УДК 004.056
к.т.н., доц. **Стрельбіцький М.А.** (НАДПСУ)

КЛАСИФІКАЦІЯ ЗАГРОЗ ІНФОРМАЦІЇ В ІНТЕГРОВАНІЙ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНІЙ СИСТЕМІ ПРИКОРДОННОГО ВІДОМСТВА НА ЕТАПІ МОДЕРНІЗАЦІЇ

Функціонування інтегрованої інформаційно-телекомунікаційної системи «Гарт» Державної прикордонної служби України здійснюється в умовах ведення проти держави гібридної війни, реформування системи державного управління, сектору безпеки та оборони України, її інтеграції в європейське та світове демократичне співтовариство. Постійне вдосконалення існуючих та впровадження нових інформаційно-телекомунікаційних систем виявляє проблему захисту інформації і в умовах спільного використання як старих так і нових версій програмного і апаратного середовища. Першочерговим етапом у створенні надійного та ефективного захисту інформації у відомчій корпоративній системі є аналіз та класифікація можливих загроз інформації.

В статті на підставі аналізу умов функціонування відомчої інформаційно-телекомунікаційної системи на стадії модернізації наведена класифікація загроз надійності інформації.

Ключові слова: загроза інформації, захист інформації, інтегрована інформаційно-телекомунікаційна система.

Актуальність теми. Реалізація завдань Мирного плану Президента України, посилення рівня захищеності державного кордону з урахуванням нової безпекової сфери, а також базових підходів щодо реформування системи державного управління, сектору безпеки та оборони України, її інтеграції в європейське та світове демократичне співтовариство вимагає інтенсивного та ефективного реформування Державної прикордонної служби України [1, 6]. Побудова системи охорони та захисту державного кордону з урахуванням сучасних викликів і загроз гібридної війни [8], повинна забезпечуватись раціональним використання наявних ресурсів та удосконаленням управлінської діяльності прикордонного відомства. Однією з складових, що забезпечує ефективне функціонування органів і підрозділів охорони державного кордону є інтегрована інформаційно-телекомунікаційна система «Гарт» (ІІТС), яка містить більше 20 інформаційно-телекомунікаційних систем, що забезпечують виконання різних функціональних завдань, систем забезпечення та взаємодії з іншими відомствами з питань національної безпеки України в прикордонній сфері.

Доцільно зазначити, що на теперішній час вже розгорнуті та виконують завдання прикордонні підрозділи нового типу. У зоні проведення антитерористичної операції на сході України їх використання потребує модернізації існуючих складових ІІТС та інтеграції нових інформаційно-телекомунікаційних систем (ІТС).

Крім того, впровадження в експлуатацію нових програмно-технічних комплексів не повинно вплинути на функціонування існуючих ІТС та підсистем. У якості прикладу наведемо функціонування ІТС автоматизації прикордонного контролю (АПК) «Гарт-1», яка постійно змінює (вдосконалює) як програмну так і апаратну складову. Розгортання прикордонних підрозділів із специфічними функціями у зоні проведення антитерористичної операції, а саме контрольних постів в'їзду-виїзду (КПВВ), які здійснюють реєстрацію осіб, що переміщуються з (на) непідконтрольні території. Основним призначенням ПТК АПК «Гарт-1» була автоматизація обліку і контролю за базами даних паспортних (ідентифікаційних) даних осіб та реєстраційних даних транспортних засобів, що перетинають державний кордон України в пунктах пропуску через державний кордон [2]. Але потреба у автоматизації КПВВ призвела до модернізації цієї ІТС з питань обліку громадян України які не перетинають державний кордон. Вищезазначене обґрунтовує вимогу функціонування ІТС ПТК АПК як на старій так і новій програмно-апаратних платформах (в залежності від оснащення підрозділу) та виконання функції автоматизації

обліку і контролю за пропуском осіб як за кордон так і всередині держави (пункти пропуску, КПВВ).

Постановка задачі. Метою статті є проведення класифікації сучасних загроз інформації на підставі аналізу умов функціонування інтегрованої інформаційно-телекомунікаційній системі прикордонного відомства на стадії модернізації.

Основна частина. Ключовим питанням ефективного функціонування складових ІІТС та системи в цілому є забезпечення надійності інформації, яка в ній циркулює. Під надійністю інформації будемо розуміти її комплексну властивість протидіяти загрозам, які розділені на чотири типи [3], а саме: конфіденційності, цілісності, доступності, спостереженості.

