НАЦИОНАЛЬНАЯ АКАДЕМИЯ НАУК УКРАИНЫ
ИНСТИТУТ ПРОБЛЕМ МОДЕЛИРОВАНИЯ В ЭНЕРГЕТИКЕ

НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

КИБЕРБЕЗОПАСНОСТЬ ЭНЕРГЕТИКИ

ПРИГЛАШЕНИЕ
ПРОГРАММА
МАТЕРИАЛЫ

29 мая -02 июня 2018 г.
г. Одесса,
Аркадия,
ОК «Одесса»

2018

Глубокоуважаемый участник _____

_____

Приглашаем Вас принять участие в работе научно-практической конференции «Кибербезопасность энергетики», которая будет проходить в период с 29 мая по 02 июня 2018 года на базе отельного комплекса «Одесса» (г. Одесса).

СООРГАНИЗАТОРЫ КОНФЕРЕНЦИИ

ГОСУДАРСТВЕННАЯ СЛУЖБА СПЕЦИАЛЬНОЙ СВЯЗИ И ЗАЩИТЫ ИНФОРМАЦИИ УКРАИНЫ

МИНИСТЕРСТВО ЭНЕРГЕТИКИ И УГОЛЬНОЙ ПРОМЫШЛЕННОСТИ УКРАИНЫ

НАЦИОНАЛЬНАЯ КОМИССИЯ ГОСУДАРСТВЕННОГО РЕГУЛИРОВАНИЯ В СФЕРАХ ЭНЕРГЕТИКИ И КОММУНАЛЬНЫХ УСЛУГ

НАЦИОНАЛЬНОЕ АГЕНТСТВО ПО АККРЕДИТАЦИИ УКРАИНЫ

КИЕВСКАЯ ТОРГОВО-ПРОМЫШЛЕННАЯ ПАЛАТА

АССОЦИАЦИЯ «ИНФОРМАТИО-КОНСОРЦИУМ»

ООО «ИНФОРМАТИО»

РЕГЛАМЕНТ
РАБОТЫ КОНФЕРЕНЦИИ

29 мая – вторник

Время	Мероприятие
13.00 – 19.00	Регистрация, оформление и размещение участников конференции.
19.00 – 21.00	Неформальное открытие конференции. Приветственный ужин.
Время для неформального общения участников	

30 мая – среда

Время	Мероприятие
08.00 – 11.00	Завтрак
11.00 – 13.00	Работа конференции. Выступления участников.
13.00 – 14.00	Обед
14.00 –16.00	Работа конференции. Выступления участников.
16.00 –18.00	Работа семинара «Менеджмент информационной безопасности.
Время для неформального общения участников	

31 мая – четверг

Время	Мероприятие
08.00 – 11.00	Завтрак
11.00 – 13.00	Работа конференции. Выступления участников.
13.00 – 14.00	Обед
14.00 –16.00	Работа конференции. Выступления участников.
16.00 –18.00	Работа семинара «Менеджмент информационной безопасности.
Время для неформального общения участников	

01 июня – пятница

Время	Мероприятие
08.00 – 11.00	Завтрак
11.00 – 13.00	Работа конференции. Выступления участников.
13.00 – 14.00	Обед
14.00 –16.00	Работа конференции. Выступления участников.
16.00 –18.00	Работа семинара «Менеджмент информационной безопасности.
Время для неформального общения участников	

02 июня – суббота

Время	Мероприятие
08.00 – 09.00	Завтрак
09.00 – 12.00	Подведение итогов работы конференции. Принятие решений. Закрытие конференции. Сдача номеров (до 12.00).
Время для неформального общения участников	

Примечание: в регламенте работы конференции возможны изменения

ПРОГРАММА
РАБОТЫ КОНФЕРЕНЦИИ

29 мая. Вторник

ВСТУПИТЕЛЬНАЯ ИНФОРМАЦИЯ

НЕФОРМАЛЬНОЕ ОТКРЫТИЕ КОНФЕРЕНЦИИ.

30 мая. Среда

ОФИЦИАЛЬНОЕ ОТКРЫТИЕ КОНФЕРЕНЦИИ.

ВСТУПИТЕЛЬНОЕ СЛОВО.

Мохор Владимир Владимирович –
член-корреспондент Национальной академии наук Украины, доктор технических наук, профессор, директор Института проблем моделирования в энергетике им. Г.Е. Пухова Национальной академии наук Украины

ПЛЕНАРНОЕ ЗАСЕДАНИЕ - ДИСКУССИЯ

ЗАГАЛЬНІ ВИМОГИ З КІБЕРЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В КОНТЕКСТІ ВИМОГ ЗАКОНУ УКРАЇНИ «ПРО ОСНОВНІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ»

Бакалинский Александр Олегович –
заместитель директора департамента формирования и реализации государственной политики в сфере киберзащиты, Государственная служба специальной связи и защиты информации Украины

SPEAR: ПРОТОКОЛЫ И ПОЛИТИКИ КИБЕРГИГИЕНЫ В ЭНЕРГЕТИКЕ

Коцюба Игорь Васильевич –
помощник директора Института проблем моделирования в энергетике им. Г.Е. Пухова Национальной академии наук Украины

GDPR - ШЛЯХ ДО ВІДПОВІДНОСТІ

Макаревич Александр Евгеньевич –
офицер по кибербезопасности,
юридическая фирма «Астерс»

GDPR – УЧЕБНЫЙ КУРС ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

Гончар Сергей Феодосьевич –
кандидат технических наук, ученый секретарь Института проблем моделирования в энергетике им. Г.Е. Пухова Национальной академии наук Украины

СЕМИНАР «МЕНЕДЖМЕНТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ».

