УДК 341.824:338.47 (043.2)

Рогов П. Д., к.т.н.;
Ворович Б. О., к.військ.н., доцент;
Ткаченко В. А., к.військ.н.

[1]Центр воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського, Київ;

Шляхи забезпечення кібернетичної безпеки об'єктів критичної інформаційної інфраструктури держави у воєнній сфері

Резюме. В статті розглянуто питання кібернетичної безпеки об'єктів критичної інформаційної інфраструктури, які є суттєвими в обороноздатності держави, її економічному та соціальному розвитку. Визначені принципи та шляхи покращення захисту об'єктів критичної інформаційної інфраструктури держави.

Ключові слова: безпека інформаційної інфраструктури, критична інформаційна інфраструктура держави, об'єкти критичної інформаційної інфраструктури держави, паспортизація об'єктів критичної інформаційної інфраструктури.

Постановка проблеми. У XXI столітті спостерігається подальший динамічний розвиток воєнних технологій, які суттєво впливають та визначають форми і способи ведення бойових дій. На сьогодні інформаційний простір поряд із сушею, морем, повітрям та космосом активно використовується у військовому протиборстві. Стає очевиднішим, що чим більше можливості в інформаційній сфері, тим більше політичні та воєнні переваги. Тому проблеми формування ефективної системи протидії інформаційним загрозам, зокрема кіберзагрозам у сфері оборони держави, стають вкрай актуальними з огляду на процеси реформування та розвитку ЗС України.

Інформаційний простір, ресурси, інфраструктура та технології, значною мірою впливають на рівень воєнного потенціалу держави та її збройних сил. Сьогодні, як ніколи, інформаційна компонента в стратегії забезпечення національної та воєнної безпеки держави вийшла на перший план [1, 4, 12].

Це обумовлено наступним:

результати руйнування та дезорганізація інформаційної інфраструктури держави порівнюються з наслідками застосування зброї масового ураження;

в умовах припинення холодної війни і нормалізації міждержавних відносин у традиційній військовій сфері, центр тяжіння протиборства розвинених держав переміщується до інформаційної сфери;

засоби, які використовуються для негативного впливу на інформаційні та телекомунікаційні системи, стали доступними не лише державним спецслужбам, але і окремим кримінальним та терористичним угрупованням, внаслідок чого проблема забезпечення інформаційної безпеки стала міжнародною і порівняною з глобальною економічною та екологічною безпекою.

Стрімкий розвиток інформаційних технологій та глобалізація Інтернету 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. Через це проблема забезпечення безпеки інформаційної інфраструктури є суттєвою в обороноздатності держави, її економічному та соціальному розвитку. Процеси глобальної інформатизації привели до того, що сучасне суспільство практично повністю залежить від стану безпеки інформаційної інфраструктури.

Кіберпростір поступово перетворюється на окрему, поряд із традиційними "земля", "повітря", "море" та "космос", сферу ведення бойових дій, у якій все активніше діють відповідні підрозділи збройних сил провідних держав світу [4]. З урахуванням широкого застосування сучасних інформаційних технологій у секторі безпеки і оборони, створення єдиної автоматизованої системи управління Збройних Сил України кібероборона нашої держави стає уразливішою до кіберзагроз.

У Конституції України забезпечення інформаційної безпеки названо серед найважливіших функцій держави, справою

всього українського народу (ст. 17). Сферу інформаційної безпеки регламентують чинні нормативно-правові документи: Конституція України; Стратегія національної безпеки України (у редакції Указу Президента України від 26 травня 2015 року № 287/2015); Концепція розвитку сектору безпеки і оборони України, введена в дію Указом Президента України від 14 березня 2016 року № 92/2016); Воєнна доктрина України, затверджена Указом Президента України від 24 вересня 2015 року; Стратегія кібербезпеки України (у редакції Указу Президента України від 15 березня 2016 року № 96/2016); Стратегічний оборонний бюлетень України (введений в дію Указом Президента України від 6 червня 2016 року № 240/2016); Стратегія комунікацій Збройних Сил України, затверджена наказом Міністра оборони України від 30 вересня 2015 року; ратифіковані міжнародні угоди, зокрема, Конвенція про кіберзлочинність [12].

