INFORMATION SECURITY RISK MANAGEMENT

УДК 004.056.53::006.034

ЮЛІЯ КОЖЕДУБ

РЕАЛІЗАЦІЯ ПРОЦЕСНОГО ПІДХОДУ ДО КЕРУВАННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ДОКУМЕНТАХ NIST

Досліджуються методологічні основи діяльності Національного інституту стандартів і технологій Сполучених Штатів Америки (National Institute of Standards and Technology, NIST). Зосереджується увага на процесному підході до створення рекомендацій, настанов, керівних вказівок, рамкових документів. Встановлені такими документами принципи спрямовують діяльність організацій щодо керування ризиками інформаційної безпеки. У цій статті аналізуються методичні документи щодо інформаційної безпеки, кібербезпеки та комп'ютерної безпеки, що дозволяють допомогти вибрати набір заходів контролю безпеки. Зокрема, цей аналіз стосується таких етапів робіт зі захисту інформації. По-перше, класифікування інформації та інформаційних систем. По-друге, застосування базових правил, що належать до організаційних заходів захисту інформації. По-третє, це вжиття вибіркових заходів контролю захисту, що є відповідними й адекватними певній інформаційній системі. Методичні документи NIST, що досліджуються, надають практичні поради фахівцям із захисту інформації для зниження ризиків інформаційної безпеки. Застосування методичних документів NIST у США є обов'язковим для державних установ та організацій. Розроблену на їх основі систему захисту спрямовано на зменшення ризиків безпеки інформації та інформаційних систем для будь-яких організацій, і не лише державної форми власності. Запропоновані базові заходи захисту можна адаптувати для практичного застосування із незначним модифікуванням. Створення дієвої індивідуальної комплексної системи захисту інформації є важливим завданням, в основі якої покладено процес керування ризиками інформаційної безпеки. Система захисту дасть змогу зберегти як прибутковість організації, так і її репутацію за допомогою зменшення ризиків інформаційної безпеки.

Ключові слова: методичні документи, кібербезпека, ризики інформаційної безпеки, процесний підхід, ризик-менеджмент, стандарти, спеціальні публікації, NIST.

Постановка проблеми. На служби захисту інформації та служби безпеки організацій усіх видів і форм власності, а особливо державних структур, покладається завдання забезпечення інформаційної безпеки. Уразливості кіберсистем сучасного інформаційного простору постійно спричинюють занепокоєння через їхню вразливість та зацікавленість з боку порушників інформаційної безпеки. Все частіше і більш цілеспрямованими та складнішими є атаки, а тому дуже важливо, щоб працівники – від керівників найвищої ланки до персоналу – керували довіреними їм активами та відповідними ризиками їх безпеки за допомогою найкращих стандартизованих методик, що їх викладено в документах Національного інституту стандартів і технологій (National Institute of Standards and Technology, NIST). Щоб зробити це правильно, їм потрібні найбільш дієві, сучасні, прості у використанні підходи та інструменти з комплексним і цілісним підходами. Це відображається у процесному підході до керування ризиками інформаційної безпеки, що реалізовано в документах NIST.

NIST відповідає за розробку стандартів і настанов, включаючи мінімальні вимоги, для забезпечення інформаційної безпеки, насамперед, для федеральних інформаційних систем. Цей набір стандартів та керівних принципів щодо керування ризиками інформаційної безпеки надає інструкції для інтегрованої, загальноорганізаційної програми керування ризиками інформаційної безпеки. Відповідно до [1], і в рамках своєї ініціативи щодо постійного вдосконалення ресурсів з керування ризиками державних організацій, NIST видав Звіт [2].

У цьому Звіті державним організаціям запропоновано керуватись вказівками щодо модернізації Рамкових принципів кібербезпеки (*Framework for Cyber Security*). Ці принципи доповнюють наявні практики керування ризиками та вдосконалюють чинні програми керування ризиком кібербезпеки. Розроблені NIST в 2013-2014 р.р., у тісній співпраці з приватним та державним секторами, Рамкові принципи кібербезпеки реалізують процесний підхід до керування ризиками. Рамкові принципи на добровільних засадах використовують приватні організації США, але є обов'язковими для державних організацій і установ США. Ці принципи набули поширення в інших країнах та регіонах світу, оскільки їх підготовлено для вирішення проблем забезпечення кібербезпеки в галузях критичної інфраструктури. Рамкові принципи узгоджуються із чинними стандартами й інструкціями з керування ризиками інформаційної безпеки NIST і доповнюють їх удосконаленими практиками. В [2] ілюструються вісім випадків застосування Рамкових принципів кібербезпеки для вирішення нагальних завдань забезпечення кібербезпеки. Таким чином, організації можуть інтегрувати Рамкові принципи забезпечення кібербезпеки з іншими стандартами й інструкціями з керування ризиками на різних організаційних рівнях.

Аналіз останніх досліджень і публікацій. Широкий спектр документів, що пропонує NIST, привертає увагу фахівців з інформаційної, кібер- та комп'ютерної безпеки. Це спричинює широке розмаїття критичних робіт зазначених спеціалістів, які застосовують в своїй діяльності методичні документи, пропоновані NIST. Зокрема, щодо загальних питань інформаційної безпеки (Владімір Шпаковський, В.А. Довгаль), хмарних обчислень (Андрій Колесов, В.А. Довгаль), застосування стійких парольних фраз (Анатолій Алізар), антивірусний захист (Вадим Грибунін), комбінаторних методів побудови тестів для програмного забезпечення (Олексій Баранцев), безконтактного сканування відбитків пальців (Андрій Бєлокріницький), пропозицій і інноваційних технологій, пов'язаних з квантовими комп'ютерами, що матимуть змогу подолати сучасний криптозахист (Олег Парамонов). Зазначені опубліковані роботи стосуються обговорення практичного застосування спеціальних публікацій NIST. Їх створено відповідно до головної концепції NIST: охопити широке коло сучасних аспектів інформаційної, кібер- та комп'ютерної безпеки. Застосування наукових підходів до створення інструментів захисту інформації та інформаційних активів дає змогу видавати фахівцям NIST найсучасніші методичні документи для реагування на ризики інформаційної безпеки.

