УДК 004.056

Роман РАЧОК,
кандидат технічних наук, доцент,
Національна академія Державної прикордонної служби України
імені Богдана Хмельницького, м. Хмельницький

Дмитро МУЛ,
кандидат технічних наук, доцент,
Національна академія Державної прикордонної служби України
імені Богдана Хмельницького, м. Хмельницький

Євгеній ПРОКОПЕНКО,
кандидат технічних наук, доцент,
Національна академія Державної прикордонної служби України
імені Богдана Хмельницького, м. Хмельницький

АНАЛІЗ ФУНКЦІОНУВАННЯ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ УКРАЇНИ У КОНТЕКСТІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Аналіз спільного функціонування спеціального програмного забезпечення різних інформаційно-телекомунікаційних систем показав наявність загроз інформаційній безпеці. У статті розглянуті можливості порушника щодо реалізації загроз конфіденційності, доступності, цілісності та спостереженості. Показано, що наявність доступу до Інтернет мережі є ключовою загрозою надійності інформації. У статті сформовані шляхи ліквідації зазначених загроз шляхом шифрування

© Рачок Р., Мул Д., Прокопенко Є.

мережного трафіку та усунення можливостей використання "інженерної" автентифікації.

Ключові слова: *інформаційна безпека, інформаційно-телекомунікаційна система*

Постановка проблеми у загальному вигляді. Ефективне виконання завдань Державною прикордонною службою України (ДПСУ) в сучасних умовах безпосередньо залежить від ефективно побудованої системи управління, яка значною мірою ґрунтується на впровадженні і застосуванні сучасних засобів телекомунікацій та інформаційних технологій. У ДПСУ створена й активно застосовується в оперативно-службовій діяльності (ОСД) інтегрована інформаційно-телекомунікаційна система (ІІТС) прикордонного відомства "Гарт", яка являє собою сукупність інформаційно-телекомунікаційних систем (ІТС), інформаційних системи і підсистем. Дана система є складовою загальнодержавного інформаційного поля, в якому циркулює інформація, що використовується всіма суб'єктами забезпечення національної безпеки держави [1]. Модель інформаційного обміну, яка використовується в ІІТС "Гарт" характеризується наявністю чотирьох рівнів управління, між якими здійснюється активний інформаційний обмін. При цьому, всі бази даних з основною службовою інформацією зберігаються в основному на одному рівні, зокрема у Центральному сховищі даних ІІТС "Гарт". Мережею переміщуються не лише запити до баз даних та відповіді на них, а й інформація, яка стосується оперативно-службової діяльності ДПСУ. Мережею переміщується і картографічна службова інформація. Застосування даних телекомунікаційних та інформаційних технологій, значна залежність ефективності ОСД від застосування таких технологій гостро ставить питання захисту інформації. Необхідність підвищення інформаційної безпеки ІІТС ДПСУ вимагає аналізу загроз інформаційної безпеки, які виникають при такому використанні.

Аналіз останніх досліджень і публікацій, в яких започатковано вирішення даної проблеми та на які опираються автори. Окремі аспекти використання ІІТС в ДПСУ досліджувались у працях [2-4].

Однак у цих дослідженнях недостатня увага приділялась питанням захисту інформації в ІТС, у тому числі в системах з використанням геоінформаційних технологій. Як свідчить джерело [5], серед основних типів загроз, а саме здатності системи протидіяти загрозам, які розділені на чотири типи: загрози конфіденційності, загрози цілісності, загрози доступності та загрози спостереженості.

Ще однією особливістю функціонування ІІТС ДПСУ є те, що спеціальне програмне забезпечення даної інформаційно-телекомунікаційної системи достатньо різнопланове та різноманітне, яке функціонує спільно у складі однієї системи. Крім того, застосовується програмне забезпечення від різних виробників як вітчизняних, так і закордонних. Наприклад, програмне забезпечення провідної світової геоінформаційної системи ArcGIS від компанії ESRI. Саме аналізу загроз інформації в умовах спільного використання різних програмних платформ в ІТС є питанням актуальним. Указана проблема існує в ситуації, коли надійність інформації забезпечена окремо у різних програмних модулях, але при їх спільному функціонуванні в гетерогенному середовищі ІІТС в загальному випадку надійність інформації буде не забезпечена.

