**DOI:** https://doi.org/10.17721/ISTS.2019.1.3-10
УДК 004.056

# КОНЦЕПЦІЯ КІБЕРБЕЗПЕКИ В ІНФОРМАЦІЙНИХ СИСТЕМАХ ДЕРЖПРИКОРДОНСЛУЖБИ НА СТАДІЇ МОДЕРНІЗАЦІЇ

**Стрельбіцький Михайло**
**orcid.org/0000-0001-8030-3228**

м. Хмельницький, Національна академія Державної прикордонної служби України імені Богдана Хмельницького, m.strelb@ukr.net

**Історія статті:**
Надійшла до редакції 25.06.2019
Прийнято 06.08.2019

**Ключові слова:**
концепція;
кібербезпека;
інформаційна система;
модернізація;
Держприкордонслужба.

**Анотація:** В статті проведено аналіз функцій прикордонної служби України та її інформаційних систем. Визначено, що модернізація складових інтегрованої інформаційної системи спричиняє порушення існуючої системи кіберзахисту. Проведений аналіз існуючих підходів до забезпечення захисту інформації в інформаційних системах показав достатньо глибоке опрацювання досліджень окремо за кожною інформаційною системою. Однак залишаються невивченими особливості взаємодії зазначених систем, зокрема при модернізації окремих інформаційних систем з точки зору забезпечення кіберзахисту загалом. Сам процес модернізації інформаційних систем здійснюється за окремими складовими системи або комплексно та вимагає їх узгодження в процесі спільного функціонування В статті наведено обґрунтування стратегій модернізації за групами критеріїв: рівня кібербезпеки, особливостей функціонування інформаційних систем. Зазначено, що значення ймовірності порушення властивостей інформаційного ресурсу змінюється протягом всього терміну модернізації. Тому обирати стратегію модернізації за значенням ймовірності в довільний момент часу є не коректним. Необхідно враховувати загальну тенденцію функції зміни зазначеної ймовірності. Найбільш доцільними є розподіл цієї групи критеріїв на три складових критерії рівня забезпечення кібербезпеки: нормативний – критерій, за якого поточне значення ймовірності порушення кібербезпеки не перевищуватиме заданого; середній – критерій, за якого середнє значення ймовірності порушення кібербезпеки не перевищуватиме заданого; зважений – критерій, за якого середнє зважене значення ймовірності порушення кібербезпеки не перевищуватиме заданого. В статті наведені функціональні залежності для визначення ймовірності порушення кібербезпеки для кожної із груп. В результаті дослідження з'ясовано, що пріоритетним показником ефективності процесу модернізації інформаційних систем прикордонного відомства є максимальне значення ймовірності порушення властивостей інформації у процесі модернізації.

**Abstract:** The article analyzes the functions of the Border Guard Service of Ukraine and its information systems. It is determined that the modernization of the components of the integrated information system causes a violation of the existing system of cyber defense. The analysis of existing approaches to ensuring the protection of information in information systems has shown a sufficiently deep study of research separately for each information system. However, unexperienced features of the interaction of these systems remain, in particular, with the modernization of certain information systems in terms of providing cyber defense in general. The process of modernization of information systems is carried out according to individual components of the system or complex and requires their coordination in the process of joint operation. The article gives the justification of modernization strategies according to the groups of criteria: the level of cyber security, the peculiarities of the functioning of information systems. It is noted that the value of the probability of violating the properties of the information resource varies over the entire period of modernization. Therefore, to choose the strategy of modernization at the value of probability at any time is not correct. It is necessary to take into account the general tendency of the function of changing this probability. The most expedient is the distribution of this group of criteria into three components

of the criteria for the level of cyber security: the normative - the criterion in which the current value of the probability of violating cybersecurity does not exceed the given; average - the criterion for which the average probability of a violation of cybersecurity does not exceed the prescribed; weighted - a criterion for which the average weighted probability of cybersecurity violation will not exceed the given. The article presents functional dependencies for determining the probability of cyber security violations for each of the groups. As a result of the study, it was determined that the priority indicator of the effectiveness of the process of modernizing the information systems of the border agency is the maximum value of the probability of violating the properties of information in the process of modernization.

