УДК 004.056

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

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 ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРИ ВИКОРИСТАННІ У ДЕРЖАВНІЙ ПРИКОРДОННІЙ СЛУЖБІ УКРАЇНИ ГЕОІНФОРМАЦІЙНИХ СИСТЕМ

Аналіз спільного функціонування спеціального програмного забезпечення та геоінформаційних систем показав наявність загроз інфор-

маційній безпеці. У статті розглянуті можливості порушника щодо реалізації загроз конфіденційності, доступності, цілісності та спостережності. Показано, що наявність доступу до інтранет-мережі є ключовою загрозою надійності інформації. Сформовані шляхи ліквідації зазначених загроз шляхом шифрування мережного трафіку та усунення можливостей використання "інженерної" автентифікації.

Ключові слова: *інформаційна безпека, геоінформаційна система.*

Постановка проблеми у загальному вигляді. Виклики національній безпеці в інформаційній сфері вимагають активного впровадження сучасних інформаційних технологій з метою підвищення ефективності виконання функціональних завдань правоохоронними структурами. Державна прикордонна служба України (ДПСУ) як суб'єкт національної безпеки оперує державними інформаційними ресурсами, які зосереджені в інформаційно-телекомунікаційних системах (ІТС) прикордонного відомства [1]. Сукупність ІТС, інформаційних системи та підсистем, що взаємодіють на загальному полі даних, утворюють інтегровану інформаційно-телекомунікаційну систему (ІІТС) "Гарт" прикордонного відомства. Особливості виконання завдань оперативно-службової діяльності в умовах значного територіального розосередження органів та підрозділів ДПСУ обумовлюють нагальну потребу у використанні окремими ІТС інформації, яка містить об'єкти, що потребують географічної прив'язки до місцевості. Для вирішення задач зберігання, управління, аналізу і відображення географічної інформації у світовій практиці широко використовуються геоінформаційні системи (ГІС). Провідними розробниками програмного забезпечення проводиться робота з удосконалення сучасних ГІС, розширення їх функцій. Це обумовило широке впровадження геоінформаційних систем в ІТС ДПСУ. У різних ІТС геоінформаційні системи задіяні в складі програмно-технічних комплексів. Однак їх застосування поряд зі спрощенням вирішення багатьох завдань гостро ставить питання захисту інформації. Необхідність підвищення інформаційної безпеки ІТС ДПСУ, у складі яких використовуються ГІС, 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 ГІС в ІІТС ДПСУ досліджувались у працях [2–4]. Однак у цих дослідженнях не приділялась увага питанням захисту інформації в ІТС з використанням ГІС, а саме здатності системи протидіяти загрозам, які розділені на чотири типи [5]: конфіденційності, цілісності, доступності, спостережності.

Разом із тим особливість функціонування ІТС з інтегрованою ГІС вимагає додаткових досліджень, а саме аналізу загроз інформації в умовах спільного функціонування ІТС та ГІС у складі однієї системи. Указана проблема існує в ситуації, коли надійність інформації забезпечена окремо як у спеціальному програмному забезпеченні, так і в ГІС, але при їх спільному функціонуванні в гетерогенному середовищі ІІТС у загальному випадку надійність інформації буде не забезпечена.

Мета статті – проведення аналізу загроз інформаційної безпеки в ІТС ДПСУ при використанні в них геоінформаційних систем.

Виклад основного матеріалу дослідження. На сьогодні в Державній прикордонній службі використовується або знаходиться в стадії розробки понад два десятки ІТС. В окремих з цих систем для вирішення задач урахування географічної інформації використовуються ГІС.