Мета статті – проведення аналізу загроз інформаційної безпеки в ІТС ДПСУ при використанні в них різних програмних платформ.

Виклад основного матеріалу дослідження. На сьогодні в Державній прикордонній службі України використовується або знаходиться у стадії розробки понад два десятка ІТС. В окремих з цих систем для вирішення задач урахування географічної інформації використовуються геоінформаційні системи (ГІС). Ціла низка підсистем ІІТС "Гарт" використовує доступ до інформаційних ресурсів через WEB-технології. До таких підсистем можна віднести підсистеми "Ризик", "Реєстрація подій", "Оперативні повідомлення", "Доступ і моніторинг" та інші.

Розглянемо особливості функціонування подібних систем на прикладі ІТС геоінформаційного забезпечення "Гарт-17". В основі функціонування подібних систем лежить, як правило, технологія "клієнт-сервер". Серверна складова звичайно використовується у різноманітних прикладних застосуваннях під час вирішення завдань у межах інших

ІТС та окремих автоматизованих робочих місць. Зручною є функції розробки спеціальних веб-додатків, які дають змогу використовувати можливості сервера ArcGIS з клієнтських робочих місць без установлення на них спеціалізованого програмного забезпечення. Слід зазначити, що останнім часом значна частина додатків розробляється з використанням цього підходу. Зокрема таким чином створена підсистема "Контроль несення служби прикордонними нарядами ДПСУ", призначена для висвітлення переміщення дільничних інспекторів по периметру державного кордону.

Останнім часом дана система отримала подальший розвиток і ввійшла до складу інтегрованого додатка ("Комплексна обстановка"), який додатково дозволяє контролювати надводну обстановку, переміщення прикордонної авіації та метеорологічну обстановку.

Використання таких WEB додатків дозволяє використовувати на автоматизованих робочих місцях (АРМ) різноманітні апаратно-програмні платформи, у яких реалізовано функціонування мереж і WEB браузера (для підтримки останніх версій цих додатків також необхідне встановлення програмного забезпечення Silverlight). Перевагою такого підходу є відсутність необхідності встановлення спеціального програмного забезпечення на АРМ та подальшого його оновлення. Однак на противагу перевагам у зручності використання такий підхід створює додаткові загрози інформаційній безпеці. Це пов'язано з тим, що вся інформація, якою обмінюються WEB браузер та WEB сервер передається по мережі з використанням загальновідомих протоколів і може бути перехоплена. Перехоплення трафіку може здійснюватися: при використанні в сегменті мережі концентраторів (хабів) звичайним "прослуховуванням" мережного інтерфейсу; підключенням сніфера в розрив каналу; відгалуженням трафіку зі спрямуванням його копії на сніфер (Network tap); через аналіз побічних електромагнітних випромінювань і відновлення таким чином прослуховування трафіку; через атаку на канальному (2) (MAC-spoofing) або мережному (3) рівні (IP-spoofing), що приводить до спрямування трафіку жертви або всього трафіку сегмента на сніфер з подальшим поверненням трафіку адресату.

Перехоплення пакетів мережного рівня надає можливість аналізу інформації, якою обмінюються клієнт та сервер. На рис. 2 показано вікно програми для аналізу мережних пакетів з перехопленим пакетом з логіном користувача, який було введено для роботи з додатком.

Для обмеження доступу до додатка "Комплексна обстановка" використовується автентифікація з застосуванням логіну та паролю. Як видно з рис. 1, логін користувача можливо достатньо просто перехопити.

