МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ КОРАБЛЕБУДУВАННЯ
імені адмірала Макарова

СУЧАСНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ТРАНСПОРТІ

СПІБТ–2021

МАТЕРІАЛИ

IX Всеукраїнської науково-технічної конференції з міжнародною участю

01–03 грудня 2021 року

Національний університет кораблебудування
імені адмірала Макарова
Навчально-науковий інститут автоматики та електротехніки
просп. Центральний, 3, м. Миколаїв

МИКОЛАЇВ • НУК • 2021

УДК 004
У 45

ОРГАНІЗАТОРИ:

1. Міністерство освіти і науки України
2. Національний університет кораблебудування імені адмірала Макарова
3. ТОВ «БЕЗПЕКАІНФОСЕРВІС»
4. Науково-технічний центр «Квант»

Відповідальна за випуск В. В. Трибулькевич

У–45 **Сучасні** проблеми інформаційної безпеки на транспорті: матеріали IX Всеукраїнської науково-технічної конференції з міжнародною участю. – Миколаїв : НУК, 2021. – 219 с.

У збірнику подано матеріали IX Всеукраїнської НТК "Сучасні проблеми інформаційної безпеки на транспорті".

Розглянуті питання теорії та практики систем інформаційної безпеки транспортних засобів і систем, захисту інформації в каналах зв'язку та глобальних мережах передачі даних, захисту інформації на об'єктах інформаційної діяльності та в інформаційно-телекомунікаційних системах, а також питання підготовки кадрів у галузі знань «Інформаційна безпека».

Збірник може бути корисним для наукових співробітників, викладачів, інженерів та студентів.

УДК 004

[URL]: https://www. researchgate.net/publication/327449459_Survey_of_Attack_Projection_Prediction_and_Forecasting_in_Cyber_Security.

2. Бил Дж., Бейкер Э., Казуэлл Б. *Snort* 2.1. Обнаружение вторжений. – Бином-Пресс, 2009. – 656 с.

3. Бурячок В.Л. Технології забезпечення безпеки мережевої інфраструктури. [Підручник] / В.Л. Бурячок, А.О. Аносов, В.В. Семко, В.Ю. Соколов, П.М. Складанний. – К.: КУБГ, 2019. – 218 с.

4. Жук С.Я. Тенденції та перспективи розвитку інформаційної боротьби й інформаційної зброї / С.Я. Жук, В.О. Чмельов, Т.М. Дзюба // Наука і оборона. – 2006. – № 2. – С. 35–41.

5. Зоріна Т.І. Системи виявлення і запобігання атак в комп'ютерних мережах // Вісник Східноукраїнського Нац. ун-ту імені Володимира Даля. -2013 – № 15 (204). – Ч.1 2013. – С.48-52

6. Левченко М.П. Перспективи технології Honeypot, як засобу виявлення та дослідження атак // Матеріали VIII Всеукраїнської науково-технічної конференції з міжнародною участю «Сучасні проблеми інформаційної безпеки на транспорті».-Миколаїв: НУК, 2018 – С.130 – 133.

7. Турти М. Методика оптимізації систем захисту периметра // Матеріали 8-ої Міжнародної науково-технічної конференції «Інформаційні системи та технології ІСТ-2019». 9-14 вересня 2019 р. Харків – Коблеве. – Харків: ХНУРЕ, 2019. – С.254-259.

8. Турти М., Гратій А. Методика вибору спеціалізованого програмного забезпечення для захисту комп'ютерних мереж // Матеріали 9-ої Міжнародної науково-технічної конференції «Інформаційні системи та технології ІСТ-2020». – Харків: ХНУРЕ, 2020. – С.262-266.

УДК 004.056

РОЗРОБКА СИСТЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ЩОДО ПРОТИДІЇ ЕЛЕКТРОННІЙ РОЗВІДЦІ

Автори: *Худаніна Н.В., магістрант; Турти М.В., к.т.н., доцент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Україна, як і багато інших країн світу, в останні роки зробила сміливі кроки для побудови інформаційного суспільства, забезпечення кібербезпеки та технічного захисту об'єктів критичної інфраструктури.

При цьому Україна набула великий досвід протидії засобам електронної розвідки, у тому числі в ході збройного конфлікту на сході України.

Досвід показує, що особливу роль з точки зору противника в ході отримання закритої інформації відіграє використання засобів оптико-електронної розвідки.