ОНТОЛОГИЧЕСКИЙ ПОДХОД К ПОСТРОЕНИЮ АРХИТЕКТУР СИСТЕМ УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ

Коваленко Алексей Епифанович –
кандидат технических наук, доцент, старший научный сотрудник отдела № 235 Института проблем математических машин Национальной академии наук Украины

31 мая. Четверг

ПЛЕНАРНОЕ ЗАСЕДАНИЕ - ДИСКУССИЯ.

АСПЕКТИ ПРАКТИЧНОЇ ДІЯЛЬНОСТІ ДЕРЖАВНОГО ЦЕНТРУ КІБЕРЗАХИСТУ ТА ПРОТИДІЇ КІБЕРЗАГРОЗАМ ДЕРЖСПЕЦЗВ'ЯЗКУ У ЗАБЕЗПЕЧЕННІ КІБЕРБЕЗПЕКИ ТА КІБЕРЗАХИСТУ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Худинцев Николай Николаевич –
первый заместитель начальника Государственного центра киберзащиты и противодействия киберугрозам, Государственная служба специальной связи и защиты информации Украины

СОВРЕМЕННЫЕ ТЕХНОЛОГИИ КИБЕР-АТАК НА ИНФОРМАЦИОННЫЕ СИСТЕМЫ

Мисник Алексей Игоревич –
аспирант Института проблем моделирования в энергетике им. Г.Е. Пухова Национальной академии наук Украины.

СЕМИНАР «МЕНЕДЖМЕНТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ».

ОНТОЛОГИЧЕСКИЙ ПОДХОД К ПОСТРОЕНИЮ АРХИТЕКТУР СИСТЕМ УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ

Коваленко Алексей Епифанович –
кандидат технических наук, доцент, старший научный сотрудник отдела № 235 Института проблем математических машин Национальной академии наук Украины

01 июня. Пятница

ПЛЕНАРНОЕ ЗАСЕДАНИЕ - ДИСКУССИЯ.

ПРАКТИЧНІ АСПЕКТИ ПОБУДОВИ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ
Комаров Максим Юрьевич –
начальник отдела Государственного научно-исследовательского института специальной связи и защиты информации, Государственная служба специальной связи и защиты информации Украины

МОДЕЛЮВАННЯ НАДІЙНОСТІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ОБЛАДНАННЯ ЕНЕРГЕТИЧНИХ СИСТЕМ УКРАЇНИ
Гнатюк Сергей Евгеньевич –
кандидат технических наук, Администрация Государственной службы специальной связи и защиты информации Украины

15.00–17.00 ***СЕМИНАР «МЕНЕДЖМЕНТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ».***

АКТУАЛИЗАЦИЯ СЕМЕЙСТВА МЕЖДУНАРОДНЫХ СТАНДАРТОВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ISO / IEC 27K
Бакалинский Александр Олегович –
заместитель директора департамента формирования и реализации государственной политики в сфере киберзащиты, Государственная служба специальной связи и защиты информации Украины

02 июня. Суббота

ПОДВЕДЕНИЕ ИТОГОВ РАБОТЫ КОНФЕРЕНЦИИ.

ПРИНЯТИЕ РЕШЕНИЙ.

ЗАКРЫТИЕ КОНФЕРЕНЦИИ.

Примечание: в регламенте работы конференции возможны изменения

ЗАГАЛЬНІ ВИМОГИ З КІБЕРЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В КОНТЕКСТІ ВИМОГ ЗАКОНУ УКРАЇНИ «ПРО ОСНОВНІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ»

Бакалинський О.О., Державна служба спеціального зв'язку та захисту інформації України, Київ

З початком військової агресії Російської Федерації проти України розпочалась активна фаза війни і у кіберпросторі. Об'єктами нападу супротивника стали українські інформаційні ресурси, сайти центральних органів державної влади, інформаційна інфраструктура об'єктів критичної інфраструктури держави, в тому числі і об'єкти енергетики. Однією із нагальних потреб української держави стало забезпечення кібербезпеки держави, суспільства та громадянина.

Першим документом, який визначив основні напрями забезпечення кібербезпеки стала затверджена Указом Президента України від 27.01.2016 року "Стратегія кібербезпеки України" (далі - Стратегія) [1]. В підтримку Стратегії у 2016-2017 роках вийшла ціла низка документів, яки розвивали положення Стратегії та підкріплювали основні напрями забезпечення кібербезпеки України. Ними стали, розроблені Радою національної безпеки та оборони документи, які було введено Указами Президента України: «Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури». від 16.01.2017 року, «Про загрози кібербезпеці держави й негайні заходи з їх нейтралізації» від 29.12.2016 року, Постанови Кабінету Міністрів України «Порядок формування переліку ІТС об'єктів критичної інфраструктури держави» № 563 від 23.08.2016 року та інші нормативно-правові акти. Одночасно з цим, Верховною Радою України було розроблено та 05.10.2017 року прийнято Закон України «Про основні засади забезпечення кібербезпеки України» (далі - Закон) [2].

Закон є «рамковим» – тобто він є основою для розробки та ухвалення інших законодавчих та підзаконних актів, а також містить низку норм прямої дії, що дає змогу застосовувати значну частину нових інструментів державної політики та реалізовувати новітні технологічні проекти. Майже 80% дій і заходів, визначених Законом – компетенції Держспецзв'язку. Він вводить новий сучасний термінологічний і поня-

тійний апарат основних визначень таких як кіберпростір, кібербезпека, кіберзахист, кіберзлочин (комп'ютерний злочин), кібершпіонаж, кібертероризм, кібероборона, кіберзагроза, кібератака, інцидент кібербезпеки, об'єкт критичної інфраструктури (далі - ОКІ), об'єкт критичної інформаційної інфраструктури (далі - ОКІІ), національні електронні інформаційні ресурси, аудит інформаційної безпеки. Визначає основних суб'єктів забезпечення кібербезпеки, їх повноваження, протоколи взаємодії, систему координації та контролю їх діяльності. Врегульовує питання кібербезпеки ОКІ усіх форм власності, кіберзахисту їх ІТС, а також запроваджує систему незалежного аудиту інформаційної безпеки. Встановлює відповідальність власників та/або керівників ОКІ за забезпечення кіберзахисту, невідкладне інформування про інциденти кібербезпеки, організацію проведення незалежного аудиту інформаційної безпеки. Визначає та врегульовує діяльність Державного центру кібербезпеки, урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA.