Водночас доцільно врахувати роботи з фундаментальних основ забезпечення інформаційної безпеки таких авторів, як Ромака В.А., Корж Р.О., Гарасим Ю.Р., Старостіна А.О., Кравченко В.А., Гольдштейн Г.Я., Гуц А.Н., Бугрова С.М., Гук Н.М. Ці роботи щодо теорії і практики застосування фундаментальних основ забезпечення інформаційної безпеки використовують під час викладання основ менеджменту інформаційної безпеки у вищих навчальних закладах України.

Постановка завдання. Розуміння і керування взаємопов'язаними процесами як системою сприяє результативності та ефективності діяльності організації для досягнення намічених результатів – зменшення ризиків інформаційної безпеки. Такий підхід дає змогу організації контролювати взаємозв'язки та взаємозалежності між процесами системи, так, щоб загальна продуктивність організації була підвищена [4] - [9]. Застосування наукових методів і підходів до керування ризиками інформаційної безпеки як дієвою системою, спрямовано на пошук загроз і вразливостей інформаційної безпеки, а це є шлях до зменшення інцидентів та подій інформаційної безпеки.

Процесний підхід охоплює систематичне визначення і керування процесами, а також їх взаємодією. Щоб досягнути бажаних результатів – зменшення ризиків інформаційної безпеки – розробляють політику інформаційної безпеки, що повністю відповідає усім аспектам діяльності організації, основуючись і враховуючи положення сучасних актуальних документах [10] - [14] щодо обробляння ризиків, що показали свою результативність і ефективність застосування. Керування процесами і системи в цілому може бути досягнуто, застосовуючи цикл PDCA (Plan-Do-Check-Act, Плануй-Роби-Перевіряй-Дій, інакше відомий

як цикл Шухарта-Демінга). Водночас враховують процесний підхід із загальним акцентом на ризику, що спрямовано на використання можливостей уникнення і запобігання небажаних результатів діяльності.

Перевагами процесного підходу є:

– інтеграція й узгодження процесів для досягнення бажаних результатів;
– здатність зосередити зусилля на результативності та ефективності процесів;
– забезпечення довіри клієнтів та інших зацікавлених сторін щодо стабільної роботи організації;
– прозорість операцій всередині організації;
– зменшення витрат і тривалості циклу загального керування організацією, за рахунок ефективного використання ресурсів;
– послідовне й передбачуване збільшення результатів;
– забезпечення можливостей для фокусування і пріоритетності ініціатив щодо поліпшення діяльності організації;
– активізація й заохочення участі персоналу, роз'яснення їхніх відповідальностей.

Проте основна перевага процесного підходу полягає у керуванні і контролюванні взаємодій між цими процесами в межах функціональної ієрархії організації (див. рис. 1).

Рисунок 1 – Представлення процесу в загальному вигляді [4]

Призначені входи і виходи можуть бути матеріальними (наприклад, обладнання, матеріали чи компоненти) або нематеріальними (наприклад, енергія чи інформація). Виходи можуть бути і ненавмисні, такі як: відходи або забруднення навколишнього середовища.

Кожен процес має клієнтів та інших зацікавлених сторін, що можуть бути внутрішнім або зовнішнім відносно організації. Процесний підхід також розглядає потреби, очікування, вимоги, що є входами процесу, які й визначають результати, наслідки, необхідні виходи процесу.

Система, що є ядром процесу, сердечником процесного підходу, має використовувати отримані дані про функціонування процесу – зворотній зв'язок. Цей матеріал треба проаналізувати, щоб визначити, чи є необхідність в коригувальних і превентивних діях або поліпшенні діяльності системи.

Усі процеси треба привести у відповідність з цілями, масштабами і складністю організації, і їх слід розробити так, щоб додати цінності для організації.

Результативність і ефективність діяльності організації (як процесу) можна оцінити за допомогою внутрішніх або зовнішніх оглядів, що є елементом загального процесу керування організацією.

Розуміння процесного підходу пов'язано з тим, що цей підхід є потужним засобом організації і його спрямовано на керування діяльністю, щоб створити або додати цінності для споживача та інших зацікавлених сторін.

Організації часто структуровані за ієрархією функціональних блоків, елементами їх є організаційна структура. Організації, як правило, керуються по вертикалі, з відповідальністю за передбачуваність виходів, що поділяться між собою функціональними блоками (структурні одиниці організації: підрозділи з виділеними та закріпленими функціями).

Кінцевого споживача або іншу зацікавлену сторону не завжди видно всім учасникам. Отже, проблемам, що виникають на границях розділення процесів часто надають меншого пріоритету, ніж короткостроковим цілям підрозділів. Це призводить до незначних результатів або не відбувається ніякого поліпшення для зацікавленої сторони, так як дії зазвичай фокусуються на виконуваних функціях, а не на передбачуваному виході.

Процесний підхід створює керування по горизонталі (на противагу вертикальним відносинам), перетинаючи бар'єри між різними функціональними блоками та звертає увагу на основних цілях організації. Він також покращує керування взаємозв'язаними процесами.

Ефективність організації зростає за рахунок використання процесного підходу. Процеси керують системою, певною мережею процесів і їх взаємодій, створюючи тим самим більш глибоке розуміння доданої вартості від діяльності організації.

Виклад основного матеріалу дослідження. Робота фахівців NIST в рамках виконання Федерального закону про керування інформаційною безпекою (*Federal Information Security Management Act,* FISMA) спрямована на упровадження політики керування ризиками інформаційної безпеки [11]. Ця політика – це економічно ефективні заходи безпеки для усього життєвого циклу інформаційних систем. Документи містять вимоги до захисту інформаційних ресурсів організацій і допомагають вирішувати проблеми безпеки, пов'язані з інформаційною системою. Ці потреби потрібно правильно визначати та розглядати, починаючи з задач проектування інформаційних систем, а також відслідковувати це протягом усього життєвого циклу цієї системи.

Це зводиться до вирішення таких завдань:

– забезпечити основу для формалізації керування ризиками для убезпечення інформаційної системи з точки зору її принципів, концепцій і заходів;

– досягнути єдиного підходу до забезпечення безпеки інформаційних систем, незалежно від їх масштабів, розміру, складності та стадії життєвого циклу;

– використовувати науковий підхід та демонструвати, що принципи, концепція та дії щодо забезпечення безпеки систем інженерної діяльності;

– створювати основу діяльності, що слугуватимуть для розроблення освітніх і навчальних програм, включаючи розробку індивідуальних програм навчання персоналу.