Основною ІТС, яка пов'язана з використанням геоінформаційних технологій, є ІТС геоінформаційного забезпечення "Гарт-17". Основою даної системи є серверна складова, яка реалізована з використанням програмного забезпечення провідної світової геоінформаційної системи ArcGIS від компанії ESRI. Ця серверна складова звичайно використовується у різноманітних прикладних застосуваннях при вирішенні завдань у межах інших ІТС та окремих автоматизованих робочих місць. Зручною є можливість розробки спеціальних веб-додатків, які дають змогу використовувати можливості сервера ArcGIS з клієнтських робочих місць без установлення на них спеціалізованого програмного забезпечення. Слід відзначити, що останнім часом значна частина додатків розробляється з використанням цього підходу. Зокрема, таким чином створена підсистема "Контроль несення служби прикор-

донними нарядами ДПСУ", призначена для висвітлення переміщення дільничних інспекторів по периметру державного кордону (рис. 1).

Рис. 1. Підсистема "Контроль несення служби прикордонними нарядами ДПСУ"

Останнім часом дана система набула подальшого розвитку і увійшла 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, в 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 трафіка може здійснюватися: при використанні в сегменті мережі концентраторів (хабів) звичайним "прослуховуванням" мережного інтерфейса; підключенням сніферу в розрив каналу; відгалуженням трафіка зі спрямуванням його копії на сніфер (Network tap); через аналіз побічних електромагнітних

випромінювань і відновлення таким чином прослуховування трафіка; через атаку на канальному (2) (MAC-spoofing) або мережному (3) рівні (IP-spoofing), що приводить до спрямування трафіка жертви або всього трафіка сегмента на сніфер з подальшим поверненням трафіка 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 із застосуванням логіна та пароля. Однак, як видно з рис. 2, логін користувача можливо достатньо просто перехопити.

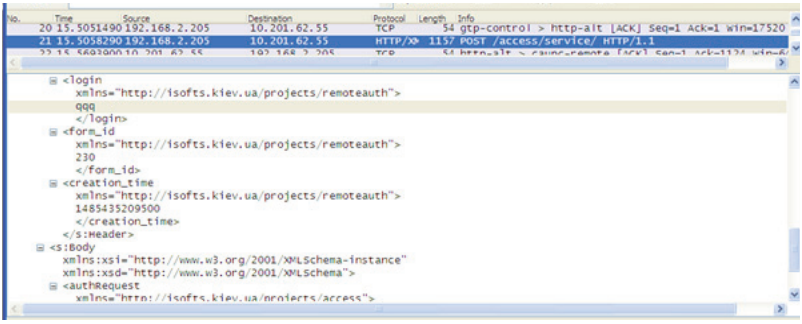

Рис. 2. Перехоплення пакета на стадії автентифікації

Однак по мережі передається не тільки логін і 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 як цілісне зображення. На сьогодні існують спеціалізовані сніфери, які дозволяють відтворювати зображення перехопленої WEB сторінки. Тобто наявність можливості перехоплення мережного трафіка дозволяє отримувати практично всю конфіденційну інформацію, якою обмінюються браузер та WEB сервер.

На теперішній час підрозділами ДПСУ використовується геоінформаційна система і ІТС прикордонної служби "Гарт-3", яка забезпечує суттєве скорочення часу на планування та контроль оперативно-службової діяльності підрозділів охорони кордону, а також контроль за пересуванням прикордонних нарядів [6].

У перших версіях спеціального програмного забезпечення (СПЗ) програмно-технічного комплексу (ПТК) автоматизації прикордонної служби "Гарт-3/П" встановлювалась ГІС isGeoMap. В останніх версіях СПЗ використовується більш потужна геоінформаційна система ArcGIS (рис. 3).

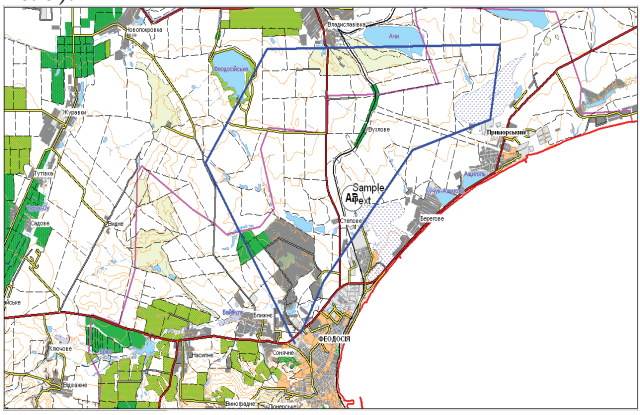

Рис. 3. Управління ділянками несення служби в СПЗ ПТК "Гарт-3/П"