Одже, Законом встановлено наступні основні завдання Адміністрації Держспецзв'язку: формування та реалізацію державної політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту ОКІ, здійснення державного контролю у цих сферах; координація діяльності інших суб'єктів забезпечення кібербезпеки щодо кіберзахисту; забезпечує створення та функціонування Національної телекомунікаційної мережі, впровадження організаційно-технічної моделі 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 впровадження аудиту інформаційної безпеки на ОКІ, встановлення вимог до аудиторів інформаційної безпеки, визначення порядку їх атестації (переатестації); координація, організація та проведення аудиту захищеності комунікаційних і технологічних систем ОКІ на вразливість; забезпечення функціонування Державного центру кіберзахисту, урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA.

Найбільш новаторською та цікавою нормою Закону є стаття 10, яка присвячена державно-приватній взаємодії у сфері кібербезпеки. Зокрема зазначено, що «державно-приватна взаємодія у сфері кібербезпеки може здійснюватись різними шляхами, наприклад: створенням системи своєчасного виявлення, запобігання та нейтралізації кіберзагроз, у тому числі із залученням волонтерських організацій; підвищенням цифрової грамотності громадян та культури безпекового поводження в кіберпросторі, комплексних знань, навичок і вмінь, необхідних для підтримки цілей кібербезпеки, реалізації державних і громадських проектів з підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту та іншими».

З метою виконання вимог Закону було розроблено «План дій уряду», згідно яким Адміністрація Держспецзв'язку повинна розробити в рамках своєї компетенції низку нормативно-правових актів, а саме – пректи Постанов Кабінету міністрів України: «Про затвердження порядків формування переліку об'єктів критичної інформаційної інфраструктури та порядку внесення об'єктів критичної інформаційної інфраструктури до державного реєстру, його формування та забезпечення функціонування», «Вимоги та порядок проведення незалежного аудиту на об'єктах критичної інфраструктури», «Загальні вимоги з кіберзахисту об'єктів критичної інфраструктури», «Про затвердження порядків формування переліку об'єктів критичної інфраструктури та порядку внесення об'єктів критичної інфраструктури до державного реєстру, його формування та забезпечення функціонування».

В рамках реалізації Стратегії, Адміністрації Держспецзв'язку також необхідно підготувати та подати на розгляд Верховної Ради України проект Закону України «Про внесення змін до Закону України «Про Державну службу спеціального зв'язку та захисту інформації України»», прийняття якого б надало Службі повноважень щодо забезпечення можливості резервного копіювання інформації, необхідність зберігання якої повинні визначати центральні органи виконавчої влади, та до Постанови кабінету Міністрів України «Про затвердження Порядку підключення до глобальних мереж передачі даних». Ці зміни повинні дозволити, як державним органам, так і об'єктам критичної інфраструктури держави отримати гарантовані послуги із забезпечення кіберзахисту своїх ресурсів.

Як відмічалось раніше, одним із основних завдань Адміністрації Держспецзв'язку є визначення загальних вимог з кіберзахисту ОКІ та мінімального складу заходів із забезпечення кіберзахисту ОКІ. Такі вимоги, як відмічалось раніше, будуть вводитись в дію постановою Кабінету Міністрів України. Складність формування вимог визначаєть-

ся різноманітністю ОКІ України, належністю до різних галузей, різною ступеню залежності їх функціонування від інформаційно-телекомунікаційних систем, різною формою власності, наявністю міжнародних та галузевих вимог для певних видів ОКІ, різними потенціальними наслідками реалізації кіберзагроз. Крім того, специфікою функціонування деяких ОКІ є обробка в їх інформаційно-телекомунікаційних системах інформації, необхідність захисту якої визначено законодавством та задля захисту якої має бути побудована комплексна система захисту інформації з підтвердженою відповідністю.

З метою розмежування підходів щодо забезпечення кіберзахисту ОКІІ ОКІ в яких циркулює інформація, необхідність захисту якої визначено законодавством, та ОКІІ в яких така інформація не циркулює, в проекті постанови пропонується ввести нове визначення: «система інформаційної безпеки – сукупність організаційних та технічних заходів, а також засобів і методів захисту інформації, які впроваджуються на ОКІІ ОКІ (далі – ОКІІ або Система) з метою запобігання кіберінцидентам, виявлення та захисту від кібератак, порушення конфіденційності, цілісності та доступності інформаційних ресурсів, що обробляються (передаються, зберігаються) в ОКІІ, порушення режиму функціонування та/або недоступності служб (функцій) Системи, порушення функціонування компонентів Системи тощо». В проекті Постанови пропонується будувати систему інформаційної безпеки на ОКІ, в ОКІІ яких не обробляється інформація, обов'язковість захисту якої визначено законодавством, а на інших ОКІ будувати комплексну систему захисту інформації з урахуванням Загальних вимог з кіберзахисту.

Визначено що метою забезпечення кіберзахисту ОКІ є запобігання кіберінцидентам, виявлення та захисту від кібератак, порушення конфіденційності, цілісності та доступності інформаційних ресурсів, що обробляються (передаються, зберігаються) в ОКІІ, порушення режиму функціонування та/або недоступності служб (функцій) Системи, порушення функціонування компонентів Системи тощо. Кіберзахист ОКІ забезпечується впровадженням на ОКІІ сукупності організаційних та технічних заходів, а також засобів і методів захисту інформації.

Необхідно зауважити на те, що кіберзахист ОКІ є складовою частиною робіт зі створення (модернізації) та експлуатації ОКІІ. Заходи з кіберзахисту повинні бути передбачені та впроваджені на всіх стадіях життєвого циклу ОКІІ.