Публікації FISMA – це документи, стандарти, настанови, що містять керівні принципів зі забезпечення інформаційної безпеки [12]. Це мінімальні вимоги для федеральних інформаційних систем. Ці публікації не можуть застосовуватись до інформаційних систем національної безпеки без погодження відповідних посадових осіб. Публікації NIST серії SP 800 (*Special Publication,* SP) використовують федеральні агентства для класифікації інформації та інформаційних систем. Їх засновано на забезпеченні належного рівня інформаційної безпеки відповідно до діапазону рівнів ризиків для покласифікованих інформації та інформаційних систем. Публікації NIST серії SP 800 – це рекомендації щодо правил з інформаційної безпеки для встановлених типів інформації та інформаційних систем, які треба включити відповідно в кожну категорію. Ці документи містять мінімальні вимоги до інформаційної безпеки (заходи контролю, оперативні і технічні засоби безпеки) для інформації та інформаційних систем в кожній такій покласифікованій категорії.

Закон про модернізацію Федеральної інформаційної безпеки від 2014 року [10] вносить зміни в Закон про керування інформаційною безпекою 2002 року (FISMA) [11] і передбачає декілька модифікацій, що удосконалюють методи щодо безпеки інформаційних технологій. По-перше, це інтегрована система керування ризиками, що ефективно об'єднує пов'язані стандарти безпеки та настанови FISMA задля розробки комплексних і збалансованих програм інформаційної безпеки. По-друге, вибір заходів контролю безпекою для інформаційної системи виконується в рамках чинної програми інформаційної безпеки всієї організації. Ця програма охоплює керування організаційним ризиком – це ризик для організації або особи, пов'язаний з роботою інформаційної системи. Керування організаційним ризиком є ключовим елементом в програмі інформаційної безпеки організації. Він забезпечує ефективну основу для вибору відповідних заходів контролю безпеки, необхідних для захисту окремих осіб, операцій

і активів організації. По третє, це ризик-орієнтований підхід. Структура керування ризиками забезпечує процес, який об'єднує діяльність щодо безпеки та керування ризиками в життєвому циклі розвитку системи. Ефективність процесу керування ризиками обмежується чинним законодавством: закони, регламенти, постанови, директиви, декрети, політики, стандарти і правила. Керування організаційними ризиками має важливе значення для ефективної програми інформаційної безпеки і може застосовуватись як для нових щойно створених інформаційних систем, так і для успадкованих та/чи застарілих систем в контексті життєвого циклу розробки системи керування ризиками.

NIST рекомендує визначати пріоритети керування безпекою на основі важливих елементів керування, робить на них акцент. Окрім того, надання інформації громадськості про пріорітизацію базових вимог безпеки і контролю сприяв би загрозі поширення важливої інформації для порушників, агентів і недоброзичливців, яка може завдати шкоди. Проте така відкритість надає прозору видимість щодо своєї стратегії захисту громадськості. Підхід, рекомендований NIST щодо системи керування ризиками, забезпечує федеральні агентства плановим, структурованим і гнучким процесом вибору відповідних елементів керування безпекою інформаційних систем. Методологія визначає ефективність контролю та прозорої видимості, зрозумілості залишкового ризику для діяльності організацій, фондів, приватних осіб тощо. Розгортання заходів контролю безпеки використовує підхід посиленої глибинної оборони, що поєднує управлінські, операційні, технічні заходи і контрзаходи для убезпечення всіх елементів інформаційної системи від загроз кіберпростору. Збалансований підхід до вибору й впровадження заходів контролю свідчить, що ця технологія не може захистити федеральні інформаційні системи. Федеральні агентства потребують комплексного підходу до захисту критично важливих активів і бізнес-функцій, що охоплюють людей, процеси і технології, усе разом, доповнюючи і взаємно підсилюючи їх таким чином.

На сьогодні відомо три серії документів NIST [12] у сфері безпеки:

- спеціальні публікації NIST SP 800 Комп'ютерна безпека,
- спеціальні публікації NIST SP 500 Технології комп'ютерних систем,
- спеціальні публікації NIST SP 1800 Практичні настанови з кібербезпеки.

Усі ці три серії стосуються комп'ютерної/кібер/інформаційної безпеки, надаючи рекомендації, настанови та вихідні дані спеціалістам з безпеки сучасних інформаційних систем.

Кількість документів: спеціальні публікації NIST SP 500 Технології комп'ютерних систем – два, спеціальні публікації NIST SP 1800 Практичні настанови з кібербезпеки – вісім, спеціальні публікації NIST SP 800 Комп'ютерна безпека – 182, разом зі змінами, доповненням, а також нові розробки.

Розробка раціональної політики та процедур безпеки є одним з найважливіших аспектів побудови ефективної програми інформаційної безпеки. Політики безпеки, незважаючи на їх декларативний характер, демонструють в чітких і однозначних правилах, ранжовані команди, показуючи прихильність і прагнення усього персоналу до забезпечення інформаційної безпеки. Політики безпеки показують, що захисту операцій організації (через встановлені місію, функції, статус і репутацію) і активів фізичних осіб, інших організації, загалом державних інтересів, інтересів нації (*Nation*), дотримано. Процедури забезпечення безпеки використовуються професіоналами організацій для ефективної реалізації політики безпеки. Ефективна політика та процедури, в поєднанні з технологією керування на основі правил безпеки, забезпечують глибинний захист і комплексний підхід до інформаційної безпеки організації і керування ризиками інформаційних систем.

FIPS (Federal Information Processing Standards, FIPS) [13] розробляються NIST відповідно до FISMA [10]. FIPS затверджуються міністром торгівлі США і є обов'язковими до виконання федеральними агентствами. FISMA вимагає, щоб інформаційні (комп'ютерні) системи федеральних агентств відповідали цим стандартам, а тому органи влади не можуть відмовитись від їх застосування у повсякденній діяльності. Такими стандартами є FIPS 199 і FIPS 200. Надання рекомендації для мінімальних заходів безпеки інформаційних систем та

віднесення їх до категорії федерального рівня, виконується відповідно до FIPS. Вимоги щодо обов'язкових параметрів конфігурації, що випливають із Федерального закону про керування інформаційною безпекою встановлено у FIPS 200.

На рис. 2 представлено структурну схему взаємопов'язаних стандартів (FIPS 199, FIPS 200) і спеціальних публікацій серії NIST SP 800.

