Олександр Олегович Бакалинський, заступник завідувача кафедри управління та тактико-спеціальної підготовки, Державний заклад "Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут", Київ, Україна.

Олександр Михайлович Богданов, доктор технічних наук, професор, завідувач кафедри управління та тактико-спеціальної підготовки, Державний заклад "Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут", Київ, Україна.

Василь Васильович Цуркан, кандидат технічних наук, доцент кафедри кібербезпеки та застосування автоматизованих інформаційних систем та технологій, Державний заклад "Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут", Київ, Україна.

Volodymyr Mokhor, doctor of technical sciences, professor, director, Pukhov institute for modeling in energy engineering of National academy of sciences of Ukraine, Kyiv, Ukraine.

Oleksandr Bakalynskyi, deputy head of management and tactical and special training academic department, State institution "Institute of special communications and information protection National technical university of Ukraine "Kyiv polytechnic institute", Kyiv, Ukraine.

Oleksandr Bohdanov, doctor of technical sciences, professor, head of management and tactical and special training academic department, State institution "Institute of special communications and information protection National technical university of Ukraine "Kyiv polytechnic institute", Kyiv, Ukraine.

Vasyl Tsurkan, candidate of technical sciences, associate professor at the cybersecurity and application of information systems and technologies academic department, State institution "Institute of special communications and information protection National technical university of Ukraine "Kyiv polytechnic institute", Kyiv, Ukraine.

УДК 004.056.5

ЮЛІЯ КОЖЕДУБ

АНАЛІЗ ДОКУМЕНТІВ З КЕРУВАННЯ РИЗИКОМ КІБЕРБЕЗПЕКИ

У статті подано аналіз новітніх документів щодо менеджменту ризиків в сфері забезпечення інформаційної безпеки та кібербезпеки. Дослідження сучасних стандартів показують, що їхню увагу зосереджено на ризиках, як це було започатковано в стандартах на системи менеджменту Міжнародної організації зі стандартизації. У статті показано, що проблемою дослідження ризиків інформаційної безпеки та кібербезпеки займаються організації різного статусу, підпорядкованості й форми власності. Зазначені організації набули великого досвіду у питаннях, пов'язаних з процесом керування ризиками інформаційної безпеки та кібербезпеки. Значення їхньої роботи має планетарний характер, оскільки розробки у цій сфері діяльності було покладено як основа створення документів різного виду, що вони їх пропонують різним країнам і організаціям для упровадження в діяльність щодо забезпечення інформаційної безпеки та кібербезпеки. У статті запропоновано розглядати комплексно документи, розроблені для роботи ризик-менеджера з інформаційної безпеки та кібербезпеки. Модель інструментарію побудовано на центральному ядрі, який визначено нормативними документами як процес управління ризиками. Нормативні документи, що визначають процес управління ризиками – це основоположні стандарти, що застандартизовують поняття «ризик» і це є відправною точкою для менеджерів усіх ланок, які

розуміють важливість опрацювання ризиків. У статті відображено розвиток наукової думки щодо термінологічного апарату й наукового підходу до осмисленого розуміння важливості процесу управління ризиками сфери діяльності із забезпечення інформаційної безпеки та кібербезпеки. У статті проаналізовано-документи, розроблені міжнародними й національними організаціями для допомоги у роботі ризик-менеджерів. Додатково до дослідження в рамках цілей цієї статті відображено інші документи, що є деталізованими інструкціями для ризик-менеджерів сфери діяльності забезпечення інформаційної безпеки та кібербезпеки.

Ключові слова: менеджмент, менеджер, нормативні документи, ризик, стандарти.

Постановка проблеми. На сьогодні вже не можливо не враховувати чинник сучасного світу – ризики, що мають прояви поза нашої волі, бажання і є сутністю життя людини. Відриваючись від побутового значення терміну “ризики”, зазначимо, що сучасний стан кіберзагроз значно відрізняється від того, яким він був ще декілька років тому. Фахівці різних країн світу, експерти цієї сфери діяльності й урядовці погоджуються з тим, що швидкість нападів і їхня складність змінюються радикально. Ще одна важлива різниця полягає в їхньому розмаїтті. Кіберризики загрожують вигодам, отримуваним від застосування інформаційних технологій – економічним, політичним або соціальним, – усі надбання, які надає людству винахід кіберпростору та його утіленням в повсякденне життя. Глобальне впровадження інформаційних технологій і його наслідок, неминучість вторгнення його в особисте, приватне життя, змушує звернути увагу на безпеку його застосунків, а тому є потреба в урегулюванні ризиків та урахування “наслідків” від вигод новинок інформаційних технологій.

Зростає кількість держав, що сьогодні розуміють значимість та вважають кіберзасоби для подолання кіберризиків необхідним елементом свого стратегічного набору інструментів поряд з дипломатичними заходами, економічною силою і військовою потужністю [1] - [2]. Це зумовлює занепокоєння спеціалістів цієї галузі знань і діяльності, і вони шукають відповідь на запитання: «Чи не стануть люди у найближчому майбутньому свідками повномасштабної війни в кіберпросторі між державами?». І це не дивне питання, оскільки злочинні дії в кіберпросторі збільшуються день-від-дня, і, зокрема, останнім часом, певні дійові особи час від часу виявляють зацікавленість у застосуванні кіберзасобів – хоча наразі є небагато свідчень їх фактичного використання.

Проте науковці вважають, що кібервійна не відбудеться [1]. Сучасний досвід фактичного застосування державами кіберзасобів вказує на те, що для таких засобів більш характерні інші інструменти прояву застосування інформаційних технологій на шкоду суспільству і світу: шпигунство або саботаж, що робить більш вірогідним їх застосування нижче порогу, що визначає збройний напад. Попри певну логічність цього аргументу, стає дедалі більш зрозуміло, що деякі держави розглядають кіберзасоби частиною своїх оперативних військових сил і засобів, і не бояться застосовувати їх, навіть, якщо вони не схильні до публічного визнання цього факту.