На сьогодні загрози кібербезпеці актуалізуються через дію таких чинників:

недостатній рівень захищеності критичної інфраструктури, державних електронних інформаційних ресурсів та інформації від кіберзагроз;

безсистемність заходів кіберзахисту критичної інфраструктури;

недостатній розвиток організаційно-технічної інфраструктури забезпечення кібербезпеки та кіберзахисту критичної інфраструктури і державних електронних інформаційних ресурсів.

Великої актуальності набувають дії в кібернетичному просторі. Інтелектуальний вплив на інформаційні та телекомунікаційні мережі з метою порушення функціонування системи управління військами і зброєю відкриває широкі асиметричні можливості щодо зниження бойового потенціалу противника.

Стратегія кібербезпеки України (далі - Стратегія) має за мету створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави [4].

Для досягнення цієї мети необхідними є:

створення національної системи кібербезпеки;

посилення спроможностей суб'єктів сектору безпеки і оборони для забезпечення ефективної боротьби з кіберзагрозами воєнного характеру, кібершпигунством, кібертероризмом та кіберзлочинністю, поглиблення міжнародного співробітництва у цій сфері;

забезпечення кіберзахисту державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, а також інформаційної інфраструктури, яка знаходиться під юрисдикцією України та порушення сталого функціонування якої матиме негативний вплив на стан національної безпеки і оборони України (критична інформаційна інфраструктура).

Аналіз останніх досліджень і публікацій. Для фахівців в інформаційній сфері відомі погляди вітчизняних та закордонних вчених Бірюкова Д.С., Грачева Г.В., Дубова Д.В., Кондратова С.І., Турка Н.І., Устименка О.В., Манойла А.В., Петренка А.І., Фролова Д.Б, Прохожева А.А., Литвиненка О.В., Почепцова Г.Г., Козер Л. та ін. [6, 11-14].

Аналіз робіт показує, що у сучасних умовах розвитку особи, суспільства, держави роль та місце інформаційної складової діяльності підвищується, набуває дедалі ще більшої ваги і стає одним із найважливіших елементів забезпечення її національної безпеки, інформаційної безпеки тощо.

Враховуючи, що останнім часом інформаційні війни постійно удосконалюються, змінюються і все більше використовуються для досягнення політичних, економічних та воєнних цілей, це питання вимагає поглибленого вивчення, системності й постійності.

Приклади багатьох країн світу (США, країни ЄС, Південна Корея тощо) з розвиненою інформаційною інфраструктурою свідчать про значне збільшення залежності соціально-економічної стабільності, національної безпеки, інформаційної та кібербезпеки загалом від рівня захищеності інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем. Одним із важливіших завдань є розроблення і реалізація заходів щодо запобігання, усунення та нейтралізації загроз інтересам держави, суспільства та правам громадян у сфері інформаційної безпеки.

Віртуальний простір глобальних інформаційних мереж стає стратегічним полем бою, яке докорінно змінює геополітичні та військово-політичні пріоритети. Вже немає гострої необхідності завойовувати територію та тримати її під контролем. Кібератаки є набагато дешевші та ефективніші за "класичні" війни. Достатньо вивести з ладу не самі командні центри, а системи та лінії управління цивільної і військової інформаційної інфраструктури держави для того, аби розпочався некерований

процес, тобто хаос.

Науковці та військові аналітики відзначають такі фактори, що обумовили вказану ситуацію [6, 11, 12]:

зміна змісту головної мети війни, яка тепер спрямована на подавлення волі противника до опору, руйнування його політичного, воєнно-економічного та морально-психологічного потенціалу, з подальшим встановленням лояльного політичного режиму;

висока бойова ефективність високоточної зброї та засобів інформаційного впливу (особливо інформаційно-психологічного), що визначило домінуючу роль електронно-вогневої та інформаційної операцій, створення високоефективних засобів інформаційного впливу (протиборства) і високоточної зброї з елементами "штучного інтелекту";

зростаюче неприйняття суспільством силових методів вирішення міжнародних суперечок, що вимагає заміну традиційних засобів ураження на нові більш ефективні: інформаційні, енергетичні, біотехнічні, нелетальні тощо.

Метою статті є розроблення методичних підходів щодо забезпечення кібернетичної безпеки об'єктів критичної інформаційної інфраструктури, які є вирішальними в обороноздатності держави, її економічному та соціальному розвитку.

