УДК 351.7:316.7

к.т.н., с.н.с. **Рогов П.Д.** (НУОУ)
д.т.н., доц. **Лисий М.І.** (НАДПСУ)
Добровольський А.Б. (НАДПСУ)

УДОСКОНАЛЕННЯ СИСТЕМИ БЕЗПЕКИ ОБ'ЄКТІВ ПІДВИЩЕНОЇ НЕБЕЗПЕКИ НА ОСНОВІ ТЕХНІЧНОЇ ТАКТИКИ

Розглянуто деякі питання комплексного підходу, концептуального напрямку охорони та захисту об'єктів критичної інформаційної інфраструктури держави на основі технічної тактики. Визначено, що перспективним напрямом удосконалення системи безпеки об'єктів підвищеної небезпеки є створення відомчих охоронно-інформаційних систем України з використанням інформаційних технологій, як багаторівневих систем збору, обробки та передавання інформації про стан безпеки об'єктів.

Ключові слова: інформаційна інфраструктура, безпека, технічна тактика

Аналіз останніх досліджень і публікацій. Стрімкий розвиток інформаційних технологій та їх широке використання у всіх сферах життєдіяльності держави призвели до того, що інформаційна інфраструктура держави стала об'єктом злочинної діяльності, з'явилося більше уразливих місць для протиправних посягань, злочинні та терористичні угруповання отримали можливість використання глобальної мережі для досягнення своїх цілей [1]. Через це проблема забезпечення безпеки інформаційної інфраструктури відіграє вирішальну роль в обороноздатності держави, її економічному та соціальному розвитку. Процеси глобальної інформатизації привели до того, що сучасне суспільство практично

повністю залежність від стану безпеки інформаційної інфраструктури [2; 3].

Постановка проблеми. Об'єкти підвищеної небезпеки є одними із елементів критичної інфраструктури держави та потребують надійного забезпечення їх охорони і захисту у будь-який час. Головною метою системи забезпечення охорони та захисту об'єктів підвищеної небезпеки є створення умов їх стійкого функціонування, попередження загроз, своєчасне виявлення протиправних дій, недопущення крадіжок, знищення або руйнування. Отже, невідповідність у потребі інформаційного забезпечення, джерелом якого є в першу чергу технічні засоби, тактики їх застосування та можливостями і забезпеченістю такими засобами, методиками їх використання щодо охорони та захисту об'єктів критичної інформаційної інфраструктури держави становить сутність проблемного питання.

Критична інформаційна інфраструктура держави - частина інформаційної інфраструктури держави, сукупність інформаційно-телекомунікаційних систем, державного та приватного сектору, що забезпечують функціонування та безпеку стратегічних об'єктів (інститутів, систем) держави і безпеку громадян, виведення з ладу, руйнація або несанкціоноване втручання в роботу яких матиме згубні наслідки для національної безпеки (національних інтересів) держави. Тому, потребує розгляд окремих питань щодо розвитку технічної тактики охорони та захисту об'єктів критичної інформаційної інфраструктури держави, що окреслило **мету роботи.**

Виклад основного матеріалу. Об'єкт критичної інформаційної інфраструктури – елемент інформаційної інфраструктури держави, інформаційні, телекомунікаційні та інформаційно-телекомунікаційні системи, порушення функціонування, виведення з ладу або руйнація яких матиме згубні наслідки для національної безпеки держави чи завдасть шкоди її міжнародному іміджу.

До критичних об'єктів інформаційної інфраструктури відносяться: інформаційні, телекомунікаційні та інформаційно-телекомунікаційні системи реального часу (спостереження, навігації, автоматизації управління технологічними процесами, системи військового призначення), а також інформаційні ресурси та системи управління національної транспортної системи, енергетичної системи, фінансової системи, оборонно-промислового комплексу, хімічного виробництва, медицини катастроф, цивільного захисту населення, галузі освіти та науки, засобів масової інформації тощо.

Основними напрямами підвищення рівня захищеності об'єктів критичної інфраструктури держави є:

забезпечення комплексного підходу до вирішення завдань безпеки з урахуванням необхідності диференціювання її рівнів;

розробка моделей загроз безпеки (паспортів небезпек – викликів, загроз, впливів);

визначення технічних вимог і критеріїв категорування об'єктів критичної інфраструктури (у тому числі – оцінка уразливості зазначених об'єктів);

створення державного реєстру (державної системи паспортизації) об'єктів критичної інфраструктури, розробка заходів і засобів їх захисту;

забезпечення ефективного моніторингу стану безпеки;

вдосконалення нормативно-правової та методичної бази (концепцій) в області захисту об'єктів критичної інфраструктури;

створення ефективно діючої системи раннього виявлення та протидії негативним впливам.