## 1. ВСТУП

Виконання основних функцій Державної прикордонної служби України [1–4] з питань здійснення в установленому порядку прикордонного контролю і пропуску через державний кордон України осіб, транспортних засобів, вантажів, а також виявлення і припинення випадків незаконного їх переміщення, ведення інформаційно-аналітичної діяльності, координація діяльності військових формувань та відповідних правоохоронних органів, пов'язаної із захистом державного кордону України, а також діяльності державних органів, що здійснюють різні види контролю при перетинанні державного кордону України, пов'язане із зберіганням, обробкою та передаванням інформаційних повідомлень службового характеру між суб'єктами інтегрованого управління кордонами.

Розвиток інформаційних технологій спричинив створення на державному та відомчих рівнях великої кількості взаємно не пов'язаних інформаційних систем спрямованих здебільшого на накопичення даних та використання їх лише за напрямками діяльності суб'єктів національної безпеки. Практично повна відсутність стандартизації підходів до розробки та функціонування систем збору, обробки, аналізу, висвітлення, а саме головне ефективного обміну інформацією між суб'єктами забезпечення національної безпеки, а також технологічна комерціалізація цього напрямку досліджень є передумовою для уповільнення розвитку загальнодержавних систем моніторингу обстановки та підтримки прийняття управлінських рішень.

Інтегрована інформаційна система (ІІС) прикордонного відомства оперує критичним для прийняття рішення інформаційним ресурсом, що в свою чергу вимагає від її підсистеми кіберзахисту забезпечення дотримання всіх властивостей її інформаційних ресурсів.

В умовах складної та динамічної зміни обстановки виникає необхідність адаптації ІІС Держприкордонслужби України до потреб діяльності посадових осіб з виконання ними своїх функціональних обов'язків. Вищенаведена обставина потребує врахування підсистемою кіберзахисту факту модернізації складових інтегрованої інформаційної системи.

## 2. АНАЛІЗ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

Значний внесок у розвиток інформаційних технологій створення гарантоздатних автоматизованих систем управління критичного застосування та захисту інформації внесли відомі вчені Бараннік В.В., Богуш В.М., Грицюк Ю.І., Грушо А.А., Дудикевич В.Б., Катеринчук І.С., Корнієнко Б.Я., Конахович Г.Ф., Ліпаєв В.В., Литвиненко О.Є., Мачалін І.О., Харченко В.С., Юдін О.К. та інші.

Проведений аналіз існуючих підходів до забезпечення захисту інформації в інформаційних системах показав достатньо глибоке опрацювання досліджень окремо за кожною інформаційною системою. Однак залишаються невивченими особливості взаємодії зазначених систем, зокрема при модернізації окремих інформаційних систем з точки зору забезпечення кіберзахисту загалом.

Інтегрована інформаційна система Держприкордонслужби України, як суб'єкта національної безпеки, має велику кількість підсистем які розподілені на всій території держави. Особливістю такої системи є вимога функціонування в реальному масштабі часу та оперування критичним для прийняття рішень інформаційним ресурсом, при чому, навіть незначне порушення властивостей якого може призвести до серйозних збитків національного масштабу [5].

При такому розумінні інформаційного ресурсу прикордонного відомства виникає потреба у забезпечені його кіберзахисту, зокрема дотриманні властивостей інформаційного ресурсу: цілісності, доступності, конфіденційності та спостереженості, тобто забезпечення комплексного кіберзахисту інтегрованої інформаційної системи прикордонного відомства в цілому [3].

Аналіз такого типу систем показав з одного

боку сталу тенденцію до зростання множини інформаційних дестабілізаційних факторів які впливають на кібернетичну безпеку, що спричинено:

розширенням умов застосування та функціонування інформаційних систем прикордонного відомства;

збільшенням кола користувачів системи, в тому числі суб'єктами інтегрованого управління кордонами;

зростанням кількості складових інтегрованої інформаційної системи;

потребою у взаємодії з міжвідомчими та міжнародними інформаційними ресурсами;

збільшенням обсягів інформації, необхідної для прийняття обґрунтованого управлінського рішення посадовими особами Держприкордонслужби;

збільшенням числа дестабілізаційних інформаційних впливів;

запровадженням нових інформаційних технологій.

З іншого боку, захист життєво важливих інтересів держави вимагає від таких систем:

забезпечення підвищених вимог з дотримання властивостей інформаційного ресурсу прикордонного відомства;

оперативності доступу до інформаційних ресурсів;

реалізації розширених можливостей щодо аналізу та узагальнення інформації;

скорочення часу для прийняття рішень;

контроль за виконанням розпоряджень.

