DOI: 10.51369/2707-7276-2025-1(38)-7
УДК 35.004

ГОРДІЄНКО Сергій Борисович
ORCID ID: 0000-0001-2345-6789

ОСОБЛИВОСТІ ФУНКЦІОНУВАННЯ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

У зв'язку з активним проведенням інформаційно-психологічних операцій (ІПсО) і поширенням деструктивних інформаційних впливів зі сторони країни-агресора російської федерації на нашу державу проблема забезпечення інформаційної безпеки загострюється. Убезпечити інформаційну систему щодо оптимальних умов функціонування процесів інформаційного обміну з питань управління в державній та військовій сферах тільки набором технічних засобів на сьогодні практично неможливо. До того ж додаються питання забезпечення стійкості функціонування процесів управління активною протидією воєнній агресії російської федерації та повного розуміння процесу кібернетично-гібридного впливу, де застосовуються спеціальні ІПсО проти України, її військових формувань і цивільного населення.

Вирішити ці проблеми можливо шляхом упровадження адаптивного підходу до використання ефективної системи управління інформаційною безпекою (СУІБ) щодо об'єктів критичної інформаційної інфраструктури, у державному та військово-політичному управлінні.

У статті визначені основні особливості застосування СУІБ та сучасні підходи до етапів її створення на об'єктах критичної інформаційної інфраструктури, у державному та військово-політичному управлінні, при обробці інформації, поширення якої призводить до деструктивного впливу на державний устрій країни й інформаційну безпеку громадян. З огляду на реалії сьогодення в питаннях протидії активній воєнній агресії з урахуванням особливостей побудови системи управління інформаційною безпекою розглядаються підходи, які базуються на ДСТУ ISO/IEC 27001:2015 «Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги». За результатами аналізу визначені взаємозв'язок процесів і підсистем інформаційної безпеки, відповідальних за них, політичні, фінансові та військові ресурси, які мають бути задіяні для ефективного функціонування цих процесів і підсистем за умов воєнного стану.

Одним із надважливих та актуальних напрямів протиборства у військовій сфері є активні інформаційно-психологічні операції та різні деструктивні спрямування стосовно військово-політичної складової функціонування України, зокрема й у кіберпросторі.

Зроблено висновок, що створення та застосування ефективної СУІБ дають змогу за умов воєнної агресії та протидії ІПсО російської федерації вийти на новий рівень якості ефективного управління військово-політичними процесами держави, зменшити інформаційні й організаційні загрози, покращити керованість процесами оперативного управління, продемонструвати ефективність і надійність результатів за прийнятими

управлінськими рішеннями, що дасть можливість успішно протидіяти планам країни-агресора разом із провідними країнами НАТО на глобальному міжнародному рівні.

Ключові слова: *воєнна агресія, заходи кібербезпеки, інформаційна безпека, інформаційно-психологічні операції, кібербезпека, критична інформаційна інфраструктура, політики безпеки, політики і процедури СУІБ, ризик-орієнтований підхід, система управління інформаційною безпекою, сучасні інформаційно-комунікаційні системи та технології, управлінське рішення.*

Постановка проблеми. За умов інтенсивного розвитку сучасних інформаційно-комунікаційних систем і технологій, воєнної агресії російської федерації, у зв'язку з поширенням деструктивних інформаційних впливів на нашу державу проблема забезпечення інформаційної безпеки загострюється. Убезпечити інформаційну систему тільки набором технічних засобів – не є достатньою мірою для забезпечення оптимальних умов функціонування процесів інформаційного обміну, зокрема в управлінні державної та військової сфер, питаннях військової протидії державі-агресору – російській федерації.

Відсутність регулярного аналізу ризиків, неінформованість учасників інформаційних відносин щодо правил використання конфіденційної інформації, порушення режиму доступу до інформації, її спотворення із використанням у деструктивних цілях є реальною загрозою забезпеченню інформаційної безпеки як об'єктів критичної інформаційної інфраструктури, так і громадянського суспільства країни.

До функціонального використання інформаційних систем для підтримки основних процесів управління в державній та військовій сферах додаються питання забезпечення стійкості функціонування процесів управління активною протидією воєнній агресії російської федерації та повного розуміння процесу кібернетично-гібридного впливу, де застосовуються спеціальні інформаційно-психологічні операції проти України, її військових формувань і цивільного населення.