Виклад основного матеріалу. Чинними нормативно-правовими документами визначені такі основні терміни та визначення їх понять, які використовуються в статтях [1-5, 8-10].

Кібернетична безпека (кібербезпека) - стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі.

Кібернетичний захист – сукупність методів і заходів організаційного, нормативно-правового та технічного характеру, спрямованих на забезпечення кібернетичної безпеки.

Примітка. Здійснюється шляхом захисту елементів інформаційної інфраструктури, які утворюють власний кібернетичний простір (автоматизовані системи управління, інформаційні системи моделювання та підтримки рішень, інформаційно-телекомунікаційні системи тощо) від деструктивних інформаційних дій.

Критична інфраструктура - сукупність об'єктів інфраструктури держави, які є найбільш важливими для економіки та промисловості, функціонування суспільства та безпеки населення і виведення з ладу або руйнування яких може мати суттєвий вплив на національну безпеку і оборону, природне середовище та призвести до значних фінансових збитків і людських жертв.

Об'єкти критичної інфраструктури - підприємства та установи (незалежно від форми власності) таких галузей як енергетика, хімічна промисловість, транспорт, банки та фінанси, інформаційні технології та телекомунікації (електронні комунікації), продовольство, охорона здоров'я, комунальне господарство, що є стратегічно важливими для функціонування економіки і безпеки держави, суспільства та населення.

Кібератака – несанкціоновані дії, що здійснюються з використанням інформаційно-комунікаційних технологій та спрямовані на порушення конфіденційності, цілісності і доступності інформації, яка обробляється в інформаційно-телекомунікаційній системі, або порушення сталого функціонування такої системи;

Інші терміни вживаються у значенні, наведеному в Законах України "Про основи національної безпеки", "Про оборону України", "Про інформацію", "Про телекомунікації", "Про захист інформації в інформаційно-телекомунікаційних системах".

Заходи кібернетичного захисту спрямовані на захист власних автоматизованих систем управління, систем управління зброєю та критичної інфраструктури від кібератак і кіберударів противника, попередження спроб реалізації та нейтралізація виявлених кіберзагроз, виявлення і блокування вбудованих програмних та програмно-апаратних закладних засобів, реалізації антивірусного захисту, проведення контролю (моніторингу) стану кібернетичної безпеки та її забезпечення в інформаційно-телекомунікаційних системах воєнного призначення.

Державна інформаційна політика у сфері кібероборони – це діяльність суб'єктів забезпечення кібероборони, пов'язана із запобіганням кібервійні та воєнним конфліктам у кіберпросторі, організацією та здійсненням підготовки Збройних Сил України, Державної служби спеціального зв'язку та захисту інформації України, інших утворених відповідно до законів України військових формувань, державних, розвідувальних органів, а також правоохоронних органів спеціального призначення до кібероборони держави.

До основних об'єктів критичної інформаційної інфраструктури можна віднести системи управління в: уряді; обороні; охороні

здоров'я; соціальному захисті; інформатизації; кредитно-фінансовій і банківській системі; науково-дослідному секторі; промисловості; енергетиці, у тому числі атомної; нафтовому виробництві; сільському господарстві; громадському харчуванні; транспорті; водопостачанні; комунальному господарстві; телекомунікації; цивільній обороні.

До об'єктів критичної інформаційної інфраструктури України, які у першу чергу потребують захисту, можна віднести інформаційні системи та засоби спостереження, навігації, автоматизації управління технологічними процесами, інформаційно-телекомунікаційні системи, а також інформаційні ресурси та системи управління суб'єктів сектору безпеки і оборони України, національної транспортної системи, енергетичної системи, фінансової системи, оборонно-промислового комплексу, хімічного виробництва, медицини, цивільного захисту населення тощо.

До об'єктів критичної інформаційної інфраструктури у сфері оборони, на нашу думку, можна віднести:

системи управління центральних органів військового управління, органів управління видів Збройних Сил України та родів військ, об'єднань, з'єднань, військових частин і організацій, що входять до Збройних Сил України, державних підприємств Міністерства оборони України;

інформаційні ресурси підприємств оборонного комплексу і провідних науково-дослідних установ, що виконують державні оборонні замовлення або займаються оборонною проблематикою;

програмно-технічні засоби автоматизованих і автоматичних систем керування військами та зброєю, озброєння і військової техніки, оснащених засобами інформатизації;

інформаційні ресурси, системи зв'язку та інформаційна інфраструктура інших військ, військових формувань і органів;

військові об'єкти підвищеної небезпеки (арсенали, бази і склади зберігання озброєння, ракет, боєприпасів, компонентів ракетного палива та пального Збройних Сил України).