Розмаїття способів можливого застосування кіберзасобів ставить перед спеціалістами цієї сфери діяльності одне з найбільших завдань щодо розуміння її власної ролі в кіберзахисті. Розглядаючи роль фахівців з ризиків на кіберсцені особливо важливо звертати увагу на два головні типи кібернападів. По-перше, шпигунство за допомогою кіберзасобів – як на стратегічному, так і на оперативному рівнях – може поставити під загрозу конфіденційність інформації і інформаційних систем, потенційно видаючи супротивнику секретну й конфіденційну інформацію. По-друге, саботаж за допомогою кіберзасобів може призвести до важливих фізичних наслідків, особливо коли мішенню стають особливо важливі об’єкти держав, такі як: енергетичні компанії, банківські установи або транспортні корпорації, або коли виконують маніпулювання даними з метою заплутати ціль і зірвати процес командування, управління і прийняття керівних й політичних рішень.

До того ж співробітники служб захисту інформації, служб безпеки усіх рівнів і в усіх сферах можуть стати мішенню для зловмисників, щоб отримати фінансову вигоду, або як попередній етап нападів. Поширення Інтернету на мобільних пристроях разом з поширенням

соціальних мереж ще більше ускладнює завдання забезпечення оперативної безпеки в кіберпросторі. Щоб протистояти цим викликам, потрібно забезпечити комплексний підхід до вирішення усіх питань щодо кібербезпеки, щоб протистояти різноманітним загрозам, що розвиваються, за допомогою єдиної дієвої спеціалізованої мережі з захисту інформації із задіянням спеціалістів сфери інформаційної безпеки і кібербезпеки.

Аналіз останніх досліджень і публікацій. Дослідження цієї проблеми можна розпочати з термінології, що її започатковано в міжнародному стандарті ISO/IEC 27032:2012 [3]. Алпеєв А.С., Архіпов О.Є., Чепуренко Я.О. продовжили термінологічні дослідження. Мохор В.В. і Богданов О.М. займаються методологічними дослідженнями зазначеної теми. Грибунін В.Г. є дослідником різноманітних документів щодо різних аспектів кібербезпеки. Горбатько О.В. публікує статті про кібербезпеку сучасного інформаційного простору (на прикладі м. Москва). Цікавими для дослідження можуть бути роботи Тіма Клау про планування ресурсів на інформаційну безпеку організації, зокрема, на його думку, інвестування в кваліфікованих спеціалістів дасть змогу збільшити прибутки компаній від інвестицій в технології, спрямовані на забезпечення безпеки. Напрями розвитку кібербезпеки було описано Лєбєдєвим В., Огороднiковим Д., Олейніком М., Прозоровим Д., Свищевим А. на сторінках журналу «Information Security / Информационная безопасность». Практичні застосунки методів і способів захисту від кібернебезпеки знайшли своє відображення в роботах Є.В. Брежнєва, А.А. Коваленка, О.О. Ілляшенка. Аналізуванню оцінки ризиків кібербезпеки у банківській сфері присвячено роботу Євсеєва С.П. та інших. Наразі тема щодо безпеки у кіберпросторі є найпоширенішою і найбільш затребуваною суспільством, оскільки це стосується кожного, хто стикається зі світом інформаційних технологій.

Постановка завдання. Використання інструментів в сфері кібербезпеки, де найголовнішим пріоритетом є захист мереж є складним завдання, зважаючи на широке поширення й необхідність забезпечити захист інформаційно-комунікаційних систем, для захисту інформації від загроз, джерела яких знаходяться в кіберпросторі.

Нормативними документами пропонується платформа для дорадчої діяльності й обміну деталями щодо належної практики серед менеджерів з ризиків, використовуючи більш широкий спектр формальних і неформальних каналів, в тому числі процес з оборонного та безпекового планування. Такі механізми пропонують: політику на місцях, оперативну і технічну підтримку та поради менеджерам з інформаційної безпеки та кібербезпеки щодо розвитку й впровадження сил та засобів захисту. Завдяки цьому можливе надання рекомендацій щодо створення військової програми кібербезпеки або допомогу з обміну належними практиками забезпечення кіберзахисту необхідними ресурсами, а цими елементами менеджменту не можна нехтувати, кожен є надзвичайно важливим.

Міжнародна діяльності з нормотворення та відповідальна поведінка держав в кіберпросторі заохочує до створення заходів з розбудови довіри в кіберпросторі. Така діяльність сприяє обміну інформацією про стан справ в кіберпросторі як між менеджерами з кіберзахисту, так і між іншими міжнародними організаціями, особливо з тими, які розуміють, які зловживання можливі в кіберпросторі й знаються на «результатах» такої діяльності.

Виклад основного матеріалу дослідження. Систему понять щодо ризик-менеджменту було запропоновано спеціалістами австралійської та новозеландської митниці і прикордонних військ цієї країни. Значна берегова лінія, що її потрібно було охороняти спонукала до прийняття неординарних рішень, що в свою чергу призвела до появи видатного, без перебільшення говоримо про це, документа: ISO 31000 [4]. Застандартизовані терміни мали скласти фундамент для фахівців цієї галузі знань: так виник ISO Guide 73 [5]. Поява таких документів, що мають універсальний характер, а їх можна застосовувати до ризиків різних сфер діяльності людини, свідчить про вкрай необхідну потребу реагувати на виклики несподіванок від діяльності людини. На сьогодні чинні чергові версії цих нормативних документів застосовуються і їх підтримують спеціалісти цієї галузі діяльності. Проте початкові редакції були специфічними, вони стосувались виключно митної справи та питань охорони кордону.

На основі досвіду фахівців Митної служби Австралії та Нової Зеландії щодо стандартизації процедур управління ризиками [6] розроблено міжнародний стандарт ISO 31000:2009. Застосування правил, розроблених австралійськими митниками є передовим досвідом, їх покладено в подальші розробки сучасних стандартів.