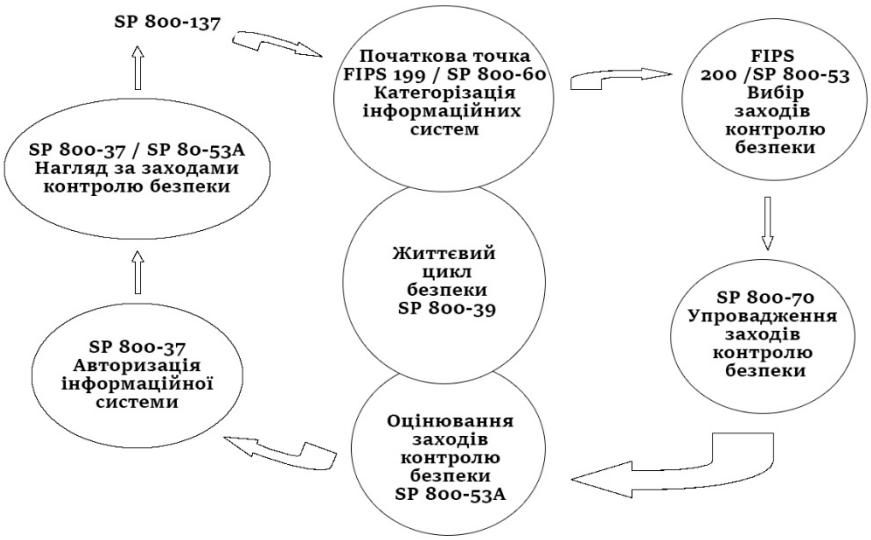

Рисунок 2 – Взаємозв'язок документів FISMA і NIST SP [14]

NIST SP 800-30 описує процес керування ризиками, оцінку ризиків і їх застосування, а також ключові концепції роботи з ризиками.

Стратегія керування ризиками полягає в описі того, як організація оцінює ризики, реагує на них і відстежує їх.

Оцінювання ризиків полягає в тому, щоб ідентифікувати ризики для організації або наскрізні ризики, спрямовані через організацію в сторону інших організацій, виявити внутрішні і зовнішні загрози, оцінювати наслідки цих ризиків при їх настанні і визначити ймовірності реалізації цих ризиків.

Після оцінки ризиків організації обробляють ризики шляхом вироблення альтернативних варіантів дій, оцінки цих варіантів, вибору прийнятного варіанту дій, вироблення конкретних дій.

Моніторинг ризиків полягає у визначенні ефективності наявних заходів, визначенні тих змін в організації і інформаційних системах, що привносять нові ризики і перевірці на відповідність запланованих заходів вимогам законодавства й іншим організаційним вимогам.

NIST SP 800-30 і NIST SP 800-60 – це методики загального користування.

NIST SP 800-30 фокусується в основному на комп'ютерних системах. Команда фахівців збирає інформацію з мережі і від людей, які працюють в даній організації. Ці дані використовують як початкові значення, а далі вони підлягають обробці відповідно до вищезазначених пунктів.

NIST SP 800-39 описує алгоритм дій. Початковими даними для цієї методики є аналіз впливу втрат, визначення ресурсів і оцінка критичності інформації. Маючи цю інформацію, створюють рейтинг ресурсів. Потім на основі визначених імовірності експлуатації загрози, величини збитку і адекватності запланованих або наявних заходів безпеки відбувається безпосередньо оцінювання ризиків. Після встановлення оцінки ризиків визначаються рекомендовані заходи безпеки і оформляється звітна документація. Таким чином створюють модель захисту.

Важливо зазначити, що методика NIST SP 800-39 найкраще підходить до керування ризиками саме інформаційної безпеки, оскільки враховує майже всі канали витоку інформації. Також перевагою цієї методики є можливість застосування для різних підприємств та організацій. Недоліками методики можна вважати надто тривалий процес аналізу і відсутність автоматизації деяких функцій.

Метою NIST SP 800-53A є встановлення загальних процедур оцінювання ефективності засобів контролю безпеки в федеральних інформаційних системах, зокрема, ці заходи контролю перераховано в іншій спеціальній публікації цієї серії – NIST SP 800-53. Методи і процедуру оцінювання використовують для визначення того, що контроль безпеки реалізовано правильно, працює, як передбачалося, і можливо отримати бажаний результат щодо виконання вимог безпеки організацією. Організації використовують рекомендовані процедури оцінювання з NIST SP 800-53A як відправну точку для розробки більш конкретних процедур оцінювання. Процедури оцінювання в NIST SP 800-53A можуть бути доповнені, в разі необхідності, на основі оцінки організаційного ризику. Організації повинні створювати додаткові процедури оцінювання для тих заходів безпеки, які не містяться в NIST SP 800-53. Застосування стандартизованих процедур оцінювання сприяє більш послідовним діям, які можна порівняти і надати їм відтворювану оцінку безпеки федеральних інформаційних систем.

Метою спеціальної публікації NIST SP 800-53A є забезпечення керівних принципів для застосування системи керування ризиками федеральних інформаційних систем, що охоплює проведення заходів категоризації безпеки, вибір і упровадження заходів контролю безпеки, оцінювання заходів контролю безпеки, авторизації інформаційної системи й перевірку заходів контролю безпеки.

NIST наводить схему з шести кроків для пояснення взаємозв'язку FIPS та SP на основі процесного підходу до керування ризиками (Кроки 3, 4, 5 перебувають на доопрацюванні).

Крок № 1. Категоризація безпеки забезпечує структурований спосіб визначення критичності і чутливості інформації, що обробляється, зберігається і передається за допомогою інформаційної системи. Категорія безпеки на основі потенційного впливу (в гіршому випадку) на організацію – це розвиток і дії певних подій, які ставлять під загрозу інформацію та інформаційні системи організації.

Власник інформації (власник інформаційної системи) ідентифікує типи інформації, пов'язані з інформаційною системою і присвоює значення небезпеки (низький, середній, високий) щодо цілей безпеки для кожного типу інформації. Концепція категоризації небезпеки використовується для визначення рівня впливу небезпеки на інформаційну систему та встановлення мети пріоритизації – це вибір початкового набору заходів з трьох базових рівнів контролю безпеки, як зазначено в NIST SP 800-53.