Відповідно до [1] за забезпечення кіберзахисту об'єкта критичної інфраструктури відповідає власник та/або керівник ОКІ. Крім того, Загальними вимогами з кіберзахисту об'єктів критичної інфраструктури

вводиться обов'язок власника та/або керівника ОКІ організувати невідкладне інформування урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA (у разі наявності – галузевий CERT) про кіберінциденти та кібератаки, які стосуються його ОКІІ, у порядку встановленому Адміністрацією Держспецзв'язку. Такий порядок має бути визначено у «Протоколі спільних дій суб'єктів забезпечення кібербезпеки», який має вводитись в дію також Постановою Уряду.

До того ж, з метою підвищення рівня кіберзахисту та з метою оперативного виявлення та реагування на кібератаки, моніторингу подій, які відносяться до мережевої безпеки, на ОКІІ державних органів влади, а також на ОКІІ підприємств, установ та організацій різних форм власності, перелік яких визначається Кабінетом Міністрів України, пропонується встановлювати засоби Системи кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури Держспецзв'язку, які взаємодіють з Центром реагування на кіберінциденти. Задля забезпечення захищеного доступу та запобігання кібератакам державні органи влади можуть отримувати доступ до мережі Інтернет через Систему захищеного доступу державних органів до Інтернету, а з метою забезпечення захищеного обміну та зберігання державних інформаційних ресурсів, підключення до Системи захищеного доступу державних органів до Інтернету, державні органи влади можуть використовувати засоби Національної телекомунікаційної мережі.

Ще одним із важливих аспектів забезпечення кіберзахисту ОКІ є забезпечення відмовостійкості компонентів ОКІІ, власник та/або керівник якого, забезпечує створення резервних копій своїх інформаційних ресурсів, для оперативного відновлення у разі їх пошкодження або знищення. Органи державної влади для збереження резервних копій своїх інформаційних ресурсів використовують основний та резервний захищений дата-центр збереження інформації і відомостей державних інформаційних ресурсів Держспецзв'язку.

Організаційні та технічні заходи з кіберзахисту, які впроваджуються в ОКІІ, повинні забезпечувати: визначення в ОКІ загальної політики інформаційної безпеки; управління доступом суб'єктів доступу до об'єктів захисту ОКІІ; ідентифікацію та автентифікацію суб'єктів доступу та об'єктів захисту ОКІІ; реєстрацію подій компонентами ОКІІ та їх періодичний аудит; мережевий захист компонентів та інформаційних ресурсів ОКІІ; забезпечення доступності та відмовостійкості компонентів та інформаційних ресурсів ОКІІ; визначення умов використання змінних носіїв інформації в ОКІІ; визначення умов використання про-

грамного та апаратного забезпечення ОКІІ; визначення умов розміщення компонентів ОКІІ.

Також в Загальних вимогах передбачено можливість застосування заходів нейтралізації загроз за допомогою окремих заходів, або групи заходів, які або повністю блокують загрозу, або зменшують ризик її реалізації. Вибір необхідного складу заходів, доповнення, заміна та/або виключення заходів з переліку мінімально необхідного складу заходів можливо на підставі аналізу розрахованих ризиків, методичною основою для розрахунку яких пропонується міжнародний стандарт із сімейства ISO/IEC 27k.

Отже, перспективними напрямами розвитку системи кіберзахисту України є:

- нормативно-правове врегулювання питань кіберзахисту та кібербезпеки.
- налагодження міжнародного співробітництва з питань кіберзахисту та кібербезпеки.
- дооснащення Команди реагування на комп'ютерні надзвичайні події України CERT-UA.
- розбудова оперативного центру реагування на кіберінциденти.
- модернізація центрального сегменту Системи захищеного доступу державних органів до Інтернету.
- побудова Національної телекомунікаційної мережі.
- модернізація системи освіти за спеціальністю 125 Кібербезпека.
- побудова галузевих Центрів реагування на кіберінциденти.

До того ж, розроблені Загальні вимоги з кіберзахисту ОКІ держави є сучасними та актуальними, перспективою подальшого розвитку цих вимог вбачається подальша гармонізація українського законодавства з європейським. При побудові систем інформаційної безпеки (комплексних систем захисту інформації) ОКІІ необхідно пам'ятати, що подібні системи мають створюватись, розвиватись та масштабуватись в залежності від специфіки роботи ОКІ та періодично переглядатись як під час незалежного аудиту інформаційної безпеки, так і після суттєвих кіберінцидентів та кібератак, або у заплановані проміжки часу.

Література

1. Указ Президента України №96/2016 Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України", режим доступу - http://www.president.gov.ua/documents/962016-19836.

2. Закон України «Про основні засади забезпечення кібербезпеки України» від 5.10.2017 року - режим доступу http://zakon5.rada.gov.ua/laws/show/2163-19.

МОДЕЛЮВАННЯ НАДІЙНОСТІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ОБЛАДНАННЯ ЕНЕРГЕТИЧНИХ СИСТЕМ УКРАЇНИ

Гнатюк С.Є., Адміністрація Державної служби спеціального зв'язку та захисту інформації України, Київ.

Сакович Л.М., Інститут спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут» ім. Ігоря Сікорського, Київ.

Романенко В.П., Інститут спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут» ім. Ігоря Сікорського, Київ.

У забезпеченні кібербезпеки енергетики важливим елементом є надійність програмного забезпечення (ПЗ) обладнання енергетичних систем України. Об'єм ПЗ постійно збільшується і оновлюється з удосконаленням і модернізацією обладнання в напрямку забезпечення захищеності інформації.