Створення означених документів підтверджено в регіональних австралійсько-новозеландських документах: AS/NZS 4360:1994 і AS/NZS ISO 31000:2009, Настанові щодо управління ризиками Всесвітньої митної служби, Звіті з використання системи управління ризиками австралійської митної служби NO:PS 2008/23, Доповіді департаменту аудиту при Уряді Австралії про впровадження системи управління ризиками в роботу митної служби країни.

Управління ризиками у процесі діяльності австралійської Митної і Прикордонної служби містить чітко визначені заходи, які за їх послідовного застосування підтримують оптимальний процес прийняття рішення шляхом поглибленого розуміння ризиків і їх впливу на зовнішньоторговельну діяльність, як наслідок від означених дій. Через значну довжину кордону цієї материкової країни, плюс острови цього конгломерату, треба було вживати заходи щодо недопущення на внутрішній ринок контрабандних товарів. Уведення системи управління ризиками в цій сфері і послідовні заходи для цього призвели до зменшення витрат на державний апарат, грошове утримання прикордонників й митників. Треба зазначити, що правильна й послідовна політика співпраці з місцевим населенням, така як: створення добровільних груп допомоги прикордонникам і митникам, сприяла упровадженню процедур обробляння ризиків.

Окремі положення системи управління ризиками було застосовано на окремих дільницях митниці в Австралії у 1994 році, повністю її було запроваджено в 1996 році. Основу було закладено загальними положеннями австралійсько-новозеландського стандарту AS/NZS 4360:1994, які згодом доповнили Рекомендації з ризик-менеджменту Всесвітньої митної служби, а також переглянутої в розділі 6 Кіотської конвенції 1999 року.

Дуже важливо відмітити, що саме Уряд Австралії уперше в світі в 1996 році зрозумів важливість застосування системи управління ризиками на загальнодержавному рівні з метою спрощення і підвищення ефективності діяльності усіх державних структур, зокрема виявлення проблемних прогалин, їх оперативного вирішення, а також недопущення подібних ситуацій в подальшому разом зі зменшенням державних витрат на ці цілі.

Після того, як вдало запрацювала система управління ризиками на митниці, її було поширено на інші ключові сфери діяльності: нафтова промисловість, тютюнова промисловість, торгівля неоподаткованими митом товарами, текстильна промисловість, транспортні засоби, загальні питання упорядкування бізнесу. Система працювала й у цих сферах промисловості.

Для кожної з цих сфер передбачалось створення типових напрямів щодо накопичення інформації з метою застосування її у подальшому для загальної системи управління ризиками, а саме: питання вивчення статистики, ведення Єдиного реєстру ризиків, актуалізація національного профілю ризику для кожного з часткових ризиків.

Підсумуємо сказане: започатковані система управління ризиками разом з процесом управління ризиками є початковою точкою для розуміння важливості опрацювання ризиків. Набір системи для управління ризиками має базуватись на наукових підходах і методології, запропонованої базовими документами, а разом з процесом управління ризиками свідчить про зрілість менеджерів усіх ланок, готовність до роботи за умов мінливості й нестабільності ринкових умов.

Наступним на розгляді нашої статті є робота фахівців Національного інституту стандартів і технологій міністерства торгівлі Сполучених Штатів Америки (далі – NIST, National Institute of Standards and Technology) [7] в рамках виконання Закону про модернізацію Федеральної інформаційної безпеки від 2014 р. (далі – FISMA, Federal Information Security Modernization Act of 2014, S.2521), які упроваджують політику управління ризиками

інформаційної безпеки на основі економічно ефективних заходів безпеки для усього життєвого циклу інформаційних систем.

Їхня робота зводиться до того, що потреби в захисті зацікавлених сторін і проблеми безпеки, пов'язані з інформаційною системою, потрібно правильно визначити та розглядати, починаючи з задач проектування інформаційних систем, і відслідковувати це питання протягом усього життєвого циклу цієї системи.

Ця головна мета зводиться до вирішення наступних завдань:

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

– досягнути єдиного мислення, щоб забезпечити безпеку для будь-якої інформаційної системи, незалежно від її масштабів, розміру, складності та стадії життєвого циклу цієї системи;

– забезпечити подробиці та деталі для міркування і продемонструвати, що принципи безпеки, концепція та дії щодо забезпечення безпеки можуть бути ефективно застосовано до систем інженерної діяльності;

– поширювати техніку безпеки системи, проголосивши її за основоположну дисципліну, що їх може бути застосовано і вивчено;

– створювати основу, що буде слугувати розробленню освітніх і навчальних програм, включаючи розробку індивідуальних програм навчання з наданням сертифікатів та інших документів з професійними критеріями оцінки роботи персоналу з забезпечення інформаційної безпеки у повсякденній роботі.

Публікації FISMA розробляють спеціалісти NIST відповідно до своїх статутних обов'язків. NIST відповідає за розробку стандартів і керівних принципів з інформаційної безпеки та кібербезпеки, в тому числі мінімальні вимоги для федеральних інформаційних систем, але такі стандарти та керівні принципи не будуть застосовуватись до систем національної безпеки без погодження відповідних федеральних посадових осіб, які здійснюють повноваження політики щодо таких систем. Публікації серії NIST SP 800 використовуються федеральними агентствами для класифікації інформації та інформаційних систем, і засновані на цілях забезпечення належного рівня інформаційної безпеки та кібербезпеки відповідно до діапазону рівнів ризиків для класифікованих інформації та інформаційних систем. Публікації серії NIST SP 800 – це рекомендації щодо правил з інформаційної безпеки для встановлених типів інформації та інформаційних систем, які повинні бути включено відповідно в кожну категорію. Як вище було зазначено, ці документи містять мінімальні вимоги до інформаційної безпеки (управління, оперативні і технічні засоби безпеки) для інформації та інформаційних систем в кожній такій класифікованій категорії.