Вирішити ці питання можна шляхом упровадження адаптивного підходу до використання ефективної системи управління інформаційною безпекою щодо об'єктів критичної інформаційної інфраструктури, у державному та військовому управлінні.

Процес СУІБ полягає у плануванні, виконанні, контролі та технічному обслуговуванні всієї інфраструктури безпеки. Це необхідна сфера впливу на шляху побудови захищеного простору обігу інформації. Вирішення вказаних питань є актуальним, адже успішне та позбавлене загроз використання інформаційного простору забезпечує злагоджену роботу всіх ланок управління функціональними можливостями протидії активній воєнній агресії в її кібернетично-гібридній формі.

Аналіз останніх досліджень і публікацій. Сьогодні в умовах воєнного стану, коли максимальні зусилля спрямовуються на забезпечення ефективної протидії воєнній агресії, у науковій літературі активно обговорюються питання адаптації процесів створення та функціонування системи

управління інформаційною безпекою, форми й технології, які застосовуються в цьому процесі. Помітний внесок у висвітлення вказаної проблематики з відповідним обґрунтуванням для творчого та практичного вирішення конкретних питань зробили А. Астахов, В. Богуш, В. Домарєв, В. Остроухов, В. Хорошко, О. Юдін та ін. Зокрема проводяться наукові розробки щодо реагування, обробки та керування інцидентами інформаційної безпеки телекомунікаційних мереж (С. Гладиш, В. Кононович, М. Тардаскін) [10; 11]. Низка вчених вивчає питання управління інформаційною безпекою в банківських установах (С. Арбузов, В. Домарєв, Д. Домарєв, Ю. Колобов, В. Міщенко, С. Науменкова) [3; 12], побудови системи й основних підсистем управління інформаційною безпекою та кібербезпекою організації (В. Богуш, В. Бровко, С. Гордієнко, В. Козюра, А. Кудін) [2].

Метою статті є визначення основних особливостей застосування системи управління інформаційною безпекою та повніше розкриття сучасних підходів до етапів створення СУІБ на об'єктах критичної інформаційної інфраструктури, у державному й військово-політичному управлінні, при обробці інформації, поширення якої призводить до деструктивного впливу на державний устрій країни й інформаційну безпеку громадян. А також акцентування уваги на особливостях реалізації цього процесу в умовах воєнного стану, спрямованого на забезпечення ефективної протидії воєнній агресії російської федерації.

Виклад основного матеріалу. У процесі вивчення питання використання СУІБ необхідно розглянути технологічну схему процесу проєктування систем управління інформаційною безпекою, яка базується, відповідно, на п'яти етапах процесу розробки та проєктування СУІБ.

Прогнозоване збільшення структурної та функціональної складності СУІБ, насамперед, використання в її складі елементів системи штучного інтелекту, визначає актуальність розробки технологій і, на їхній основі, засобів проєктування СУІБ [3].

З огляду на реалії сьогодення в питаннях протидії активній воєнній агресії та необхідність урахування особливостей побудови системи управління інформаційною безпекою розглянемо підходи, які базуються на ДСТУ ISO/IEC 27001:2015 «Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги».

Відповідно до цього документа система управління інформаційною безпекою повинна містити в собі організаційну структуру, політики, планування, посадові обов'язки, практики, процедури, процеси й ресурси. Створення й експлуатація СУІБ з урахуванням особливостей побудови потребує того ж підходу, що і будь-яка інша система управління безпекового спрямування або військово-політичного управління.

Використовувана в ISO 27001 для опису СУІБ модель передбачає безперервний цикл заходів: планування, реалізація, перевірка, дія (вдосконалення) (ПРПД). Вона дає змогу досягати загальнодержавних цілей ін-

формаційної безпеки й ефективної протидії деструктивним спрямуванням держави-агресора у вигляді ІПсО.

Побудова СУІБ з урахуванням особливостей воєнного стану, питань протидії воєнній агресії та ІПсО дає можливість визначити взаємозв'язок процесів і підсистем ІБ, відповідальність за них, політичні, фінансові, військові та трудові ресурси, які необхідні для їхнього ефективного функціонування за умов воєнного стану. Весь процес створення поділяється на декілька основних етапів.

