ISSN 2078–4333. Вісник Львівського університету. Серія міжнародні відносини. 2018. Випуск 44 С. 163–170
Visnyk of the Lviv University. Series International Relations. 2018. Issue 44. P. 163–170

УДК 327.51:351.746.1(477+437.6)
DOI dx.doi.org/10.30970/vir.2018.44.0.9450

ГЛОБАЛЬНА АВТОМАТИЗОВАНА ІНФОРМАЦІЙНА СИСТЕМА «ГАРТ» У СФЕРІ ЗАХИСТУ ДЕРЖАВНОГО КОРДОНУ УКРАЇНИ ТА СЛОВАЧЧИНИ

Наталя Мелінчук

Державна прикордонна служба України,
Чорноморський національний університет імені Петра Могили,
вул. 68 Десантників 10, м. Миколаїв, Україна, 54003, тел. (0512)-50-03-33,
e-mail: natalia.melinchuk@gmail.com

Розглянуто військове співробітництво України та Словаччини у сфері захисту державного кордону, зокрема, між Державною прикордонною службою України та Поліцейськими силами Словаччини (словац. **Policajný zbor**) у галузі криптографічного захисту інформації. Автор статті характеризує пункти пропуску через державний кордон України на кордоні зі Словаччиною, зокрема: Малий Березний, Малі Селменці, Павлове, Ужгород, Чоп (Страж). Використання інформаційно-телекомунікаційних систем «ГАРТ» є складовими безпекового сектору обох країн. Прикордонне українсько-словацьке співробітництво у сфері кіберзахисту в оперативно-службовій діяльності спирається на низку нормативно-правових документів, які регулюють міждержавні відносини щодо національної безпеки цих країн, наприклад, Закон України «Про основні засади забезпечення кібербезпеки України» (2017), «Конвенція про кіберзлочинність» (2005), «Стратегія кібербезпеки України» (2016) та ін. Глобальна автоматизована інформаційна система «ГАРТ» використовується фахівцями-зв'язківцями та спеціалістами-криптографами у розвідувальній та контррозвідувальній діяльності з метою протидії загрозам національної безпеки України та Словаччини. Уважного ставлення військовими експертами та державними експертами з питань таємниць потребує галузь автоматизованих систем управління, оскільки інформація, що підлягає криптографічному захисту є таємною згідно Закону України «Про державну таємницю» (1994). Автор статті зазначає, що витоком з каналів зв'язку та захистом інформації займаються спеціалісти «Банкомзв'язку», які є розробниками інструкцій щодо експлуатації обладнання програмно-технічного комплексу «ГАРТ», що прийняте на оззброєння Державною прикордонною службою України та Поліцейськими силами Словаччини. «ГАРТ» надає можливість доступу до баз даних «Інтерпол», «Паспорт» та «Ризик» з метою: виявлення осіб, причетних до підготовки і здійснення терористичних актів; протидії нелегальній міграції іноземців легальним шляхом з використанням чужих або підроблених документів; виявлення підроблених паспортів громадянина України та Словаччини; протидії торгівлі людьми, тобто протидії протиправній діяльності у пунктах пропуску через державний кордон.

Ключові слова: військове співробітництво; власна і внутрішня безпека; глобальна автоматизована інформаційна система «ГАРТ»; криптографічний захист інформації; Поліцейські сили Словаччини (словац. Policajný zbor).

Постановка наукової проблеми та її значення. Захист та охорона державного кордону є пріоритетним напрямом національної безпеки України та Словаччини. Власне «ГАРТ» слугує інформаційним захистом різного виду інформації, зокрема, таємної. Глобальна автоматизована інформаційна система

«ГАРТ» спирається на Закон України «Про контррозвідувальну діяльність», Закон України «Про розвідувальні органи України» та Закон України «Про державну таємницю».