Як один з ключових елементів проекту щодо впровадження FISMA, NIST також розробила інтегровану систему управління ризиків, яка ефективно об'єднує всі, розроблені під егідою FISMA пов'язані стандарти безпеки та керівництва з метою сприяння розробки комплексних і збалансованих програм інформаційної безпеки.

NIST розробляє і видає стандарти, настанови та інші публікації, щоб допомогти федеральним агентствам у виконанні Федерального закону про управління інформаційною безпекою (FISMA) і в управлінні економічно ефективних програм для захисту їх інформації та інформаційних систем.

FIPS (Federal Information Processing Standards) [8] також розробляються NIST відповідно до FISMA. FIPS затверджуються міністром торгівлі і є обов'язковими до виконання федеральними агентствами/організаціями. FISMA вимагає, щоб інформаційні системи федеральних агентств/організацій відповідали цим стандартам, а тому органи влади не можуть відмовитись від їх застосування у повсякденній діяльності.

Надання рекомендації для мінімальних заходів безпеки для інформаційних систем та віднесення їх до категорій, виконується відповідно до FIPS 199 Стандарти категоризації безпеки федеральних інформації та інформаційних систем.

Вимоги щодо обов'язкових параметрів конфігурації, що випливають із Федерального закону про управління інформаційною безпекою встановлено у FIPS 200 Мінімальні вимоги безпеки для федеральних інформації та інформаційних систем.

Настанови, нормативні документи і рекомендації оформляють як спеціальні публікації (далі позначка SP) 800-й серії NIST. Документи FIPS та спеціальні публікації NIST серії SP 800 взаємопов'язані.

Щоб забезпечити зворотний зв'язок щодо змісту кожної з публікацій FISMA, NIST активно залучає і заохочує осіб й організації в державному та приватному секторах. У більшості випадків публікація безпеки FISMA має пройти три повних цикли громадських обговорень, забезпечуючи можливість для окремих осіб і організацій, активно брати участь в розробці стандартів і керівних принципів. NIST також працює в тісній співпраці з власниками, операторами й адміністраторами інформаційних систем, щоб отримати зворотній зв'язок в режимі реального часу стосовно можливості реалізувати конкретні контрзаходи (засоби безпеки), що їх запропоновано для федеральних інформаційних систем. Нарешті, NIST має велику програму допомоги, яка підтримує тісні контакти з професіоналами з безпеки на всіх рівнях, щоб вони мали змогу в майбутньому оновлювати стандарти і правила безпеки. Поєднання широкого суспільного процесу огляду стандартів і розробки керівних принципів, досвід створення інструментарію й реалізації гарантій і контрзаходів (засоби безпеки) в інформаційних системах, все це працює на високу якість широко визнаних стандартів безпеки та керівних принципів, які використовуються не лише федеральним урядом Сполучених Штатів Америки, але часто застосовується на добровільній основі багатьма організаціями в приватному секторі Америки.

Закон про модернізацію Федеральної інформаційної безпеки 2014 р. вносить зміни в Закон про управління інформаційною безпекою 2002 р. і передбачає декілька модифікацій, що модернізують федеральні методи безпеки, щоб вирішити проблеми безпеки, які так швидко еволюціонують в сучасному світі.

По-перше, це згадувана інтегрована система управління ризиками, що ефективно об'єднує всі, розроблені під егідою FISMA пов'язані стандарти безпеки та настанови задля розробки комплексних і збалансованих програм інформаційної безпеки.

По-друге, вибір заходів контролю управління безпекою для системи здійснюються в рамках чинної програми інформаційної безпеки всієї організації, яка охоплює управління організаційним ризиком: це є ризик для організації або особи, пов'язаний з роботою інформаційної системи. Управління організаційним ризиком є ключовим елементом в програмі інформаційної безпеки організації і забезпечує ефективну основу для вибору відповідних елементів системи керування безпекою, необхідних для захисту окремих осіб, операцій і активів організації.

По третє, це ризик-орієнтований підхід. Структура управління ризиками забезпечує процес, який об'єднує діяльність щодо безпеки та управління ризиками в життєвому циклі розвитку системи. Підхід на основі ризику для вибору заходів контролю безпеки бере до уваги ефективність процесу управління ризиками. Вибір заходів контролю безпеки має й обмеження згідно з чинним законодавством: директиви, декрети, політики, стандарти і правила. Управління організаційними ризиками мають першорядне значення для ефективної програми інформаційної безпеки і може застосовуватись як для нових щойно створюваних інформаційних систем так і для успадкованих та/чи застарілих систем в контексті життєвого циклу розробки системи управління ризиками.

Підсумовуючи діяльність NIST в цій галузі знань зазначимо, що окрім вказаної серії стандартів NIST SP 800 (комп'ютерна безпека) [9], є серія NIST SP 500 щодо технологій комп'ютерних систем і серія NIST SP 1800 стосовно практичних настанов з кібербезпеки. Усі ці три серії стосуються комп'ютерної/кібер/інформаційної безпеки, надаючи рекомендації, настанови та вихідні дані спеціалістам з безпеки сучасних систем.

Наступним в нашому дослідженні є міжнародний стандарт ISO/IEC 27005:2011 Інформаційна технологія. Методи захисту. Менеджмент ризиків інформаційної безпеки [10].

Першу редакцію міжнародного документа було створено 2008 р. на основі скасованих міжнародних стандартів серії ISO/IEC 13335. Це такі технічні звіти (TR): ISO/IEC TR 13335-3:1998 Інформаційна технологія. Настанови для менеджменту безпеки інформаційних технологій. Частина 3. Методи захисту для менеджменту безпеки інформаційних технологій, ISO/IEC TR 13335-4:2000 Інформаційна технологія. Настанови для менеджменту безпеки інформаційних технологій. Частина 4. Вибір заходів захисту. Варто зазначити, що наразі готується [11] нова версія: ISO/IEC WD 27005, що свідчить як про розвиток («еволюцію») нових загроз для інформаційної безпеки, так і про готовність фахівців з захисту їм протистояти [1].

