УДК 621.396 DOI: 10.30748/nitps.2019.35.06

С.В. Сальник, А.С. Сторчак, К.К. Герасімов

Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут ім. І. Сікорського", Київ

АНАЛІЗ ФУНКЦІОНУВАННЯ СИСТЕМ УПРАВЛІННЯ ДЕРЖАВНИМИ ІНФОРМАЦІЙНИМИ РЕСУРСАМИ

В статті розглядаються засоби обробки та функціонування державних інформаційних ресурсів. Визначено процеси формування і використання інформаційних ресурсів. Охарактеризовано складові інформаційно-телекомунікаційних систем. Розглянуто комплекс систем і механізмів захисту для забезпечення безпеки кіберпростору та основні характеристичні особливості сучасних інформаційних ресурсів. Визначено найбільш актуальні завдання, що вирішують інформаційно-телекомунікаційні мережі. Розглянуто елементи інформаційно-телекомунікаційних систем та вказані основні вразливості, які виникають при обробці державних інформаційних ресурсів. Визначено множину вимог до інформаційно-телекомунікаційних систем в кіберпросторі з метою обробки та збереження державних інформаційних ресурсів. Визначено зміст захисту державних інформаційних ресурсів. Запропоновано забезпечити безпеку державних інформаційних ресурсів з урахуванням вразливостей інформаційно-телекомунікаційних систем та їх властивостей. Запропоновано провести детальний аналіз вразливостей інформаційно-телекомунікаційних систем, загроз державним інформаційним ресурсам та атак.

Ключові слова: *державні інформаційні ресурси, інформаційно-телекомунікаційні системи, кіберпростір, вразливості інформаційних систем, захист державних інформаційних ресурсів.*

Вступ

Реформування та розвиток системи забезпечення національної безпеки держави, спеціального зв'язку та захисту інформації, як складової частини системи забезпечення національної безпеки, залишаються на сьогодні одними з ключових питань. Система забезпечення національної безпеки ґрунтується на національних інтересах та формується з урахуванням реальних загроз, небезпек та викликів безпеці.

В свою чергу підрозділи спеціального зв'язку та захисту інформації є суб'єктами забезпечення функціонування і розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, формування та реалізації державної політики у сферах кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, криптографічного та технічного захисту інформації, телекомунікацій, користування радіочастотним ресурсом, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку, а також інших завдань відповідно до закону. Гостра необхідність інформатизації системи управління, створення баз даних та знань державних інформаційних ресурсів зумовлена зростанням кількості техногенних катастроф та загостренням військової агресії (гібридних, інформаційних, кібернетичних операцій або війн) з боку інших держав. Інформаційна війна як соціально-технічний інструмент стала важливою частиною військово-політичного втручання держав у життєві процеси інших держав.

Національна система кібербезпеки є сукупністю суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного, технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури [1].

Значну роль у протидії гібридним, інформаційним, кібернетичним війнам слід приділяти захисту державних інформаційних ресурсів на основі сформованої інформаційної політики країни та впровадженню комплексного підходу до побудови систем захисту. Проте аналіз сучасних досліджень цього питання [2–15], зокрема публікації таких вітчизняних науковців, як Бурячок В.Л., Гнатюк С.О., Корнейко О.В., Корченко О.Г., Довбня С.Я., Юдін О.К., Бучик С.С., Смірнов Є.Б., Конахович Г.Ф., Дубчак О.В., Довгань О.Д., Марущак А.І. Дудикевич В.Б., вказує на те, що нормативно-правові акти та питання створення політики безпеки, моделі загроз, моделі порушників, методів захисту державних інформаційних ресурсів в передових країн світу розглядались дуже загально та не враховували сучасні виклики.

Метою даної роботи є аналіз функціонування сучасних систем управління державними інформаційними ресурсами в інформаційно-телекомунікаційних системах.

Об'єктом є процес управління державними інформаційними ресурсами.

Предметом є механізми функціонування та засоби захисту державних інформаційних ресурсів в сучасних інформаційно-телекомунікаційних системах.

Виклад основного матеріалу

Інформаційні ресурси формуються і використовуються на основі соціальних процесів та різних способів організації суспільно корисної діяльності. Процеси перетворення та реалізації знань через матеріалізацію інформаційного ресурсу отримують розвиток за рахунок високих інформаційних технологій, а для отримання і збереження переваг в умовах конкуренції кожна дія в інформаційному середовищі буде мати значний вплив у світі фізичних ресурсів: предметних, фінансових – і в різних абстрактних галузях. Усе це систематизується в мережевих банках даних, з якими взаємодіють користувачі мережі. Ці ресурси визначають споживчу цінність інформаційної мережі, тому їх необхідно: постійно створювати та поповнювати; вчасно архівувати та оновлювати; користування мережею повинно забезпечувати можливість отримання актуальної інформації саме тоді, коли в ній виникає необхідність.