Метою інформаційної діяльності суб'єктів забезпечення кібернетичної безпеки держави є попередження, своєчасне виявлення та запобігання зовнішнім і внутрішнім кіберзагрозам безпеці об'єктів критичної інформаційної інфраструктури держави, усунення умов, що їм сприяють, та причин їх виникнення.

Основу національної системи кібербезпеки становитимуть Міністерство оборони України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція України, Національний банк України, розвідувальні органи, на які мають бути покладені в установленому порядку такі основні завдання [4]:

на Міністерство оборони України, Генеральний штаб Збройних Сил України відповідно до компетенції - здійснення заходів з підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборона); здійснення військової співпраці з НАТО, пов'язаної з безпекою кіберпростору та сумісним захистом від кіберзагроз; забезпечення у взаємодії з Державною службою спеціального зв'язку та захисту інформації України і Службою безпеки України кіберзахисту власної інформаційної інфраструктури;

на Державну службу спеціального зв'язку та захисту інформації України - формування та реалізація державної політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту критичної інформаційної інфраструктури, державний контроль у цих сферах; координація діяльності інших суб'єктів кібербезпеки щодо кіберзахисту; здійснення організаційно-технічних заходів із запобігання, виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків, інформування про кіберзагрози та відповідні методи захисту від них; забезпечення функціонування державного центру кіберзахисту; проведення аудиту захищеності об'єктів критичної інформаційної інфраструктури на вразливість;

на Службу безпеки України - попередження, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, які вчиняються у кіберпросторі; здійснення контррозвідувальних та оперативно-розшукових заходів, спрямованих на боротьбу з кібертероризмом та кібершпигунством, а також щодо готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів; протидія кіберзлочинності, можливі наслідки якої безпосередньо створюють загрозу життєво важливим інтересам України; розслідування кіберінцидентів та кібератак щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної

інфраструктури; забезпечення реагування на комп'ютерні інциденти у сфері державної безпеки;

на Національну поліцію України - забезпечення захисту прав і свобод людини та громадянина, інтересів суспільства і держави від злочинних посягань у кіберпросторі; запобігання, виявлення, припинення та розкриття кіберзлочинів; підвищення інформованості громадян про безпеку в кіберпросторі;

на Національний банк України - формування вимог щодо кіберзахисту критичної інформаційної інфраструктури у банківській сфері;

на розвідувальні органи України - здійснення розвідувальної діяльності щодо загроз національній безпеці України у кіберпросторі, інших подій і обставин, що стосуються сфери кібербезпеки.

До основних напрямів підвищення рівня захищеності об'єктів критичної інформаційної інфраструктури держави можна віднести:

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

розроблення загальної моделі загроз інформаційній безпеці (паспортів інформаційних небезпек – викликів, загроз, впливів);

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

створення державного реєстру (державної системи паспортизації) об'єктів критичної інформаційної інфраструктури, розроблення заходів щодо їх захисту і засобів технічного нагляду за дотриманням відповідних вимог;

забезпечення ефективного моніторингу стану інформаційної безпеки;

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

розвиток і вдосконалення захищених засобів обробки інформації загального застосування, а також систем їх аудиту;

створення ефективно діючої системи виявлення та протидії негативним інформаційно-психологічним впливам.

Слід зазначити, що у зв'язку з реалізацією Стратегії кібербезпеки України, Рада національної безпеки і оборони України ухвалила рішення про створення спеціального робочого органу – Національного координаційного центру кібербезпеки.

Стратегія кібербезпеки України визначає, зокрема, такі основні пріоритети для безпечного, стабільного і надійного кіберпростору в Україні:

розроблення та оперативна адаптація державної політики у сфері кібербезпеки, досягнення сумісності з відповідними стандартами ЄС і НАТО;

створення національної нормативно-правової та термінологічної основи в цій сфері, гармонізація нормативних актів у сфері електронних комунікацій, захисту інформації, інформаційної та кібербезпеки відповідно до міжнародних стандартів та стандартів ЄС і НАТО;

розроблення технологій кібербезпеки мобільних засобів зв'язку;

розвиток електронної інфраструктури зв'язку;

розвиток і вдосконалення системи державного контролю інформаційної безпеки, а також незалежний аудит системи інформаційної безпеки;

розроблення мережі команд реагування на комп'ютерні надзвичайні ситуації;

розвиток міжнародного співробітництва у сфері кібербезпеки, підтримка міжнародних ініціатив у сфері кібербезпеки, які відповідають національним інтересам України, активізація співробітництва між Україною та ЄС і НАТО з метою зміцнення можливостей України у сфері кібербезпеки.

