Мартинюк В.В. ORCID 0000-0003-0244-7861 (ВІТІ)
Паламарчук Н.А. ORCID 0000-0003-8818-7794 (ВІТІ)
Паламарчук С.А. ORCID 0000-0001-7483-9165 (ВІТІ)
Сівоха О.М. ORCID 0000-0002-8076-7425 (ВІТІ)

ЗАДАЧІ ВДОСКОНАЛЕННЯ ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

У статті розглянуто становлення сфери забезпечення кібербезпеки в Україні та її імплементація зі сферами захисту інформації та інформаційної безпеки. Зазначено, що неодмінною умовою вирішення питань щодо забезпечення інформаційної та кібербезпеки є розуміння того, що держава знаходиться в нерозривному зв'язку і взаємодії з іншими структурами і суб'єктами, що відображається законодавчими, організаційними та технічними (технологічними) аспектами /рівнями взаємодії, в межах розглянутих аспектів (рівнів взаємодії), визначені задачі щодо вдосконалення інформаційної та кібернетичної безпеки об'єктів критичної інфраструктури.

Наведено, що становлення та формування сфери кіберзахисту та кібербезпеки в Україні нерозривно пов'язано із забезпеченням сфер захисту інформації та інформаційної безпеки. Дані сфери в Україні одночасно мали дві організаційні парадигми: комплексна система захисту інформації (КСЗІ) та система управління інформаційною безпекою (СУІБ). Визначено, що головною невідповідністю забезпечення безпеки сьогодні – є відсутність комплексного підходу (люди, системи, процеси), ігнорування питань безпеки, зайва впевненість у безпеці.

Також наведено, що ефективну кібербезпеку можливо забезпечити лише шляхом комплексної реалізації низки правових, організаційних, технічних, наукових заходів, кадрового та ресурсного забезпечення на національному та відомчому (з врахуванням особливостей та специфіки діяльності в основних сферах діяльності держави) рівнях. В рамках цієї концепції розглянуто роль та місце операційних центрів безпеки (Security Operations Center, SOC), які є ключовою частиною сучасних систем кіберзахисту та з реалізації протидії кібератакам.

Подальші дослідження доцільно спрямувати на адаптацію математичного апарату для оцінювання вимог кіберзахисту та кібербезпеки, з метою повноцінного врахування визначених організаційних та технічних аспектів функціонування об'єктів критичної інфраструктури, а також реагування на атаки в режимі реального часу.

Ключові слова: *інформаційна безпека, кібербезпека, кібератака, обєкт критичної інфраструктури.*

В.Мартынюк, Н.Паламарчук, С.Паламарчук, Е.Сивоха. Задачи совершенствования информационной и кибернетической безопасности объектов критической инфраструктуры.

В статье рассмотрено становление сферы обеспечения кибербезопасности в Украине и ее имплементация со сферами защиты информации и информационной безопасности. Отмечено, что непременным условием решения вопросов по обеспечению информационной и кибербезопасности является понимание того, что государство находится в неразрывной связи и взаимодействии с другими структурами и субъектами, что отражается законодательными, организационными и техническими (технологическими) аспектами / уровнями взаимодействия, в рамках рассмотренных аспектов (уровней взаимодействия), определенны задачи по совершенствованию информационной и кибернетической безопасности объектов критической инфраструктуры.

Показано, что становление и формирование сферы киберзащиты и кибербезопасности в Украине неразрывно связано с обеспечением сфер защиты информации и информационной безопасности. Данные сферы в Украине одновременно имели две организационные парадигмы: комплексная система защиты информации (КСЗИ) и система управления информационной безопасностью (СУИБ). Определено, что главным несоответствием обеспечения безопасности сегодня - является отсутствие комплексного подхода (люди, системы, процессы), игнорирование вопросов безопасности, лишняя уверенность в безопасности.

Также показано, что эффективную кибербезопасности возможно обеспечить только путем комплексной реализации ряда правовых, организационных, технических, научных мер, кадрового и ресурсного обеспечения на национальном и ведомственном (с учетом особенностей и специфики деятельности в основных сферах деятельности государства) уровнях. В рамках этой концепции рассмотрена роль и место операционных центров безопасности (Security Operations Center, SOC), которые являются ключевой частью современных систем киберзащиты и реализации противодействия кибератакам.