Аналіз основних етапів створення СУІБ – процес досить складний і тривалий. Тому доцільно розглянути лише особливо важливі напрями діяльності щодо застосування специфічних підходів створення та використання СУІБ.

Одним із надважливих та актуальних напрямів протиборства у військовій сфері є активні ІПсО та різні деструктивні спрямування стосовно військово-політичної складової функціонування України, зокрема й у кіберпросторі.

Створення системи управління інформаційною безпекою дає змогу за умов воєнної агресії та протидії інформаційно-психологічним операціям російської федерації вийти на новий рівень якості ефективного управління військово-політичними процесами держави, зменшити інформаційні й організаційні загрози, покращити керованість процесами оперативного управління, продемонструвати ефективність і надійність результатів за прийнятими управлінськими рішеннями, що дасть можливість успішно протидіяти агресивним планам різних «недодержавоутворень» відповідного спрямування разом із провідними країнами НАТО на міжнародному рівні.

Розглянемо можливе змістове наповнення основних етапів процесу створення СУІБ з урахуванням актуальних питань функціонування за умов воєнної агресії. Оскільки система управління інформаційною безпекою – це механізм, звід правил, за якими повинні функціонувати всі процеси управління безпекою, то для її впровадження потрібно визначити необхідні процедури, описати правила їхнього функціонування та впровадити в інформаційний простір [2]. Ці, здавалося б, нехитрі дії на практиці викликають багато проблем і питань.

У нашому випадку слід розуміти всю складність і неможливість детальної розробки процесу створення СУІБ в масштабі загальнодержавного військово-політичного управління та визначення конкретних управлінських рекомендацій. Тому пропонуються узагальнювальні специфічні позиції, що притаманні основним етапам застосування СУІБ, орієнтовані на використання інформаційного простору, позбавлене загроз, злагоджену роботу всіх ланок управління функціональними можливостями протидії активній воєнній агресій в її кібернетично-гібридній формі, а саме:

Етап 1. *Прийняття рішення про створення СУІБ.* Рішення про створення СУІБ за окремим специфічним напрямом діяльності повинні розробляти безпосередньо керівники відповідних органів, підрозділів та інших формувань безпекової спрямованості із залученням досвідчених фахівців цього напряму за згодою та під керів-

ництвом керівників вищої ланки управління.

У разі прийняття рішення про створення системи управління інформаційною безпекою з метою її ефективного застосування для досягнення кінцевої мети цього заходу необхідно забезпечити процес повного усвідомлення та сприйняття процедури використання результатів управління процесом за специфічним напрямом діяльності.

Етап 2. *Попередня підготовка.* Зважаючи на важливість запобігання розголошенню інформаційної складової в період воєнних дій та складність підготовки організаційних і технічних заходів попередньої підготовки щодо застосування технологій СУІБ, створювати робочу групу та призначати керівника доцільно з того ж складу посадових осіб, які брали участь у розробленні рішення про створення СУІБ за конкретним специфічним напрямом діяльності.

У її складі мають бути фахівці, які забезпечують інформаційну безпеку за напрямом застосування управлінських процесів. Члени робочої групи забезпечуються необхідною нормативно-методичною документацією відповідно до визначених вимог задля успішного досягнення кінцевої мети управлінських рішень у сфері специфічного напряму діяльності.

Попередній аналіз дає змогу оцінити специфічний напрям діяльності, який буде охоплений СУІБ. Упровадження механізмів створення СУІБ повинно проводитися з урахуванням усіх критеріїв щодо збирання, обробки та передачі інформації. Результатом є узгоджені та затверджені керівництвом межі діяльності об'єктів критичної інформаційної інфраструктури, пов'язаної із плануванням створення СУІБ.

Також у процесі створення системи потрібно постійно аналізувати та виявляти невідповідності наявної інформаційної складової її заявленому аналогу.

Для уточнення обсягу завдань і необхідних витрат на створення та подальше застосування СУІБ проводяться роботи з виявлення та аналізу заходів захисту на об'єктах критичної інформаційної інфраструктури. Аналізуються як прийняті організаційні заходи з планування, впровадження, аудиту та модернізації, так і використовувані програмно-технічні засоби й механізми.