Одна з найважливіших задач, яку доводиться вирішувати фахівцям з технічного захисту інформації – це аналіз наявних властивостей об'єкта захисту, виділення напрямів загроз, визначення критеріїв, що впливають на вибір моделей захисту, вибір кращого варіанта моделі технічного захисту із можливих до застосування.

Прийняти рішення в складних умовах в короткий часовий проміжок для повного і об'єктивного аналізу обстановки дозволяє Система підтримки прийняття рішень.

Розробка структури Системи підтримки прийняття рішень щодо протидії засобам оптико-електронної розвідки є складним завданням. Для досягнення поставленої мети необхідно розв’язати ряд задач:

– проведення аналізу нормативно-правової бази;
– проведення аналізу засобів оптико-електронної розвідки;
– проведення аналізу існуючих систем підтримки прийняття рішень;
– вибір сукупності критеріїв, на основі яких в подальшому будуть оцінюватися і зіставлятися можливі рішення;
– розробка структури Системи підтримки прийняття рішень щодо протидії засобам оптико-електронної розвідки.

Під оптико-електронної розвідкою розуміється процес добування інформації за допомогою засобів, що включають вхідну оптичну систему з оптичним приймачем і електронні схеми обробки електричного сигналу, які забезпечують прийом електромагнітних хвиль видимого та інфрачервоного діапазонів, випроменених або відбитих об'єктами і місцевістю.

Апаратура оптико-електронної розвідки встановлюється на космічних і повітряних носіях, а також може застосовуватися в наземних умовах.

Основними завданнями, які вирішуються при здійсненні захисних заходів від оптико-електронних засобів розвідки (ОЕЗР), є:

– виключення можливості (або зменшення ймовірності) виявлення об'єктів;

– виключення можливості (або зменшення ймовірності) розпізнавання об'єкта;

– виключення можливості (або зменшення ймовірності) визначення параметрів і характеристик об'єкта.

Завдання захисту від ОЕЗР повинні вирішуватися на всіх етапах життєвого циклу об'єкта: проектування, розробка, випробування, виробництво та експлуатація.

До числа основних загальних способів захисту від ОЕЗР відносяться:

– екранування;
– зменшення різниці випромінювання об'єкта і фону;
– зміна параметрів випромінювання та форми об'єкта;
– зміна складу і взаємного розташування об'єктів;
– створення активних перешкод.

З точки зору інформаційної безпеки засоби оптико-електронної розвідки (ОЕР) є одними з найбільш небезпечних, тому мета захисту інформації від несанкціонованого доступу через ОЕР дуже актуальна.

Також варто звернути увагу на те, що прийняття рішення про протидію, потрібних для цього сил і засобів в короткий часовий проміжок вимагає від оператора використання великого обсягу базової інформації, знання нормативних документів, вміння аналізувати інформацію, що надходить. Прийняти рішення в складних умовах дозволяє Система підтримки прийняття рішень.

Система підтримки прийняття рішень (СППР) (англ. Decision Support System, DSS) – це комп'ютерна автоматизована система, метою якої є допомога людям, які приймають рішення в складних умовах для повного та об'єктивного аналізу предметної діяльності.

Система підтримки прийняття рішень вирішує два основних завдання:

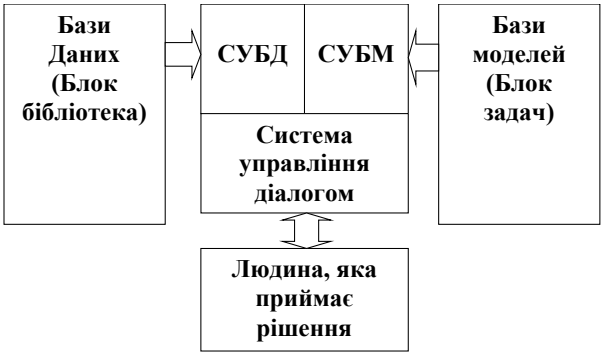
– вибір найкращого рішення з безлічі можливих (оптимізація);
– упорядкування можливих рішень за переважністю (ранжування).

В обох завданнях першим і найбільш принциповим моментом є вибір сукупності критеріїв, на основі яких в подальшому будуть оцінюватися і зіставлятися можливі рішення. Система СППР допомагає користувачеві зробити вибір.

Функціональні СППР є найбільш простими з точки зору архітектури. Відмінною особливістю функціональних СППР є те, що аналізу піддаються дані, що містяться у файлах операційних систем. Перевагами подібних СППР є компактність через використання однієї платформи і оперативність у зв'язку з відсутністю необхідності перевантажувати дані в спеціалізовану систему.