Однак по мережі передається не тільки логін та пароль користувача при вході в систему. Практично вся інформація, яка відображається у вікні браузера, передається по мережі. Зокрема картографічна та інша інформація, яка візуалізується на карті, передається у вигляді набору стиснених растрів, які можливо перехопити і відтворити цілісне зображення. На сьогодні існують спеціалізовані сніфери, які дозволяють відтворювати зображення перехопленої WEB сторінки. Тобто наявність можливості перехоплення мережного трафіку дозволяє отримувати практично всю конфіденційну інформацію, якою обмінюються браузер та WEB сервер.

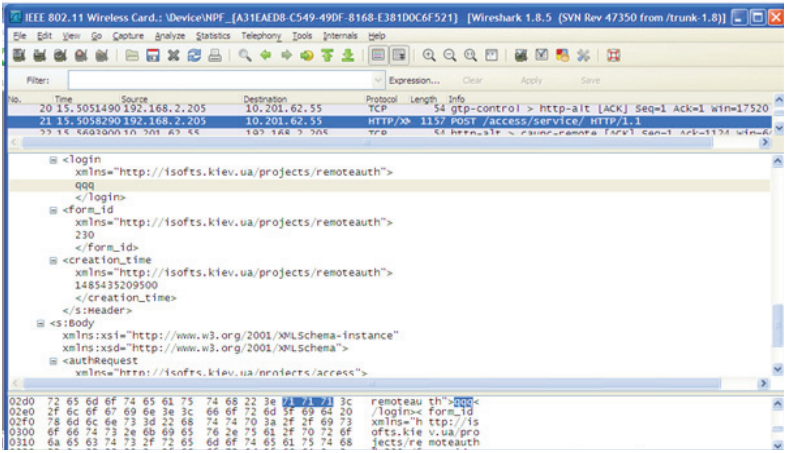

Рис. 1. Перехоплення пакета на стадії автентифікації

Ще один приклад інформаційно-телекомунікаційної системи, яка активно застосовується в оперативно-службовій діяльності, – це ІТС

прикордонної служби “Гарт-3” у складі масиву програмно-технічних комплексів (ПТК) прикордонних підрозділів “Гарт-3/П”. Дана система використовується для автоматизації процесів планування та контролю оперативно-службової діяльності підрозділів охорони кордону, а також для контролю за пересуванням прикордонних нарядів [6].

Аналіз свідчить, що низка особливостей побудови ПТК “Гарт-3/П” створює загрози інформаційній безпеці. При побудові даного програмно-технічного комплексу використана клієнт серверна архітектура. Уся інформація зосереджена на сервері баз даних. На клієнтських АРМ установлюється спеціальне програмне забезпечення (СПЗ), яке приєднується до цього серверу і залежно від ролі користувача, якій ввів логін і пароль, реалізує різні функції.

При перехопленні трафіку в ПТК “Гарт-3/П” існує можливість отримання конфіденційної інформації (рис. 2).

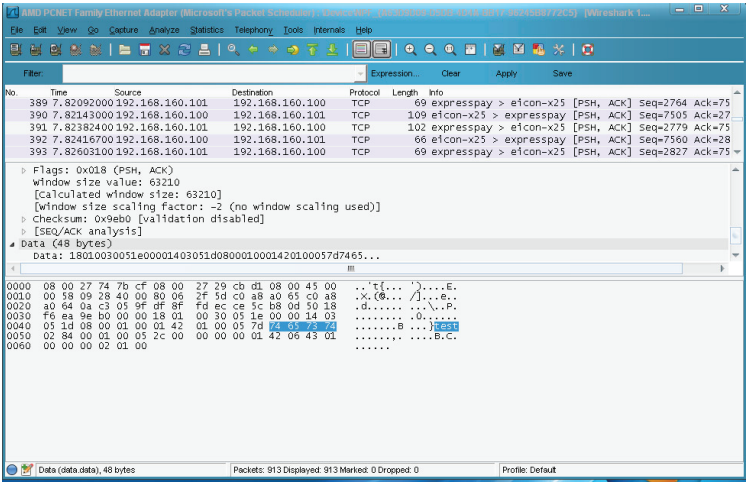

Рис. 2. Перехоплення інформації в ПТК “Гарт-3/П”