Дальнейшие исследования целесообразно направить на адаптацию математического аппарата для оценки требований киберзащиты и кибербезопасности, с целью полноценного учета определенных организационных и технических аспектов функционирования объектов критической инфраструктуры, а также реагирования на атаки в режиме реального времени.

Ключевые слова: *информационная безопасность, кибербезопасность, кибератака, объект критической инфраструктуры.*

V. Martynyuk, N. Palamarchuk, S. Palamarchuk, E. Sivokha. The tasks of improving information and cybernetic security of critical infrastructure facilities.

The article discusses the formation of the sphere of ensuring cybersecurity in Ukraine and its implementation with the spheres of information protection and information security. It is noted that an indispensable condition for resolving issues of ensuring information and cyber security is the understanding that the state is inextricably linked and interacts with other structures and subjects, which is reflected in legislative, organizational and technical (technological) aspects / levels of interaction, within the framework of the considered aspects (levels of interaction), the tasks for improving the information and cybernetic security of critical infrastructure facilities are defined.

It is shown that the formation and formation of the sphere of cyber defense and cyber security in Ukraine is inextricably linked with the provision of the spheres of information protection and information security. These spheres in Ukraine simultaneously had two organizational paradigms: an integrated information security system (ISPS) and an information security management system (ISMS). It was determined that the main inconsistency in ensuring security today is the lack of an integrated approach (people, systems, processes), ignorance of security issues, excess confidence in security.

It is also shown that effective cybersecurity can be ensured only through the comprehensive implementation of a number of legal, organizational, technical, scientific measures, personnel and resource support at the national and departmental (taking into account the specifics and specifics of activities in the main spheres of state activity) levels. Within the framework of this concept, the role and place of Security Operations Centers (SOCs), which are a key part of modern cyber defense systems and the implementation of countering cyber attacks, are considered.

Further research should be directed to the adaptation of the mathematical apparatus for assessing the requirements of cyber defense and cyber security, in order to fully take into account certain organizational and technical aspects of the functioning of critical infrastructure facilities, as well as respond to attacks in real time.

Постановка завдання у загальному вигляді. Переваги сучасного цифрового світу та розвиток інформаційних технологій обумовили виникнення нових загроз національній та міжнародній безпеці. Функціонування об’єктів критичної інфраструктури в такому специфічному середовищі, як кіберпростір, пов’язане з уразливістю і загрозами і вимагає розробки нового інструментарію. Поряд з інцидентами природного (ненавмисного) походження зростає кількість та потужність кібератак, вмотивованих інтересами окремих держав, груп та осіб. Неодмінною умовою вирішення питань щодо забезпечення інформаційної та кібербезпеки є розуміння того, що держава знаходиться в нерозривному зв’язку і взаємодії з іншими структурами і суб’єктами, що відображається законодавчими, організаційними та технічними (технологічними) аспектами /рівнями взаємодії. Управління інформаційною та кібернетичною безпекою об’єктів критичної інфраструктури ґрунтується на знаннях про стан об’єктів управління, стан середовища функціонування і про впливи, які відбуваються [1].

В аналітичному дослідженні корпорації “РЕНД” на замовлення сухопутних військ ЗС США (звіт 2013 року, код звіту по проекту – *RAND10473*) зазначено, що в практичній діяльності інформаційне середовище необхідно розглядати, як єдине середовище у двох вимірах: людському та технічному. Розгляд інформаційного середовища та кіберсередовища (відповідно інформаційної безпеки (ІБ) та кібербезпеки), як окремих інституцій (напрямів діяльності) американськими дослідниками визнано необґрунтованим та штучним (тобто визнано методологічною помилкою). Також, за результатами Варшавського саміту НАТО (2016 рік) кіберпростір офіційно визнано, як четвертий домен (четверта сфера) для збройного протиборства (разом з наземним, повітряним та морським простором) [2].

Головна невідповідність забезпечення безпеки сьогодні – це відсутність комплексного підходу (люди, системи, процеси), ігнорування питань безпеки, зайва впевненість у безпеці. Тому, належне забезпечення повинне мати комплексний характер і відповідну методологічну базу.