Етап 3. *Оцінка ризиків.* Завданням найбільшої складності при створенні СУІБ за обраним напрямом діяльності є прийняття рішення про вибір заходів щодо обробки оцінених ризиків. У процесі оцінки ризиків здійснюються процедури процесу аналізу ризиків та їхнього оцінювання.

Однак обсяг процедур загального процесу аналізу ризиків не є обов'язковим для виконання при створенні СУІБ за конкретним специфічним напрямом діяльності, тому що проходження всіх процедур може бути економічно недоцільним і неефективним.

Отже, насамперед варто визначити, які процедури доцільно виконувати в конкретному випадку. Природно, що для цього слід зрозуміти, які з активів потребують захисту та якою мірою. Це завдання вирішують за допомогою аналізу інформаційних ризиків, у процесі якого визначають

усі цінні активи, їхню критичність, а також загрози й уразливості, що діють на інформаційні активи. У процесі аналізу інформаційних ризиків можуть виникати певні складності.

По-перше, необхідність вибору найактуальнішого алгоритму оцінювання ризиків. Подібних алгоритмів не так багато, і всі вони, тією або іншою мірою, базуються на методиках оцінки матеріальних ризиків.

По-друге, категоріювання інформаційних активів. Основною складністю в цьому процесі є те, що учасникам процесу важко визначити вартість інформації. Фахівцям з інформаційної безпеки потрібно пояснити спеціалістам, які працюють з інформацією, що від них потрібно, а також розробити методики та критерії категоріювання інформації.

У межах такої роботи повинні бути розглянуті всі процеси, що входять в обрану сферу діяльності об'єкта критичної інформаційної інфраструктури. Наступним кроком у проведенні аналізу ризиків щодо активів є визначення їхньої цінності.

Потрібно розуміти, що визначення вартості активів дійсно дуже складний процес. Однак для оцінювання інформаційних ризиків досить оцінити цінність активів приблизно, тобто проранжувати ресурси відносно один одного. Для цього можна, зокрема, використовувати шкалу із трьох–п'яти рівнів. Крім того, спеціалістам, які оцінюють вартість активів, варто докладно описати, що потрібно від цих активів. Наприклад, буде набагато зрозуміліше фраза «визначте збитки користувача, якщо він одну годину не матиме доступу до певного інформаційного активу», ніж «визначте збитки по доступності певного інформаційного активу».

По-третє, визначення ймовірності реалізації загроз і вразливостей. При визначенні загроз і уразливостей інформаційної системи зазвичай значних труднощів не виникає (можливо, крім визначення меж безлічі загроз і вразливостей, що, як відомо, нескінченно). Однак визначити ймовірність реалізації загроз і вразливостей – набагато складніше завдання. Для його спрощення можна використовувати трирівневу шкалу для ймовірності, так як визначити рівень імовірності реалізації (низький, середній або високий) набагато простіше, ніж визначити ймовірність реалізації у відсотках. Крім того, імовірність уразливості можна розбити на параметри, її складові, тоді оцінити буде куди простіше.

Оцінка ризиків є основним процесом СУІБ. Для цього необхідна методика оцінки ризиків, яку можна було б використати з мінімальними затратами часу та ресурсів. Можна використовувати існуючу чи розробити власну методику, яка найкраще підходитиме до специфіки діяльності об'єкта [4].

Після оцінювання можливих ризиків реалізується підетап «План обробки ризиків». Прийняття плану обробки ризиків і контроль за його виконанням здійснює керівництво вищої ланки управління об'єктом. Виконання всіх заходів плану є основою для прийняття рішення про введення СУІБ в експлуатацію.

Етап 4. *Розробка політик і процедур СУІБ.* На цьому етапі розробляються конкретні документи, які є

основною складовою виконання управлінських рішень за окремим специфічним напрямом діяльності об'єкта критичної інформаційної інфраструктури щодо СУІБ. Зазвичай реалізуються такі процедури та заходи: управління документацією, управління записами, внутрішні аудити, коригувальні дії, попереджуючі дії, управління інцидентами, аналіз функціонування СУІБ керівництвом [7].