Згідно з наказом АДПСУ № 810 від 30.09.2008 р. «Про затвердження Положення про інформаційно-телекомунікаційну систему прикордонного контролю «Гарт-1» Державної прикордонної служби України» [9]: «Система «Гарт-1» створюється і використовується в інтересах розвідки, контррозвідувального забезпечення охорони державного кордону України, оперативно-розшукової діяльності, участі в боротьбі з організованою злочинністю та протидії незаконній міграції з метою своєчасного та достовірного інформаційно-аналітичного забезпечення діяльності підрозділів та органів Державної прикордонної служби України для здійснення ними заходів із запобігання і недопущення в'їзду в Україну або виїзду з України осіб, яким, згідно із законодавством, не дозволяється в'їзд в Україну або тимчасово обмежено право виїзду з України, у тому числі згідно з дорученням правоохоронних органів, розшуку в пунктах пропуску через державний кордон осіб, які переховуються від органів дізнання, слідства та суду, ухиляються від відбуття кримінальних покарань, посилення контролю за додержанням правил в'їзду, виїзду, перебування в Україні іноземців та осіб без громадянства, а також виконання інших завдань у правоохоронній сфері згідно із законодавством».

Аналіз останніх досліджень і публікацій з цієї проблеми. Наукові розвідки у вітчизняній і закордонній науці у сфері захисту державного кордону між Україною та Словаччиною відстутні. Це й обумовило вибір теми нашого дослідження.

Нормативно-правова база щодо захисту інформації в автоматизованих інформаційних системах між Україною та Словаччиною у сфері захисту державного кордону становить: *Закони України* [1; 2; 3], *накази Адміністрації Державної прикордонної служби України* [4; 5; 6; 7; 8; 9; 10; 11; 12], *наказ МВС України* [13].

Формулювання завдання дослідження. Завдання полягає у тому, щоб розглянути військове співробітництво України та Словаччини у сфері захисту державного кордону, зокрема, між Державною прикордонною службою України та Поліцейськими силами Словаччини (словац. **Policajný zbor**) у галузі інформаційної безпеки, розглянувши глобальну автоматизовану інформаційну систему «ГАРТ».

Виклад основного матеріалу дослідження з обґрунтуванням отриманих наукових результатів. З-поміж «ГАРТів» виокремлюють: «ГАРТ-1» – прикордонний контроль, «ГАРТ-2» – інформаційно-телекомунікаційні системи оперативно-чергової частини, «ГАРТ-3» – прикордонна служба, «ГАРТ-5» – інформаційно-аналітична служба, «ГАРТ-6» – фінансове забезпечення, «ГАРТ-7» – кадрове забезпечення, «ГАРТ-8» – професійна підготовка, «ГАРТ-9» – санітарно-епідеміологічне забезпечення, «ГАРТ-10» – оперативно-розшукова діяльність, «ГАРТ-11» – виховна робота, «ГАРТ-12» – морська охорона, «ГАРТ-13» – правове забезпечення, «ГАРТ-14» – спостереження, «ГАРТ-15» –

інформаційно-телекомунікаційні системи радіаційного, хімічного, біологічного захисту та екологічної безпеки, «ГАРТ-16» – авіаційна служба, «ГАРТ-17» – геоінформаційна система, «ГАРТ-18» – документальне забезпечення, «ГАРТ-19» – електронна пошта, «ГАРТ-20» – факсимільне повідомлення, «ГАРТ-21» – внутрішня безпека.

У Законі України «Про контррозвідувальну діяльність» [2] наголошено: «Стаття 1. Поняття контррозвідувальної діяльності.

Контррозвідувальна діяльність – спеціальний вид діяльності у сфері забезпечення державної безпеки, яка здійснюється з використанням системи контррозвідувальних, пошукових, режимних, адміністративно-правових заходів, спрямованих на попередження, своєчасне виявлення і запобігання зовнішнім та внутрішнім загрозам безпеці України, розвідувальним, терористичним та іншим протиправним посяганням спеціальних служб іноземних держав, а також організацій, окремих груп та осіб на інтереси України.