Вищезазначене потребує постійної модернізації відомчих систем, що призводить до спільного функціонування на загальному полі даних старих, модернізованих та нових версій інформаційних систем, як складових суперсистеми. Це призводить до виникнення протиріччя між наявною теоретичною базою забезпечення кібербезпеки та потребою у постійній модернізації інформаційних систем у складі інтегрованої інформаційної системи.

Таким чином, на цій стадії життєвого циклу виникає проблема переходу на нову програмно-апаратну платформу без порушення життєвого циклу, при цьому для відомчих інформаційних систем одною з найважливіших задач є забезпечення кібербезпеки інформаційних систем, що і визначає актуальність дослідження.

**Метою статті** є розробка концепції кібербезпеки інтегрованої інформаційної системи Держприкордонслужби на стадії модернізації.

## 3. ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Проведений аналіз підходів до забезпечення кібернетичної безпеки в інтегрованих інформаційних системах показав, що більшість досліджень зосереджені на проблемах захисту інформації окремо в кожній інформаційній системі. Уперше уніфіковану концепцію захисту інформації запропонував Герасименко В. А. [6]

Застосування зазначеної концепції створює передумови для впровадження всіх досліджень в галузі захисту інформації, а саме: структурованого середовища захисту, всебічної оцінки уразливості інформації залежно від дії дестабілізаційних факторів зовнішніх та внутрішніх загроз, формування вимог до захисту, побудова системи захисту інформації в залежності від умов функціонування, формування рекомендацій з підвищення ефективності захисту.

Концепція загалом передбачає циклічний процес вдосконалення системи захисту інформації. Разом із тим, сам процес модернізації, його методологічні засади в уніфікованій концепції не розглянуті. Для наявних систем захисту, які реалізовані в сучасних ІС, загалом не передбачається спільного функціонування різних версій програмно-апаратного забезпечення, систем захисту тощо. Вищенаведене вимагає структурованого аналізу та декомпозиції факторів, що впливають на дотримання властивостей інформації на стадії модернізації.

Сам процес модернізації інформаційних систем здійснюється за окремими складовими системи або комплексно та загалом вимагає їх узгодження в процесі спільного функціонування (рис. 1).

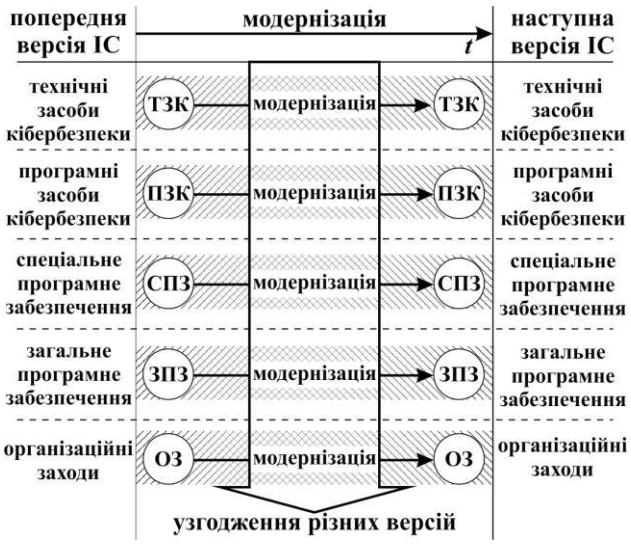


**Рис. 1 – Структура процесу модернізації ІС**

Отже, з точки зору кібербезпеки модернізація вимагає формулювання стратегії як головної

мети зазначеного процесу. Стратегія кібербезпеки на стадії модернізації як модель узагальнених дій, спрямованих на досягнення зазначеної мети, полягає у такій сукупності заходів по заміні складових інформаційної системи (ІС), за якої рівень кібербезпеки відповідає нормативному.

Водночас, умови функціонування різних інформаційних систем, їх структура та вимоги до кібербезпеки можуть суттєво відрізнятись. Через це загальне формулювання стратегії кібербезпеки на стадії модернізації може дещо відрізнятись один від одного. Загалом, організація процесу модернізації в рамках розглянутої стратегії полягає в пошуку раціонального співвідношення між вимогами до нової версії ІС та рівнем інформаційних дестабілізаційних факторів, викликаних невідповідністю версій. Таке формулювання проблеми належить до галузі оптимізаційних завдань. Разом із тим, значна кількість випадкових факторів не дозволяє сформувати функціональні залежності для їх вирішення відомими оптимізаційними методами.