Однак ця потужна ГІС у межах даного ПТК забезпечує лише облік інформації про ділянки несення служби, координати автоматизованих робочих місць "Патруль" та візуалізацію картографічної інформації. У національному програмному забезпеченні практично не реалізовані аналітичні функції, властиві сучасним системам підтримки прийняття рішень.

На жаль, ряд 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 установ-

люється СПЗ, яке приєднується до цього серверу і залежно від ролі користувача, який ввів логін і пароль, реалізує різні функції.

При перехопленні трафіка в ПТК “Гарт-3/П” існує можливість отримання конфіденційної інформації (рис. 4).

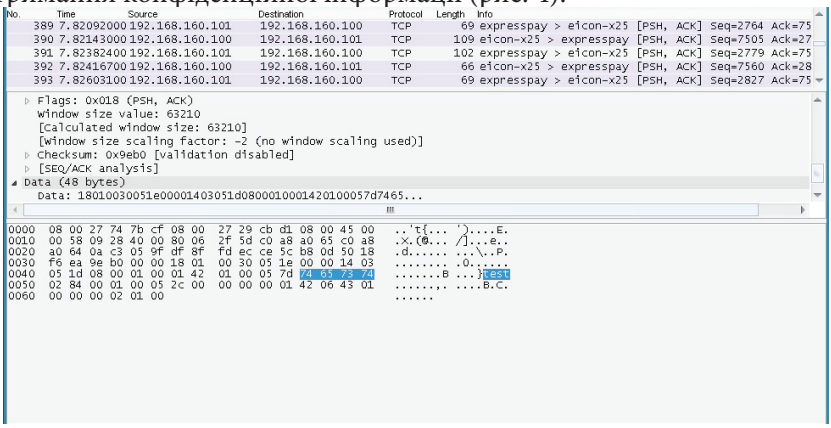

Рис. 4. Перехоплення інформації в ПТК “Гарт-3/П”

Окрім передачі логіна та пароля, по мережі передається також багато іншої службової інформації, яка може розкрити структуру бази даних комплексу. Провівши аналіз перехоплених SQL запитів до системи управління базою даних, можливо визначити інформацію, яка заноситься до таблиць бази даних (рис. 5).

Окрім небезпеки перехоплення мережних пакетів, у СПЗ 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 геоінформаційних систем дозволяє стверджувати таке:

1. У різних ІТС Державної прикордонної служби України обмін інформацією здійснюється з використанням стандартних мережних протоколів, дані з яких в окремих випадках можуть бути перехоплені.

2. В окремих додатках спеціального програмного забезпечення використовуються приховані інженерні засоби для доступу до ПТК.

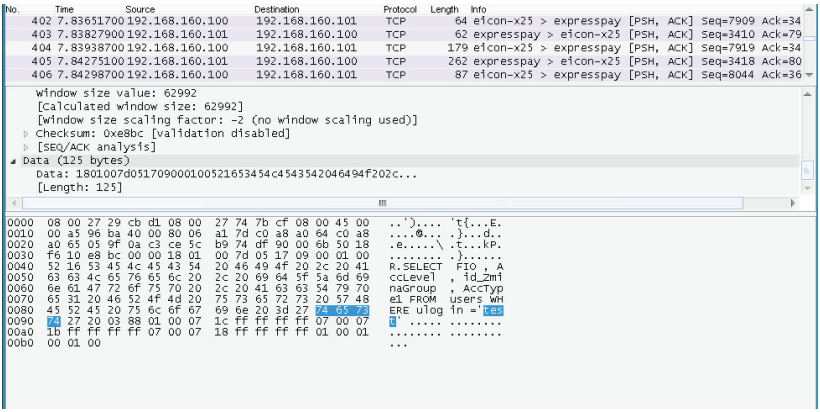

Рис. 5. Перехоплений фрагмент SQL запиту в ПТК “Гарт-3/П”

У зв’язку з цим для підвищення рівня захисту інформації в ІТС ДПСУ пропонується забезпечити шифрування мережного трафіка й усунути можливості використання “інженерної” автентифікації на діючих ІТС.