Після того, як загальний рівень впливу небезпеки на інформаційну систему визначено (тобто, після того, як систему й інформацію класифіковано), початковий набір заходів контролю безпеки вибирають з NIST SP 800-53. Організації мають гнучкість для налаштування базових ліній контролю безпеки, виконуючи рамкові вказівки, застосовуючи механізми контролю, а також із зазначенням організації й певних параметрів, як визначено в NIST SP 800-53. Категорія безпеки і рівень впливу системи безпеки використовується також для визначення рівня деталізації документації і рівня зусиль, необхідних для оцінювання інформаційної системи.

Керування організаційними ризиками інформаційних систем в рамках загальної виконавчої ризик функції застосовується для вирішення проблем, пов'язаних з керуванням ризиком і пов'язаною з цим інформацією про наявні небезпеки, щоб досягнути адекватного захисту для інформації і інформаційної системи організації. Виконавча ризик функція допомагає гарантувати, що міркування стосовно інформаційної безпеки для окремих інформаційних систем розглядаються залежно від сфери діяльності організації в перспективі з урахуванням загальних стратегічних цілей і завдань організації в проведенні своєї місії, бізнес-процесів.

Під час категоризації, виконавчу ризик функцію покладено на керівництво і ним виконується нагляд за виконанням послідовних рішень на етапі категоризації для окремих інформаційних систем всієї організації. Виконавча ризик функція полегшує обмін, пов'язаний з безпекою і ризиками, стосовно інформації серед керівників.

Категоризація безпеки є найбільш важливим кроком і впливає на рішення з інформаційної безпеки як для усієї організації, так і на окремі інформаційні системи. Цей крок також впливає на всі інші основні етапи керування ризиками від вибору заходів контролю безпеки стосовно рівня зусиль, необхідних для оцінювання, до підтримання заходів контролю безпеки. Категоризацію безпеки встановлюють за FIPS 199 і NIST SP 800-60, щоб оцінити критичність і чутливість інформації та інформаційної системи, щоб визначити рівень впливу небезпеки на систему. Категоризацію безпеки слід розглядати на постійній основі.

Отримане рішення щодо категоризації використовується для вибору й адаптації заходів контролю безпекою інформаційної системи, використовуючи NIST SP 800-53. Власники інформації (інформаційних систем) несуть відповідальність за категоризацію своїх інформаційних систем. Система Perspective [15] це один з прикладів того, як NIST SP 800-60 може бути застосовано для категоризації федеральних інформації та інформаційних систем відповідно до FIPS 199.

NIST SP 800-60 надає алгоритм для категоризації інформації і інформаційних систем:

1) визначити типи даних;
2) вибрати часові рівні впливу для типів інформації та виконати огляд часових рівнів впливу;
3) скоригувати рівень інформаційного впливу для типів інформації;
4) призначити категорію системи безпеки і загальний рівень впливу.

Рівень впливу системи використовується для вибору базового набору заходів контролю безпекою інформаційною системою з NIST SP 800-53, яку потім адаптують для кращого відображають унікальних параметрів конкретної інформаційної системи. Крім того, рівень впливу системи визначає жорсткість застосування решти кроків в рамках керування ризиками, включаючи оцінювання заходів контролю безпеки.

Крок № 2. Вибір заходів контролю безпеки виконується відповідно до FIPS 200 та NIST SP 800-53. Урахування базових заходів контролю безпеки, що їх наведено в NIST SP 800-53A, сприяє більш сталому рівню безпеки федеральних інформаційних систем та організацій. Такий підхід надає більшу гнучкість для модифікування заходів контролю безпеки на основі конкретних стратегій, вимог, обставин, загроз і вразливостей організації.

Подробиці щодо виконавчої ризик функції містяться в NIST SP 800-53. Організації потрібно комплексний підхід щодо ризик орієнтованого підходу. Такий підхід визначається балансом між місією і бізнес-функціями організації, що використовує інформаційні системи для забезпечення їх місії і досягнення своїх бізнес-цілей. Керування організаційними ризиками досягається за рахунок реалізації загальної виконавчої ризик функції. Виконавча ризик функція – це керівництво і нагляд за усіма ризиками та діяльністю з інформаційної безпеки в рамках усієї організації (наприклад, категоризація безпеки, загальний ідентифікаційний контроль безпеки, неперервний моніторинг і перерозподіл повноважень), щоб забезпечити послідовне прийняття рішень щодо прийнятності ризиків. NIST SP 800-53 містить рекомендації для вибору і визначення заходів контролю безпеки і мінімальні вимоги щодо їх забезпечення, що дають змогу організаціям захистити свою інформацію та інформаційні системи. У додатку F NIST SP 800-53 наведено майстер-каталог заходів контролю безпеки для зменшення ризику, що демонструє їх відповідність до різних урядових чи інших організацій з необхідними вимогами безпеки. Додаток E NIST SP 800-53 описує мінімальні вимоги до забезпечення заходів контролю безпеки для низького, середнього, високого рівня захисту інформаційної системи. Він несе відповідальність за організацію, щоб вибрати відповідні заходи контролю безпеки щодо забезпечення безпеки інформаційних систем.

Вибір належних заходів контролю безпеки для інформаційних систем організацій може мати серйозні наслідки для операцій і активів організації, а також добробуту окремих осіб і нації (*Nation*). FIPS 200 визначає мінімальні вимоги до безпеки федеральних інформації та інформаційних систем у 17 областях, які пов’язані з безпекою. Всі федеральні агентства повинні відповідати мінімальним вимогам безпеки, визначеним у FIPS 200, використовуючи

заходи контролю безпекою, визначені в NIST SP 800-53, рекомендовані заходи контролю безпеки федеральних інформаційних систем у NIST SP 800-53A. NIST SP 800-53 це документ про поточний стан справ і практику надання гарантій і контрзаходів для інформаційних систем, що їх використовують для встановлення рівня належної перевірки захисту інформаційної системи організації.

Поради та методи для інформаційних систем забезпечуються через вибір заходів контролю безпеки під час реалізації NIST SP 800-53. NIST SP 800-53 визначає процес вибору відповідного набору заходів контролю безпеки інформаційної системи, який складається з наступних завдань:

(I) вибрати набір базових заходів безпеки;

(II) адаптувати базову лінію заходів контролю безпеки, застосовуючи оглядове керівництво, параметризацію і компенсоване керівництво;

(III) доповнити базові заходи контролю безпеки, за необхідності, додатковими заходами контролю безпеки або контролювати удосконаленням для вирішення унікальних потреб організації, заснованих на оцінці ризику (формалізованій або неформалізованій) і локальному аналізі витрат і вигоди, або особливих обставин;

(IV) зазначити мінімальні вимоги до забезпечення інформаційної безпеки.