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). Предметом методології інформаційної безпеки є дослідження способів, методів, засобів та каналів реалізації загроз національним інтересам на інформаційному рівні, їх своєчасного виявлення, запобігання і нейтралізації.

Державна інформаційна політика у сфері кібербезпеки має бути спрямована на:

вироблення та адаптацію державної політики у сфері кібербезпеки, спрямованої на розвиток кіберпростору воєнної сфери, досягненні сумісності з відповідними стандартами ЄС та НАТО;

створення вітчизняної та відомчої нормативно-правової і термінологічної бази у цій сфері, гармонізацію нормативних документів у сфері електронних комунікацій, захисту інформації, інформаційної та кібербезпеки відповідно до міжнародних стандартів і стандартів ЄС та НАТО;

підвищення інформаційної грамотності обслуговуючого персоналу та культури безпекового поводження в кіберпросторі, комплексних знань, навичок і здібностей, необхідних для підтримки цілей кібербезпеки, впровадження державних проектів підвищення рівня обізнаності особового складу бойових обслуг щодо кіберзагроз та кіберзахисту (кібероборони);

періодичне проведення навчань щодо реагування на можливі надзвичайні ситуації та інциденти у кіберпросторі;

розвиток та удосконалення системи контролю за станом захисту інформації в телекомунікаційних системах, а також запровадження кращих світових практик і міжнародних стандартів із питань кібербезпеки та кіберзахисту (кібероборони);

покращення інформаційно-аналітичної діяльності (роботи) в інтересах кібербезпеки держави у воєнній сфері (сфері оборони);

кіберрозвідку (моніторинг) кіберпростору, оперативне виявлення потенційних та реальних кіберзагроз національній безпеці та обороні України, проведення аналізу воєнно-політичної та інформаційної (кібернетичної) обстановки та визначення рівня потенційної (реальної) загрози національній безпеці України з використанням кіберпростору;

підготовку об'єктів критичної інформаційної інфраструктури держави до функціонування в особливий період та умовах воєнного стану.

Водночас, помітна недооцінка методів управління кібернетичною безпекою, які дають змогу структурувати проблеми, відбирати показники, оптимізувати рішення, що приймаються. Часто про управління безпекою навіть не згадують, обговорюючи забезпечення безпеки взагалі та ігноруючи той факт, що вирішити проблеми безпеки (кіберзахисту) важливих телекомунікаційних та інформаційних систем неможливо без вирішення завдань управління ними, таких як побудова моделей загроз, виявлення впливів, оцінка та аналіз ризиків, побудова моделей і профілів захисту, контроль виконання вимог щодо безпеки.

Розроблені й прийняті до виконання, у тому числі в Україні, міжнародні стандарти в області інформаційної та кібернетичної безпеки, такі як ISO 15408, ISO 27001, дають змогу сформувати певну культуру в забезпеченні кібербезпеки.

Забезпечення необхідного рівня інформаційної безпеки об'єктів критичної інформаційної інфраструктури має бути засновано на використанні єдиних вимог захисту інформації від несанкціонованого доступу або зміни, дії деструктивних інформаційних впливів, а також сертифікованих засобів попередження і виявлення інформаційних небезпек та захисту інформації, що постачаються підприємствами, які отримали в установленому порядку необхідні ліцензії (дозволи).

Для реалізації комплексного підходу щодо забезпечення інформаційної безпеки необхідне розроблення Концепції захисту об'єктів критичної інформаційної інфраструктури держави та реалізація практичних заходів щодо її забезпечення [13].