Сукупність ресурсів, що функціонують між кінцевими точками інформаційних систем та надають користувачам конкретні послуги (або набір послуг), називають платформою надання послуг. До ресурсів обробки та зберігання даних відносять продуктивність процесорів та обсяги пам'яті комп'ютерів, які працюють у мережі, а також час, протягом якого вони використовуються.

До програмних ресурсів відносять мережеве програмне забезпечення, а саме:

– мережеві операційні системи, серверне програмне забезпечення, програмне забезпечення робочих станцій;

– прикладне програмне забезпечення;

– інструментальні засоби: утиліти, аналізатори проходження трафіку, засоби мережевого контролю, програми додаткових функцій, навігація (забезпечення пошуку інформації в мережі), обслуговування мережевих електронних поштових скриньок, організація мостів для телеконференцій, криптозахист інформації, автентифікація.

Ресурси інформаційної системи дозволяють:

– виконувати обробку інформації;

– забезпечувати ефективний пошук її в будь-якому місці мережі;

– накопичувати й зберігати дані.

Сукупність мережевих ресурсів забезпечують:

– можливість перенесення в просторі інформаційних повідомлень;

– взаємодію інформаційних систем;

– виробництво нових послуг та інформації.

Державні інформаційні ресурси являють собою систематизовану інформацію, що є доступною за допомогою інформаційних технологій, а саме інформаційних процесів, що використовують засоби обчислювальної техніки та забезпечують високу швидкість обробки даних, швидкий пошук інформації, розосередження даних, доступ до джерел інформації незалежно від місця їх розташування. Державні інформаційні ресурси включають в себе відкриту інформацію (інформацію державних органів, статистичну, соціологічну, довідкову, правову, науково-технічну), конфіденційну інформацію (в тому числі персональні дані) та таємну інформацію. В свою чергу інформаційні технології класифікують:

– за способом реалізації;

– за ступенем охоплення задач управління;

– за класом реалізуючих технологічних операцій;

– за типом користувацького інтерфейсу;

– за способом побудови мережі;

– за обслуговуючими предметними сферами.

Однією з найпоширеніших інформаційних технологій є інформаційно-телекомунікаційна система (ІТС), тобто сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле. ІТС (разом з інформаційними ресурсами та сервісами) відіграють важливу роль в процесах інтеграції державних інформаційних ресурсів у сферах життєдіяльності країни та суспільства.

Телекомунікаційна система становить системоутворюючу сукупність засобів телекомунікацій, що надає територіально віддаленим об'єктам можливість інформаційної взаємодії шляхом обміну сигналами (електричними, оптичними або радіо) [16]. Об'єктами при цьому можуть виступати: термінальні пристрої користувачів; кінцеві системи мережі; окремі мережі.

Кінцевою точкою (інтерфейсною точкою) телекомунікаційної системи є або телекомунікаційний роз'єм, до якого під'єднано пристрій користувача (мережевий або міжмережевий інтерфейс), або кінцеве мережеве обладнання, яке забезпечує з'єднання мереж (рис. 1).

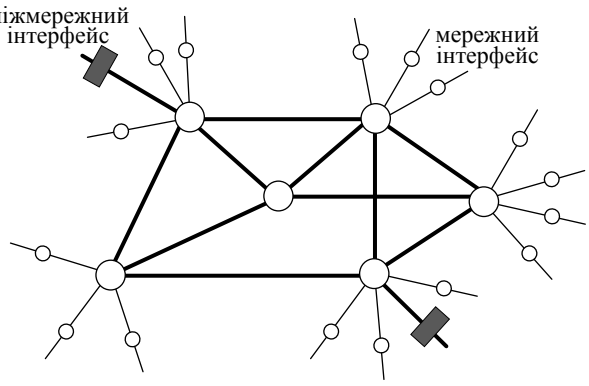

Рис. 1. Структура телекомунікаційної мережі

Телекомунікаційні системи класифікують за:

– типом режиму перенесення інформації (синхронні, асинхронні);

– технологічними характеристиками (середовищем передавання, заданою шириною смуги пропускання, якістю передавання сигналів, швидкістю передавання та ін.).

Під інформаційною системою як фізичним об'єктом будемо розуміти сукупність територіально розрізнених кінцевих систем, об'єднаних телекомунікаційною мережею, за допомогою якої забезпечуються взаємодія прикладних процесів, активізованих в кінцевих системах, та їх колективний доступ до ресурсів мережі.

Інформаційна система відображає інформаційні процеси, які протікають в мережі в результаті взаємодії кінцевих систем, під'єднаних до телекомунікаційної системи.

Інформаційна система передбачає розгляд телекомунікаційної мережі в сукупності зі взаємодіючими за допомогою неї об'єктами [17]. У такому розумінні інформаційна система являє собою навантажену телекомунікаційну систему.

Інформаційні процеси в мережі можливо поділити на дві групи: прикладні процеси та процеси взаємодії. Прикладні процеси ініціюються кінцевими системами під час запуску програм користувача. В свою чергу під процесами взаємодії розуміють процеси в мережі, призначені для обслуговування прикладних процесів. Прикладні процеси та процеси взаємодії підтримуються мережевими операційними системами.