Розроблені політики та процедури є ключовими процесами СУІБ, які характерні для конкретного об'єкта критичної інформаційної інфраструктури або обраного процедурного напряму тактичних чи стратегічних управлінських дій, а саме: управління ризиками, управління інцидентами, управління ефективністю системи, управління персоналом чи особовим складом, управління документацією та записами системи управління ІБ, перегляд і модернізація системи, управління безперервністю функціонування технологічних процесів і відновлення після переривань.

Обов'язки з виконання вимог СУІБ за допомогою відповідних наказів і розпоряджень покладаються на відповідальних співробітників керівної ланки управління. Усі розроблені положення політики, процедури й інструкцій доводяться до відома конкретних співробітників у процесі їхнього навчання та інформування.

Етап 5. *Введення СУІБ в експлуатацію* – вважається з моменту затвердження положення про внутрішній регламент обробки інформації. Положення включає таке: існуючі засоби управління, засоби, що забезпечують виконання вимог оперативно-тактичних заходів щодо ефективного забезпечення функціонування діяльності об'єкта критичної інформаційної інфраструктури тощо.

Розглянувши основні етапи створення СУІБ, очевидно, що роботи з розробки та впровадження не можуть бути успішними без сприяння керівництва створенню СУІБ. Створивши систему управління інформаційною безпекою, можна досягти нового рівня якості діяльності, зменшити інформаційні й організаційні загрози, покращити управління та продемонструвати надійність і стійкість функціональних процесів.

Розробити правила управління, забезпечення безпеки та домогтися їхнього виконання – першорядне, але не єдине завдання системи управління інформаційною безпекою. Набагато важливіше «настроїти» циклічність усіх процесів управління безпекою, тобто необхідно, щоб усі процедури системи управління (і, як наслідок, сама система управління) послідовно проходили основні етапи: планування, впровадження, оцінювання ефективності, удосконалення. Отже, система управління буде працювати на основі PDCA-моделі, що означатиме відповідність стандарту ISO 27001 і, що важливо, забезпечуватимуться безперервні контрольованість і вдосконалення системи управління [5; 6; 13].

Оцінювання ефективності процедур системи управління інформаційною безпекою необхідне для того, щоб визначити, чи виконується процедура на практиці належним чином і які поліпшення потрібно впровадити у її виконання [6; 9]. Оцінюється ефективність найчастіше за резуль-

татами перевірок. Перевірки можуть являти собою як перевірки налагодження та конфігурації інформаційних ресурсів, так і просте спостереження за захистом інформаційного ресурсу об'єкта критичної інформаційної інфраструктури.

За результатами оцінювання ефективності виявляється, чи потрібно впроваджувати коригувальні дії для вдосконалення процедури або перебування процедури виконання на необхідному рівні.

При розробці й упровадженні системи управління інформаційною безпекою стосовно процесів управління та функціонування специфічних сфер діяльності за умов воєнного стану, активних воєнних дій і спецоперацій не варто нехтувати одним із найважливіших аспектів ефективного функціонування СУІБ – безпосередньою участю військово-політичного керівництва, керівництва воєнізованих формувань, військово-цивільних адміністрацій і керівництва сфери управління безпекових напрямів діяльності.

Роль керівництва полягає як у постановці завдання забезпечення й управління безпекою та контролі за його виконанням, так і у виконанні всіх правил забезпечення вимог політик і процедур безпеки щодо об'єктів критичної інформаційної інфраструктури й окремих спеціальних процесних стратегій і тактичних дій щодо активної протидії агресору.

Отже, підготовка системи управління інформаційною безпекою – досить трудомістке завдання. І головна проблема полягає в тому, що систему управління необхідно постійно підтримувати. Усе коло зацікавлених осіб повинно знати й чітко виконувати всі необхідні дії, залучатися в цей процес. А процеси системи управління, усі без винятку, необхідно регулярно контролювати та перевіряти. Тільки тоді система управління буде досить ефективною, щоб протистояти будь-яким змінам і залишатися надійною, працездатною й ефективною [2].