Концепція має бути офіційно прийнятою системою поглядів на проблему забезпечення інформаційної безпеки України в цілому та захисту критичної інформаційної інфраструктури і представляти собою систематизоване викладання цілей і завдань, принципів, джерел загроз; методів запобігання і нейтралізації інформаційних впливів; об'єкти та суб'єкти захисту критичної інформаційної інфраструктури держави; основи узгодженої державної політики ресурсного забезпечення; роль та місце державного і недержавного сектору проведення державної інформаційної політики та забезпечення інформаційної безпеки; повноваження і відповідальність за стан та забезпечення захисту об'єктів критичної інформаційної інфраструктури держави.

Концепція повинна становити основу для формування єдиної державної інформаційної політики (діяльності), розроблення і проведення заходів, зокрема превентивних, щодо захисту національних інформаційних ресурсів, інформаційного середовища, інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури сектору безпеки і оборони України.

Положення цієї Концепції мають бути враховані при:

формуванні і реалізації державної інформаційної політики (діяльності) в галузі захисту об'єктів критичної інформаційної інфраструктури держави;

розробленні плану заходів та вдосконалення системи ресурсного забезпечення захисту об'єктів критичної інформаційної інфраструктури держави;

розробленні та реалізації цільових програм забезпечення інформаційної безпеки України та заходів захисту об'єктів критичної інформаційної інфраструктури держави.

При розробленні Концепції захисту об'єктів критичної інформаційної інфраструктури держави слід враховувати, що на зміну принципам управління у багатьох галузях інформаційної діяльності, заснованим на централізації, все більше уваги приділяється управлінню, коли в його основі не тільки звиклі об'єкти (людина, машина, зразок техніки, системи тощо), але і ситуація, в якій здійснюється їх діяльність або функціонування. Інформаційне забезпечення слід ретельно враховувати при прийнятті рішень стосовно інформаційної сфери та сфери безпеки.

Включені до переліку інформаційно-телекомунікаційні системи об'єктів критичної інфраструктури є критичною інформаційною інфраструктурою держави, що захищається від кібератак у першу чергу (пріоритетно).

Захист інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави від кібератак забезпечується власником (розпорядником) таких систем відповідно до законодавства у сфері захисту інформації та кібербезпеки.

Можливими шляхами покращення захисту об'єктів критичної інформаційної інфраструктури держави можуть бути [6, 11, 12]:

створення систем раннього виявлення інформаційних небезпек (викликів, загроз, впливів);

створення ефективної системи захисту об'єктів критичної інформаційної інфраструктури з урахуванням їх категорій за ступенем уразливості;

підвищення ефективності інформаційно-аналітичної роботи;

створення бази даних порушників (порушень), у тому числі кіберзлочинців (кібертерористів).

Також необхідно створити умови для дотримання режиму експортного контролю та нерозповсюдження несертифікованих програмно-апаратних засобів та систем, комп'ютерної техніки, оперативного реагування на інциденти, які пов'язані з виведенням із ладу телекомунікаційних систем оборонного сектору; створення каналів формального і неформального обміну інформацією про загрозу комп'ютерної злочинності та кібертероризму.

Оцінку ефективності систем захисту об'єктів критичної інформаційної інфраструктури у сучасних методиках рекомендується проводити з використанням програмних комплексів, які вимагають великого обсягу фактичної інформації про стан захисту об'єкта критичної інформаційної інфраструктури.

Для реалізації цілей і завдань проведення державної політики у інформаційному просторі щодо захисту об'єктів критичної інформаційної інфраструктури держави відповідні суб'єкти забезпечення інформаційної безпеки повинні керуватися такими принципами:

принцип безперервного моніторингу та прогнозування можливих загроз, який полягає в збиранні інформації щодо соціально-політичної, технологічної, кримінальної та іншої обстановки в інформаційному (кібернетичному тощо) просторі, її своєчасному аналізі стосовно змін у досягнутому рівні його захищеності, прогнозуванні подальшого розвитку подій та розробленні пропозицій щодо адекватного реагування на зміни, що відбуваються, та загрози (впливи), що виникають;

принцип відповідності системи реагування поточному та очікуваному ступеням (рівням) загроз, який полягає у створенні системи оперативної протидії, яка базується на всебічному її оснащенні сучасними технічними системами та засобами, врахуванні факторів зовнішніх і внутрішніх, навмисних та ненавмисних, природних (стихійні лиха) загроз. Створена система протидії повинна бути розрахована на протидію професійно підготовленому та оснащеному зловмиснику (групі зловмисників);