Питанням класифікації загроз інформації присвячено багато досліджень. В роботах В. Ліпкана, А. Логінова, Б. Кузьменка, О. Чайковської, С. Гуцу, А. Погребняка класифікація загроз інформації розглянута також і в аспекті інформаційної безпеки. Разом з цим, особливість функціонування ІІТС «Гарт» вимагає додаткових досліджень, а саме забезпечення надійності інформації на стадії модернізації. Вказана проблема існує в ситуації, коли надійність інформації забезпечена окремо як у старій так і в новій версіях спеціального програмного забезпечення, але при спільному функціонуванні обох версій в гетерогенному середовищі ІІТС в загальному випадку надійність інформації буде не забезпечена.

Аналіз функціонування ІІТС «Гарт» показав, що експлуатація відомчої інформаційно-телекомунікаційної системи здійснюється 4-ма категоріями персоналу:

перша категорія – персонал підрозділів зв'язку, автоматизації та захисту інформації, якій здійснює розгортання, налагодження та введення в експлуатацію всіх складових ІІТС, а також персонал організації розробника програмно-апаратного забезпечення, який безпосередньо здійснює розробку системи. Вказаний персонал має безпосередній доступ до апаратних складових, програмного забезпечення, засобів комунікації, засобів забезпечення політики безпеки та інше;

друга категорія – персонал органів та підрозділів охорони кордону (за винятком першої категорії) яким надано доступ до використання в повсякденній діяльності складових відомчої корпоративної системи;

третя категорія – персонал органів та підрозділів охорони кордону (за винятком першої та другої категорій) у яких відсутній доступ до ІІТС «Гарт», а також персонал організації розробника програмно-апаратного забезпечення, який безпосередньо не здійснює розробку системи та не має доступу до системи;

четверта категорія – всі інші особи, які опосередковано причетні до функціонування інформаційної системи прикордонного відомства (співробітники організацій які надають в оренду канали зв'язку, подорожуючі та інші). Вказана категорія є найбільш небезпечною, так як вона знаходиться поза межами впливу прикордонного відомства. Під цю категорію підпадають особи, що реалізують загрози національній безпеці України, а саме загрози кібербезпеці і безпеці інформаційних ресурсів [7].

Агрегуючи типи загроз, які наведені в [3] в статті під загрозою в загальному розумінні будемо розуміти подію або дію, яка може викликати порушення функціонування ІІТС, включаючи спотворення, знищення або несанкціоноване використання (розмноження) оброблюваної і збереженої в ній інформації та неможливість відслідковування дій персоналу з інформацією.

Окремі автори [4, 5] вносять в класифікацію загроз надійності інформацію такий фактор, як навмисність (помилковість) дій користувача. Разом із тим, з точки зору кінцевого результату функціонування системи, це не має значення. У випадку, наприклад, знищення інформації порушується вимога доступності без врахування мотивів користувача (навмисні вони чи помилкові). Тому, класифікацію загроз надійності інформації, викликаних стадією модернізації ІІТС доцільно здійснити з урахуванням впливу програмно-апаратних засобів та можливостей користувачів системи (рис. 1).