Стаття 2. Мета і завдання контррозвідувальної діяльності

Метою контррозвідувальної діяльності є попередження, своєчасне виявлення і запобігання зовнішнім та внутрішнім загрозам безпеці України, припинення розвідувальних, терористичних та інших протиправних посягань спеціальних служб іноземних держав, а також організацій, окремих груп та осіб на державну безпеку України, усунення умов, що їм сприяють, та причин їх виникнення.

Завданнями контррозвідувальної діяльності є:

добування, аналітична обробка та використання інформації, що містить ознаки або факти розвідувальної, терористичної та іншої діяльності спеціальних служб іноземних держав, а також організацій, окремих груп та осіб на шкоду державній безпеці України;

протидія розвідувальній, терористичній та іншій діяльності спеціальних служб іноземних держав, а також організацій, окремих груп та осіб на шкоду державній безпеці України;

розроблення і реалізація заходів щодо запобігання, усунення та нейтралізації загроз інтересам держави, суспільства та правам громадян».

У Законі України «Про розвідувальні органи України» [3]:

«Стаття 4. Основні завдання розвідувальних органів України

На розвідувальні органи України покладаються:

добування, аналітична обробка та надання визначеним законом органам державної влади розвідувальної інформації;

здійснення спеціальних заходів, спрямованих на підтримку національних інтересів і державної політики України в економічній, політичній, воєнній, військово-технічній, екологічній та інформаційній сферах, зміцнення обороноздатності, економічного і науково-технічного розвитку, захисту та охорони державного кордону; (Абзац третій статті 4 в редакції Закону N 3200-IV (3200–15) від 15.12.2005);

забезпечення безпечного функціонування установ України за кордоном, безпеки співробітників цих установ та членів їх сімей у країні перебування, а

також відряджених за кордон громадян України, які обізнані у відомостях, що становлять державну таємницю;

участь у боротьбі з тероризмом, міжнародною організованою злочинністю, незаконним обігом наркотичних засобів, незаконною торгівлею зброєю і технологією її виготовлення, незаконною міграцією у порядку, визначеному законом; (Абзац п'ятий статті 4 в редакції Закону № 3200-IV (3200–15) від 15.12.2005);

вжиття заходів протидії зовнішнім загрозам національній безпеці України, життю, здоров'ю її громадян та об'єктам державної власності за межами України. (Статтю 4 доповнено абзацом шостим згідно із Законом № 3200-IV (3200–15) від 15.12.2005)».

У наказі МВС України № 1261 від 19.10.2015 р. «Про затвердження Інструкції про службу прикордонних нарядів Державної прикордонної служби України» [13] зазначено: «Черговий інформаційно-телекомунікаційних систем (далі – черговий ІТС) – прикордонний наряд у складі одного та більше прикордонників, який призначений для забезпечення цілодобового функціонування та обслуговування засобів телекомунікацій, програмно-технічних комплексів (далі – ПТК), автоматизованих робочих місць посадових осіб підрозділу охорони кордону, пункту управління системи оптико-електронного спостереження та інших компонентів інформаційно-телекомунікаційних систем.

Черговий ІТС повинен знати склад, призначення, тактико-технічні характеристики, будову, правила експлуатації, функціональні можливості і принцип роботи засобів телекомунікації, ПТК інформаційно-телекомунікаційних систем, установлених на об'єктах інформаційної діяльності, порядок надання доступу до інформації, що обробляється в інформаційно-телекомунікаційних системах.

Під час виконання завдань черговий ІТС зобов'язаний:

– здійснювати постійний моніторинг стану баз даних ПТК, виконувати функції адміністрування ПТК та компонентів локальної обчислювальної мережі об'єкта інформаційної діяльності (у частині, що їх стосується);

– підтримувати засоби телекомунікації та ПТК інформаційно-телекомунікаційних систем у робочому стані;

– надавати доступ до роботи на відповідних автоматизованих робочих місцях складу зміни прикордонного наряду та визначеним посадовим особам;

– здійснювати контроль за дотриманням посадовими особами-користувачами ПТК правил експлуатації автоматизованих робочих місць та периферійного обладнання;

– вести облік роботи засобів телекомунікації та ПТК інформаційно-телекомунікаційних систем;

– суворо дотримуватись вимог щодо забезпечення передачі документальних повідомлень, обміну інформації, правил техніки безпеки, технічного захисту інформації, заходів пожежної безпеки.