Висновки. Ураховуючи актуальність, змістове наповнення процесів і процедур створення та функціонування СУІБ на основі PDCA-моделі за основними її етапами (планування, упровадження, оцінювання ефективності й удосконалення процесів управління та функціонування специфічних сфер діяльності за умов воєнного стану, активних воєнних дій і спецоперацій), можемо визначити деякі специфічні особливості застосування СУІБ за умов воєнного стану.

При плануванні процесів управління інформаційною безпекою щодо об'єктів критичної інформаційної інфраструктури особлива увага приділяється питанням доступу осіб, які не задіяні в процесі формування політики безпеки, створення СУІБ, до інформаційних та інших особливо важливих ресурсів безпекового й оперативного характеру з метою забезпечення унеможливлення витоку інформації з обмеженим доступом.

До спеціальної групи з планування та створення ефективної, спрямованої на конкретні процеси оперативно-службової діяльності, системи управління інформаційною безпекою, за рішенням керівництва, доцільно залучати найпідготовленіших фахівців, які за своїми професійними й

організаторськими здібностями здатні виконувати поставлені специфічні завдання. Загальне керівництво діяльністю спеціально створеної групи з огляду на специфіку оперативно-службових завдань, затверджені плани організації та функціонування політик безпеки й заходи протидії витоку інформації з обмеженим доступом має здійснювати вище керівництво.

При впровадженні СУІБ контекст, межі її застосування та критерії діяльності визначають одну з найважливіших складових подальшого цільового завдання системи управління з ефективного функціонування процесів оперативної, тактичної та стратегічної діяльності об'єктів критичної інформаційної інфраструктури за умов воєнного стану.

При співставленні з критеріями функціонування оцінені ризики можуть бути неприйнятними для подальшого виконання спеціальних завдань, що потребує особливого підходу до прийняття управлінських рішень з ефективного забезпечення оперативно-службової діяльності.

Особливу увагу слід приділяти ризикам, які виходять за межі критеріїв функціонування об'єкта критичної інформаційної інфраструктури або оперативно-тактичної, стратегічної ситуації, щодо управління оперативно-службовою чи військовою діяльністю, а рішення все одно необхідно приймати з урахуванням оперативної обстановки. У такому разі рішення щодо кожного ризику приймають окремо після детального колегіального аналізу фахівцями високого професійного рівня з урахуванням результатів оцінювання впливу на ефективне виконання управлінських рішень.

Передача на аутсорсинг є неприйнятною формою обробки ризиків ІБ за умов воєнного стану при можливому функціонуванні інформації з обмеженим доступом та за інших режимних обмежень.

Що стосується ризиків, які приймаються в деяких конкретних ситуаціях, слід дуже уважно «моніторити» їхній еволюційний розвиток, можливі впливи на загальну оперативну ситуацію та ефективність прийняття управлінських рішень.

Ризик у конкретному випадку вважається усвідомлено припустимим, і керівництво повинно змиритися з можливими наслідками. Зазвичай це означає, що вартість контрзаходів значно перевершує фінансові втрати та можливі управлінські помилки чи неточності при виконанні прийнятих рішень у разі реалізації загрози [3]. Такий підхід полягає в усвідомленому прийнятті ризику об'єктом відповідної сфери управління.

Список використаних джерел

1. Богуш В. М., Бровко В. Д., Гордієнко С. Б., Козюра В. Д., Кудін А. М. Управління інформаційною безпекою та кібербезпекою організації : навчальний посібник : в 2 ч. Ч. 1: Основи менеджменту інформаційної безпеки та кібербезпеки. Київ : НА СБУ, 2023. 168 с.

2. Богуш В. М., Бровко В. Д., Гордієнко С. Б., Козюра В. Д., Кудін А. М. Управління інформаційною безпекою та

кібербезпекою організації : навчальний посібник : в 2 ч. Ч. 2: Основи побудови системи і основних підсистем управління інформаційною безпекою та кібербезпекою організації. Київ : НА СБУ, 2023. 208 с.

3. Домарєв В. В., Домарєв Д. В. Управління інформаційною безпекою в банківських установах (Теорія і практика впровадження стандартів серії ISO 27k). Донецьк : Велстар, 2012, 146 с.

