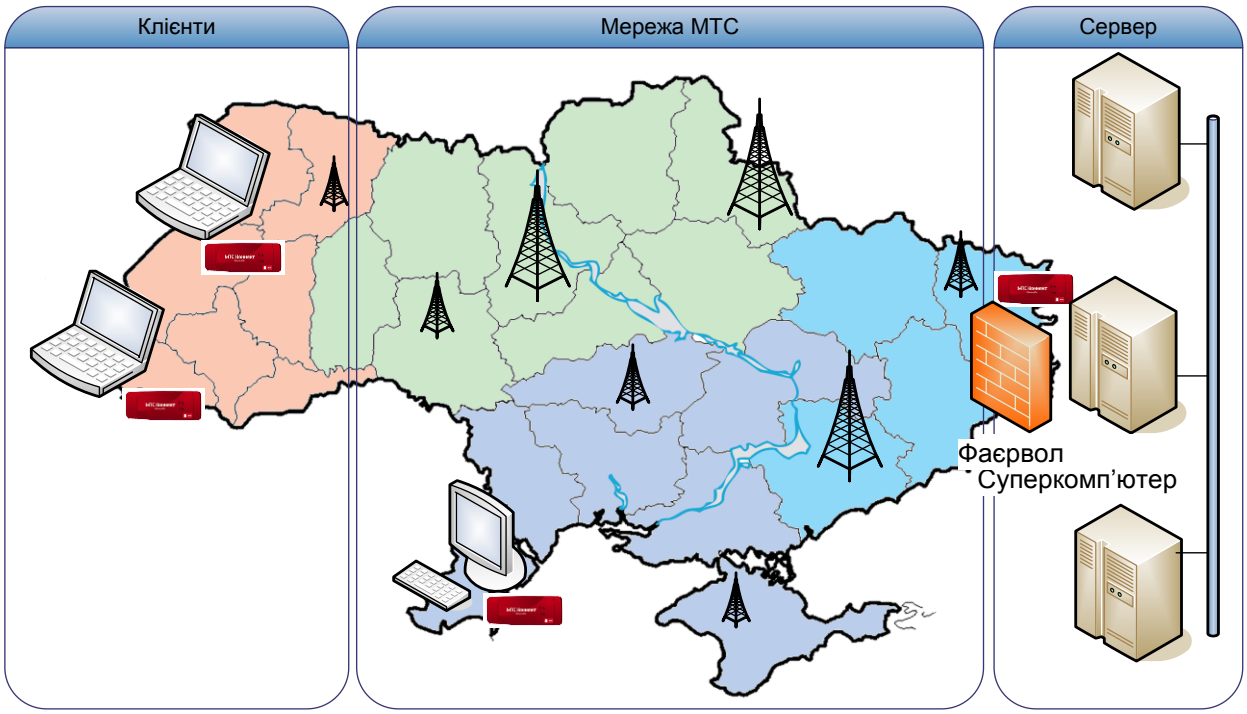

Рис. 5 – Робота з віддаленими користувачами

Висновки

Для забезпечення захисту інформації між Верховною Радою України та установами НАН України розроблено чотири варіанти заходів із захисту інформації:

1. Автономні клієнти ВРУ (не підключені до локальної мережі ВРУ) передають дані до програмно-апаратного комплексу "Бюджет" ІТГІП НАНУ за допомогою бездротового модему каналами зв'язку Оператора, які мають захист за рахунок Оператора (захист від зовнішніх вторгнень), технології побудови мережі (мобільний радіозв'язок) та налаштувань у клієнтів та сервера.

2. Клієнти ВРУ передають дані до програмно-апаратного комплексу "Бюджет" ІТГІП НАНУ за загальними каналами зв'язку, які мають захист за рахунок провайдерів та налаштувань відповідних маршрутизаторів і фаєрволів.

3. Клієнти ВРУ передають дані до серверу комплексу "Бюджет", на якому встановлено спеціалізоване програмне забезпечення для захисту інформації у каналах загального користування. Цей сервер передає зашифровані дані до програмно-апаратного комплексу "Бюджет" ІТГІП НАНУ за загальними каналами зв'язку, які мають захист за рахунок спеціалізованого програмного забезпечення.

4. Клієнти ВРУ передають дані до серверу комплексу "Бюджет", який за каналами Національної системи конфіденційного зв'язку (через вузол комутації НСКЗ) передає їх до програмно-апаратного комплексу "Бюджет" ІТГІП.

Список використаної літератури

1. Про затвердження плану заходів з виконання завдань, передбачених Законом України "Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки ": Розпорядження Кабінету Міністрів України від 15 серп. 2007 р. № 653-р [Електронний ресурс]. – Режим доступу : http/www.kmu.gov.ua.

2. Довгий С.О., Копійка О.В., Черепін Ю.Т. Засади регіональної інформатизації. – К.: ВПЦ "Тираж", 2004. – 540 с.

3. Довгий С.О., Савченко О.Я., Воробієнко П.П., Копейка О.В. Сучасні телекомунікації: мережі, технології, економіка, управління, регулювання. – К.: Український Видавничий Центр, 2002. – 520 с.

Стаття надійшла до редакції 26.02.13 українською мовою

© С.А. Довгий, О.В. Копейка, П.М. Сиверский, А.Н. Трофимчук, А.Г. Лебедь

ОБЕСПЕЧЕНИЕ РЕГЛАМЕНТИРОВАННОГО ЗАЩИЩЕННОГО УДАЛЕННОГО ДОСТУПА ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЙ СИСТЕМЫ СОПРОВОЖДЕНИЯ БЮДЖЕТНОГО ПРОЦЕССА

В статье рассмотрены вопросы различных вариантов обеспечения регламентированного защищенного удаленного доступа пользователей информационно-аналитической системы сопровождения бюджетного процесса.

© S.O. Dovgyi, O.V. Kopiyka, P.M. Siverskyi, O.M. Trofimchyk, O.G. Lebid

PROVISION OF REGULATION SECURE REMOTE ACCESS TO USERS OF INFORMATION-ANALYTICAL SYSTEM WHICH SUPPORT THE BUDGET PROCESS

The article deals with the questions of different variants regulation secure remote access to users of information-analytical system which support the budget process.