принцип достатності чергових сил реагування ступеню загроз із боку порушників, який полягає у негайному та безумовному припиненні порушення, достатній кількості оперативних (чергових) сил, відповідній їх оснащеності та підготовці;

принцип аналогій, який обумовлює використання апробованих технічних та технологічних рішень і тенденцій розвитку систем розвідки (виявлення) та оперативного моніторингу інших аналогічних структур;

принцип недопущення асиметричності

протиправних дій, який полягає у проведенні превентивних заходів щодо недопущення втручання у роботу об'єктів критичної інформаційної інфраструктури, тобто створити інваріантну систему до несанкціонованого втручання в роботу об'єктів критичної інформаційної інфраструктури;

принцип доказовості та документування неправомірних дій у кібернетичному просторі оборонного сектору, який полягає в отриманні та зберіганні інформації про несанкціоноване втручання для правової оцінки дій порушників;

принцип системного інтегрованого підходу, який передбачає обов'язкову безперервність процесу ведення розвідки кіберпростору можливих об'єктів негативного впливу (по всьому технологічному циклу діяльності) з обов'язковим обліком всіх можливих видів впливів (несанкціонований доступ, знімання інформації, тероризм, пожежа, стихійні лиха тощо), розуміння та реалізації того, як, від кого, чим захищатися.

На нашу думку, доцільне розроблення та прийняття Концепції захисту об'єктів критичної інформаційної інфраструктури держави, запровадження державної системи паспортизації інформаційних небезпек та державного реєстру найважливіших об'єктів критичної інформаційної інфраструктури (у тому числі у воєнній сфері), сприятиме виробленню єдиної технічної політики щодо забезпечення кібербезпеки (кіберзахисту) об'єктів критичної інформаційної інфраструктури держави протягом їхнього життєвого циклу.

Паспорт безпеки об'єкта - це документ, що містить інформацію про забезпечення захищеності об'єкта і план заходів щодо забезпечення захищеності об'єкта.

При формуванні паспорта інформаційної небезпеки та державного реєстру найважливіших об'єктів критичної інформаційної інфраструктури (у тому числі у воєнній сфері) необхідно дати послідовні відповіді на ряд питань, які в загальному вигляді можна сформулювати так:

що/хто підлягає захисту? (національні цінності, технічні системи інформаційної інфраструктури, особовий склад військ, органи військового управління тощо);

від кого/чого потрібно захищати? (інформаційні небезпеки, інформаційні виклики, ризики, стихійні лиха тощо);

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

хто має захищати? (система забезпечення інформаційної безпеки, заходи інформаційного протиборства тощо);

наскільки ефективна система захисту об'єкта критичної інформаційної інфраструктури щодо можливих протиправних дій?;

наскільки система захисту кожного об'єкта критичної інформаційної інфраструктури відповідає сучасним вимогам?

Висновки:

1. Розроблення та прийняття Концепції захисту об'єктів критичної інформаційної інфраструктури держави, запровадження державної системи паспортизації інформаційних небезпек та державного реєстру найважливіших об'єктів критичної інформаційної інфраструктури (у тому числі у воєнній сфері) сприятиме виробленню єдиної технічної політики щодо забезпечення захисту об'єктів критичної інформаційної інфраструктури держави протягом їхнього життєвого циклу.

2. Необхідним є застосування комплексу заходів для покращення захисту об'єктів критичної інформаційної інфраструктури оборонного сектору у нормативно-правовій, організаційній та технологічній сфері (створення систем раннього виявлення загроз, (впливів); підвищення ефективності інформаційно-аналітичної роботи; створення бази даних кіберзлочинців (кібертерористів); матеріально-технічне забезпечення; кадрове забезпечення; інформаційне забезпечення).

3. Необхідно створити умови для дотримання режиму експортного контролю та нерозповсюдження несертифікованих програмно-апаратних засобів та систем, комп'ютерної техніки, оперативного реагування на інциденти, які пов'язані з виведенням із ладу телекомунікаційних систем оборонного сектору; створення каналів формального і неформального обміну інформацією про загрозу комп'ютерної злочинності та кібертероризму.

4. Реалізацію проведення заходів щодо захисту об'єктів критичної інформаційної інфраструктури держави доцільно здійснити шляхом створення підрозділів швидкого реагування на злочини проти зазначених об'єктів, здатних на співробітництво з міжнародними організаціями тощо.