Питання забезпечення необхідних значень показників надійності ПЗ досить глибоко розглянуті й досліджені в наукових роботах вітчизняних і зарубіжних авторів, серед яких Волочій Б.Ю., Маєвський Д.А., Половко А.М., Харченко В.С., Яковина В.С., Pham H., Nordmann L., Zhang X., Yamada S., Tokuno K., Osaki S., Okumoto K.A. та багато інших. У цих роботах досліджені моделі, методи, способи оцінки надійності ПЗ на етапах його розробки, але недостатньо враховуються особливості оцінки показників надійності після завершення тестових випробувань в початковий період використання за призначенням. Тобто виникає необхідність створення моделей надійності ПЗ для оцінки кількості помилок, які невиявлені під час попередніх випробувань. Рішення зазначеної задачі пропонується у доповіді за рахунок отриманих нових аналітичних виразів обчислення і прогнозування показників надійності ПЗ за критерієм мінімуму середньоквадратичного відхилення (СКВ) результатів моделювання від експериментальних даних початкового періоду експлуатації. Авторами удосконалено статичну та розроблено нову динамічну моделі надійності ПЗ, які відрізняються

мінімізацією значення СКВ результатів від показників надійності у період дослідної експлуатації обладнання.

Статична модель надійності ПЗ – сукупність аналітичних виразів, що описують функціональні залежності показників надійності від часу і дозволяють отримати їх кількісну оцінку для визначення надійності системи в цілому у реальних умовах експлуатації при щомісячному обліку кількості відмов в постійних умовах використання за призначенням. Модель призначена для кількісної оцінки і прогнозування значень показників надійності ПЗ за результатами обробки статистичних даних про відмови за деякий період часу із заданою достовірністю.

В результаті аналізу даних підконтрольної експлуатації за n місяців і припущенні про експоненціальний закон зміни числа відмов ПЗ від часу з використанням методу найменших квадратів виконується апроксимація залежності експериментальних даних від часу, після чого обчислюються значення коефіцієнтів статичної моделі надійності ПЗ.

Сутність моделі полягає в отримані кількісної оцінки показників надійності ПЗ при заданих обмеженнях і припущеннях на базі використання нових функціональних залежностей, які враховують зміну значень показників від часу, та нових алгоритмів їх розрахунку.

Вихідні дані для використання методу у випадку щомісячного підведення підсумків про відмови: K_m – число відмов ПЗ за місяць m; T – період прогнозування показників надійності ПЗ.

Обмеження на використання моделі: умови експлуатації за час отримання початкових даних і на період прогнозування постійні; ПЗ функціонує у середовищі близькому до реальних умов експлуатації.

Припущення при використанні моделі: інтенсивність виявлення помилок пропорційна їх поточному числу в ПЗ; всі помилки ПЗ однаково ймовірні й їх поява незалежна одна від іншої; проява кожної помилки веде до порушення правильності функціонування ПЗ; час до наступної відмови ПЗ розподілений експоненціально; помилки ПЗ після виявлення усуваються без внесення нових; інтенсивність виявлення помилок постійна в інтервалі між двома суміжними моментами появи помилок.

Основні аналітичні вирази і функціональні залежності використаних моделей зведені в табл. 1. Адекватність моделі підтверджується за критерієм узгодження χ^2 Пірсона за виразом

$$\chi^2 = \sum_{m=1}^{n} \frac{(N_m - K_m)^2}{N_m},$$

де Nm – прогнозована кількість відмов ПЗ. У даному випадку адекватність моделі кількісно оцінюється мінімальним значенням СКВ результатів моде-

лювання від статистичних даних про відмови, отримані в процесі дослідної або підконтрольної експлуатації обладнання.

Ефект від використання удосконаленої моделі в порівняні з відомими полягає в підвищенні точності кількісної оцінки і прогнозування значень показників надійності ПЗ: розрахункове значення числа відмов ПЗ за T місяців експлуатації відрізняється від істинного всього на 1,5 %; помилка в оцінці числа відмов ПЗ за місяць експлуатації не перевищує 0,6%; зменшення значення СКВ результатів обчислень від експериментальних даних за n місяців експлуатації, порівняно із кращими з відомих моделей, до 9%.

Таблиця 1

Функціональні залежності та аналітичні вирази кількісних оцінок значень показників надійності ПЗ статичної моделі надійності

Показник надійності ПЗ	Розрахунок a і b	Розрахунок A_1, K, u
Значення коефіцієнтів моделі за результатами апроксимації даних про відмови ПЗ	$b = \ln(A_n / A_1)/(1-n)$ $a = A_1 (A_n/A_1)^{1/(1-n)}$	Розрахунок методом найменших квадратів на ЕОМ
Кількість відмов ПЗ за місяць m (N_m)	$a \exp(-mb)$	$A_1 (A_n/A_1)^{(1-m)/(1-n)}$
Сумарна кількість відмов ПЗ за T місяців (N_T)	$\frac{a(e^{bT}-1)}{e^{bT}(e^{b}-1)}$	$\frac{A_1\left[A_n/A_1\right)^{T/(1-n)}-1]}{(A_n/A_1)^{(T-1)/(1-n)}\left[A_n/A_1\right)^{1/(1-n)}-1]}$
Ймовірність безвідмовної роботи ПЗ за місяць m (Pnm)	$\exp(-ae^{-mb})$	$\exp\left[-A_1\left(\frac{A_n}{A_1}\right)^{\frac{m-1}{n-1}}\right]$
Інтенсивність потоку відмов ПЗ за місяць m (λ_m)	$-ab(A_n/A_1)^{m}$	$\frac{A_1(A_n/A_1)^{\frac{m-1}{n-1}}\ln(A_n/A_1)}{1-n}$
Напрацювання ПЗ на відмову за місяць m (T_{nm})	$-(A_n/A_1)^{-m}/ab$	$\frac{1-n}{A_1(A_n/A_1)^{\frac{m-1}{n-1}}\ln(A_n/A_1)}$
Середньоквадратичне відхилення результатів прогнозування N_m від даних про відмови ПЗ за n місяців (σ)	$\sqrt{\frac{1}{n}\sum_{m=1}^{n}\left(ae^{-mb}-K_m\right)^2}$	$\sqrt{\frac{1}{n}\sum_{m=1}^{n}\left(A_1\left(A_n/A_1\right)^{\frac{m-1}{n-1}}-K_m\right)^2}$

Відрізняється від відомих: доступним набором вихідних даних і можливістю використання в реальних умовах експлуатації обладнання для оцінки та прогнозування надійності ПЗ; припущеннями та обмеженнями на використання, які відповідають реальним умовам експлуатації обладнання; зменшенням значення СКВ результатів моделювання від експериментальних даних за рахунок використання нових алгоритмів розрахунку значень коефіцієнтів моделі; позитивним ефектом від використання, що полягає у підвищенні точності оцінки і прогнозування значень показників надійності ПЗ.