До складу СППР крім оператора входять три головні компоненти:

– підсистема обробки і зберігання даних;
– підсистема зберігання і використання моделей;
– програмна підсистема та блок інтерфейсу. Програмна підсистема включає в себе систему управління базою даних (СУБД), систему управління базою моделей (СУБМ) і систему управління діалогом між користувачем і комп'ютером (СУД).



Бази даних (Блок бібліотека) включає до себе:

– блок засобів ОЕР;
– блок засобів протидії ОЕР;
– блок засобів лазерного випромінювання;
– блок нормативно-правової бази.

Бази моделей (Блок задач) включають до себе:

– модель дослідження засобів ОЕР;
– модель дослідження захисту від ОЕР;

– модель дослідження засобів лазерного випромінювання.

СППР на базі ПЕОМ має функціонувати за наступним алгоритмом:

– моделюється процес зняття інформації засобами ОЕР з лазерного випромінювання;

– аналізуються канали витоку інформації;

– застосовуються заходи протидії засобам ОЕР;

– розраховується ефективність використання саме цих засобів;

– отриманий результат ефективності зіставляється з існуючими нормами захисту;

– формується перелік рішень з різними заходами протидії.

Якщо розрахована ефективність перевищує нормативні параметри, то використаний захисний комплекс є дієвим і користувач може приймати рішення про використання його на практиці з урахуванням специфіки організаційних питань. Якщо ж ефективність є низькою, даний захід не пропонується оператору до переліку рішень.

Список літератури:

1. Бабурин А.В., Пахомова А.С. Физические основы защиты информации // Воронеж – 2015

2. Глушков А.Н., Дробышевский Н.В., Кулешов П.Е Модель оптико-электронного средства как объекта разведки [URL]: https://cyberleninka.ru/article/n/model-optiko-elektronnogo-sredstva-kak-obekta-razvedki/viewer

3. Гуца О.Н., Ельчанинов Д.Б., Порван А.П., Якубовская С.В. Системы поддержки принятия решений в управлении проектами, основанные на качественных методах. [URL]: http://repository.kpi.kharkov.ua/handle/KhPI-Press/28278

4. Крюков С.В., Березовская Е.А. Системы поддержки принятия решений // Ростов на Дону, Таганрог. 2020

5. Куприянов В.В. Компьютерные системы поддержки принятия решений. Учебное пособие. М.: МГГУ, 2010.

6. Майстренко А.В., Майстренко Н.В. Информационные технологии в науке, образовании и инженерной практике // Тамбов – 2009 [URL]: https://www.tstu.ru/book/elib3/mm/2017/maistrenko/t6.html

7. Муромцев Д.Ю., Шамкин В.Н. Методы оптимизации и принятие проектных решений // Тамбов – 2015

8. Оптико-электронная разведка (ОЭР) [URL]: *https://studopedia.su/10_119247_optiko-elektronnaya-razvedka-oer.html*
9. Томашевський В.М. Моделювання систем // Київ – 2005

УДК 004.891.2

УСОВЕРШЕНСТВОВАНИЕ СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ДЛЯ ОЦЕНКИ УРОВНЯ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ

Авторы: *Чжан Фучен, магистрант, Национальный университет кораблестроения имени адмирала Макарова, г. Николаев, Украина; Ван Цяньци, магистрант, Государственный университет «Одесская политехника», г. Одесса, Украина*

Научный руководитель: *Нужний С.Н., к.т.н., доцент, зав. каф. КТИБ, Национальный университет кораблестроения имени адмирала Макарова, г. Николаев,Украина*

Аннотация: Эта статья основана на системе оценки распознавания речи искусственной нейронной сети, сочетающей искусственную нейронную сеть и традиционные методы для преодоления недостатков низкой производительности искусственной нейронной сети при описании временных динамических характеристик речевых сигналов и использования преимуществ традиционной речи, распознавание и нейронная сеть. Во-первых, речь предварительно обрабатывается, обнаруживается конечная точка, извлекаются признаки, и, наконец, MATLAB используется при исследовании и проектировании нейросетевой системы, благодаря чему возможности конструктора претерпевают качественные изменения и значительно расширяются.