Кінцеві точки інформаційної системи класифікуються таким чином:

– термінальні системи – комп'ютери користувачів мережі;

– хостингові системи – містять інформаційні та програмні ресурси мережі;

– сервери – дозволяють надавати мережеві сервіси.

Комунікаційні ресурси беруть участь у транспортуванні та перерозподілі потоків інформації в мережі, основними з яких є пропускні спроможності ліній зв'язку та устаткування вузлових пунктів, а також їх використання під час взаємодії користувача з мережею. Вони класифікуються відповідно до використаного середовища передачі та телекомунікаційної технології. Ресурси інформаційної мережі можуть використовуватися одночасно кількома прикладними процесами, тобто розділятися в часі.

Робота в інформаційній мережі виконується периферією, тобто в кінцевих системах мережі, а телекомунікаційна мережа виконує функції транспортувальної системи (рис. 2).

Параметри оцінки ефективності інформаційної мережі визначаються рівнем продуктивності інформаційної мережі, як системи розподільчих ресурсів, та складаються з:

– часу реакції мережі;

– затримки передачі;

– варіації затримки передачі;

– прозорості.

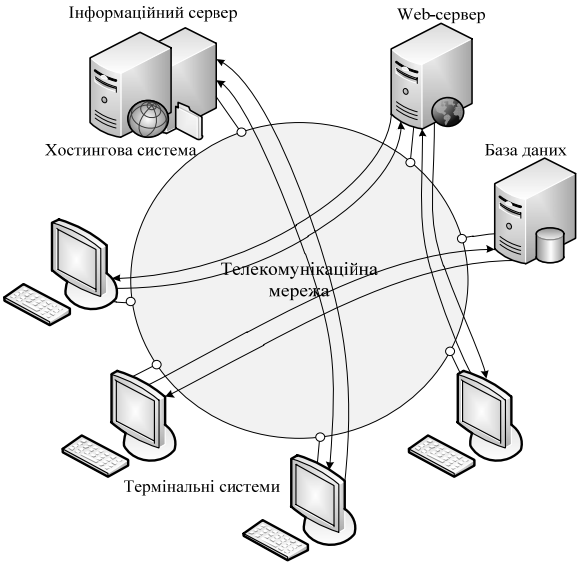

Рис. 2. Структура інформаційної системи

Інформаційно-телекомунікаційна мережа є комплексом термінальних пристроїв користувачів, кінцевих систем мережі та універсальної платформи виробництва та надання послуг, які відповідають різноманітним вимогам користувачів до їх типу та якості (рис. 3).

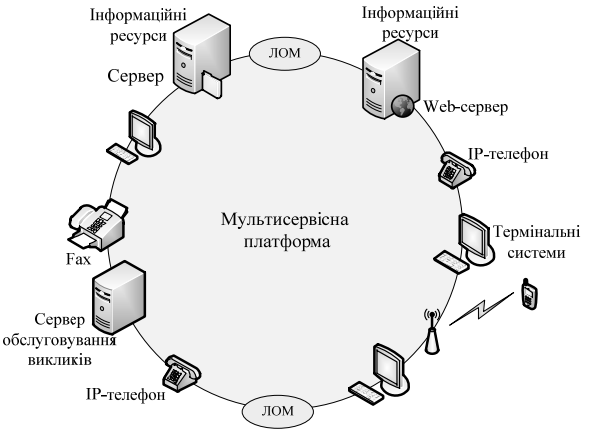

Рис. 3. Структура ІТС

Таким чином, інформаційно-телекомунікаційна мережа дозволяє вирішувати найбільш актуальні завдання:

– надання користувачам можливості обміну інформаційними повідомленнями різного типу (мова, відео, дані);

– швидке та якісне отримання необхідної інформації з будь-якого віддаленого джерела в мережі;

– автоматизацію процесів обробки, накопичення, зберігання великих обсягів інформації в мережі, самого процесу виробництва інформації.

Отже, до ІТС входять наступні елементи:

– обчислювальна техніка;

– канали зв'язку;

– система доступу до каналів зв'язку (комутаційне обладнання);

– бази даних та системи управління базами даних;

– системи захисту;

– програмне забезпечення.

ІТС, інформаційні ресурси ІТС, інформаційні продукти, проміжна і технологічна інформація, інформаційні сервіси ІТС та користувачі ІТС загалом функціонують та підлягають захисту в кіберпросторі, тобто у віртуальному просторі, що надає можливості для здійснення комунікацій, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних [18–19]. Для забезпечення безпеки кіберпростору необхідне впровадження комплексу систем і механізмів захисту, а саме системи [20]:

– розмежування доступу користувачів;
– міжмережного екранування;
– криптографічного захисту інформації;
– віртуальні приватні мережі;
– антивірусного захисту елементів ІТС;
– виявлення і запобігання вторгнень;
– автентифікації, авторизації і аудиту;
– попередження втрати даних;
– управління безпекою та подіями;
– аналізу захищеності.