Обґрунтування стратегій модернізації будемо здійснювати за групами критеріїв: рівня кібербезпеки та особливостей функціонування ІС.

Формуванню першої групи критеріїв присвячена велика кількість робіт [7–11], в яких дослідники обґрунтовують його фізичний сенс. У більшості досліджень як показник рівня кібербезпеки пропонується використовувати ймовірність попередження шкоди, враховуючи стохастичну природу дестабілізаційних впливів. Варто зазначити, що значення ймовірності виникнення шкоди протягом всього терміну модернізації буде різною, тобто $P(t)$. Так обирати стратегію модернізації за значенням ймовірності в довільний момент часу є не коректним. Необхідно враховувати загальну тенденцію функції зміни зазначеної ймовірності.

На наш погляд, найбільш доцільними є розподіл цієї групи критеріїв на три складових критерії рівня забезпечення кібербезпеки:

нормативний – критерій, за якого поточне значення ймовірності порушення кібербезпеки не перевищуватиме заданого;

середній – критерій, за якого середнє значення ймовірності порушення кібербезпеки не перевищуватиме заданого;

зважений – критерій, за якого середнє зважене значення ймовірності порушення функціональної безпеки не перевищуватиме заданого.

Друга група критеріїв, яка визначає особливості функціонування ІС [12–14] на стадії модернізації, характеризує можливості щодо втручання в процес роботи системи. За цією групою критерії поділяються на три види:

системи реального часу характеризуються практичною відсутністю будь-яких можливостей щодо втручання в процес їх функціонування. Прикладом такої системи є ІС "Гарт-1", система автоматизації пропуску осіб, транспортних засобів через державний кордон України. Зупинка такої системи навіть на невеликий термін є недопустимою, оскільки може призвести до збитків національного масштабу;

системи з можливістю часткової зупинки характеризуються більшими можливостями для процесу модернізації. Прикладом такої ІС може бути "Гарт-5", система автоматизації інформаційно-аналітичної діяльності. Ці системи функціонують, як правило, під час робочого дня, тобто третину доби.

системи з можливістю повної зупинки характеризуються максимальними можливостями для процесу модернізації. Такого типу системи мають обмеження тільки терміном експлуатації.

Вищенаведене дозволяє сформувати узагальнену таблицю раціональних стратегій модернізації як декартового добутку обох критеріїв (таблиця 1)

Отже, нормативний рівень варто застосовувати до систем реального часу з причини забезпечення неперевищення значення ймовірності порушення кібербезпеки протягом всього терміну модернізації.

**Таблиця 1 – Раціональні стратегії модернізації**

| Критерій рівня забезпечення кібербезпеки | Особливості ІС | | |
|---|---|---|---|
| | реального часу | часткова зупинка | повна зупинка |
| Нормативний | + | – | – |
| Середній | – | + | – |
| Зважений | – | + | – |

Середній та зважений критерії захисту доцільно використовувати при модернізації систем з можливістю часткової зупинки функціонування. Вибір критерію залежить від величин часу та періодичності часткової зупини системи.

Такі дослідження дозволяють сформувати загальну концепцію забезпечення кібербезпеки ІС на стадії модернізації як інструментально-методологічну базу що забезпечує виконання розглянутих стратегій (рис.2).

Першочерговим етапом є обґрунтування самого об’єкту системи кібербезпеки. Саме від визначення цього поняття та його властивостей залежить формування всієї концепції кібербезпеки на стадії модернізації. Разом із тим,

ключовим питанням є визначення стратегії модернізації як напрямку зосередження основних зусиль всієї системи. Базуючись на визначених обох складових, здійснюється узгодження різних версій ІС.

У більшості випадків модернізація загального програмного забезпечення не здійснює впливу на уразливість ІС з причини завчасної перевірки можливості функціонування різних версій [15]. Загальне програмне забезпечення не є частиною ІС, а використовується як платформа для функціонування спеціального програмного забезпечення (СПЗ) на конкретному автоматизованому робочому місці (АРМ) або серверному обладнанні. Організаційні заходи, що спрямовані на забезпечення кібербезпеки, теж не є складовою ІС, хоча здійснюють вплив на процес кібербезпеки. Ці два елементи виходять за межі дослідження та не включені в загальну концепцію забезпечення кібербезпеки на стадії модернізації.