Аналіз останніх досліджень і публікацій. Становлення та формування сфери кіберзахисту та кібербезпеки в Україні нерозривно пов’язано із забезпеченням сфер захисту інформації та інформаційної безпеки [2 – 8, 12]. Дані сфери в Україні одночасно мали дві організаційні парадигми: комплексна система захисту інформації (КСЗІ) та система управління інформаційною безпекою (СУІБ, яка була обов’язковою лише в банківській сфері СОУ Н НБУ 65.1 СУІБ 1.0: 2010) [9, 10].

В межах завдань захисту інформації основним є забезпечення визначених властивостей об’єкту захисту інформації (конфіденційності, цілісності, доступності), тоді як для завдань кібербезпеки/кіберзахисту основним є збереження штатного режиму функціонування системи, коли несанкціоновані дії не призведуть до втрати керованості системою (порушення штатного режиму роботи) та збереження властивостей електронних інформаційних ресурсів (як і для об’єктів захисту) [4, 8, 12 – 13].

В роботах [15-18] розглянуті методологічні та теоретичні засади інформаційного синтезу систем кіберзахисту, формалізовані критерії безпеки та методи автоматизованого детектування атак в системах проактивного кіберзахисту. ***Метою статті*** є визначення задач вдосконалення інформаційної та кібернетичної безпеки об’єктів критичної інфраструктури.

Виклад основного матеріалу. Історично, першим кроком у сфері кібербезпеки було створення в 1996 р. Комісії по захисту життєво важливої інфраструктури при Президентові США, якій було поставлене завдання розробити всеохоплюючу національну стратегію захисту інфраструктури від фізичних і кібернетичних загроз. Подібна директива видана в ЄС у 2008 р. [3]. Забезпечення безпеки критичної інфраструктури *(Critical Infrastrurture Protection, CIP)* представляє собою концепцію готовності протистояти серйозним загрозам діяльності важливих об’єктів інфраструктури та об’єктів підвищеної загрози в регіоні чи державі, особливо в умовах розповсюдження інформаційних технологій.

Законодавчий та організаційний аспект. На противагу світовому досвіду із стандартизації, який відображено двома напрямами – в частині забезпечення вимог захищеності (“Загальні критерії”), що оперують оцінкою сукупності програмно-апаратних засобів (міжнародний стандарт ISO/IEC 15408) та в частині менеджменту інформаційної безпеки, що впроваджує систему управління інформаційною безпекою (СУІБ) та дозволяє правильно організувати процес захисту інформаційних ресурсів, управління ризиками для цих ресурсів (міжнародний стандарт ISO/IEC 27001 та подальші стандарти серії 27000 (рис. 1), Україна обрала власний вектор розвитку, прийнявши серію нормативних документів системи технічного захисту інформації (НД ТЗІ) та фактично, не приєднавшись до загальносвітового процесу стандартизації в частині менеджменту ІБ [9].

Рис.1. Позиція кібербезпеки відносно інформаційної безпеки за ISO 27032

Більше того, до прийняття Закону України “Про захист інформації в інформаційно-телекомунікаційних системах” в редакції від 04.07.2020 року [5], система НД ТЗІ України для захисту державних інформаційних ресурсів регламентувала лише створення КСЗІ.

При цьому, власне визначення КСЗІ, як взаємозалежної сукупності організаційних та інженерно-технічних заходів, засобів і методів захисту інформації наводиться в даному Законі.

Лише в редакції від 04.07.2020 року розширюються умови обробки інформації, а саме: “державні інформаційні ресурси та інформація з обмеженим доступом, крім державної таємниці, службової інформації та державних і єдиних реєстрів, створення та забезпечення функціонування яких визначено законами, можуть оброблятися в системі без застосування КСЗІ у разі виконання умови: “*Підтвердження відповідності системи управління інформаційною безпекою за результатами процедури з оцінки відповідності національним стандартам України щодо систем управління інформаційною безпекою*”.