При побудові ІТС важливо враховувати можливі вразливості, що виникають на кожному із рівнів моделі OSI (табл. 1).

Таблиця 1

Відповідність вразливостей рівням моделі OSI

Рівень OSI	Вразливості
Фізичний рівень	- втрата потужності; - фізичні крадіжки даних і устаткування; - фізичне пошкодження або знищення даних і устаткування; - несанкціоновані зміни у функціональному середовищі; - вимкнення фізичних каналів передачі даних; - перехоплення за рахунок побічних електромагнітних випромінювань та наводок.
Канальний рівень	- підміна mac-адреси; - обхід технологій vlan; - переповнення cam-таблиць; - spanning tree для передачі пакетів у нескінченний цикл; - затоплення комутаторами всіх портів vlan.
Мережевий рівень	- підміна маршруту; - підміна ip-адреси; - проблеми одноразової ідентифікації.
Транспортний рівень	– неправильна передача пакетів; – перевантаження за рахунок великої кількості звернень до номерів портів обмежує можливості для ефективної фільтрації трафіку; – механізми передачі пакетів можуть бути предметом атаки на основі сформованих пакетів і призводити до руйнування або захоплення контролю над мережею.
Сеансовий рівень	– слабкі механізми автентифікації; – передача під час сеансу інформації (ім'я користувача і пароль) у відкритому вигляді; – ідентифікація сеансу може бути предметом підміни і викрадення; – витік інформації на основі невдалих спроб автентифікації; – здійснення атаки на облікові дані для доступу в разі необмеженої кількості спроб на встановлення сеансу.
Рівень представлень	– погана обробка даних може призвести до збою програми; – ненавмисне використання зовнішніх даних, що вводяться в контексті управління, може призвести до віддаленої маніпуляції або витоку інформації; – криптографічні недоліки можуть бути використані для обходу захисту конфіденційності.
Прикладний рівень	– використання безкоштовних ресурсів та програм невідомого походження; – недоліки програмного забезпечення, наявність backdoors; – недостатній контроль засобів захисту за принципом "все або нічого"; – надмірно ускладнений механізм контролю безпеки; – збої програмного забезпечення при великих навантаженнях.

Зазначені основні загрози впливають і на безпеку державних інформаційних ресурсів [21–23]. Загалом зміст захисту державних інформаційних ресурсів представлено на рис. 4 [5].

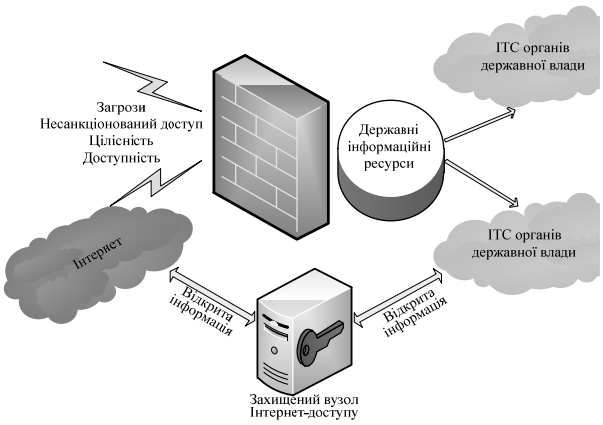

Рис. 4. Захист державних інформаційних ресурсів

В цілому сучасні системи обробки державних інформаційних ресурсів здебільшого функціонують в кіберпросторі та мають враховувати особливості функціонування інформаційно-телекомунікаційної мережі. Тому доцільно висунути до ІТС множину вимог:

– наявність технології прийняття рішень, самонавчання, інтелектуалізації тощо;

– врахування особливостей функціонування державних інформаційних ресурсів;

– можливість проведення аналізу трафіку;

– оптимізація при визначенні критеріїв оцінки (наприклад: час доставки пакетів, мінімальна відстань, швидкість передачі даних);

– врахування обмежень (енергоресурсу, потужності вузлів, тощо);

– застосування при нечіткій мережевій активності або наявності дестабілізуючих факторів;

– можливість як автономного так і кооперованого функціонування;

– забезпечення необхідної якості обслуговування різних типів трафіку.

З проведеного аналізу зрозуміло, що сучасним ІТС притаманні вищевизначені вразливості. В цілому ефективність захисту ІТС визначається стійкістю ІТС до атак та роботі в умовах впливу дестабілізуючих факторів. Тому з метою оцінки функціонування державних інформаційних ресурсів за умов існуючих викликів безпеці та загроз доцільно провести детальний аналіз вразливостей ІТС, загроз державним інформаційним ресурсам та атак, за допомогою яких вони можуть бути реалізовані.