Окрім передачі логіну та паролю, по мережі передається також багато іншої службової інформації, яка може розкрити структуру бази даних комплексу. Провівши аналіз перехоплених SQL запитів до сис-

теми управління базою даних, можливо визначити інформацію, яка заноситься до таблиць бази даних (рис. 3).

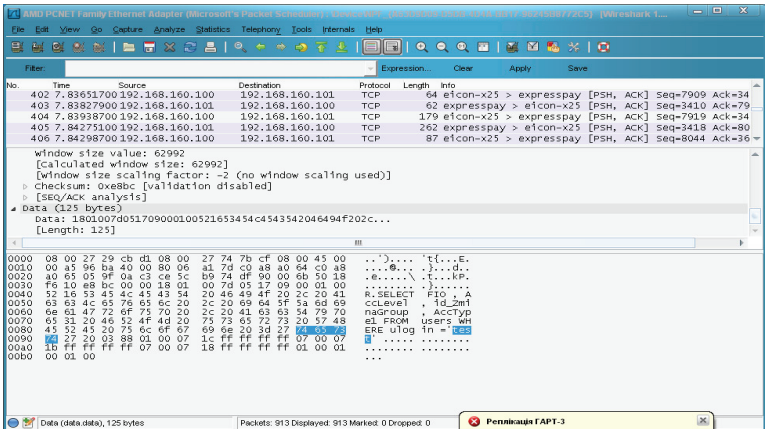

Рис. 3. Перехоплений фрагмент SQL запиту в ПТК "Гарт-3/П"

Окрім небезпеки перехоплення мережних пакетів, у ПТК "Гарт-3/П" реалізовані можливості для входу в систему з використанням "інженерної" автентифікації. Причому необхідна для цього інформація практично не прихована.

Висновки. Аналіз загроз інформаційної безпеки при використанні у Державній прикордонній службі України різних програмних підходів і платформ дозволяє стверджувати таке:

1. Спеціальне програмне забезпечення ІІТС ДПСУ "Гарт" реалізовує доступ до службової інформації як через використання стандартних веб-браузерів, так і через використання спеціально створених для ДПСУ програмних додатків. Обмін даними як між собою, так і між різними програмними платформами здійснюється з використанням стандартних мережних протоколів дані з яких, в окремих випадках, можуть бути перехоплені.

2. В окремих додатках спеціального програмного забезпечення (наприклад, СПЗ ПТК "Гарт-3/П") використовуються приховані інженерні засоби для доступу до ПТК.

У зв'язку з цим, для підвищення рівня захисту інформації в ІІТС ДПСУ пропонується забезпечити шифрування мережного трафіку та усунути можливості використання "інженерної" автентифікації на діючих ІТС.

Список використаної літератури

1. Про затвердження Положення про інформаційно-телекомунікаційну систему прикордонного контролю "Гарт-1" Державної прикордонної служби України : наказ Голови Держприкордонслужби № 810 від 30 вересня 2008 року.

2. Шинкарук О. М. Аналіз досвіду створення та використання інтегрованих телекомунікаційних систем "Гарт" в Державній прикордонній службі України / О. М. Шинкарук, А. В. Федорченко // Зб. наук. пр. Сер. : Військ. та техн. науки. – Хмельницький : Вид-во НАДПСУ, 2015. – № 64. – С. 275–282.