Достовірність результатів моделювання підтверджується використанням апробованого математичного апарату, подібністю результатів до відомих в часткових випадках, а її адекватність – перевіркою відповідності результатів розрахунків дослідним даним за критерієм узгодження і мінімізацією значення СКВ.

Динамічна модель надійності ПЗ – функціональна залежність загальної кількості відмов з початку експлуатації, що прогнозується на заданий період часу, від статистичних даних для оцінки надійності системи в реальних умовах експлуатації при фіксації відмов у момент їх виявлення в постійних умовах використання за призначенням.

Аналіз залежності сумарних даних про відмови (N_{cm}) від часу з початку експлуатації (m) показує можливість їх апроксимації функцією виду

$$N_{cm} = a\left(\frac{m}{T}\right)^{b} \exp\left(-\frac{m}{T}b\right),$$

де T – період прогнозування числа відмов ПЗ.

Значення коефіцієнтів a і b обчислюються за результатами апроксимації експериментальних даних за час i та j із початку експлуатації ($1 < i < j < m$) та уточнюються методом найменших квадратів. Основні математичні вирази для кількісних оцінок доступності і показників надійності ПЗ приведені в табл. 2.

Укрупнений алгоритм реалізації моделі складається з наступних операцій: отримання та аналіз вихідних даних за результатами підконтрольної експлуатації виробів; апроксимація залежності сумарної кількості відмов від часу; розрахунок коефіцієнтів динамічної моделі за алгоритмом; розрахунок кількісних показників надійності ПЗ за виразами табл. 2; вивід результатів моделювання у вигляді таблиць або функціональних залежностей.

Адекватність динамічної моделі кількісно оцінюється мінімальним значенням СКВ результатів моделювання від вихідних статистичних даних про відмови ПЗ.

Ефект від використання динамічної моделі полягає в зменшенні значень σ (більше 9%), δN (до 5%), δNст (до 3,1%).

Наукова новизна моделі полягає в тому, що вперше: запропонована нова динамічна модель надійності ПЗ із обґрунтуванням достовірності та адекватності отриманих результатів; в моделі на відмінну від відомих використані нові аналітичні вирази для розрахунку показників надійності ПЗ (табл. 2), які уточнюють функціональні залежності їх зміни з часом; пропонується новий алгоритм розрахунку коефіцієнтів моделі; розроблений новий алгоритм реалізації динамічної моделі надійності ПЗ, що забезпечує мінімізацію значення результатів моделювання від експериментальних даних про експлуатаційну надійність.

Таблиця 2

Функціональні залежності та аналітичні вирази розрахунку кількісних оцінок значень показників надійності ПЗ в процесі експлуатації

Показник надійності ПЗ	Аналітичний вираз розрахунку показника
Значення коефіцієнтів моделі за результатами апроксимації даних про відмови ПЗ	$b = \frac{\ln(N_{ci} / N_{cj})}{(i-j)/T - \ln(i/T) + \ln(j/T)}$ $a = N_{ci} \Big/ \left[\left(\frac{i}{T} \right)^{b} \exp(-ib/T) \right];$ $0 < i < j \le T$
Кількість відмов ПЗ за місяць m (N_m)	$\frac{a}{T^{b}} \cdot \frac{m^{b} - (m-1)^{b} e^{b/T}}{e^{mb/T}}$
Сумарна кількість відмов ПЗ за T місяців (N_T)	$a \exp(-b)$
Ймовірність безвідмовної роботи ПЗ за місяць m (P_{nm})	$\exp\left[- \frac{a\left(m^{b} - (m-1)^{b} e^{b/T}\right)}{T^{b} e^{mb/T}} \right]$
Інтенсивність потоку відмов ПЗ за місяць m (λ_m)	$\left[- \frac{a\left[m^{b} e^{-b/T} - (m-1)^{b}\right]}{T^{b} \exp\left[b(m-1)/T\right]} \right]$
Напрацювання ПЗ на відмову за місяць m (T_{nm})	$\left[- \frac{T^{b} \exp\left[b(m-1)/T\right]}{a\left[m^{b} e^{-b/T} - (m-1)^{b}\right]} \right]$
Середньоквадратичне відхилення результатів прогнозування N_m від даних про відмови ПЗ за n місяців (σ)	$\sqrt{\frac{1}{n} \sum_{m=1}^{n} \left(K_{cm} - \frac{a\left[m^{b} - (m-1)^{b} e^{b/T}\right]}{T^{b} e^{b/T}} \right)^{2}}$
Коефіцієнт готовності	$A_{KC} = \left[1 - (1 - A_a)^{R}\right] A_n$

Запропонована нова динамічна модель оцінки і прогнозування надійності відрізняється від відомих зменшенням значення СКВ результатів розрахунків від дослідних даних більше 9%. Її доцільно використовувати в методах кількісної оцінки значень показників надійності спеціальних комп'ютерних систем (КС).

На основі використання моделей надійності ПЗ обґрунтований та реалізований в реальних умовах експлуатації метод кількісної оцінки і прогнозування значень показників надійності КС із врахуванням надійності їх апаратних засобів (АЗ).