**Рис. 2 – Загальна концепція забезпечення кібербезпеки на стадії модернізації**

Здійснювати завдання узгодження різних версій ІС необхідно тільки в умовах їх спільного функціонування через врахування основного припущенням дослідження, що в різних версіях ІС окремо кібербезпека забезпечується відповідно до встановлених вимог. Отже, в системах з можливістю повної зупинки функціонування на період модернізації не виникають дестабілізаційні фактори, викликані спільним функціонуванням різних версій ІС.

Концепцією передбачено три завдання узгодження. Перше завдання – це узгодження спільного функціонування спеціального програмного забезпечення АРМ інформаційних систем. Модернізація СПЗ здійснюється фахівцями відділів зв'язку, автоматизації та захисту інформації почергово кожного АРМ. Так виникає ситуація спільного функціонування в системі АРМ з різними версіями СПЗ. Вирішення цього завдання можливе шляхом визначення раціональної послідовності модернізації АРМ в інформаційній системі відповідно до обраної стратегії забезпечення кібербезпеки.

Другим завданням є узгодження програмних засобів захисту, а саме розробка сукупності методів узгодження систем розмежування доступу до інформаційних ресурсів ІС та на їх основі формування методологічного базису. Вирішення цього завдання дозволить науково обґрунтувати принципову можливість функціонування різних версій систем розмежування доступу на спільному полі даних.

Третім завданням є вдосконалення технічних (апаратних) засобів забезпечення кібербезпеки. Під час модернізації ІІС можлива зміна структури технічних засобів забезпечення кібербезпеки. Це вимагає вирішення завдання раціонального їх розподілу на стадії модернізації з урахуванням взаємодії наявних та доданих засобів, а також вимог до загального рівня безпеки інформаційної системи.

Наступними етапами концепції є визначення величини уразливості даних при проведенні заходів з модернізації та оцінювання ефективності кібербезпеки в ІС на стадії модернізації. На даних етапах враховуються умови функціонування системи та вплив зовнішнього середовища на процес кібербезпеки. Результатом є отримання оцінки ефективності проведених заходів, яка використовується власником системи для прийняття рішення щодо проведення модернізації та визначення організаційних заходів з особливості проведення самого процесу оновлення складових ІС.

Сформуємо показники ефективності за різними стратегіями модернізації.

Перший. Повна зупинка функціонування ІС та здійснення заміни визначених програмних елементів з подальшим введенням в експлуатацію зазначеної системи. Цей спосіб з точки зору кібербезпеки є найбільш раціональним. В даному випадку взагалі виключена можливість реалізації загроз, викликаних процесом модернізації. Водночас застосування першого підходу можливе тільки на невеликих системах та й на таких, які не мають вимоги функціонування в режимі

реального часу. Як правило, вимогою до переважної більшості інформаційних систем та підсистем ІІС прикордонного відомства є цілодобове функціонування. Навіть невеликий збій може призвести до непоправних збитків національного масштабу. Територіальна розподіленість елементів окремих ІС та достатньо велика їх кількість при застосуванні першого підходу вимагатиме досить значного часу на проведення модернізації. Використання такого підходу в прикордонній службі є неприпустимим.

Другий підхід передбачає модернізацію ІС в процесі її функціонування. У цьому випадку можливе порушення властивостей інформаційного ресурсу ІС і, в свою чергу, кіберзахисту, оскільки з'являються додаткові дестабілізаційні фактори, викликані невідповідністю версій СПЗ. Отже, головним чинником, який визначатиме ефективність процесу модернізації, є максимально можливе зменшення ймовірності порушення властивостей інформаційного ресурсу. Разом із тим, варто зазначити, що модернізація ІС це процес, який має певну тривалість та не може бути описаний окремими точковими показниками поза межами часу.

Визначимо основні показники, які характеризують ефективність процесу модернізації: $P_M(t)$ – ймовірність порушення властивостей інформаційного ресурсу; $t_M$ – загальний час модернізації.