4. Гордієнко С. Б. Актуальні питання управління ІТ ризиками на об'єктах критичної інформаційної інфраструктури. *Вісник Державного університету телекомунікацій «Телекомунікаційні та інформаційні технології»*. 2022. № 1 (74). С. 29–35.

5. ДСТУ ISO/IEC 27000:2015. Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Огляд і словник (ISO/IEC 27000: 2014, IDT).

6. ДСТУ ISO/IEC 27001:2015. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT).

7. ДСТУ ISO/IEC 27002:2015. Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT).

8. ДСТУ ISO/IEC 27005:2015. Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2011, IDT).

9. ДСТУ ISO/IEC 27006:2015. Інформаційні технології. Методи захисту. Вимоги до організацій, які надають послуги з аудиту і сертифікації систем управління інформаційною безпекою (ISO/IEC 27006:2011, IDT).

10. Гладиш С. В., Кононович В. Г., Тардаскін М. Ф. Розподіл відповідальності щодо реагування та обробки інцидентів безпеки в інформаційно-телекомунікаційній мережі загального користування. *Зв'язок*. 2007. № 8. С. 28–31.

11. Гладиш С. В. Інтелектуальна система керування інцидентами інформаційної безпеки телекомунікаційних мереж. *Інформаційні технології та інформаційна безпека в науці, техніці та освіті ІНФОТЕХ-2007* : матеріали міжнародної науково-практичної конференції. Севастополь : СевНТУ, 2007. С. 53–57.

12. Арбузов С. Г., Колобов Ю. В., Міщенко В. І., Науменкова С. В. Безперервність бізнесу. Банківська енциклопедія. Київ : Центр наукових досліджень Національного банку України : Знання, 2011. 504 с.

13. ISO/IEC 27031:2011 року (Інформаційні технології. Методи забезпечення безпеки. Керівництво по створенню готовності інформаційно-комунікаційних технологій до забезпечення безперервності бізнесу).

Стаття надійшла до редакції 15.08.2024

UDC 35.004

Hordiienko S. B.

PECULIARITIES OF THE IMPLEMENTATION OF THE INFORMATION SECURITY MANAGEMENT SYSTEM UNDER MARTIAL LAW CONDITIONS

Due to the active conduct of information-psychological operations (IPSO) and the spread of destructive informational impacts by the aggressor state, rf, against our country, the issue of ensuring information security is becoming increasingly urgent. Ensuring the

information system operates under optimal conditions for the functioning of information exchange processes in state and military management solely with a set of technical means is, at present, practically impossible.

Moreover, the challenge extends to ensuring the resilience of management processes related to actively countering military aggression by rf, as well as fully understanding the process of cybernetic-hybrid impact, where special IPSO are used against Ukraine, its military forces, and its civilian population.

These issues can be addressed through the implementation of an adaptive approach to the use of an effective Information Security Management System (ISMS) for critical information infrastructure objects in state and military-political administration.

This article identifies the key features of ISMS implementation and modern approaches to its development stages at critical information infrastructure objects, in state and military-political administration, and during the processing of information, the dissemination of which has a destructive impact on the country's state system and citizens' information security. Given the current realities in countering active military aggression and the need to build an effective information security management system, approaches based on DSTU ISO/IEC 27001:2015 "Information Technology. Protection Methods. Information Security Management Systems. Requirements" are discussed. The analysis reveals the interconnection of information security processes and subsystems, which are responsible for them, and the political, financial, and military resources required for their effective operation under martial law.

One of the most crucial and urgent areas of conflict in the military sphere is active information-psychological operations and various destructive strategies aimed at Ukraine's military-political infrastructure, including in cyberspace.

It is concluded that the creation and implementation of an effective ISMS will allow for a new level of quality in managing military-political processes under conditions of military aggression and counteracting IPSO by rf. This will reduce information and organisational threats, improve the controllability of operational management processes, and demonstrate the effectiveness and reliability of decision-making, enabling successful resistance to the aggressor's plans alongside leading NATO countries at the global international level.

Key words: *military aggression, cyber security measures, information security, information and psychological operations, cyber security, critical information infrastructure, security policy, ISMS policies and procedures, risk-oriented approach, information security management system, modern information and communication systems and technologies, management decision.*