Також, враховуючи особливості процесу обробки інформаційних ресурсів обчислювальними ресурсами, засобами передачі та персоналом, пропонується під державними інформаційними ресурсами розуміти взаємопов'язану сукупність інформації, що належить державі, носіїв інформації, обчислювальних ресурсів, засобів передачі та персоналу, що захищається системою захисту в ІТС.

Висновки

В статті було проведено аналіз функціонування сучасних систем управління державними інформаційними ресурсами в інформаційно-телекомунікаційних системах. Під час проведення даного аналізу було розглянуто: засоби обробки ДІР; елементи інформаційно-телекомунікаційних систем; комплекси систем і механізмів захисту для забезпечення безпеки кіберпростору; можливості та задачі ресурсів інформаційних систем, комплекси систем і механізмів захисту для забезпечення безпеки кіберпростору; зміст захисту державних інформаційних ресурсів. В статті визначено множину вимог до інформаційно-телекомунікаційних систем з метою обробки та збереження ДІР та запропоновано: забезпечити безпеку ДІР з урахуванням вразливостей інформаційно-телекомунікаційних систем та їх властивостей; провести аналіз вразливостей інформаційно-телекомунікаційних систем, загроз ДІР та атак на ДІР. Зазначена пропозиція дозволить приймати управлінські рішення з метою ефективного функціонування ДІР в інформаційно-телекомунікаційних системах.

Метою подальших дослідження є розробка методики захисту ДІР від протиправних посягань та методу визначення рівня захищеності інформаційних ресурсів від кібератак.

Список літератури

1. Закон України "Про основні засади забезпечення кібербезпеки України № 2163-VIII від 05.10.2017" [Електронний ресурс]. – Режим доступу: www.zakon.rada.gov.ua/laws/show/2163-19.

2. Ліпкан В.А. Національна система кібербезпеки як складова частина системи забезпечення Національної безпеки України / В.А. Ліпкан, І.В. Діордіца // Підприємництво, господарство і право: Інформаційне право. – 2017. – № 5. – С. 174-180.

3. Бурячок В.Л. Метод побудови класифікатора кібератак на державні інформаційні ресурси / В.Л. Бурячок, Р.В. Грищук, В.М. Мамарэв // Технологический аудит и резервы производства. – 2015. – № 1/2 (21). – С. 38-43.

4. Шевченко А.С. Комплексний підхід до побудови системи кібернетичного захисту Збройних сил України / А.С. Шевченко // Сучасна спеціальна техніка. – 2016. – № 4(47). – С. 47-54.

5. Юдін О.К. Державні інформаційні ресурси. Методологія побудови класифікатора загроз: монографія / О.К. Юдін, С.С. Бучик. – К.: НАУ, 2015. – 214 с.

6. Борисова Н.В. Гібридні системи безпеки інформаційних та комунікаційних мереж / Н.В. Борисова, Л.В. Шабанова-Кушнаренко // Системи обробки інформації. – 2017. – № 5(151). – С. 103-108. https://doi.org/10.30748/soi.2017.151.14.

7. Науково-методичне забезпечення створення та функціонування системи інформаційної безпеки держави / С.Я. Довбня, В.І. Кривцун, І.О. Четверіков, В.О. Савран, О.О.Солдатенко // Збірник наукових праць ВІКНУ. – 2014. – Вип. № 47. – С. 98-108.

8. Довгань О.Д. Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту: монографія / О.Д. Довгань, І.М. Доронін. – К.: Видавничий дім "АртЕк". – 2017. – 107с.

9. Ткаченко В.І. Шляхи формування системи забезпечення Національної безпеки / В.І. Ткаченко, Є.Б. Смірнов, О.О. Астахов // Збірник наукових праць Харківського університету Повітряних Сил. – 2015. – № 2(43). – С.3-8.

10. Горніцька Д.А. Система аналізу та оцінки рівня захищеності державних інформаційних ресурсів від соціотехнічних атак / Д.А. Горніцька, М.В. Захарова, А.І. Кладочний // Безпека інформації. – 2012. – № 2(18). – С. 70-74.

11. Довгань О.Д. Інформаційні ресурси: національні та державні, зміст, поняття / О.Д. Довгань // Інформація і право. – 2015. – № 3(15). – С. 85-91.

12. Марущак А.І. Зміст поняття "державні електронні інформаційні ресурси" / А.І. Марущак, С.Г. Петров // Інформація і право. – 2018. – № 4(27). – С. 15-21.

13. Василенко В.С. Методика оцінки захищеності інформації в ЛОМ. Графічні моделі взаємодії загроз функціональним властивостям захищеності інформаційних ресурсів ЛОМ із елементами системи захисту / В.С. Василенко, О.В. Дубчак, М.Ю. Василенко // Науково-практичний журнал "Безпека інформації". – 2012. – № 1. – С. 49-54.

14. Костяк М.Ю. Особливості проектування захищених інформаційних мереж спеціального призначення / М.Ю. Костяк, Л.Т. Пархуць // Вісник Національного університету "Львівська політехніка": Серія: Автоматика, вимірювання та керування. – 2016. – № 852. – С. 88-92.