Міжнародний стандарт ISO/IEC 27005:2011 є настановою з менеджменту ризиків інформаційної безпеки в організації. Він підтримує вимоги щодо побудови системи менеджменту інформаційної безпеки (далі – СМІБ) згідно з рекомендаціями ISO/IEC 27001:2013, в якому визначено необхідність управління ризиками під час побудови СМІБ.

Цей стандарт забезпечує настанови для ризик-менеджменту інформаційної безпеки. У ньому дотримуються генеральної концепції, яку визначену в ISO/IEC 27001, і він визначає як забезпечити задоволеність від упровадження інформаційної безпеки, що основана на підході ризик-менеджменту. Відомий як концепції, моделі та методи захисту, цей стандарт визначає, що в ISO/IEC 27001 та ISO/IEC 27002 наведено важливі положення для повного розуміння змісту ISO/IEC 27005:2011. Цей стандарт можна застосовувати до усіх типів організацій (наприклад, комерційних підприємств, урядових агенцій, непрофільних організацій) в межах яких керують ризиками, і це може задовольнити організації щодо забезпечення інформаційної безпеки. Надзвичайно важливим є поєднання у цьому документі концепції ризик-менеджменту та інформаційних технологій.

Концепцію ризик-менеджменту викладено у відомих міжнародних стандартах: ISO 31000:2009 Менеджмент ризиків. Принципи і настанови, ISO 31010:2009 Менеджмент ризиків. Методики оцінки ризиків та ISO Guide 73:2009 Менеджмент ризиків. Словник термінів. Отже, концептуально процедура управління ризиками інформаційної безпеки передбачає:

- визначення контексту;
- оцінку ризиків;
- розгляд ризиків;
- визначення ступеня допустимого ризику;
- інформування про ризики;
- моніторинг ризиків і звітність про ризики.

Проте, у міжнародному стандарті ISO/IEC 27005 не визначено конкретних методів управління ризиками інформаційної безпеки, а лише подано загальний підхід, і в цьому полягає його індивідуальність щодо застосування на практиці.

Менеджмент ризиків інформаційної безпеки в сфері інформаційних технологій (ІТ) пов’язаний з узяттям на себе відповідальностей за виконувану роботу в галузі ІТ-індустрії, зокрема, це стосується впровадження в структури організацій, що займаються цим видом діяльності/промисловості, відповідної структурної одиниці. Отже, стандарт пропонує встановити і затвердити штатну одиницю й призначити відповідальних за процес менеджменту ризиків інформаційної безпеки інформаційних технологій. У посадовців цієї структурної штатної одиниці можуть бути такі обов’язки [10]:

- розробка процесу менеджменту ризиків безпеки інформаційних технологій;
- ідентифікація та аналіз причетних сторін;
- визначення посад і закріплення відповідальностей всіх причетних сторін;
- створення необхідних взаємовідносин між організацією та причетними сторонами, також взаємодія з високорівневими функціями менеджменту ризиків організації (наприклад, менеджмент операційних ризиків, менеджмент організаційних ризиків), а також взаємодія з іншими значущими проектами або видами діяльності організації;

– визначення шляхів делегування прийняття рішень на більш високий рівень та/або іншим спеціалістам;

– визначення переліку необхідних для ведення СМІБ документів.

Документом, що показово доводить продуманість і послідовність дій з завершення концепції безпеки в сфері ризиків, може бути COBIT 5: Framework for IT Governance and Control (Принципи для організації управління й управління інформаційними технологіями) [12] – методика аудиту персоналу, який працює в сфері надання послуг інформаційних технологій на основі, створених СМІБ. Результативність й ефективність дій персоналу щодо захисту інформації, інформаційних систем, комп'ютерних мереж, інформаційних технологій підтверджується пройденим аудитом створеної й дієвої СМІБ. Міжнародна асоціація ISACA (Information Systems Audit and Control Association) об'єднує фахівців в сфері управління інформаційними технологіями. Діяльність цієї асоціації пов'язана з аудитом, безпекою і корпоративним управлінням інформаційними технологіями.

Метою цієї асоціації є [13]: дослідження, розробка, опублікування й упровадження стандартизованого набору документів щодо менеджменту інформаційними технологіями.

В інтересах професійних аудиторів, керівників інформаційних систем, адміністраторів і всіх зацікавлених осіб асоціація розбудовує свою концепцію менеджменту інформаційними технологіями відповідно до вимог інформаційної безпеки.

На основі концепції описуються елементи інформаційної технології, надаються рекомендації щодо системи менеджменту й забезпечення інформаційної безпеки.

Методології аудиту СМІБ притаманно багато специфічних властивостей, але в основу покладено такі фундаментальні принципи [14] - [16]:

– публічність під час прийняття й обговорення результатів;

– відкритість результатів аудиту.

Варто зазначити, що в цьому разі висновок про те, наскільки успішно функціонує об'єкт інформаційної діяльності і наскільки він відповідає заданим вимогам, робиться на основі вивчення якості виконання персоналом цього об'єкта своїх обов'язків, а також функціональними елементами СМІБ відповідних функцій, що зафіксовані у технологічних регламентах, які створені, своєю чергою, за заздалегідь встановленим стандартом. Цей метод є прогнозованим, а висновки за результатами аудиту мають імовірнісний характер.

Основними нормативними документами щодо проведення аудиту є [14]:

ISO 19011:2011 Настанови щодо аудиту систем менеджменту [15] – цей міжнародний стандарт містить настанови щодо аудиту систем менеджменту організацій;

ISO/IEC 27007:2011 Інформаційні технології. Методи захисту. Настанови щодо проведення аудиту систем менеджменту інформаційної безпеки [16], де конкретизовано процедури аудиту інформаційної безпеки. Ці стандарти розроблено Міжнародною організацією зі стандартизації разом з Міжнародною Електротехнічною Комісією (IEC, International Electrotechnical Commission) згідно з Віденською домовленістю.