Крок № 6. Перевірка заходів контролю безпеки. Неперервний моніторинг безпосередньо впливає на вибрані заходи контролю для забезпечення безпеки інформаційних систем через зміни в апаратних засобах, програмному забезпечені, програмно-апаратному й операційному середовищі. Кінцевою метою неперервного моніторингу є визначення того, що заходи контролю безпеки в інформаційній системі продовжують діяти через зміни в системі та середовищі, в якому інформаційна система працює. Неперервний моніторинг також забезпечує ефективний механізм для поновлення планів забезпечення безпеки, звітів з оцінки безпеки, а також плани дій і етапів.

Під час неперервного моніторингу, виконавча ризик функція підтримує загальний ризик організації на основі агрегованого ризику від кожної з інформаційних систем і допоміжних інфраструктур для яких організація є відповідальною і надає цю інформацію для власників інформації та/чи власників інформаційної системи. Ця інформація використовується для визначення неперервної стратегії моніторингу, критеріїв для вибору заходів контролю безпекою та частоти, з якою їх треба контролювати, і коли в інформаційній системі повинно виконано перерозподілення повноважень.

Ефективне керування ризиками потребує визнання того, що організації діють в дуже складному і взаємопов’язаному світі, використовуючи впроваджені й успадковані інформаційні системи, функціонування організації залежить від виконання критично важливих місій та ведення важливих щоденних справ. Добре продумана і добре керована програма неперервного моніторингу ефективно трансформує статичний процес визначення оцінки ризику і контролю безпеки в динамічний процес. Така програма забезпечує в режимі реального часу інформацією про стан безпеки, пов’язаний з прийняттям посадовими особами відповідних заходів щодо зменшення ризику.

Організації залежать від інформаційних систем, що їх активно застосовують для успішного виконання своїх завдань і бізнес-функцій. Ці організації ведуть бізнес в динамічних середовищах з постійно змінюваними загрозами, вразливостями і технологіями. Структурований і дисциплінований процес необхідний, щоб визначати вплив змін на інформаційні системи організації. Неперервна програма моніторингу дає уточнені знання, що їх потребує вище керівництво для забезпечення державної безпеки щодо ризиків організації, і у такий спосіб вони можуть отримувати відповіді, стосовно того як відбуваються зміни. Надійна неперервна програма моніторингу для організації вимагає активної участі власників інформації та/чи власників інформаційних систем і, загалом, усіх учасників керування. Для цього і слугує виконавча ризик функція, що надає вказівки щодо захисту таких інтересів головній службі інформації, головному інформаційному агентству та службі безпеки. Неперервну програму моніторингу описано в NIST SP 800-37. Наведений в цьому документі

огляд може бути одним з прикладів того як може бути створено неперервний моніторинг інформаційних систем. Цей документ конкретизує основні кроки і настанови. Це є прикладом того, як стимулювати ідеї в реалізації процесу безперервного моніторингу в масштабах всієї організації.

Неперервний моніторинг – це процес усунення впливу небезпеки на інформаційні системи в результаті змінення апаратних засобів, програмного забезпечення, вбудованого програмного забезпечення чи операційного середовища. Добре продумані і добре керовані програми неперервного моніторингу можуть ефективно трансформувати статичну безпеку. Оцінка керування і процес визначення ризику видозмінює її в динамічний процес, який забезпечує суттєве, в режимі реального часу, надходження інформації про стан, пов'язаний з виявленням загроз безпеки, вжиттям заходів щодо зменшення ризику, прийняттям рішень, заснованих на розумінні ризику щодо впливу його на функціонування інформаційної системи. За цим документом головний підрозділ, що розробляє програму інформаційної безпеки організації (як правило, це спеціально призначений співробітник служби безпеки) відповідає за виконання організаційної програми неперервного моніторингу, яка підтримує взаємини з іншими підрозділами організації.

Ефективний процес неперервного моніторингу інтегрований з життєвим циклом розвитку системи для того, щоб визначити, чи є заходи контролю безпеки в інформаційній системі дієвими протягом довгого часу, які відбуваються в системі, а також його робочого середовища.

Це виконується, коли власник інформації та/чи власник інформаційної системи несе відповідальність за моніторинг інформаційних систем. Власник має гарантувати, що створена система забезпечення безпеки зберігає свою актуальність, що оновлюються документи, якщо відбуваються зміни в системі чи операційному середовищі.

Ці поради і прийоми для систем наведено у NIST SP 800-37. Цей документ визначає процес авторизації безпеки інформаційних систем. Процес авторизації безпеки складається з трьох етапів:

(I) етап підготовки;

(II) фаза виконання;

(III) фаза обслуговування або підтримувальна.

Підтримувальна фаза визначає неперервний процес моніторингу інформаційних систем організації. Підтримувальна фаза складається з дев'яти завдань.

Поради та методи в цьому документі детально показують як реалізується неперервне керівництво моніторингом в організаціях. Їх адаптують до інформаційних систем, що мають конкретні умови середовища функціонування.

Висновки. NIST пропонує три серії методичних документів, що стосуються інформаційної безпеки, кібербезпеки та комп'ютерної безпеки. Застосування таких документів є обов'язковим для державних установ та організацій США за погодженням зі спеціальним агентствами, що підтверджують правильність вибору заходів контролю безпеки після проходження відповідного аналізу. Усі ці дії сплановано, контрольовано та спрямовано на зменшення ризиків інформаційної безпеки будь-яких організацій, різних форм і власності. Заходи контролю безпеки адаптують для практичного застосування із незначним модифікуванням. Виконання заходів контролю безпеки дає змогу забезпечити інформаційну безпеку за допомогою зменшення ризиків інформаційної безпеки.

Згідно з NIST Special Publication 800-37 є шість кроків, що відображають рамкові принципи щодо керування ризиками: Категоризація, Вибір, Упровадження, Оцінювання, Авторизація та Перевірка. Разом з п'ятьма функціями рамкових принципів кібербезпеки – Ідентифікація, Захист, Виявлення, Відповідь та Відновлення, вони складають методологічну основу роботи ризик-менеджера щодо захисту інформації та інформаційних систем організації. Ці основоположні принципи базуються на процесному підході, що передбачає систематичне визначення і керування процесами, а також їх взаємодії, з тим, щоб досягнути бажаних результатів відповідно до політики інформаційної безпеки та стратегічного напрямку діяльності організації, зокрема отримання прибутку та/чи виконання владних повноважень.