3. Боровик О. В. Дослідження характеристик ефективності функціонування інформаційно-телекомунікаційної системи "Гарт-1" на основі застосування методів імітаційного моделювання / О. В. Боровик, Л. В. Боровик, Л. М. Трасковецька // Збірник наукових праць Національної академії Державної прикордонної служби України. Сер. : Військові та технічні науки. – Хмельницький : Вид-во НАДПСУ, 2015. – № 63. – С. 167–182

4. Стрельбіцький М. А. Класифікація загроз інформації в інтегрованій інформаційно-телекомунікаційній системі прикордонного відомства на етапі модернізації / М. А. Стрельбіцький // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К. : ВІКНУ, 2015. – Вип. № 50. – С. 248–252

5. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу НД ТЗІ 2.5-004-99, затверджено наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації служби безпеки України від 28 квітня 1999 р. № 22, із змінами згідно з наказом адміністрації Держспецзв'язку від 28.12.2012 № 806

6. Про затвердження Тимчасової інструкції про порядок використання та застосування програмно-технічного комплексу автоматизації прикордонної служби "Гарт-3/П" : наказ Адміністрації Державної прикордонної служби України від 21 листопада 2005 року № 864. – К. : АДПСУ, 2005.

Рецензент – доктор технічних наук, професор Андрощук О. С.

Рачок Р., Мул Д., Прокопенко Е. **Анализ функционирования информационно-телекоммуникационных систем Государственной пограничной службы Украины в контексте обеспечения информационной безопасности**

Анализ совместного функционирования специального программного обеспечения различных информационно-телекоммуникационных систем показал наличие угроз информационной безопасности. В статье рассмотрены возможности нарушителя по реализации угроз конфиденциальности, доступности, целостности и наблюдаемости. Показано, что наличие доступа к интранет сети является ключевой угрозой надежности информации. В статье сформированы пути ликвидации указанных угроз путем шифрования сетевого трафика и устранения возможностей использования "инженерной" аутентификации.

Ключевые слова: *информационная безопасность, информационно-телекоммуникационная система.*

Rachok R., Mul D., Prokopenko Y. **Analysis of the functioning of information and telecommunication systems of the state border guard of Ukraine in the context of security of information security**

The tasks of national security in the information sphere require the active implementation of modern information technologies. The State Border Guard Service of Ukraine is a subject of national security on the state border. It makes extensive use of information resources in its operational and official activities. These resources are concentrated in the frontier departmental information and telecommunication systems. The model of information exchange that is used in IITS Gart is characterized by the presence of four levels of management, between which an active information exchange is taking place. At the same time, all databases with the main service information are stored basically on the same level, in particular in the Central Data Warehouse of IITS "Gart". The network moves not only requests to databases and answers to them, but also information related to the operational and official activities of the border guard service. In particular, the cartographic service information is also moved by the network. This leads

to the emergence of the problem of information security. All this requires an analysis of the corresponding threats to information security.

To date, the State Border Service is using or is in the process of developing more than two dozen ITS. In some of these systems geoinformation systems (GIS) are used to solve problems of geographic information accounting. A number of subsystems of IITS "Gart" use access to information resources through WEB-technologies. Such subsystems include subsystems "Risk", "Event registration", "Operational messages", "Access and monitoring" and others. However, this approach creates additional threats to information security. Exchange of information between the WEB-browser and WEB-server, transmitted over the network using known protocols. Therefore, it can be intercepted. Studies have shown that vulnerable information is an attacker when intercepting network packets.

The information and telecommunications system of the Gart-3 border service also used a geographic information system. This system provides a significant reduction in time for the planning and management of border guard services; control over the movement of border fees. In software and hardware, Gart-3 uses a network to exchange information between workstations and the server. This makes it possible to intercept network packets. As a result, you can get confidential information. The software "Gart-3 / P" has hidden capabilities for logging in using so-called "engineering" authentication.

In this regard, to increase the level of information security in the information and telecommunications systems of the State Border Guard Service of Ukraine, it is proposed to ensure the encryption of network traffic and exclude the possibility of using "engineering" authentication.

Keywords: *information security, information-telecommunication system.*