Подальші дослідження доцільно присвятити питанням розроблення Концепції захисту об'єктів критичної інформаційної інфраструктури держави, вдосконалення

нормативно-правової бази кіберзахисту об'єктів критичної інформаційної інфраструктури, організації та ведення державного реєстру найважливіших об'єктів критичної інформаційної інфраструктури у воєнній сфері.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Стратегія національної безпеки України, (в редакції Указу Президента України від 26 травня 2015 року № 287/2015).
2. Концепція розвитку сектору безпеки і оборони України, введена в дію Указом Президента України від 14 березня 2016 року № 92/2016).
3. Воєнна доктрина України, затверджена Указом Президента України від 24 вересня 2015 року.
4. Стратегія кібербезпеки України, (в редакції Указу Президента України від 15 березня 2016 року № 96/2016).
5. Стратегічний оборонний бюлетень України (введений в дію Указом Президента України від 6 червня 2016 року № 240/2016).
6. Бірюков Д.С. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні: аналітична доповідь / Д.С. Бірюков, С.І. Кондратов. – К.: НІСД, 2012. – 102 с.
7. Постанова Кабінету Міністрів України від 3 серпня 1998 року № 1198 "Про єдину державну систему запобігання і реагування на надзвичайні ситуації техногенного та природного характеру" [Електронний ресурс]. – Законодавство України. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/1198-98-%D0%BF
8. Стратегія комунікацій Збройних Сил України, затверджена наказом Міністра оборони України від 30 вересня 2015 року.
9. ВСТ 01.004.004 – 2014 (01) Інформаційна безпека держави у воєнній сфері. Терміни та визначення.
10. Постанова Кабінету Міністрів України від 23 серпня 2016 р. № 563 "Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави".
11. А. Бочков. Категорирование критически важных объектов по уязвимости к возможным противоправным действиям. Экспертный подход. БДИ, № 1 (82), январь-февраль 2009. – С. 22 - 24.
12. Проблеми і напрями розвитку Збройних Сил України в сучасних умовах. Аналітична доповідь [Електронний ресурс]. – Національний інститут стратегічних досліджень, 2013. – Режим доступу: www.niss.gov.ua/content/articles/files/ZSU-73823.pdf
13. Концепція захисту критичної інфраструктури: стан, проблеми та перспективи її впровадження в Україні: зб. матеріалів міжнар. наук.-практ. конф. (7-8 листопада 2013 р., Київ – Вишгород) / упоряд. Д.С. Бірюков, С.І. Кондратов.– К. : НІСД, 2014. – 148 с.
14. Рогов П.Д., Ворович Б.О., Ворона Т.О. Війна в кіберпросторі. – К.: Оборонний вісник № 1, 2017. – С. 16 – 21.

Стаття надійшла до редакції 22.02.2017

Рогов П. Д., к.т.н.;
Ворович Б. А., к.воен.н., доцент;
Ткаченко В. А., к.воен.н.

Центр военно-стратегических исследований Национального университета обороны Украины имени Ивана Черняховского, Киев

Пути обеспечения кибернетической безопасности объектов критической информационной инфраструктуры государства в военной сфере

Резюме. В статье рассмотрен вопрос кибернетической безопасности объектов критической информационной инфраструктуры, которые играют решающую роль в обороноспособности государства, ее экономическому и социальному развитию. Определены принципы и пути улучшения защиты объектов критической информационной инфраструктуры государства.

Ключевые слова: безопасность информационной инфраструктуры, критическая информационная инфраструктура государства, объекты критической информационной инфраструктуры государства, паспортизация объектов критической информационной инфраструктуры.

P. Rogov, Ph.D;
B. Vorovich, Ph.D;
V. Tkachenko, Ph.D

Center for Military and Strategic Studies National Defence University of Ukraine named after Ivan Chernyhovsky, Kyiv

Ways of providing of cybernetic safety of objects of critical informative infrastructure of the state are in a military sphere

Resume. The question of cybernetic safety of objects of critical informative infrastructure, which play a decision role in the defensive capacity of the state, is considered in the article, to her economic and social development. Certain principles and ways of improvement of defence of objects of critical informative infrastructure of the state.

Keywords: safety of informative infrastructure, critical informative infrastructure of the state, objects of critical informative infrastructure of the state, passport system of objects of critical informative infrastructure.