УДК 004.456

ДЕРЖАВНІ ІНФОРМАЦІЙНІ РЕСУРСИ ТА ЇХ ЗАХИСТ

Грищенко Д. В., здобувач вищої освіти гр. КБ-181
Науковий керівник: **Ткач Ю. М.**, д.пед.н., доцент
Національний університет «Чернігівська політехніка»

У сучасному світі інформаційні ресурси стають одним з головних чинників прискорення розвитку країни та підвищення її іміджу у світовому співтоваристві. Розрізняють інформаційні ресурси державні та недержавні. Розглянемо захищеність державних інформаційних ресурсів.

Державні інформаційні ресурси – це систематизована інформація, що є доступною за допомогою інформаційних технологій, право на володіння, використання або розпорядження якою належить державним органам, військовим формуванням, утвореним відповідно до законів України, державним підприємствам, установам та організаціям, а також інформація, створення якої передбачено законодавством та яка обробляється фізичними або юридичними особами відповідно до наданих їм повноважень суб'єктами владних повноважень [1].

До державних інформаційних ресурсів відносяться інформаційні ресурси створені, придбані, накопичені за рахунок коштів державного бюджету, позабюджетних державних фондів та платників податків [3].

Державні інформаційні ресурси забезпечують виконання завдань державного управління; забезпечення прав та безпеки громадян; підтримки соціально-економічного розвитку країни, розвитку культури, науки, освіти і т. д.

Під загрозою безпеки інформаційним ресурсам будемо розуміти дії, які можуть призвести до спотворення, несанкціонованого використання або, навіть, до руйнування інформаційних ресурсів керованої системи, а також програмних і апаратних засобів.

Щоб запобігти цих загроз, ми визначили основні рекомендації щодо забезпечення захисту державних інформаційних ресурсів:

– Регулярно проводити оцінку стану захищеності державних інформаційних ресурсів та об'єктів, що належать до критичної інформаційної інфраструктури держави.

– Забезпечувати безпечне зберігання та сканування на предмет вразливості державних інформаційних ресурсів, розміщених в Інтернеті.

– Утворити захищений центр оброблення даних для розміщення державних інформаційних ресурсів.

– Модернізувати та вдосконалити апаратне і програмне оснащення комплексів, а саме впровадити спеціалізоване програмне забезпечення, призначене для автоматизації процесу оцінки стану захищеності державних інформаційних ресурсів, та додаткове спеціалізоване апаратне забезпечення для захисту від мережевих атак.

– Мати комплексні системи захисту інформації з підтвердженою відповідністю в інформаційно-телекомунікаційних системах, у яких обробляється або передбачається оброблення інформації, вимога щодо захисту якої встановлена законом, а також створити та атестувати комплекси технічного захисту інформації на об'єктах інформаційної діяльності органів державної влади, підприємств, установ та організацій, що входять до сфери управління таких органів.

Контроль за забезпеченням захисту державних інформаційних ресурсів відбувається наступним чином:

– Контроль за забезпеченням захисту державних інформаційних ресурсів здійснюється Департаментом спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України і полягає у перевірці виконання власниками автоматизованих систем та операторами мереж передачі даних вимог нормативно-правових актів і нормативних документів з технічного та криптографічного захисту інформації.

– Власники автоматизованих систем та оператори мереж передачі даних повинні створювати необхідні умови для здійснення державного контролю за забезпеченням захисту державних інформаційних ресурсів.

– Власники автоматизованих систем та оператори мереж передачі даних повинні повідомляти ДСТСЗІ СБ України про виявлені ними спроби та факти здійснення несанкціонованих дій щодо державних інформаційних ресурсів [2].

Безпека державних інформаційних ресурсів та інформаційних технологій є одними з найбільш вагомих чинників забезпечення національних інтересів держави. Державні інформаційні ресурси є першоосновою інформаційного суверенітету, за їхньою допомогою держава контролює та регулює інформаційні потоки. Це головний ресурс людської діяльності. Отже, захист державних інформаційних ресурсів повинен забезпечуватися впровадженням комплексу технічних, криптографічних, організаційних та інших заходів і засобів комплексної системи захисту інформації, спрямованих на недопущення блокування інформації, несанкціонованого ознайомлення з нею та/або її модифікації.

Список використаних джерел

1. Про Державну службу спеціального зв'язку та захист інформації України : Закон України. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/3475-15

2. Про затвердження Порядку захисту державних інформаційних ресурсів у інформаційно-телекомунікаційних системах : Закон України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/z0027-02#Text

3. Довгань О.Д. Інформаційні ресурси: національні та державні, зміст, поняття // Державне управління : інформація і право. – 2015. – № 3. – Режим доступу : //www.ippi.org.ua/sites/default/files/dovgan.pdf

---

УДК 004.056.5

ОСНОВНІ ПОНЯТТЯ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГО ПРОТИБОРСТВА

Дубиніна В. М., здобувачка вищої освіти. КБ-171
Науковий керівник**: Гур'єв В. І.,** к.т.н., доцент
Національний університет «Чернігівська політехніка»

Інформаційне протиборство - форма боротьби сторін, що представляє собою використання спеціальних (політичних, економічних, дипломатичних, військових та інших) методів, способів і засобів для впливу на інформаційне середовище протилежної сторони і захисту власної в інтересах досягнення поставлених цілей.

Основними сферами ведення інформаційного протиборства є:

−політична;

−дипломатична;

−фінансово-економічна;

−інноваційна;

−військова.

Інформаційно-психологічне протиборство – це система інформаційних і психологічних впливів на інформаційні ресурси противника, свідомість і почуття його військовослужбовців і населення, а також комплекс заходів щодо захисту власних інформаційних і психологічних ресурсів. Об'єктами інформаційно-психологічного протиборства виступають населення, армії і уряди протиборчих, дружніх і нейтральних країн. Сферою його відання можуть бути системи управління, канали зв'язку і електронні комунікації, бази і банки даних, засоби масової