Застосування проаналізованих методичних документів NIST SP в практичній діяльності ризик-менеджерів можливе після їх адаптування в Україні, оскільки їх розроблено на основі процесного підходу до керування ризиками інформаційної безпеки і відображає усі сучасні аспекти захисту інформаційних технологій.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] Budget and Presidential Materials, Compilation of Presidential Documents, Office of the Federal Register, National Archives and Records Administration, Donald J. Trump (May 11, 2017). *DCPD-201700327. Executive Order 13800. Strengthening the cybersecurity of federal networks and critical infrastructure*. [Online]. Available: https://www.gpo.gov/fdsys/pkg/dcpd-201700327/pdf/dcpd-201700327.pdf. Accessed on: July 03, 2017.

[2] National Institute of Standards and Technology. *DRAFT NISTIR 8170 The Cybersecurity Framework. Implementation Guidance for Federal Agencies*. Matt Barrett, Jeff Marron, Victoria Yan Pillitteri, Jon Boyens, Greg Witte, and Larry Feldman. [Online]. Available: http://csrc.nist.gov/publications/drafts/nistir-8170/nistir8170-draft.pdf. Accessed on: July 03, 2017.

[3] В.А. Ромака, В.Б. Дудикевич, Ю.Р. Герасим, П.І. Гаранюк, та І.О. Козлюк, *Системи менеджменту інформаційної безпеки.* Львів, Україна : Вид-во Львівської політехніки, 2012.

[4] International Organization for Standardization. *ISO 9000 Introduction and Support Package: Guidance on the Concept and Use of the Process Approach for management systems.* Document: ISO/TC 176/SC 2/N 544R3. ISO, 2008 [Online]. Available: http://www.iso.org. Accessed on: July 03, 2017.

[5] Institute for Standardization of the French Republic. *Final draft international standard ISO/FDIS 9001:2015(E). Quality management systems. Requirements* [Online]. Available: http://www.afnor.fr. Accessed on: July 03, 2017.

[6] International Organization for Standardization. *ISO 9001:2015*. ISBN 978-92-67-10648-9. ISO Central Secretariat, Chemin de Blandonnet 8 Case Postale 401, CH – 1214 Vernier, Geneva, Switzerland, ISO, 2015 [Online]. Available: http://www.iso.org. Accessed on: July 03, 2017.

[7] International Organization for Standardization. *Moving from ISO 9001:2008 to ISO 9001:2015*. ISO Central Secretariat, Chemin de Blandonnet 8 Case Postale 401, CH – 1214 Vernier, Geneva, Switzerland, ISO, 2015 [Online]. Available: http://www.iso.org. Accessed on: July 03, 2017.

[8] International Organization for Standardization. *Quality management principles.* ISBN 978-92-67-10650-2. ISO Central Secretariat, Chemin de Blandonnet 8 Case Postale 401, CH – 1214 Vernier, Geneva, Switzerland, ISO, 2015 [Online]. Available: http://www.iso.org. Accessed on: July 03, 2017.

[9] International Organization for Standardization. *ISO 9001:2015 Quality management systems. Requirements* [Online]. Available: http://www.iso.org. Accessed on: July 03, 2017.

[10] Library of the US Congress. *Federal Information Security Modernization Act of 2014, Pub. L. 107-347 (Title III), 116 Stat 2946*. [Online]. Available: https://www.gpo.gov/fdsys/pkg/PLAW-113publ283/pdf/PLAW-113publ283.pdf. Accessed on: July 03, 2017.

[11] Library of the US Congress. *Federal Information Security Management Act of 2002, Pub. L. 107-347 (Title III), 116 Stat 2946*. [Online]. Available: https://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf. Accessed on: July 03, 2017.

[12] National Institute of Standards and Technology. *NIST Special Publication*. [Online]. Available: http://csrc.nist.gov/publications/PubsSPs.html. Accessed on: July 03, 2017.

[13] National Institute of Standards and Technology. *Federal Information Processing Standards (FIPS)*. [Online]. Available: http://csrc.nist.gov/publications/PubsFIPS.html. Accessed on: July 03, 2017.

[14] National Institute of Standards and Technology. Computer Security Division. Information Technology Laboratory. *Risk Management Framework*. [Online]. Available: http://csrc.nist.gov/groups/SMA/fisma/Risk-Management-Framework/index.html. Accessed on: July 03, 2017.

[15] National Institute of Standards and Technology. NIST Risk Management Framework. *Categorize Step – System Perspective. Draft.* [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/Risk-Management/documents/categorize/QSG_categorize-system-perspective.pdf. Accessed on: July 03, 2017.

Стаття надійшла до редакції 21 липня 2017 року.

REFERENCES

[1] Budget and Presidential Materials, Compilation of Presidential Documents, Office of the Federal Register, National Archives and Records Administration, Donald J. Trump (May 11, 2017). *DCPD-201700327. Executive Order 13800. Strengthening the cybersecurity of federal networks and critical infrastructure*. [Online]. Available: https://www.gpo.gov/fdsys/pkg/dcpd-201700327/pdf/dcpd-201700327.pdf. Accessed on: July 03, 2017.

[2] National Institute of Standards and Technology. *DRAFT NISTIR 8170 The Cybersecurity Framework. Implementation Guidance for Federal Agencies*. Matt Barrett, Jeff Marron, Victoria Yan Pillitteri, Jon Boyens, Greg Witte, and Larry Feldman. [Online]. Available: http://csrc.nist.gov/publications/drafts/nistir-8170/nistir8170-draft.pdf. Accessed on: July 03, 2017.

[3] V.A. Romaka, V.B. Dudykevych, Yu.R. Herasym, P.I. Haraniuk, and I.O. Kozliuk, *Information security management systems.* Lviv, Ukraine: Publisher Lviv Polytechnic, 2012.

[4] International Organization for Standardization. *ISO 9000 Introduction and Support Package: Guidance on the Concept and Use of the Process Approach for management systems.* Document: ISO/TC 176/SC 2/N 544R3. ISO, 2008 [Online]. Available: http://www.iso.org. Accessed on: July 03, 2017.

[5] Institute for Standardization of the French Republic. *Final draft international standard ISO/FDIS 9001:2015(E). Quality management systems. Requirements* [Online]. Available: http://www.afnor.fr. Accessed on: July 03, 2017.