Список використаної літератури

1. Катеринчук І. С. Програмно-технічні комплекси підрозділів охорони кордону : навчальний посібник / І. С. Катеринчук, Д. А. Мул та інші. – Хмельницький : Видавництво НАДПСУ, 2010. – 270 с.

2. Рачок Р. В. Сучасні підходи до геомоделювання з використанням Arcgis / О. В. Боровик, І. І. Балицький, Р. В. Рачок // Збірник наукових праць / Національної академії Державної прикордонної служби України ім. Б. Хмельницького. Сер. : Військ. та техн. науки. – Хмельницький : НАДПСУ, 2015. – № 66. – С. 275–282.

3. Катеринчук І. С. Використання хвильового алгоритму для визначення раціонального маршруту руху в геоінформаційних системах / І. С. Катеринчук, Р. В. Рачок, Д. А. Мул // Збірник наукових праць Національної академії Державної прикордонної служби України. – Хмельницький : Видавництво НАДПСУ, 2007. – № 40.– Ч. 2. – С. 29–30.

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 28.04.1999 № 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 21.11.2005 № 864. – К. : АДПСУ, 2005.

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

Стрельбицкий М., Рачок Р., Мул Д., Прокопенко Е. **Анализ угроз информационной безопасности при использовании в Государственной пограничной службе Украины геоинформационных систем**

Анализ совместного функционирования специального программного обеспечения и геоинформационных 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. Сформированы пути ликвидации указанных угроз путем шифрования сетевого трафика и устранения возможностей использования "инженерной" аутентификации.

Ключевые слова: *информационная безопасность, геоинформационная система.*

Strelbitskii M., Rachok R., Mul D., Prokopenko Y. **Analysis of information security threats when used in the state border service of Ukraine of geographic information systems**

Challenges to national security in the information sphere require active introduction of modern information technologies. The State border service of Ukraine is a subject of national security. It operates the state's information resources. These resources are concentrated in information and telecommu-

nication systems border agencies. The tasks of operational activities are performed in conditions of considerable territorial dispersal of border agencies and departments. This leads to the need to use in information and telecommunication systems information geographic location reference. To address these challenges, the border guards are widely used geographic information system. Their use simplifies the solution of many problems. However, there are problems of information security. All this requires analysis of the relevant information security threats.

The main system that is associated with the use of GIS technology for its GIS software "Garth 17". The basis of this system is a server component. This component is implemented using the ArcGIS software from ESRI. Based on GeoServer ArcGIS developed specialized web applications. These apps give the ability to use the capabilities of the server from the client workstations. Therefore, the generated subsystem "Monitoring of dips" and "Integrated setting". However, this approach creates additional threats to information security. Information exchanged between a WEB browser and the WEB server, transmitted over the network using well known protocols. So it can be intercepted. Studies have shown the possibility that an attacker sensitive information when intercepting network packets.

In information and telecommunications system of border service "Garth-3" also used geographic information system. This system provides considerable reduction of time for planning and control service departments of border protection; control of movement of border duties. In software and hardware of "Garth-3" used network for the exchange of information between the workstations and the server. This gives the possibility of intercepting network packets. As a result, it is possible to obtain confidential information. In the software "Gart-3/P" there are hidden opportunities to enter the system using the so-called "engineering" authentication.

In this regard, to improve the level of information protection in information and telecommunication systems of the State border service of Ukraine it is proposed to provide encryption of network traffic and to eliminate the possibility of using "engineering" authentication.

Keywords: *information security, geographic information system.*