15. Дудикевич В.Б. Аналіз моделей захисту інформації в інформаційних мережах держави / В.Б. Дудикевич, І.Р. Опірський // Системи обробки інформації. – 2016. – № 4(141). – С. 86-89.

16. Конахович Г.Ф. Захист інформації в мережах передачі даних / Г.Ф. Конахович, О.Г Корченко, О.К. Юдін. – К.: Видавництво ТОВ "НВП "ІНТЕРСЕРВІС", 2009. – 713 с.

17. Васильєв Ю. Класифікація та аналіз загроз інформаційній безпеці в ключових системах інформаційної інфраструктури / Ю. Васильєв // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2015. – № 1(29). – С. 56-61.

18. Дудикевич В.Б. Концепція та базовий підхід до побудови системи захисту інформації в багаторівневій інтелектуальній системі керування / В.Б. Дудикевич, Г.В. Микитин, Т.Б. Крет // Системи обробки інформації. – 2016. – № 8(145). – С. 105-110.

19. Климович О.К. Застосування мобільних телекомунікаційних мереж спеціального призначення в Збройних Силах України / О.К. Климович // Системи обробки інформації. – 2015. – № 5(130). – С. 135-140.

20. МСЭ-Т Х.1205. Серия Х: сети передачи данных, взаимосвязь открытых систем и безопасность. Безопасность электросвязи. Обзор кибербезопасности. –Женева, 2009. – 64 с.

21. Довбня С.Я. Аналіз загроз та визначення вимог щодо захисту інформації в інтегрованих інформаційно-телекомунікаційних системах України / С.Я. Довбня, А.А. Гришанова // Інформаційна безпека України: Збірник наукових доповідей та тез науково-технічної конференції. – 2016. – С. 11-19.

22. Корнієнко Б.Я. Дослідження моделі взаємодії відкритих систем з погляду інформаційної безпеки / Б.Я. Корнієнко // Наукоємні технології. – 2012. – № 3(15). – С. 83-89.

23. Рубан І.В. Класифікація мережевих загроз / І.В. Рубан, Д.В. Прибильнов // Комп'ютерні науки та інженерія: матеріали V Міжнародної конференції молодих вчених CSE-2011, 24–26 листопада 2011 р., Україна, Львів, Національний університет "Львівська політехніка". – Львів: Видавництво Львівської політехніки, 2011. – С. 350-353.

References

1. The Law of Ukraine (2017), "*Pro osnovni zasady zabezpechennya kiberbezpeky Ukrayiny 2017 No. 2163-VIII vid 05.10.2017*" [*About the basic principles of providing cyber security of Ukraine No. 2163-VIII dated 05.10.2017*], available at: www.zakon.rada.gov.ua/laws/show/2163-19.

2. Lipkan, V.A. and Diorditsa, I.V. (2017), "Natsional′na systema kiberbezpeky yak skladova chastyna systemy zabezpechennya Natsional′noyi bezpeky Ukrayiny" [National system of cyber security as an integral part of the system of ensuring the National Security of Ukraine], *Business, Economy and Law*, No. 5, pp. 174-180.

3. Buryachok, V.L., Grischuk, R.V. and Mamarev, V.M. (2015), "Metod pobudovy klasyfikatora kiberatak na derzhavni informatsiyni resursy" [Method of constructing a classification cyberattack on state information resources], *Technology Audit and Production Reserves*, No. 1/2(21), pp. 38-43.

4. Shevchenko, A. (2016), "Kompleksnyy pidkhid do pobudovy systemy kibernetychnoho zakhystu Zbroynykh syl Ukrayiny" [Integrated approach to building a system of cybernetic defense of the Armed Forces of Ukraine], *Modern Special Technique*, No. 4(47), pp. 47-54.

5. Yudin, O.K. and Buchyk, S.S. (2015), "*Derzhavni informatsiyni resursy. Metodolohiya pobudovy klasyfikatora zahroz*" [*State information resources. Methodology of constructing a threat classifier*], NAU, Kyiv, 214 p.

6. Borisova, N.V. and Shabanova-Kushnarenko, L.V. (2017), "Gibridnye sistemy bezopasnosti informatsionnykh i kommunikatsionnykh setei" [Hybrid security systems in information and transmission networks], *Information Processing Systems*, No. 5(151), pp. 103-108. https://doi.org/10.30748/soi.2017.151.14.

7. Dovbnya, S.Ya., Krivtsun, V.I., Chetverikov, I.O., Savran, V.O. and Soldatenko, O.O. (2014), "Naukovo-metodychne zabezpechennya stvorennya ta funktsionuvannya systemy informatsiynoyi bezpeky derzhavy" [Scientific and methodological support for the creation and functioning of the state information security system], *Collection of Scientific Works of Military Institute of Taras Shevchenko National University of Kyiv*, Vol. 47, pp. 98-108.