У службовій діяльності черговий ІТС керується нормативно-правовими актами та актами організаційно-розпорядчого характеру, що регламентують використання засобів телекомунікації, інформаційно-телекомунікаційних систем та організацію оперативно-технічної служби на вузлах зв'язку у Державній прикордонній службі України».

Згідно з Законом України «Про державну таємницю» [1]:

«Стаття 1. Визначення термінів.

У цьому Законі терміни вживаються у такому значенні:

державна таємниця (далі також – секретна інформація) – вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому цим Законом, державною таємницею і підлягають охороні державою;

віднесення інформації до державної таємниці – процедура прийняття (державним експертом з питань таємниць) рішення про віднесення категорії відомостей або окремих відомостей до державної таємниці з установленням ступеня їх секретності шляхом обгрунтування та визначення можливої шкоди національній безпеці України у разі розголошення цих відомостей, включенням цієї інформації до Зводу відомостей, що становлять державну таємницю, та з опублікуванням цього Зводу, змін до нього;

гриф секретності – реквізит матеріального носія секретної інформації, що засвідчує ступінь секретності даної інформації;

державний експерт з питань таємниць – посадова особа, уповноважена здійснювати відповідно до вимог цього Закону віднесення інформації до державної таємниці у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, зміни ступеня секретності цієї інформації та її розсекречування;

допуск до державної таємниці – оформлення права громадянина на доступ до секретної інформації;

доступ до державної таємниці – надання повноважною посадовою особою дозволу громадянину на ознайомлення з конкретною секретною інформацією та провадження діяльності, пов'язаної з державною таємницею, або ознайомлення з конкретною секретною інформацією та провадження діяльності, пов'язаної з державною таємницею, цією посадовою особою відповідно до її службових повноважень;

засекречування матеріальних носіїв інформації – введення у встановленому законодавством порядку обмежень на поширення та доступ до конкретної секретної інформації шляхом надання відповідного грифу секретності документам, виробам або іншим матеріальним носіям цієї інформації;

Звід відомостей, що становлять державну таємницю – акт, в якому зведено переліки відомостей, що згідно з рішеннями державних експертів з питань таємниць становлять державну таємницю у визначених цим Законом сферах;

категорія режиму секретності – категорія, яка характеризує важливість та обсяги відомостей, що становлять державну таємницю, які зосереджені в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях;

криптографічний захист секретної інформації – вид захисту, що реалізується шляхом перетворення інформації з використанням спеціальних даних (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо;

матеріальні носії секретної інформації – матеріальні об'єкти, в тому числі фізичні поля, в яких відомості, що становлять державну таємницю, відображені у вигляді текстів, знаків, символів, образів, сигналів, технічних рішень, процесів тощо;

охорона державної таємниці – комплекс організаційно-правових, інженерно-технічних, криптографічних та оперативно-розшукових заходів, спрямованих на запобігання розголошенню секретної інформації та втратам її матеріальних носіїв;

режим секретності – встановлений згідно з вимогами цього Закону та інших виданих відповідно до нього нормативно-правових актів, єдиний порядок забезпечення охорони державної таємниці;

розсекречування матеріальних носіїв секретної інформації – зняття в установленому законодавством порядку обмежень на поширення та доступ до конкретної секретної інформації шляхом скасування раніше наданого грифу секретності документам, виробам або іншим матеріальним носіям цієї інформації;

спеціальна експертиза щодо наявності умов для провадження діяльності, пов'язаної з державною таємницею – експертиза, що проводиться з метою визначення в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях наявності умов, передбачених цим Законом, для провадження діяльності, пов'язаної з державною таємницею;

ступінь секретності («особливої важливості», «цілком таємно», «таємно») – категорія, яка характеризує важливість секретної інформації, ступінь обмеження доступу до неї та рівень її охорони державою;

технічний захист секретної інформації – вид захисту, спрямований на забезпечення інженерно-технічними заходами конфіденційності, цілісності та унеможливлення блокування інформації.