Сутність методу полягає в отриманні кількісної оцінки показників надійності КС при заданих обмеженнях та припущеннях на базі використання нових статичної та динамічної моделей надійності ПЗ із марковським процесом виявлення помилок і нових функціональних залежностей досліджуваних показників від часу, приведених в табл. 1, 2.

Початкові дані залежать від виду моделі надійності ПЗ: R – число робочих місць (персональних комп'ютерів), $T_а$ – напрацювання на відмову АЗ у період нормальної експлуатації; $T_в$ – середній час відновлення АЗ; $T_{вп}$ – середній час відновлення ПЗ; T – період прогнозу (в місяцях); t_{rm} – час роботи (в годинах) АЗ на робочому місці r = $\overline{1, R}$ за місяць m = $\overline{1,T}$; K_m – число відмов ПЗ на R робочих місцях за місяць m підконтрольної експлуатації; n – число місяців підконтрольної експлуатації КС.

Обмеження на використання методу: умови експлуатації КС за час отримання початкових даних і на період прогнозування постійні; розглядається період нормальної експлуатації АЗ, коли значення параметру потоку відмов і напрацювання на відмову постійні.

Припущення при використанні методу: значення показників надійності АЗ і ПЗ змінюються з часом за експоненціальним законом; при усуненні виявлених помилок ПЗ нові помилки не вносяться; помилка ПЗ виявлена на одному робочому місці, усувається на усіх робочих місцях; швидкість виявлення помилок ПЗ залежить від їх кількості; помилка ПЗ усувається до наступного звернення в систему або доводяться до користувачів умови її виникнення для запобігання можливих наслідків прояву.

В роботі розроблено алгоритм реалізації методу, який складається із наступних операцій: отримання початкових даних; вибір моделі надійності ПЗ; апроксимація даних про відмови ПЗ; розрахунок коефіцієнтів a і b згідно табл.1,2; розрахунок для кожного місяця за період m = $\overline{1,T}$ значень числа відмов ПЗ (N_m), напрацювання на відмови ПЗ (T_{nm}) і КС в цілому (T_{cm}), значення ймовірностей безвідмовної роботи АЗ (P_{am}), ПЗ (P_{nm}) і КС в цілому (P_{cm}); оцінка прогнозованого числа помилок ПЗ (N); розрахунок СКВ результатів прогнозування від істинного значення числа відмов ПЗ за n місяців підконтрольної експлуатації КС

$$\sigma_n = \sqrt{\frac{1}{n}\sum_{m=1}^{n}(K_m - N_m)^2},$$

вивід отриманих результатів у вигляді таблиці і залежностей N_m, T_{nm}, T_{cm}, P_{am}, P_{nm}, P_{cm} від часу прогнозування $m = \overline{1,T}$; вивід значень N і σ_n.

Реалізацію методу розглянуто із використанням реальних початкових даних щодо експлуатації спеціальної КС: R=5, T_a=10000 год., T=12 міс., t_m=192 год., K_1=8, K_2=6, K_3=6, K_4=4, n=4 (рис. 1). У результаті апроксимації початкових даних за n=4 місяці дослідної експлуатації отримуємо A_1=8; A_2=6,7; A_3=5,5; A_4=4,5. Далі за алгоритмомЖ и=0б192ж ф=9б693ж ть=960 годюж Ть=9б693у-0б192ьжЕтьь=99б04у0б192ьж Зфь=у-0б0192ьж Зтьь=учз(-8·0б5625(ь-1). 3)б σ=1б14.

В область $N_m \pm \sigma_n$ попадає 91,7% експериментальних даних, що свідчить про достатньо високу точність прогнозу числа відмов ПЗ за n місяців експлуатації КС. Остаточно отримуємо для коефіцієнтів готовності (доступності): A_a=0,9999; $A_П$=0,9905; m=6, тоді для об'єкту в цілому $A_{кс}$=0,9905. Відповідно, при m = 12 отримуємо $A_п$ =0,996997= $A_{кс}$ (рис. 1).

Під контролем було 11 комплектів КС в режимі тестової експлуатації. Всього за рік експлуатації було зафіксовано 9 відмов ПЗ. Використання динамічної моделі надійності ПЗ з вихідними даними i=3, N_3=4, j=9, N_9=8, T=24 дозволяє отримати значення коефіцієнтів b=0,816 і a=24,2, при цьому:

N_{cm}=24,2·(m/24)0,816·exp(-0,034m); δN_{13}=6%, σ=0,3.

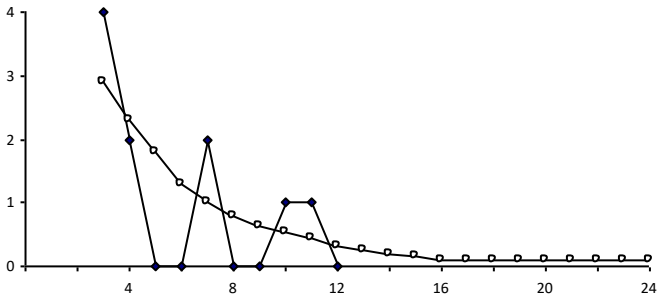

Рис. 1. Статистичні дані і моделювання відмов програмного забезпечення

Прогнозована загальна кількість відмов ПЗ за 2 роки експлуатації складає N24≈11. За наступний рік відмов ПЗ не зареєстровано, що відповідає результатам моделювання. За два роки дослідної експлуатації зафіксовано 19 відмов АЗ, при цьому отримано T_a=10000 год, τ_{nm}= 7920 год, T=24, a=24,2 і b=0,816 (рис. 2):

$$N_m = 1{,}81 \cdot \frac{m^{0{,}816} - 1{,}03(m-1)^{0{,}816}}{e^{0{,}034 \cdot m}},$$

$$T_{nm} = \frac{4376 \cdot e^{0{,}034 \cdot m}}{m^{0{,}816} - 1{,}03(m-1)^{0{,}816}}.$$