8. Dovgan, O.D. and Doronin, I.M. (2017), "*Eskalatsiya kiberzahroz natsional'nym interesam Ukrayiny ta pravovi aspekty kiberzakhystu*" [*Escalation of cyber threats to the national interests of Ukraine and legal aspects of cyber defense*], ArtEk, Kyiv, 107 p.

9. Tkachenko, V.I., Smirnov, Ye.B. and Astakhov, O.O. (2015), "Shliakhy formuvannia systemy zabezpechennia natsionalnoi bezpeky" [Ways of forming of national safety providing system], Sci*entific Works of Kharkiv National Air Force University*, No. 2(43), pp. 3-8.

10. Gornitska, D.A., Zaharova, M.V. and Kladochniy, A.I. (2012), "Systema analizu ta otsinky rivnya zakhyshchenosti derzhavnykh informatsiynykh resursiv vid sotsiotekhnichnykh atak" [System analysis and evaluation of the level of protection of state information resources from social engineering attacks], *Ukrainian Scientific Journal of Information Security*, No. 2(18), pp. 70-74.

11. Dovgan, O.D. (2015), "Informatsiini resursy: natsionalni ta derzhavni, zmist, poniattia" [Information resources: national and state, content, concept], *Information and Law*, No. 3 (15), pp. 85-91.

12. Maruschak, A.I. and Petrov, S.G. (2018), "Zmist ponyattya derzhavni elektronni informatsiyni resursy" [Content of the concept of "state electronic information resources"], *Information and Law*, No. 4 (27), pp. 15-21.

13. Vasilenko, V.S., Dubchak, O.V. and Vasilenko, M.Yu. (2012), "Metodyka otsinky zakhyshchenosti informatsiyi v LOM. Hrafichni modeli vzayemodiyi zahroz funktsional′nym vlastyvostyam zakhyshchenosti informatsiynykh resursiv LOM iz elementamy systemy zakhystu" [Methods of assessment of information security in a LAN. Graphical interaction models threats functional properties of security of information resources with elements LAN security], *Ukrainian Scientific Journal of Information Security*, No. 17(1), pp. 49-54.

14. Kostyak, M.Yu. and Parchuts, L.T. (2016), "Osoblyvosti proektuvannya zakhyshchenykh informatsiynykh merezh spetsial′noho pryznachennya" [Features of Designing Protected Information Networks of Special Purpose], *Bulletin of the National University "Lviv Polytechnic"*, No. 852, pp. 88-92.

15. Dudykevych, V.B. and Opirskyi, I.R. (2016), "Analiz modelei zakhystu informatsii v informatsiinykh merezhakh derzhavy" [Analysis of models of information security in information networks of state], *Information Processing Systems*, No. 4(141), pp. 86-89.

16. Konakhovych, G.F., Korchenko, O.G. and Judin, O.K. (2009), "*Zakhyst informatsiyi v merezhakh peredachi danykh*", [*Protection of information in data transmission networks*], NVP INTERSERVICE, Kyiv, 713 p.

17. Vasiliev,Y. (2015), "Klasyfikatsiya ta analiz zahroz informatsiyniy bezpetsi v klyuchovykh systemakh informatsiynoyi infrastruktury" [Classification and analysis of threats to information security in key information infrastructure systems], *Legal, Regulatory and Metrological Support Information Security System in Ukraine*, No. 1(29), pp. 56-61.

18. Dudykevych, V.B., Mykytyn, H.V. and Kret, T.B. (2016), "Kontseptsiia ta bazovyi pidkhid do pobudovy systemy zakhystu informatsii v bahatorivnevii intelektualnii systemi keruvannia" [The concept and basic approach to building information security system in multi-level intelligent control system], *Information Processing Systems*, Vol. 8(145), pp. 105-110.

19. Klymovych, O.K. (2015), "Zastosuvannia mobilnykh telekomunikatsiinykh merezh spetsialnoho pryznachennia v Zbroinykh Sylakh Ukrainy" [Application of mobile telecommunication networks of the special setting in Military Forces of Ukraine], *Information Processing Systems*, Vol. 5(130), pp. 135-140.

20. International telecommunication union ITU-T X.1205 (2009), *Series X: Data Networks, Open System Communications and Security. Telecommunication security. Cybersecurity Review*, Geneva, 64 p.

21. Dovbnya, S.Y. and Grishanova, A.A. (2016), "Analiz zahroz ta vyznachennya vymoh shchodo zakhystu informatsiyi v intehrovanykh informatsiyno-telekomunikatsiynykh systemakh Ukrayiny" [Analysis of threats and definition of information security requirements in integrated information and telecommunication systems of Ukraine], *Information Security of Ukraine: Collection of scientific reports and abstracts of scientific and technical conference*, pp. 11-19.

22. Kornienko, B.Y. (2012), "Doslidzhennya modeli vzayemodiyi vidkrytykh system z pohlyadu informatsiynoyi bezpeky" [Investigation of the model of interaction of open systems in terms of information security], *Science-based Technologies*, No. 3(15), pp. 83-89.