За результатами аудиту СМІБ створюються документи, як правило, це оціночні звіти, що містять доволі конкретні і жорсткі рекомендації щодо узгодження внутрішніх процесів і регламентів із загальноприйнятими стандартами або практиками сфери діяльності інформаційних технологій.

Сьогодні є позитивний досвід застосування методології аудиту для оцінювання складних систем, зокрема, СМІБ, яка нерозривно пов'язана з діяльністю колективів людей, стосунки між якими є визначальним чинником успішного функціонування цих систем.

Методи збирання інформації передбачають [14] - [16]:

– опитування;

– спостереження за діяльністю;

– аналіз документів.

Вибрані джерела інформації можуть відрізнятися залежно від сфери та складності аудиту і можуть містити [14] - [16]:

– опитування працівників та інших осіб;

– спостереження за діяльністю, виробничим середовищем та умовами функціонування;
– такі документи, як: політика, цілі, плани, методики, стандарти, інструкції, ліцензії та дозволи, технічні умови, креслення, контракти і замовлення;
– такі протоколи, як: протоколи контролю, протоколи нарад, звіти про аудит, протоколи за програмами моніторингу і результати вимірювання;
– зведені дані, результати аналізу і показники діяльності;
– інформацію про програми об'єкта аудиту щодо відбору зразків і методики з управління процесами відбору зразків та вимірювання;
– повідомлення з інших джерел, наприклад, зворотний зв'язок із замовниками та іншу відповідну інформацію від зовнішніх сторін та рейтинг постачальників;
– комп'ютерні бази даних і веб-сайти.

Основними спонукальними чинниками розвитку COBIT (*Control Objectives for Information and Related Technologies*, Цілі управління інформаційними технологіями та суміжними технологіями) стало надання рекомендацій з таких питань як [17]:
– одержання інформації від більш широкого кола зацікавлених сторін про їхні очікування від інформаційних і пов'язаних з ними технологій;
– менеджування успішністю підприємств та інформаційними технологіями;
– менеджування істотно збільшеними обсягами інформації;
– менеджування всепроникними інформаційними технологіями, які стають усе більш інтегрованими в бізнес;
– подальше розвинення технологій та інновацій;
– удосконалювання контролю над дедалі більшою кількістю IT-застосунків, створюваних і керованих користувачами.

Оцінювання ефективності або якості діяльності обов'язково потребує [17]:
– вибору ключових показників (індикаторів), що характеризують кількісний або якісний стан властивостей об'єкта інформаційної діяльності або будь-якої діяльності;
– вибору методу вимірювання вибраних ключових показників і оцінювання його точності;
– визначення критеріїв оцінювання відповідності отриманих показників певним вимогам, що характеризує прийнятний з погляду власника об'єкта інформаційної діяльності рівень його якості або якості діяльності, що підлягає аудиту;
– отримання гарантій оцінювання.

У квітні 2012 р. було запропоновано нову версію COBIT, що отримала черговий номер «5». Отже, це узагальнення COBIT 4.1, методології ValIT, методології RiskIT та стандартів (наприклад це ISO/IEC 15504 Software Engineering – Process Assessment, на цьому стандарті побудовано принципово нову модель – Модель можливостей COBIT 5, Process Capability Model) [17].

Основні зміни стосувались [17]:
– нових принципів;
– нових термінів;
– нової моделі процесів і доменів;
– нової ієрархії цілей;
– змістовного терміну «enablers (забезпечувальні сили)»;
– входів і виходів для кожного процесу;
– оновленої таблиці RACI;
– Моделі можливостей (замість застарілої Моделі зрілості).

Основні принципи COBIT 5 [17]:
– фокусування на цінностях зацікавлених осіб;
– забезпечення цілісного підходу;
– зосередження уваги на потребах і контексті бізнесу;

– основний базис – забезпечувальні сили (enablers);

– розмежування зон «Governance» (понятійний семантичний переклад терміну – організація управління) і «Management».

Висновки з даного дослідження і перспективи подальших досліджень у даному напрямку. У статті показано розмаїття документів, що їх створюють як державні, так і приватні організації щодо власного бачення розв'язання проблем у сфері кібербезпеки, інформаційної безпеки, безпеки мереж та систем. Такі документи є рефлексією і вимогою часу. Напрацьований досвід фахівців сфери захисту інформації, попри закритість таких досліджень, з'являються у відкритих джерелах і поширюється світом серед як спеціалістів цієї галузі знань, так і тих, хто лише знайомиться з цією проблематикою. Специфічність ризиків кібербезпеки, інформаційної безпеки, інформаційних технологій виходить за рамки уживаності лише означеної нами теми, оскільки запобігти зловживанням у сфері інформаційних технологій через несанкціонований доступ, використання, розкриття, порушення, модифікації або руйнування інформації, що її було довірено як приватним особам, так і державним установам, – це завдання, що під силу наявному інструментарію менеджера з інформаційної безпеки та кіберризиків. Проте, неповним буде дослідження, якщо не вказати такі організації, що опікуються цими питаннями, як: NSA (National Security Agency, USA), Інститут SANS (American internet security training company, USA), US-CERT (United States Computer Emergency Readiness Team, USA), CIS (Center for Internet Security, USA), DISA (Defense Information Systems Agency, a United States Department of Defense combat support agency), Securosis (Information security research and advisory firm, USA), FFIEC (Federal Financial Institutions Examination Council, U.S. government), OWASP (Open Web Application Security Project, Belgium), OISSG (Open Information Systems Security Group, United Kingdom), OSSTMM (Open Source Security Testing Methodology Manual, Spain), ENISA (European Union Agency for Network and Information Security, Greece), BSI (Bundesamt für Sicherheit in der Informationstechnik, German). Повний діапазон методів, засобів і заходів, механізми реалізації таких, відтворено документально у виданнях перелічених нами організацій.