Тема кібербезпеки в Україні за останні роки набула значних зрушень, прийнято мінімально необхідну нормативно-правову базу з кібербезпеки. Зокрема, метою “Стратегії кібербезпеки України” [6] (затвердженої указом Президента України №96/2016 від 27 січня 2016 року) було створення умов для безпечного функціонування кіберпростору, його

використання в інтересах особистості, суспільства і держави. При цьому, основний масив положень стратегії стосується сфери національної оборони і не зачіпає бізнес. Стратегія стала підтвердженням прийнятого Україною курсу на євроінтеграцію, початком якого було підписання і ратифікація Україною Конвенції про кібербезпеку. Низка відповідних положень щодо кібербезпеки закріплена в інших указах Президента України, *наприклад*: "Про Концепцію розвитку сектору безпеки і оборони України" (№92/2016 від 14 березня 2016 року); "Про стратегічний оборонний бюлетень України" (№ 240/2016 від 6 червня 2016 року), "Про Національний координаційний центр кібербезпеки" (№242/2016 від 7 червня 2016 року). За напрямом кібербезпеки запроваджено певний механізм керівництва і організовано роботу Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони України. Безпосереднє реагування на факти кібератак і міжвідомчу взаємодію передбачалося через розроблення "Протоколу спільних дій основних суб'єктів забезпечення кібербезпеки, суб'єктів кіберзахисту та власників (розпорядників) об'єктів критичної інформаційної інфраструктури під час попередження, виявлення, припинення кібератак та кіберінцидентів, а також при усуненні їх наслідків" (*який так і залишився проєктом*).

Деталізацію цієї діяльності передбачалося здійснювати у відповідності із щорічними планами Кабінету Міністрів України щодо реалізації Стратегії кібербезпеки України. Однак, План заходів щодо реалізації Стратегії кібербезпеки України на 2020 рік досі не затверджений, більше того, не існувало і Плану на 2019 рік. Щодо Плану на 2018 рік один з експертів у сфері інформаційної безпеки зазначив, *"Планом передбачено 27 пунктів, з яких: ні про що – 2; неефективні – 11; важко виконати/шкідливі – 3; корупційні – 3; більш менш корисні – 10. Ефективність – 37%."* [2, 14].

В 2017 році прийнято Закон України "Про основні засади забезпечення кібербезпеки України" [4], в якому визначено основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження суб'єктів у цій сфері, основні засади координації діяльності із забезпечення кібербезпеки критично важливих об'єктів інфраструктури. Порядок формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави наразі затверджено Постановою Кабінету Міністрів України від 23 серпня 2016 р. № 563 [7].

Імплементація сфери кібербезпеки з сферами захисту інформації та ІБ простежується і в наступних документах. Згідно Постанови Кабінету Міністрів України від 19.06.2019 року № 518 "Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури" [8] визначено організаційно-методологічні, технічні та технологічні умови кіберзахисту об'єктів критичної інфраструктури, які є обов'язковими до виконання на таких об'єктах. Також визначено, що кіберзахист об'єкта критичної інфраструктури забезпечується шляхом впровадження на об'єкті критичної інфраструктури КСЗІ або системи інформаційної безпеки з підтвердженою відповідністю. Незважаючи на те, що в Закон України "Про основні засади забезпечення кібербезпеки" були внесені зміни, важливо також, щоб був затверджений перелік об'єктів критичної інфраструктури держави (*який досі є проєктом*), оскільки відповідальність за виконання загальних вимог безпеки все ще залишається офіційно не затвердженою [19]. В Україні лише Національний банк України на системному рівні (для банківської сфери) упорядкував питання забезпечення кібербезпеки. Так, 28 вересня 2017 року постановою Правління Національного банку України № 95, затверджено "Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України" [11]. Імплементація норм Постанови дала можливість посилити вимоги до захисту інформації в інформаційних системах банків з урахуванням актуальних кіберзагроз; визначити принципи управління ІБ в банках; визначити принципи криптографічного захисту інформаційних систем Національного банку України; установити обов'язкові мінімальні вимоги щодо організації заходів із забезпечення безпеки інформації (такі як: захист від зловмисного коду, заходи безпеки при використанні електронної пошти; контроль доступу до інформаційних систем банку; заходи безпеки в мережі банку тощо).