Стаття 4. Державна політика щодо державної таємниці

Державну політику щодо державної таємниці *як складову засад внутрішньої та зовнішньої політики* визначає Верховна Рада України».

Висновки і перспективи подальших досліджень. Аналіз джерельної бази дає змогу дійти висновку, що означена проблема не була об'єктом спеціального вивчення у вітчизняній політичній науці та у війській справі.

Перспективи подальших досліджень. Результати дослідження можна використати в процесі професійної політичної та війської підготовки студентів/курсантів, магістрів та аспірантів/ад'юнктів за різними напрямами, у

тім числі під час викладання спецкурсів військової спрямованості політико-правничого характеру.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Закон України «Про державну таємницю». – Документ 3855-12, чинний, поточна редакція – Редакція від 05.01.2017, підстава 1798-19 [Офіційна сторінка Верховної Ради України]. – URL: http://zakon3.rada.gov.ua (09 лютого 2018 р.).

2. Закон України «Про контррозвідувальну діяльність». – Документ 374-15, чинний, поточна редакція – Редакція від 05.01.2017, підстава 1798-19 [Офіційна сторінка Верховної Ради України]. – URL: http://zakon3.rada.gov.ua (09 лютого 2018 р.).

3. Закон України «Про розвідувальні органи України». – Документ 2331-14, чинний, поточна редакція – Редакція від 28.07.2016, підстава 1437-19 [Офіційна сторінка Верховної Ради України]. – URL: http://zakon3.rada.gov.ua (09 лютого 2018 р.).

4. Наказ АДПСУ №308 від 08.08.1997 р. «Про прийняття на озброєння Державної прикордонної служби України програмно-технічного комплексу автоматизації прикордонного контролю «Гарт-1/П»» [Офіційна сторінка Державної прикордонної служби України]. – URL: http://dpsu.gov.ua (09 лютого 2018 р.).

5. Наказ АДПСУ №474 від 20.08.2002 р. «Про прийняття наозброєння військ програмних компонентів глобальної автоматизованої інформаційної системи Прикордонних військ України (шифр «Гарт»)» [Офіційна сторінка Державної прикордонної служби України]. – URL: http://dpsu.gov.ua (09 лютого 2018 р.).

6. Наказ АДПСУ № 400 від 17.05.2004 р. «Про введення в дію Інструкції з діловодства в Державній прикордонній службі України» [Офіційна сторінка Державної прикордонної служби України]. – URL: http://dpsu.gov.ua (09 лютого 2018 р.).

7. Наказ АДПСУ № 56/394 від 07.07.2005 р. «Про організацію доступу від абонентських пунктів інформаційного обміну регіональних органів Служби Безпеки України до центрального сховища даних центральної підсистеми «Гарт-ЦП» глобальної автоматизованої інформаційної системи «Гарт» Держприкордонслужби України» [Офіційна сторінка Державної прикордонної служби України]. – URL: http://dpsu.gov.ua (09 лютого 2018 р.).

8. Наказ АДПСУ № 416 від 15.05.2008 р. «Про прийняття на озброєння Державної прикордонної служби України програмно-технічних комплексів автоматизації прикордонного контролю «Гарт-1/РУ» та «Гарт-1/ООДК»» [Офіційна сторінка Державної прикордонної служби України]. – URL: http://dpsu.gov.ua (09 лютого 2018 р.).