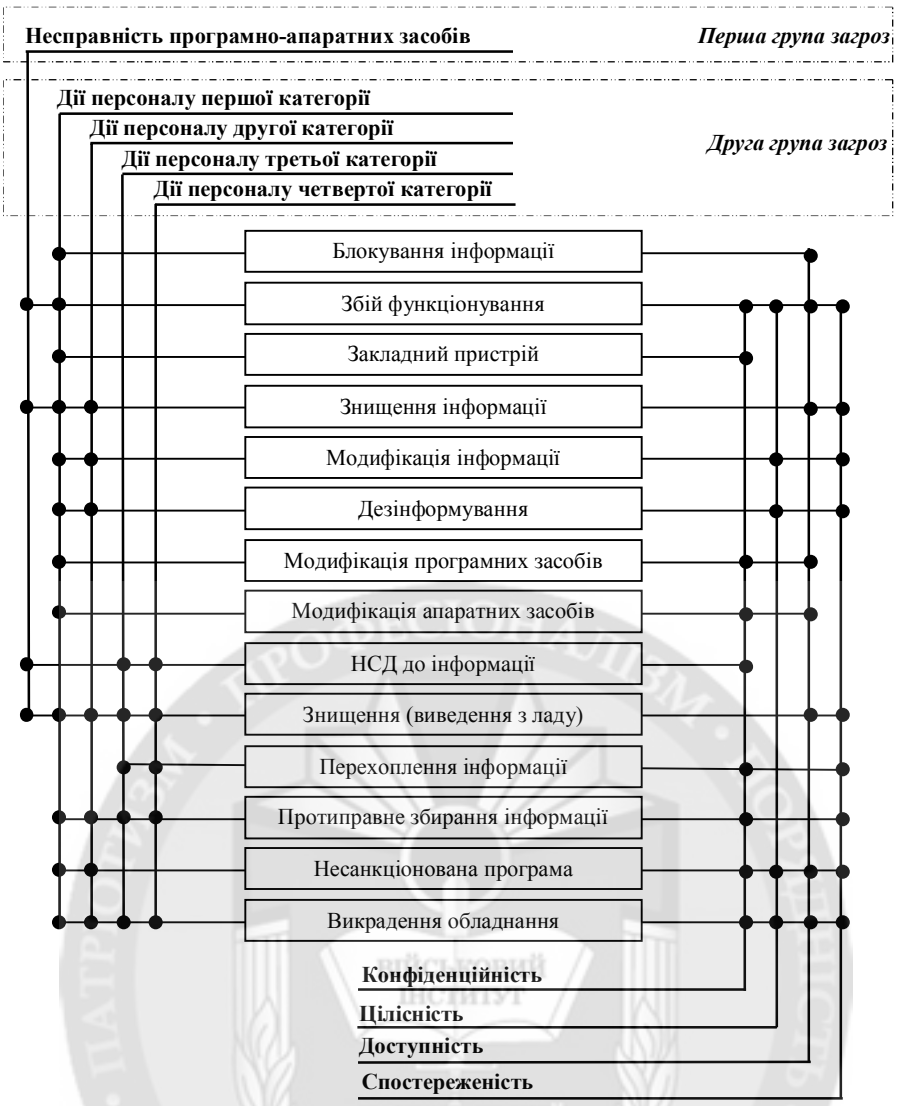

Рис. 1. Класифікація загроз надійності інформації, викликаних стадією модернізації ІІТС

До першої групи необхідно віднести загрози, пов'язані з надійністю програмно-технічних засобів ІІТС. Вони пов'язані з раптовим тимчасовим припиненням або порушенням роботи ІТС і ведуть до втрат інформації та управління об'єктами в ІТС управління.

До другої групи необхідно віднести загрози пов'язані з випадковими ненавмисними та навмисними діями користувачів, помилками адміністраторів, управлінського персоналу та інших і ведуть до модифікації (спотворення) чи знищення інформації, порушення виконання ІІТС своїх функцій, помилок в роботі програм і засобах управління безпекою ІТС, отримання особистих привілеїв і спрямовані на нанесення шкоди ІІТС. Дана група загроз є найбільш чисельною.

Загрози першої групи, як правило, обумовлені технічним станом апаратної складової гетерогенного середовища ІІТС та описуються відомими функціональними залежностями теорії надійності, тому в рамках цієї статті розглядатись не будуть. Розглянемо можливі реалізації загроз другої групи на надійність інформації на стадії модернізації ІІТС (таблиця 1), а саме:

1) маскування під законного користувача, за рахунок неузгодженості систем захисту інформації різних версій (відсутності такої в нових (старих) компонентах ІТС);

2) друк або виведення на екран (передавання в канал зв'язку) великого числа файлів (даних) з метою забезпечення витоку інформації по новим доданим каналам, які порушують системні правила розмежування доступу;

3) проникнення в систему управління захистом інформації з метою зміни її характеристик через загальне поле даних;

4) організація відмови для користувачів нової версії спеціального програмного забезпечення у використанні ресурсів старих версій;

5) передача інформації невірному користувачу через неузгодженість параметрів нової і старої ІТС;

6) умисне руйнування ресурсів при перенесенні їх у нове середовище;

7) введення некоректних даних через невідповідність форматів;

8) перехоплення чужих повідомлень;

9) незаконне копіювання або крадіжка носіїв інформації існуючої ІІТС;

10) викрадення або незаконне копіювання інформації із складових які були вилучені зі складу ІІТС в процесі модернізації (ремонту);

11) породження правдоподібних повідомлень або модифікація повідомлень, які передаються за рахунок вбудовування сторонніх обробників;

12) спотворення програм, впровадження вірусів і "троянських коней";

13) установка розвідувальної апаратури (закладок) в нові (існуючі) АПК;

14) спостереження за діями (результатом діяльності) авторизованих користувачів.