Комплексний підхід до забезпечення інформаційної безпеки передбачає єдність концептуальних, теоретичних і технологічних основ її забезпечення на інформаційному рівні безпеки всіх сфер державної та суспільної діяльності (політичної, економічної, соціальної, воєнної, екологічної, духовної тощо), а також сфер формування, обігу, накопичення і використання інформації (інформаційний простір, інформаційні ресурси, інформаційно-аналітичне забезпечення органів державного управління у всіх різновидах діяльності тощо).

Концепція захисту об'єктів критичної інформаційної інфраструктури держави має бути офіційно прийнятою системою поглядів на проблему забезпечення інформаційної безпеки

України в цілому та захисту критичної інформаційної інфраструктури та представляти собою систематизоване викладання цілій і завдання, принципи, джерела загроз та потенційні загрози, методи запобігання і нейтралізації інформаційних впливів, об'єкти захисту критичної інформаційної інфраструктури держави та суб'єкти, а також основи узгодженої державної політики ресурсного забезпечення, роль та місце державного та недержавного сектору проведення державної інформаційної політики і забезпечення інформаційної безпеки, повноваження та відповідальність за стан та забезпечення захисту об'єктів критичної інформаційної інфраструктури держави.

Широке використання різноманітних технічних засобів та систем обумовлює розроблення "технічної тактики" охорони і захисту об'єктів підвищеної небезпеки, яка розробляється власниками об'єктів [4].

Структура системи охорони і захисту повинна бути: гнучкою; мати відкриту архітектуру; будуватися у взаємозв'язку з тактико-технічними характеристиками та у кількісному відношенні (показникам) засобів і систем як одне ціле, тобто – бути комплексною (інтегрованою) системою безпеки.

Основу такої комплексної системи безпеки становлять засоби виявлення, системи дистанційного спостереження (радіолокаційні засоби, розвідувально-сигналізаційні системи, безпілотні авіаційні комплекси розвідувального типу, тепловізійні системи тощо), системи передавання інформації і управління. Прикладом успішної інтеграції технічної системи охорони в систему інтегрованого управління кордонами є Система оптико-електронного спостереження, що встановлена на державному кордоні України з Молдовою. Використання засобів розвідки (систем виявлення, дистанційного спостереження та ін.) реалізує перший принцип "технічної тактики" - "війна починається з розвідки", який незважаючи на усю очевидність часто забувають.

Для забезпечення ефективного функціонування комплексної системи безпеки кордону доцільним є комплексування принципів контролю сухопутного кордону [5]. При цьому підвищення достовірності інформації в основному визначається властивістю завадостійкого виявлення правопорушника і здійснюється за рахунок:

1) підвищення точності визначення місцеположення об'єкта при комплексуванні функцій контролю на основі різних принципів виявлення;

2) ідентифікації впливу правопорушника на чутливий елемент при комплексуванні принципів контролю.

Основою побудови комплексної системи безпеки є базові принципи: безперервного моніторингу та прогнозування можливих загроз; відповідності заходів; достатності сил реагування; превентивного забезпечення; аналогій (технічний) тощо.

При розробленні системи захисту об'єктів критичної інфраструктури необхідно визначити та виділити основоположні складові концепції їх захисту, які витікають із відповідей на такі запитання:

що або хто підлягає захисту;

які з загроз є пріоритетними;

від кого або чого потрібно захищати;

як необхідно захищати (розвідка, прогнозування, виявлення, заходи у відповідь, припинення та ліквідація впливів, усунення їх наслідків, мінімізація ризиків тощо);

хто має захищати;

наскільки ефективна система захисту об'єкта відносно до можливих протиправних дій;

наскільки система захисту кожного об'єкту відповідає сучасним вимогам?

Суттєвим є те, що саме друге питання зазначеного переліку окреслює першочерговість заходів щодо упередження виникнення найбільш суттєвих, небезпечних загроз національній безпеці держави.

Зіставлення опису загроз національної безпеки держави, які подано у Законі та низці робіт встановлено неоднозначність віднесення окремих загроз до різних сфер впливу, що може привести до неадекватних рішень. Зазначене пояснюється тим, що:

загрозам притаманна комплексність впливу на різні сфери безпеки;

класифікація загроз не має поділу на сфери контролю і сфери реалізації загроз;

державна сфера по суті є сукупністю всіх сфер національної безпеки держави, крім, можливо, релігійної, а тому є, очевидно, надлишковим елементом класифікації [5].

Щодо сфер безпеки, то звісно це воєнна сфера, оскільки реалізація загрози у цій сфері приведе до знецінення здобутків у інших сферах національної безпеки. Зазначене потребувало введення топологічної класифікаційної ознаки загроз, а саме поділу на сфери контролю (виявлення) і сфери реалізації (впливу) загроз, рис. 1 [5].