Введение: В 21 веке, пока традиционные методы оценки качества речи все ещё развиваются, благодаря непрерывному развитию нейронных сетей и технологий глубокого обучения исследователи начали применять нейронные сети для оценки качества речи и продолжают развиваться и улучшаться. Он имитирует отображение восприятия человеческого слуха и использует различные методы машинного обу-

ЗМІСТ

Секція 1. Інформаційна безпека транспортних засобів і систем 3

Взаємозв'язок політики та Інтернет-простору: концептуальні засади електронної демократії *Ключко М.О.*; *Ніколаєнко В.І.*.....3

Особливості забезпечення інформаційної безпеки *Кузьміна А.І.* 7

Інформаційна безпека в публічному управлінні *Мороз Л.В.* 11

Комунікаційні технології в інформаційному просторі *Ніколаєнко Н.О.*; *Ключко О.О.*.....16

Інформаційна безпека України в умовах трансформації суспільства та зовнішньої агресії *Нофенко А.С.*.....20

Секція 2. Захист інформації на об'єктах інформаційної діяльності та в інформаційно-телекомунікаційних системах 26

Методика ефективної компоновки спеціалізованого програмного забезпечення для захисту комп'ютерних мереж *Гратій А.О.*; *Турти М.В.* 26

Технології комп'ютерного зору в системах «Розумній будинок» *Дідківський О.О.*.....31

Захист інформації в інформаційно-телекомунікаційній системі спеціального призначення *Дмитриченко Г.Б.* 34

Удосконалення алгоритму поточного шифрування RC4 *Дюльдев В.О.*; *Михайлов М.М.*; *Пожидаев М.Г.*.....39

Оцінка впливу реверберації на розбірливість мови, спотвореної стаціонарним шумом *Змієвець В.Р.*.....42

Вплив рівня мовленнєвого сигналу на залежність розбірливості мови від відношення сигнал/шум *Касьянов Ю.І.*; *Золотченко В.В.*; *Іванова А.В.*; *Іванов В.І.* 47

Щодо текстового матеріалу при дослідженні узагальнених спектрів мовленнєвого сигналу *Касьянов Ю.І.*; *Хівріч В.В.*; *Михайличенко А.В.*; *Трощенко С.С.* 53

Виявлення локального порушення цілісності цифрового зображення в умовах геометричних перетворень неоригінальної області *Кобозєва А.А.*; *Бобок І.І.* 59

Алгоритм моніторингу технічного стану інформаційно-комп'ютерних мереж наукових установ *Козирєв С.С.* 63
Дослідження системи захищеного документообігу на базі порталу державних послуг «Дія» *Козирєва Н.Є.* 67
Розробка системи підтримки прийняття рішень щодо методів і засобів аудиту IT-інфраструктури підприємства *Кравцова О.С.* 72
Розробка шаблону комплексної системи захисту інформації для підприємства припортової галузі *Нікулін О.С.* 78
Нові підходи до створення систем запобігання витоку мовної інформації за межі контрольованої зони *Нужний С.М.* 83
Диспетчер доступу до потокового відеоресурсу *Самойленко Д.М.* 91
Методика створення космпексної системи захисту інформації в автоматизованій системі класу 1 *Смолєнцева О.Ю.* 94
Методи і засоби захисту інформації у технічних каналах на підприємствах *Ткаченко О.П.* 100
Віртуалізація системи відеоспостереження *Трибулькевич С.Л.* 105
Методики вибору системи запобігання вторгненням в корпоративну комп'ютерну мережу *Холявко О.О.* 114
Розробка системи підтримки прийняття рішень щодо протидії електронній розвідці *Худаніна Н.В.*; *Турти М.В.* 119
Усовершенствование системы поддержки принятия решений для оценки уровня защиты речевой информации *Чжан Фучен*; *Ван Цяньци* 124

Секція 3. Правові аспекти діяльності і кадрова політика в галузі інформаційної безпеки 128
Influence of power supplies on information security and quality indicators of automated systems *Li Jiaxian*; *Turty M.V.* 128
Development of methods for improving the availability of information in automated augmented reality systems *Wu Liming*; *Turty M.V.* 135
Design of integrated navigation for underwater vehicle with multiple sensor information fusion *Xue Chenglei* 142

Наукове видання

СУЧАСНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ТРАНСПОРТІ

СПІБТ–2021

IX Всеукраїнська науково-технічна конференція
з міжнародною участю

01–03 грудня 2021 року

Національний університет кораблебудування
імені адмірала Макарова
Навчально-науковий інститут автоматики та електротехніки
просп. Центральний, 3, м. Миколаїв

МАТЕРІАЛИ КОНФЕРЕНЦІЇ

(*українською, російською та англійською мовами*)

Відповідальна за випуск В. В. Трибулькевич