Різні варіанти модернізації можна порівняти за загальним часом модернізації, але в більшості випадків він задається директивно та не відображає величину порушення властивостей інформаційного ресурсу. Отже, цей показник може бути тільки як допоміжний у випадку рівності інших показників. З іншого боку порівнювати різні варіанти послідовності модернізації елементів ІС за миттєвим значенням ймовірності порушення властивостей інформаційного ресурсу є неможливим з причини її зміни протягом всього терміну модернізації.

Вищенаведене вимагає використання інтегрованих показників, що характеризують весь процес модернізації. Одним із показників такого типу є максимально можливе значення ймовірності порушення властивостей інформаційного ресурсу в процесі модернізації

$$P_M^{\max} = \max_{0 \le t \le t_M} \left( P_M(t) \right). \quad (1)$$

Перевагою цього показника є можливість визначення допустимого значення ймовірності порушення інформаційного ресурсу на стадії модернізації.

Наступним показником, який характеризує ефективність процесу модернізації, є середнє значення ймовірності порушення властивостей інформаційного ресурсу в процесі модернізації.

В інтегральній формі

$$P_M^{mid} = \frac{1}{t_M} \int_0^{t_M} P_M(t) dt \quad (2)$$

У дискретній формі

$$P_M^{mid} = \frac{1}{N} \sum_{i=1}^{N} P_M(t_i) \quad (3)$$

де $N$ – кількість інтервалів вимірювання значення ймовірності.

Такий показник доцільно застосовувати при забезпеченні якомога меншого значення ймовірності порушення властивостей інформаційного ресурсу під час модернізації. Вибір показника ефективності залежить від способу застосування ІС та процесу її модернізації.

Наступним показником ефективності процесу модернізації може бути середньозважене значення ймовірності порушення властивостей інформаційного ресурсу.

В інтегральній формі

$$P_M^w = \frac{1}{t_M} \int_0^{t_M} f^w(t) P_M(t) dt, \quad (4)$$

де $f^w(t)$ – функція ваги.

За умови, що

$$\int_0^{t_M} f^w(t) dt = 1. \quad (5)$$

У дискретній формі

$$P_M^w = \frac{1}{N} \sum_{i=1}^{N} f^w(t_i) P_M(t_i). \quad (6)$$

За умови, що

$$\sum_{i=1}^{N} f^w(t_i) = 1. \quad (7)$$

Пріоритетним показником ефективності процесу модернізації для більшості ІС прикордонного відомства є максимальне значення ймовірності порушення властивостей інформаційного ресурсу в процесі модернізації. Чим менше цей показник, тим ефективніше провадиться заміна СПЗ на елементах ІС. При рівності значень цього показника в різних

варіантах модернізації доцільно застосувати другий або третій показники.

## 4. ВИСНОВКИ

Аналіз існуючих підходів до проблеми забезпечення кібербезпеки показав наявність циклічного процесу вдосконалення такого типу систем. Водночас, сам процес модернізації, його методологічні засади у цих підходах не розглянуті. Для наявних систем забезпечення кібербезпеки, які реалізовані в сучасних ІС, загалом не передбачається спільного функціонування різних версій програмно-апаратного забезпечення, систем забезпечення кібербезпеки безпеки, тощо. Це вимагає структурованого аналізу та декомпозиції факторів, що впливають на дотримання властивостей інформаційної системи на стадії модернізації.

Опис процесу модернізації ІС дозволив сформулювати стратегію кібербезпеки, яка полягає у такій сукупності заходів по заміні складових інформаційної системи, за якої рівень кібербезпеки відповідав нормативному. Разом із тим, умови функціонування різних ІС, їх структура та вимоги до кібербезпеки можуть суттєво відрізнятись. Через це загальне формулювання стратегії кібербезпеки на стадії модернізації може дещо відрізнятись один від одного. Аналіз критеріїв та особливостей функціонування дозволив сформувати раціональні стратегії модернізації.

Вищенаведені дослідження дозволили сформувати загальну концепцію кібербезпеки на стадії модернізації як інструментально-методологічну базу, що забезпечує виконання розглянутих стратегій. Концепцією передбачено три завдання узгодження спільного функціонування: спеціального програмного забезпечення, програмних та технічних (апаратних) засобів забезпечення кібербезпеки, а також визначення величини уразливості інформаційного ресурсу системи при проведенні заходів з модернізації та оцінювання ефективності кібернетичної безпеки в ІС на стадії модернізації. Результатом є отримання оцінки ефективності проведених заходів, яка використовується власником системи для прийняття рішення щодо проведення модернізації та визначення організаційних заходів щодо особливості проведення самого процесу оновлення складових ІС.