У цій статті висвітлено лише роботу чотирьох організацій, що мають стосунок до безпеки комп'ютерних, інформаційних систем і мереж, захисту інформації, інформаційних технологій. З кожним днем загрози і вразливості еволюціонують, порушники застосовують найсучасніший арсенал засобів для виконання своїх кримінальних дій, а тому дедалі ширше застосовуються інструменти захисту, якими є стандарти, настанови, технічні звіти, технічні специфікації, методики тощо, що зможуть допомогти зменшити, знизити, модифікувати ризики у кіберсфері.

Підсумовуючи зазначимо, що кібербезпека це набір засобів, стратегій, принципів забезпечення безпеки, гарантій безпеки, підходів до керування ризиками, дій, професійної підготовки кадрів, страхування й технологій, що їх застосовують для захисту кіберсфери, продуманість використання ресурсів й обізнаності споживачів ІТ-послуг [3]. Кібербезпеки досягають збереженням інформаційних активів організації та/чи споживачів ІТ-послуг, спрямованих як відповідь на відповідні кіберзагрози. Оскільки основними завданнями щодо забезпечення безпеки інформації є збереження властивостей інформації: доступності, цілісності, конфіденційності, то інформаційна безпеки і кібербезпека є необхідною умовою розвиненого сучасного інформаційного суспільства.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] Ніл Робінсон "Зміна підходів до кіберзахисту", *НАТО Ревю.* [Електронний ресурс]. Доступно: http://www.nato.int/docu/review/2016/Also-in-2016/cyber-defense-nato-security-role/UK/index.html. Дата звернення: Бер. 15, 2017.

[2] Кабінет Міністрів України. *Розпорядження від 10.03.2017 № 155-р "Про затвердження плану заходів на 2017 рік з реалізації Стратегії кібербезпеки України"*. [Електронний ресурс]. Доступно: http://www.kmu.gov.ua/control/uk/cardnpd?docid=249807504. Дата звернення: Бер. 25, 2017.

[3] International Organization for Standardization. *International Standard "ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity"*. [Електронний ресурс]. Доступно: https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en. Дата звертання: Бер. 20, 2017.

[4] International Organization for Standardization. *International Standard "ISO 31000:2009 Risk management – Principles and guidelines"*. [Електронний ресурс]. Доступно: https://www.iso.org/standard/43170.html. Дата звертання: Бер. 20, 2017.

[5] International Organization for Standardization. *International Standard "ISO Guide 73:2009 Risk management – Vocabulary"*. [Електронний ресурс]. Доступно: https://www.iso.org/standard/44651.html. Дата звертання: Бер. 20, 2017.

[6] "Таможенная служба Австралии как инновационная площадка в области разработки международных стандартов применения систем управления таможенными рисками". [Електронний ресурс]. Доступно: http://have-right/ombudsman/645-australian-customs-service.html. Дата звертання: Бер. 20, 2017.

[7] National Institute of Standards and Technology. Computer Security Division. Information Technology Laboratory. "Risk Management Framework". [Електронний ресурс]. Доступно: http://csrc.nist.gov/groups/SMA/fisma/Risk-Management-Framework/index.html. Дата звертання: Бер. 20, 2017.

[8] National Institute of Standards and Technology. "Federal Information Processing Standards (FIPS)". [Електронний ресурс]. Доступно: http://csrc.nist.gov/publications/PubsFIPS.html. Дата звертання: Бер. 20, 2017.

[9] National Institute of Standards and Technology. "NIST Special Publication". [Електронний ресурс]. Доступно: http://csrc.nist.gov/publications/PubsSPs.html. Дата звертання: Бер. 20, 2017.

[10] International Organization for Standardization. International Standard "ISO/IEC 27005:2011 Information technology. Security techniques. Information security risk management". [Електронний ресурс]. Доступно: https://www.iso.org/standard/56742.html. Дата звертання: Бер. 20, 2017.

[11] International Organization for Standardization. "Електронна картка стандарту ISO/IEC 27005:2011 Information technology. Security techniques. Information security risk management". [Електронний ресурс]. Доступно: https://www.iso.org/search/x/query/27005. Дата звертання: Бер. 20, 2017.

[12] НОУ ИНТУИТ. Курс лекций, "COBIT 5 – Что нового?". [Електронний ресурс]. Доступно: http://www.intuit.ru/studies/courses/3704/946/lecture/15117?page=1,2. Дата звертання: Бер. 20, 2017.

[13] ISACA. Головна сторінка. [Електронний ресурс]. ДоступноЖ https://www.isaca.org/pages/ default.aspxю Дата звертання: Бер. 20, 2017.

[14] Международный форум по аккредитации (IAF). "Многостороннее соглашение о признании IAF (MLA)". [Електронний ресурс]. Доступно: Офіційна веб-сторінка. – Режим доступу: http://www.iaf.nu/upFiles/IAF_MLA_Russian.pdf. Дата звертання: Бер. 27, 2017.

[15] International Organization for Standardization. International Standard "ISO 19011:2011 Guidelines for auditing management systems". [Електронний ресурс]. Доступно: https://www.iso.org/standard/50675.html. Дата звертання: Бер. 22, 2017.

[16] International Organization for Standardization. International Standard "ISO/IEC 27007:2011 Information technology. Security techniques. Guidelines for information security management systems auditing". [Електронний ресурс]. Доступно: https://www.iso.org/standard/42506.html. Дата звертання: Бер. 24, 2017.

[17] ISACA. "What is COBIT 5? It's the leading framework for the governance and management of enterprise IT". [Електронний ресурс]. Доступно: http://www.isaca.org/cobit/pages/default.aspx. Дата звертання: Бер. 28, 2017.

Стаття надійшла до редакції 31 березня 2017 року.

REFERENCES

[1] Neil Robinson "Changing approaches to cyber defense", NATO Review. [Online]. Available: http://www.nato.int/docu/review/2016/Also-in-2016/cyber-defense-nato-security-role/UK/index.html. Accessed on: March 15, 2017.

[2] Cabinet of Ministers of Ukraine. *Order of from 10.03.2017 № 155-p of "About of the solidification of the plan for the coming years 2017 from realization of Strategy of cybersecurity of Ukraine"*. [Online]. Available: http://www.kmu.gov.ua/control/uk/cardnpd?docid= 249807504. Accessed on: March 25, 2017.