23. Ruban, I. and Prybylnov, D. (2011), "Klasyfikatsiya merezhevykh zahroz" [Classification of network threats], *Kompiuterni nauky ta inzheneriia: materialy V Mizhnarodnoi konferentsii molodykh vchenykh CSE-2011*, Lviv, pp. 350-353.

Надійшла до редколегії 19.03.2019
Схвалена до друку 9.04.2019

Відомості про авторів:

Сальник Сергій Васильович
кандидат технічних наук
заступник завідувача кафедри
Інституту спеціального зв'язку та захисту інформації
Національного технічного університету України
"Київський політехнічний інститут ім. І. Сікорського",
Київ, Україна
https://orcid.org/0000-0003-4463-5705

Сторчак Антон Сергійович
старший викладач кафедри Інституту спеціального
зв'язку та захисту інформації Національного технічного
університету України "Київський політехнічний інститут
ім. І. Сікорського",
Київ, Україна.
https://orcid.org/0000-0002-5267-3122

Герасімов Костянтин Костянтинович
старший викладач кафедри Інституту спеціального
зв'язку та захисту інформації Національного технічного
університету України "Київський політехнічний інститут
ім. І. Сікорського",
Київ, Україна
https://orcid.org/0000-0002-6202-8493

Information about the authors:

Sergey Salnyk
Candidate of Technical Sciences
Deputy Head of the Department of Institute
of Special Communications and Information Protection
of National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute",
Kyiv, Ukraine
http:orcid.org/0000-0003-4463-5705

Anton Storchak
Senior Instructor of Institute
of Special Communications and Information Protection
of National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute",
Kyiv, Ukraine
https://orcid.org/0000-0002-5267-3122

Constantine Gerasimov
Senior Instructor of Institute
of Special Communications and Information Protection
of National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute",
Kyiv, Ukraine
https://orcid.org/0000-0002-6202-8493

АНАЛИЗ ФУНКЦИОНИРОВАНИЯ СИСТЕМ УПРАВЛЕНИЯ ГОСУДАРСТВЕННЫМИ ИНФОРМАЦИОННЫМИ РЕСУРСАМИ

С.В. Сальник, А.С. Сторчак, К.К. Герасимов

В статье рассматриваются средства обработки и функционирования государственных информационных ресурсов. Определены процессы формирования и использования информационных ресурсов. Определены возможности и задачи ресурсов информационных систем. Выяснены задачи информационно-телекоммуникационных систем при их построении. Охарактеризованы составляющие информационно-телекоммуникационных систем. Представлена структура информационной системы и определены параметры оценки эффективности информационной сети. Определены наиболее актуальные задачи, которые решают информационно-телекоммуникационные сети. Рассмотрены элементы информационно-телекоммуникационных систем и указаны основные уязвимости, возникающие при обработке государственных информационных ресурсов. Определено множество требований к информационно-телекоммуникационным систем в киберпространстве с целью обработки и хранения государственных информационных ресурсов. Представлены комплексы систем и механизмов защиты для обеспечения безопасности киберпространства. Определено содержание защиты государственных информационных ресурсов. Предложено обеспечить безопасность государственных информационных ресурсов с учетом уязвимостей информационно-телекоммуникационных систем и их свойств. Предложено провести детальный анализ уязвимостей информационно-телекоммуникационных систем, угроз государственным информационным ресурсам и атак.

***Ключевые слова**: государственные информационные ресурсы, информационно-телекоммуникационные системы, киберпространство, уязвимости информационных систем, защита государственных информационных ресурсов.*

ANALYSIS OF THE FUNCTIONING OF SYSTEMS OF MANAGEMENT BY STATE INFORMATION RESOURCES

S. Salnyk, A. Storchak, K. Gerasimov

Processing facilities and functioning of state information resources are considered in the article. The possibilities and tasks of information system resources are determined. The task of information and telecommunication systems during their construction is defined. The components of information and telecommunication systems are characterized. The structure of the telecommunication network and the classification of telecommunication systems are presented. The structure of the information system is predicted and the parameters of the information network effectiveness evaluation are determined. The complex of systems and mechanisms of protection for security of cyberspace and the main characteristic features of modern information resources are considered. The most actual tasks solved by information and telecommunication networks are determined. The elements of information and telecommunication systems are considered and the main vulnerabilities that arise during the processing of state information resources are outlined. The set of requirements for information and telecommunication systems in cyberspace for the purpose of processing and preservation of state information resources has been determined. The complexes of systems and mechanisms of protection for security of cyberspace are presented. The content of the protection of state information resources is determined. It is proposed to ensure the security of state information resources taking into account the vulnerabilities of information and telecommunication systems and their properties. It is proposed to conduct a detailed analysis of vulnerabilities in information and telecommunication systems, threats to state information resumes and attacks.

***Keywords:** state information resources, information and telecommunication systems, cyberspace, vulnerabilities of information systems, security of state information resources.*