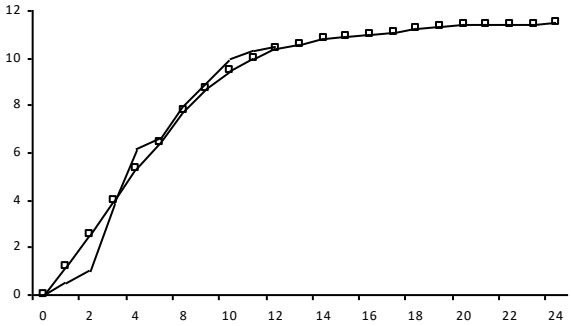

Рис. 2. Сумарна кількість відмов програмного забезпечення

Ефект від використання методу полягає в підвищенні точності прогнозу значень доступності по мірі накопичення статистичних даних, а також в уточненні значень напрацювання на відмову нових зразків КС в початковий період за рахунок обліку надійності ПЗ: напрацювання на відмову системи за перший рік експлуатації в 1,5-3,2 рази відрізняється від напрацювання на відмову тільки АЗ; прогнозування значення кількості помилок в ПЗ відрізняється від виявлених за рік експлуатації обладнання від 0,3 до 3,1%, а за місяць експлуатації не перевищує 0,6%; значення СКВ експериментальних даних від розрахункових щодо відмов ПЗ складає від 0,97 до 1,14, що краще, ніж при використанні відомих методів; метод дозволяє кількісно оцінити і прогнозувати напрацювання на відмову ПЗ і системи в цілому, а також оцінити ймовірність безвідмовної роботи АЗ, ПЗ і КС за визначений час.

Наукова новизна методу полягає в тому, що вперше: удосконалено метод оцінки показників надійності КС у напрямку врахування надійності їх ПЗ за рахунок використання нової аналітичної моделі зміни їх надійності з часом; комплексно здійснюється кількісний облік показників надійності АЗ і ПЗ при кількісній оцінці коефіцієнта готовності КС. Відрізняється від відомих: врахуванням особливостей порядку фіксації відмов залежно від умов експлуатації; достатньою для практики точністю результатів; автоматизацією процесу оцінки і прогнозування показників якості КС.

Метод може застосовуватися при дослідженні, оцінці та прогнозуванні надійності існуючих і перспективних КС.

Значення вирішеної наукової задачі для теорії і практики в цілому полягає в тому, що вона обґрунтовує можливість підвищення ефективності використання існуючих та перспективних КС без істотних економічних витрат за рахунок впровадження науково-методичних рекомендацій щодо оцінки та прогнозування значень показників надійності обладнання та систем в цілому з наступною реконфігурацією структури при невідповідності результатів потрібним значенням, які реалізують основні наукові результати досліджень. Отримані в роботі результати мають важливе наукове та практичне значення. Основні наукові результати досліджень опубліковані в [1-7].

Подальші дослідження доцільно направити на підвищення точності результатів моделювання при зменшенні періоду дослідної експлуатації обладнання енергетичних систем України.

Література

1. Сакович Л.М. Моделювання надійності програмних засобів техніки зв'язку / Л.М. Сакович, Я.Е. Небесна, С.Є. Гнатюк // Зв'язок. – 2013. – №1 – С. 15-19.
2. Сакович Л.М. Оцінювання надійності програмно-керованих засо-бів зв'язку / Л.М. Сакович, С.Є. Гнатюк // Зв'язок. – 2013. – №2. – С. 25-29.
3. Гнатюк С.Є. Динамічна модель надійності програмних засобів комп'ютерних систем озброєння / С.Є. Гнатюк // Труди університету: Зб. наук. праць. – К.: НАОУ. – 2013. – №5 (119). – С. 142-148.
4. Гнатюк С.Є. Аналітична модель надійності програмних засобів комп'ютерних систем і програмно-керованих засобів зв'язку / Наука і техніка Повітряних Сил Збройних сил України. – Х.: – 2014. – № 3 (16). – С. 104-108.
5. Гнатюк С.Є. Кількісна оцінка показників надійності комп'ютерних систем і програмно-керованих засобів зв'язку / С.Є. Гнатюк, Л.М. Сакович // Спеціальні телекомунікаційні системи та захист інформації: Зб. наук. праць. –К.: Держспецзв'язок. 2013. – Вип. 1 (23). – С. 71-79.
6. Гнатюк С.Е, Сакович Л.Н. Моделирование надежности специальных компьютерных систем // XVI Міжнародна науково-практична конференція «Безопасность информации в информационно-телекомуникационных системах», Госспецсвязь. – К.: 2013. – С. 131-132.
7. Гнатюк С.Є. Методика кількісної оцінки і прогнозування значень показників надійності спеціальних комп'ютерних систем і програмно-керованих засобів зв'язку // III Міжнародна науково-практична конференція «Фізико-технологічні проблеми радіотехнічних пристроїв, засобів телекомунікацій, нано- та мікроелектроніки», Чернівці: 2013. – С. 98.

ДЛЯ ЗАМЕТОК

Научно-практическая конференция
«КИБЕРБЕЗОПАСНОСТЬ ЭНЕРГЕТИКИ -2018»

ПРИГЛАШЕНИЕ
ПРОГРАММА
МАТЕРИАЛЫ

29 мая – 02 июня 2018 года
г. Одесса

Оператор конференції – ООО «ИНФОРМАТИО»

Формат 60×90/16. Тираж 100.
Подписано к печати 21.05.2018. Заказ № 5

Институт проблем моделирования в энергетике
им. Г.Е. Пухова Национальной академии наук Украины,
Украина, 03164, Киев, ул. Генерала Наумова, 15,
тел.: +38 044 424 10 63
https://ipme.kiev.ua/, ipme@ipme.kiev.ua