[3] International Organization for Standardization. *International Standard "ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity"*. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en. Accessed on: March 20, 2017.

[4] International Organization for Standardization. *International Standard "ISO 31000:2009 Risk management – Principles and guidelines"*. [Online]. Available: https://www.iso.org/standard/ 43170.html. Accessed on: March 20, 2017.

[5] International Organization for Standardization. *International Standard "ISO Guide 73:2009 Risk management – Vocabulary"*. [Online]. Available: https://www.iso.org/standard/ 44651.html. Accessed on: March 20, 2017.

[6] "The Australian Customs Service as an innovative platform in the development of international standards for the application of customs risk management systems". [Online]. Available: http://have-right/ombudsman/645-australian-customs-service.html. Accessed on: March 20, 2017.

[7] 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: March 20, 2017.

[8] National Institute of Standards and Technology. "Federal Information Processing Standards (FIPS)". [Online]. Available: http://csrc.nist.gov/publications/PubsFIPS.html. Accessed on: March 20, 2017.

[9] National Institute of Standards and Technology. "NIST Special Publication". [Online]. Available: http://csrc.nist.gov/publications/PubsSPs.html. Accessed on: March 20, 2017.

[10] International Organization for Standardization. International Standard "ISO/IEC 27005:2011 Information technology – Security techniques – Information security risk management". [Online]. Available: https://www.iso.org/standard/56742.html. Accessed on: March 20, 2017.

[11] International Organization for Standardization. "Electronic card of standard ISO/IEC 27005:2011 Information technology. Security techniques. Information security risk management". [Online]. Available: https://www.iso.org/search/x/query/27005. Accessed on: March 20, 2017.

[12] NOI INTUIT. Lecture course. "COBIT 5 – What's New?". [Online]. Available: http://www.intuit.ru/studies/courses/3704/946/lecture/15117?page=1,2. Accessed on: March 20, 2017.

[13] ISACA. Main Page. [Online]. Available: https://www.isaca.org/pages/default.aspx. Accessed on: March 20, 2017.

[14] International Forum for Accreditation (IAF). "Multilateral agreement on the recognition of the IAF (MLA)". [Online]. Available: Офіційна веб-сторінка. – Режим доступу: http://www.iaf.nu/upFiles/IAF_MLA_Russian.pdf. Accessed on: March 27, 2017.

[15] International Organization for Standardization. International Standard "ISO 19011:2011 Guidelines for auditing management systems". [Online]. Available: https://www.iso.org/ standard/50675.html. Accessed on: March 22, 2017.

[16] International Organization for Standardization. International Standard "ISO/IEC 27007:2011 Information technology. Security techniques. Guidelines for information security management systems auditing". [Online]. Available: https://www.iso.org/standard/42506.html. Accessed on: March 24, 2017.

[17] ISACA. “What is COBIT 5? It's the leading framework for the governance and management of enterprise IT”. [Online]. Available: http://www.isaca.org/cobit/pages/default.aspx. Accessed on: March 28, 2017.

ЮЛИЯ КОЖЕДУБ,

АНАЛИЗ ДОКУМЕНТОВ ПО УПРАВЛЕНИЮ РИСКАМИ КИБЕРБЕЗОПАСНОСТИ

Статья содержит анализ последних документов по управлению рисками в сфере информационной безопасности и кибербезопасности. Исследование современных нормативных документов показывает, что внимание их разработчиков сосредоточено на рисках, поскольку оно было инициировано в стандартах на системы управления Международной организацией по стандартизации. Значение этой работы носит планетарный характер, поскольку разработки в этой области деятельности были заложены как основа для создания различных документов, которые они предлагают различным странам и организациям для реализации в области информационной безопасности и кибербезопасности. В статье предлагается рассмотреть нормативные документы, разработанные для работы менеджера рисков для обеспечения информационной безопасности и кибербезопасности. Модель инструментария для работы риск-менеджера, основана на ядре, которое определяется нормативными документами как процесс управления рисками. Нормативные документы, определяющие процесс управления рисками, являются фундаментальными стандартами, которые стандартизируют концепцию «риска», и это является отправной точкой для менеджеров всех подразделений, которые понимают важность управления рисками. Статья отражает развитие научной мысли о терминологическом аппарате и научном подходе к содержательному пониманию важности процесса управления рисками. В статье анализируются документы, разработанные международными и национальными организациями для оказания помощи в работе менеджеров по информационной безопасности и рискам. В дополнение к исследованию в рамках этой статьи отражены другие документы, которые являются подробными инструкциями для менеджеров по рискам в области информационной безопасности и деятельности в области кибербезопасности.

Ключевые слова: менеджмент, менеджер, нормативные документы, риск, стандарты.

YULIIA KOZHEDUB,

ANALYSIS OF CYBER SECURITY RISK MANAGEMENT DOCUMENTS

The article provides an analysis of the latest documents on risk management. The research of modern standards shows that their attention is focused on risks, as it was initiated in the standards of the management systems of the International Organization for Standardization. The significance of this work is of a since developments in this area were laid as the basis for the creation of different kinds of documents that they offer to different countries and organizations for implementation in the activities for information security and cybersecurity. The article proposes to consider complex documents developed for the work of the risk manager for information security and cyber security. The toolkit model is based on the core, which is defined by normative documents as a risk management process. Regulatory documents defining the process of risk management are fundamental standards that standardize the concept of “risk” and this is the starting point for managers of all units who understand the importance of risk management. The article reflects the development of scientific thought about the terminology apparatus and the scientific approach to a meaningful understanding of the importance of the risk management process. The article analyzes documents developed by international and national organizations for assistance in the work of risk managers. In addition to the study within the scope of this article, other documents that are detailed instructions for risk managers in the field of information security and cyber security activities are reflected.

Keywords: management, manager, normative documents, risk, standards.

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.