Таблиця 1

Реалізація загроз надійності інформації категоріями персоналу

Категорії персоналу	**Пункти реалізації загроз**													
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**
Перша	+	+	–	+	–	+	–	–	+	+	+	+	+	+
Друга	+	+	+	–	+	–	+	–	+	+	+	–	+	+
Третя	–	–	+	–	–	–	–	+	+	+	–	–	+	+
Четверта	–	–	–	–	–	–	–	+	+	+	–	–	–	+

Наочно, що персонал першої та другої категорії, який має безпосередній доступ до інформаційних ресурсів прикордонного відомства може реалізовувати найбільшу кількість загроз. Разом із тим, суворий відбір персоналу на посади, пов'язані з обробкою прикордонної інформації та контроль за їхніми діями дозволяє забезпечити надійність інформації на достатньому рівні. Особи третьої та четвертої категорій не контролюються відомчими підрозділами захисту інформації. Це створює передумови до серйозних загроз надійності інформації, зокрема складовим конфіденційності та спостережливості.

Висновки. Аналіз наведеного переліку загроз інформації в ІІТС властивих на стадії модернізації свідчить, що в цей період мають місце певні особливості, які дозволяють безконтрольно маніпулювати інформацією як персоналом ІІТС так і сторонніми особами, а також таємно отримувати доступ до оброблюваної інформації, навіть на значній відстані від АРМ.

В подальших дослідженнях пропонується сформувати аналітичні залежності між групами загроз та складовими надійності інформації: конфіденційності, цілісності, доступності та спостереженості.

ЛІТЕРАТУРА:

1. Основні напрями діяльності та подальшого розвитку Державної прикордонної служби України у 2015 році. Режим доступу: http://dpsu.gov.ua/ua/about/mission.htm

2. Наказ Державного комітету у справах охорони державного кордону України від 20 серпня 2002 р. № 474 «Про прийняття на озброєння військ програмних компонентів глобальної автоматизованої інформаційної системи прикордонних військ України (шифр „Гарт").

3. 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 наказу адміністрації Держспецзв'язку від 28.12.2012 № 806

4. Інформаційні системи і технології у фінансових установах. А.В. Олійник, В.М. Шацька - навчальний посібник - Львів: "новий світ-2000", 2006 - 436 с.

5. В. Мельников. Защита информации в компьютерных системах М.: Финансы и статистика, 1997. — 368 с.

6. Закон України "Про основи національної безпеки України" Відомості Верховної Ради України (ВВР), 2003

7. Указ Президента України Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про Стратегію національної безпеки України".

8. Магда Є. В. Виклики гібридної війни: інформаційний вимір / Є. В. Магда // Наукові записки Інституту законодавства Верховної Ради України. - 2014. - № 5. - С. 138-142

Рецензент: д.військ.н, с.н.с., Кириленко В.А. заступник ректора Національної академії ДПСУ імені Б. Хмельницького з навчальної та наукової роботи

к.т.н. доц. Стрельбицкий М.А.

КЛАССИФИКАЦИЯ УГРОЗ ИНФОРМАЦИИ В ИНТЕГРИРОВАННОЙ ИНФОРМАЦИОННО-ТЕЛЕКОМУНИКАЦИЩРРЩЙ СИСТЕМЕ ПОГРАНИЧНОГО ВЕДОМСТВА НА ЭТАПЕ МОДЕРНИЗАЦИИ

Функционирования интегрированной информационно-телекоммуникационной системы "Гарт" Государственной пограничной службы Украины осуществляется в условиях ведения против государства гибридной войны, реформирования системы государственного управления, сектора безопасности и обороны Украины, ее интеграции в европейское и мировое демократическое сообщество. Постоянное совершенствование существующих и внедрение новых информационно-телекоммуникационных систем выявляет проблему защиты информации и в условиях совместного использования как старых, так и новых версий программной и аппаратной среды. Первоочередным этапом в создании надежной и эффективной защиты информации в ведомственной корпоративной системе является анализ и классификация возможных угроз информации.

В статье на основании анализа условий функционирования ведомственной информационно-телекоммуникационной системы на стадии модернизации приведена классификация угроз надежности информации.

Ключевые слова: угроза информации, защита информации, интегрированная информационно-телекоммуникационная система.

Ph.D. Strelbitskiy M.A.

CLASSIFICATION OF THREATS TO INFORMATION IN OF INTEGRATED INFORMATION AND TELECOMMUNICATIONS SYSTEM BORDER AGENCY AT THE STAGE MODERNIZATION

Operation of integrated information and telecommunications system "Gart" State Border Service of Ukraine carried out in conditions of the hybrid war, the reform of public administration, defense and security sector of Ukraine and its integration into European and world democratic community. Continuous improvement of existing and introduction of new information and telecommunications systems reveals the problem of information security and in terms of sharing of both old and new versions of software and hardware environment. The primary step in creating a reliable and effective information security in departmental corporate system is the analysis and classification of possible threats to the information.

The article is based on analysis of operating conditions departmental information and telecommunication systems at the stage of upgrading the classification of threats to the reliability of the information.

Keywords: threat information, information security, integrated information-telecommunication system.