Визначення раціональної стратегії модернізації вимагає обґрунтування показників ефективності здійснення процесу модернізації. Аналіз особливостей функціонування різних ІС дозволив сформувати три види показників: за максимально можливим значенням ймовірності порушення властивостей інформаційного ресурсу під час модернізації, за середнім значенням ймовірності порушення властивостей інформаційного ресурсу у процесі модернізації та середньозваженим значення ймовірності. З'ясовано, що пріоритетним показником ефективності процесу модернізації для більшості ІС прикордонного відомства є максимальне значення ймовірності порушення його властивостей у процесі модернізації. Чим менше цей показник, тим ефективніше провадиться заміна СПЗ на елементах інформаційної системи.

## 5. СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ


[1] Про основи національної безпеки України: Закон України // *Офіційний Вісник України*. – 2003. – № 39. – Ст. 351.

[2] *Доктрина "Інформаційної безпеки України"* [Електронний ресурс] // Офіційна веб-сторінка Верховної Ради України: Законодавство.

[3] Стрельбіцький М.А. "Прикордонний інформаційний ресурс: визначення поняття" *Сучасні інформаційні технології у сфері безпеки та оборони*. Національний університет оборони України імені Івана Черняховського №1 (25) 2016. С. 205-208

[4] Липаев В.В. *Технологические процессы и стандарты обеспечения функциональной безопасности в жизненном цикле программных средств*. / В.В. Липаев // Информационный бюллетень "JetInfo". – 2003. – № 3 (130). – 27 с.

[5] Постанова Кабінету Міністрів України від 19 червня 2019 року № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» [Електронний ресурс] // Офіційна веб-сторінка Верховної Ради України: Законодавство.

[6] Герасименко В. А. *Защита информации в АСОД* (в 2-х томах). – М.: Энергоатомиздат, 1994. – 400 с.

[7] Харибін О. В. "Інформаційна технологія забезпечення функціональної безпеки бортових інформаційно-керуючих систем авіації на етапі експлуатації" *Системи озброєння і військова техніка* № 2. – 2010. – С. 173-177.

[8] І. В. Муляр, А. В. Джулій, М. В. Костюк "Аналіз проблем забезпечення функціональної безпеки інформаційних систем обробки даних" *Вимірювальна та обчислювальна техніка в технологічних процесах*. – 2013. – № 1. – С. 133-138.

[9] Манжос Ю. С. "Використання аналізу розмірностей для підвищення рівня

функціональної безпеки I&C систем" *Радіоелектронні і комп'ютерні системи* № 7. – 2012. – С. 313-318.

[10] С. Г. Семенов, С. Ю. Гавриленко, Кассем Халіфе "GERT-модель прогнозування параметрів функціональної безпеки технічних систем" *Системи обробки інформації* № 2. – 2016. – С. 50-52.

[11] Борзов Ю. *Інформаційні технології підвищення функціональної безпеки систем обробки інформації критичного застосування*. Автореферат дисертації на здобуття наукового ступеня кандидата технічних наук / Львівський державний університет безпеки життєдіяльності. м. Львів (2015).

[12] К. В. Юдкова, Г. Г. Чернишина "Класифікація інформаційних систем" *Інформація і право* № 3. – 2015. – С. 92-98.

[13] Гужва В. М. *Інформаційні системи і технології на підприємствах*. К.: КНЕУ (2001): 133-170.

[14] П. П. Маслянко, П. М. Ліссов "Інформаційно-комунікаційні системи та технології обробки інформаційних ресурсів" *Вісн. КУЕІТУ "Нові технології* № 1-2. – 2007. – С. 15-16.

[15] Стрельбіцький М. А. "Декомпозиція технології захисту інформації в корпоративних системах" *Збірник наукових праць Національної академії Державної прикордонної служби України*. № 59: – С. 296-301.

***Стрельбіцький Михайло Анатолійович**, **доктор технічних наук, доцент**, начальник (завідувач) кафедри зв'язку, автоматизації та кібербезпеки Національної академії Державної прикордонної служби України імені Богдана Хмельницького. Закінчив військову інженерно-космічну академію імені О.Ф. Можайського, область наукових інтересів: кібербезпека, функціональна безпека, інформаційна безпека*