Рис. 1. Класифікаційна ознака розподілу загроз національній безпеці держави на загрози, які реалізуються і які контролюються у визначених сферах

Перспективним напрямом удосконалення системи безпеки об’єктів підвищеної небезпеки є створення відомчих охоронно-інформаційних систем України з використанням інформаційних технологій, як багаторівневих систем збору, обробки та передавання інформації про стан безпеки об’єктів, виклики та потенційні можливі і реальні загрози щодо їх функціонування до суб’єктів реагування на них від міністерств та відомств України. Прикладом успішної реалізації такого підходу є функціонування глобальної автоматизованої інформаційної системи “Гарт” в Державній прикордонній службі України. Структуровані складові системи дозволяють автоматизовано визначати пріоритетність ризиків і загроз, зіставляти окремі події з варіантами можливого розвитку.

Висновки. Комплексний підхід до забезпечення інформаційної безпеки передбачає єдність концептуальних, теоретичних і технологічних основ її забезпечення на інформаційному рівні безпеки всіх сфер державної та суспільної діяльності.

Концепція захисту об’єктів критичної інформаційної інфраструктури держави має бути офіційно прийнятою системою поглядів на проблему забезпечення інформаційної безпеки України в цілому.

Перспективним напрямом удосконалення системи безпеки об’єктів підвищеної небезпеки є створення відомчих охоронно-інформаційних систем України з використанням інформаційних технологій, як багаторівневих систем збору, обробки та передавання інформації про стан безпеки об’єктів.

ЛІТЕРАТУРА:

1.Городнов В.П. Теоретичні основи інформаційно-аналітичного забезпечення процесів охорони державного кордону (у контексті завдань національної безпеки України в прикордонній сфері) : монографія / В.П. Городнов, Д.В. Іщенко, В.А. Кириленко. − Хмельницький: Вид-во НАДПС України, 2009. − 472 с.

2.Богданович В.Ю. Методологические основы системных исследований проблем военной безопасности государства / В.Ю. Богданович, А.Я. Маначинский. − К., 2001. – 172 с.

3.Информационно-аналитическая деятельность в управлении пограничными органами Федеральной службы безопасности: учебник. − М. : Граница, 2005. − 190 с.

4.Лисий М.І. Технічна тактика охорони і захисту військових об'єктів підвищеної небезпеки як елементів критичної інформаційної інфраструктури держави у воєнній сфері / Лисий М. І., Рогов П.Д. // Військова освіта та наука : сьогодення і майбутнє : IX Міжнар. наук.-практ. конф., 22 листопада 2013 р. : тезы. – К. : ВІКНУ. – С 51.

5.Лисий М.І. Встановлення ознаки пріоритетності загроз воєнній безпеці держави при їх моніторингу у різних сферах діяльності / Лисий М.І. // Військова освіта та наука : сьогодення і майбутнє: VIII Міжнар. наук.-практ. конф., 23 листопада 2012 р.: тези доп. – К.: ВІКНУ. – С. 296–297.

Рецензент: д.військ.н., с.н.с. Кириленко В.А., Національна академія Державної прикордонної служби України, м. Хмельницький.

к.т.н., с.н.с. Рогов П.Д., д.т.н., доц. Лысый Н.И., Добровольский А.Б.

СОВЕРШЕНСТВОВАНИЕ СИСТЕМЫ БЕЗОПАСНОСТИ ОБЪЕКТОВ ПОВЫШЕННОЙ ОПАСНОСТИ НА ОСНОВЕ ТЕХНИЧЕСКОЙ ТАКТИКИ

Рассмотрены некоторые вопросы комплексного подхода, концептуального направления охраны и защиты объектов критической информационной инфраструктуры государства на основе технической тактики. Определено, что перспективным направлением усовершенствования системы безопасности объектов повышенной опасности является создание ведомственных охранительно-информационных систем Украины с использованием информационных технологий, как многоуровневых систем сбора, обработки и передачи информации о состоянии безопасности объектов.

Ключевые слова: информационная инфраструктура, безопасность, техническая тактика

P. Rogov, M. Lysyi, A. Dobrovolskyi

IMPROVING THE SECURITY OF HIGH-RISK FACILITIES ON THE BASIS OF TECHNICAL TACTICS

Some questions of complex approach, conceptual direction of protection of objects of critical state information infrastructure are considered on the basis of technical tactics. It is determined that prospective direction of enhancing of vulnerable objects security is oriented towards agency protective and information systems of Ukraine using information technologies, as multi-staged systems of collection, processing and transmitting of information on objects security state.

Keywords: information safety, security, technical tactics.