[6] International Organization for Standardization. *ISO 9001:2015*. ISBN 978-92-67-10648-9. ISO Central Secretariat, Chemin de Blandonnet 8 Case Postale 401, CH – 1214 Vernier, Geneva, Switzerland, ISO, 2015 [Online]. Available: http://www.iso.org. Accessed on: July 03, 2017.

[7] International Organization for Standardization. *Moving from ISO 9001:2008 to ISO 9001:2015*. ISO Central Secretariat, Chemin de Blandonnet 8 Case Postale 401, CH – 1214 Vernier, Geneva, Switzerland, ISO, 2015 [Online]. Available: http://www.iso.org. Accessed on: July 03, 2017.

[8] International Organization for Standardization. *Quality management principles.* ISBN 978-92-67-10650-2. ISO Central Secretariat, Chemin de Blandonnet 8 Case Postale 401, CH – 1214 Vernier, Geneva, Switzerland, ISO, 2015 [Online]. Available: http://www.iso.org. Accessed on: July 03, 2017.

[9] International Organization for Standardization. *ISO 9001:2015 Quality management systems. Requirements* [Online]. Available: http://www.iso.org. Accessed on: July 03, 2017.

[10] Library of the US Congress. *Federal Information Security Modernization Act of 2014, Pub. L. 107-347 (Title III), 116 Stat 2946*. [Online]. Available: https://www.gpo.gov/fdsys/pkg/PLAW-113publ283/pdf/PLAW-113publ283.pdf. Accessed on: July 03, 2017.

[11] Library of the US Congress. *Federal Information Security Management Act of 2002, Pub. L. 107-347 (Title III), 116 Stat 2946*. [Online]. Available: https://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf. Accessed on: July 03, 2017.

[12] National Institute of Standards and Technology. *NIST Special Publication*. [Online]. Available: http://csrc.nist.gov/publications/PubsSPs.html. Accessed on: July 03, 2017.

[13] National Institute of Standards and Technology. *Federal Information Processing Standards (FIPS)*. [Online]. Available: http://csrc.nist.gov/publications/PubsFIPS.html. Accessed on: July 03, 2017.

[14] National Institute of Standards and Technology. Computer Security Division. Information Technology Laboratory. *Risk Management Framework*. [Online]. Available: http://csrc.nist.gov/groups/SMA/fisma/Risk-Management-Framework/index.html. Accessed on: July 03, 2017.

[15] National Institute of Standards and Technology. NIST Risk Management Framework. *Categorize Step – System Perspective. Draft.* [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/Risk-Management/documents/categorize/QSG_categorize-system-perspective.pdf. Accessed on: July 03, 2017.

ЮЛИЯ КОЖЕДУБ

РЕАЛИЗАЦИЯ ПРОЦЕССНОГО ПОДХОДА К УПРАВЛЕНИЮ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ДОКУМЕНТАХ NIST

Исследуются методологические основы деятельности Национального института стандартов и технологий США. Сосредотачивается внимание на процессном подходе к созданию рекомендаций, руководств, руководящих указаний, рамочных документов. Установленные такими документами принципы направляют деятельность организаций по управлению рисками информационной безопасности. В этой статье анализируются методические документы по информационной безопасности, кибербезопасности и компьютерной безопасности, направленные помочь выбрать набор мероприятий контроля безопасности. В частности, этот анализ касается следующих этапов работ по защите информации. Во-первых, классификации информации и информационных систем. Во-вторых, применение базовых правил, относящихся к организационным мероприятиям защиты информации. В-третьих, это принятие выборочных мероприятий контроля защиты, которые есть подходящими и адекватными определенной информационной системе. Исследуемые методические документы NIST предоставляют практические советы специалистам по защите информации для снижения рисков информационной безопасности. Применение методических документов NIST в США является обязательным для государственных учреждений и организаций. Разработанную на их основе систему защиты направлено на уменьшение рисков безопасности информации и информационных систем для любых организаций, и не только государственной формы собственности. Предложенные базовые меры защиты можно адаптировать для практического применения с незначительным модифицированием. Создание действенной индивидуальной комплексной системы защиты информации является важной задачей, в основе которой лежит процесс управления рисками информационной безопасности. Система защиты позволит сохранить как прибыльность организации, так и ее репутацию с помощью уменьшения рисков информационной безопасности.

Ключевые слова: методические документы, кибербезопасность, риски информационной безопасности, процессный подход, риск-менеджмент, стандарты, специальные публикации, NIST.

YULIIA KOZHEDUB

IMPLEMENTATION OF THE PROCESS APPROACH TO MANAGING RISKS OF INFORMATION SECURITY IN THE NIST DOCUMENTS

The methodological foundations of activity of the National Institute of Standards and Technology of the United States (NIST) are explored. The focus is on the process approach to developing recommendations, manuals, guidelines, framework documents. The principles established by such documents direct the activities of organizations to manage information security risks. In this article analyzes methodical documents on information security, cyber security and computer security aimed to help select a set of security control measures. In particular, this analysis relates to such stages of work of the protection of information. First, the classification of information and information systems. Secondly, the application of the basic rules relating to organizational measures for information protection. Thirdly, it is the implementation of selective control measures of protection, which are appropriate and adequate to a certain information system. The explored methodical documents NIST provides practical advices to specialists in information protection for decrease the risks of information security. The use of the methodical documents NIST in the United

States is mandatory for government agencies and organizations. The security system developed on their basis is aimed at reducing the security risks of information and information systems for any organizations, and not only the state form of ownership. The proposed basic protection measures can be adapted for practical application with minor modifications. Creating an effective, individual, integrated system of information security is an important task, which is based on the process of managing information security risks. The security system will save both the profitability of the organization and its reputation by reducing the risks of information security.

Keywords: methodical documents, cyber security, information security risks, process approach, risk management, standards, special publications, NIST.

Юлія Василівна Кожедуб, кандидат технічних наук, доцент кафедри управління, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.

E-mail: JuliaKozhedub@email.ua.

Юлия Васильевна Кожедуб, кандидат технических наук, доцент кафедры управления, Институт специальной связи и защиты информации Национального технического университета Украины "Киевский политехнический институт имени Игоря Сикорского", Киев, Украина.

Yuliia Kozhedub, candidate of technical sciences, associate professor at the management academic department, Institute of special communication and information protection National technical university of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.