9. Наказ АДПСУ № 810 від 30.09.2008 р. «Про затвердження Положення про інформаційно-телекомунікаційну систему прикордонного контролю «Гарт -1» Державної прикордонної служби України» [Офіційна сторінка Державної прикордонної служби України]. – URL: http://dpsu.gov.ua (09 лютого 2018 р.).

10. Наказ АДПСУ № 949 від 09.12.2009 р. «Про затвердження Положення про інформаційно-телекомунікаційну систему прикордонної служби «Гарт-3» Державної прикордонної служби України» [Офіційна сторінка Державної прикордонної служби України]. – URL: http://dpsu.gov.ua (09 лютого 2018 р.).

11. Наказ АДПСУ № 182 від 30.11.2016 р. «Про внесення змін до Положення про Окремий відділ внутрішньої безпеки Державної прикордонної служби України» [Офіційна сторінка Державної прикордонної служби України]. – URL: http://dpsu.gov.ua (09 лютого 2018 р.).

12. Наказ АДПСУ № 192 від 16.12.2016 р. «Про затвердження Положення про управління зв'язку Адміністрації Держприкордонслужби України» [Офіційна сторінка Державної прикордонної служби України]. – URL: http://dpsu.gov.ua (09 лютого 2018 р.).

13. Наказ МВС України № 1261 від 19.10.2015 р. «Про затвердження Інструкції про службу прикордонних нарядів Державної прикордонної служби України» [Офіційна сторінка Верховної Ради України]. – URL: http://zakon.rada.gov.ua (09 лютого 2018 р.).

Стаття надійшла до редколегії 10.06.2018
Прийнята до друку 01.09.2018

GART GLOBAL AUTOMATED INFORMATION SYSTEM IN THE SPHERE OF DEFENCE OF STATE BOUNDARY OF UKRAINE AND SLOVAKIA

Natalia Melinchuk

State Border Guard Service of Ukraine,
Petro Mohyla Black Sea State University,
68 Desantnykiv Str., 10, Mykolaiv, Ukraine, 54003, tel.: (0512) 50-03-33,
e-mail: natalia.melinchuk@gmail.com

This article reviewed military cooperation of Ukraine and Slovakia in the sphere of defence of state boundary, in particular between State Border Guard Service and Police Forces of Slovakia (Slovak **Policajný zbor**) in the field of cryptographic protection of information. . The author describes the checkpoints on the state border of Ukraine and on the border of Slovakia, in particular: Malyi Bereznyi, Mali Selmentsi, Pavlove, Uzhhorod, Chop (Strazh). The use of information and telecommunication systems «GART» is a component of the security sector of both countries. Ukrainian and Slovak cooperation on the border in the sphere of cyber defense in operational and service activities is based on a number of legal documents regulating intergovernmental relations regarding the national security of these countries, for example, the Law of Ukraine «On the Basic Principles of Cybersecurity of Ukraine» (2017), «The Cybersecurity Convention» (2005), «The Cybersecurity Strategy of Ukraine» (2016) and others. The «GART» global automated information system is used by communication men and cryptographers in intelligence and counter-intelligence activities to counter the threats to the national security of Ukraine and Slovakia. The automated control systems industry requires the attentive attitude of military experts and state experts on secrets, since the information subject to cryptographic protection is classified according to the Law of Ukraine «On State Secrets» (1994). The author of the article indicates that specialists of «Bancomzvjazok», who developed the manual for equipment of «GART» software and hardware complex, which was adopted by the State Border Guard Service of Ukraine and the Police forces of Slovakia are engaged in communication channels leak and information protection. «GART» provides access to databases of «Interpol», «Passport» and «Risk» in order to: identify persons involved in the preparation and implementation of terrorist acts; counteract illegal migration of foreigners by legal means using foreign or forged documents; detection of forged passports of a citizen of Ukraine and Slovakia; counteract to human trafficking, that is, counteract to illegal activity at border checkpoints.

Key words: military cooperation; inherent and internal security; GART global automated information system; cryptographic information protection; Police forces of Slovakia (Slovak **Policajný zbor**).