Отже, в Україні зроблено перші кроки з прийняття нормативно-правової бази у сфері кібербезпеки, має місце реалізація міжнародних проектів. Сьогодні на порядку денному – нарощування зусиль та поширення отриманого досвіду. У той же час, стримуючим чинником для України є певні недоліки чинних нормативних актів: невідповідність та протиріччя в нормативно-правовій базі щодо кібербезпеки (відсутня чітка управлінська вертикаль, деякі повноваження суб'єктів забезпечення кібербезпеки "розмиті", питання активного впливу у кіберпросторі практично не розглядаються); закладено низку методологічних помилок (особливо щодо співвідношення понять "кібербезпека", "кіберзахист", "кібероборона", "інформаційна безпека" тощо); положення відомчих документів силових структур, особливо щодо кібероборони в цілому не містять системного бачення, мають суб'єктивні обмеження, в них відсутній очікуваний результат проведення заходів та чіткі критерії оцінки досягнення кінцевого стану. З іншого боку, на думку деяких експертів, складається враження, що штучно обмежено діяльність у сфері кібербезпеки (це видно з тексту статті 2 Закону України "Про основні засади забезпечення кібербезпеки України" [4], в якій визначено на що не поширюється Закон) [2, 14].

Технічний (технологічний) аспект. В рамках ***кібернетичного підходу*** приставка "кібер-" застосовується не в контексті цифрових процесів в рамках середовищ комп'ютерних систем (кіберпростір, кіберподія, кіберзахист, кібератака та інше), а для опису особливостей процесів кібернетичних (управляємих, керованих) систем.

Згідно [4] інцидент кібербезпеки (далі – кіберінцидент) – подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі, внаслідок дії людського фактора) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі, зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів.

Завдання ведення державного реєстру кіберінцидентів згідно [4] покладається на урядову команду реагування на комп'ютерні надзвичайні події України, CERT-UA (*Computer Emergency Response Team of Ukraine*). Також на CERT-UA покладаються обов'язки щодо накопичення та аналізу даних про вчинення та/або спроби вчинення несанкціонованих дій щодо державних інформаційних ресурсів в ІТС, а також про їх наслідки, інформування правоохоронних органів для вжиття заходів із запобігання та припинення кримінальних правопорушень у зазначеній сфері. Слід зазначити, що технологічна складова всіх кіберпорушень є однаковою – це використання технічних недоліків сучасних інформаційно-телекомунікаційних систем (вразливостей), сучасних технологічних можливостей впливу на цільову аудиторію, суспільну думку через кіберпростір, що робить його незрівнянно дієвим засобом досягнення злочинних цілей. Зловмисники та гравці, за якими стоять держави, вже мають необхідні знання й інструменти, тому є багато характерних, і до того ж очевидних ознак, які вказують на існування загроз (атак) та які зосереджені на трьох основних принципах, а саме зловмисники доводять шкідливе програмне забезпечення до безпрецедентних рівнів досконалості та впливу; дедалі більше використовують шифрування з метою уникнення виявлення; приховують "сліди" будь-якого втручання в системи.

Успіх атак вимірюється (визначається) на основі трьох факторів: (1-й) складність, необхідна для пошуку вразливостей (вразливих точок) в системах; (2-й) складність запуску та успішної реалізації певного виду атаки; (3-й) складність у виявленні самого факту нападу на систему. Загалом, виділяють види таких найбільш поширених кібератак (див. рис. 2):

з використанням шкідливого програмного забезпечення (окрім всім відомих епідемій *Wannacry* та *NotPetya* було чимало інших шкідливих кампаній націлених на вимагання коштів у жертв, наприклад, *Jaff* або *SOREBRECT*). При цьому, поширення шкідливого ПЗ відбувається не лише шляхом класичної фішингової розсилки листів персоналу компанії, які містять шкідливі вкладення, але і з використанням уже скомпрометованих веб-сайтів, за

рахунок веб-імплантування (мітка 1) різноманітних вірусів, троянів та інших форм шкідливого ПЗ з метою зараження користувачів, які відвідали скомпрометований веб-ресурс – “watering hole”;

з використанням соціальної інженерії, методи якої на сьогоднішній день продовжують удосконалюватися. Так, в 2017 році зловмисники найчастіше використовували фішингові розсилки (мітка 2) та фішингові сайти (мітка 3) для своїх атак на організації. Мітка (2) являє собою електронні листи з вкладенням зараженого файлу, мітка (3) являє собою сценарій веб-фішингу, де атакуючий створює сайт, як дві краплі води схожий на офіційний веб-ресурс;

компрометація даних (мітка 4), як правило, здійснюється шляхом спроби підбору паролів і у випадку погано налаштованої парольної політики в організації (отримуються облікові дані, які в подальшому використовуються для того, щоб обійти КСЗІ організації);

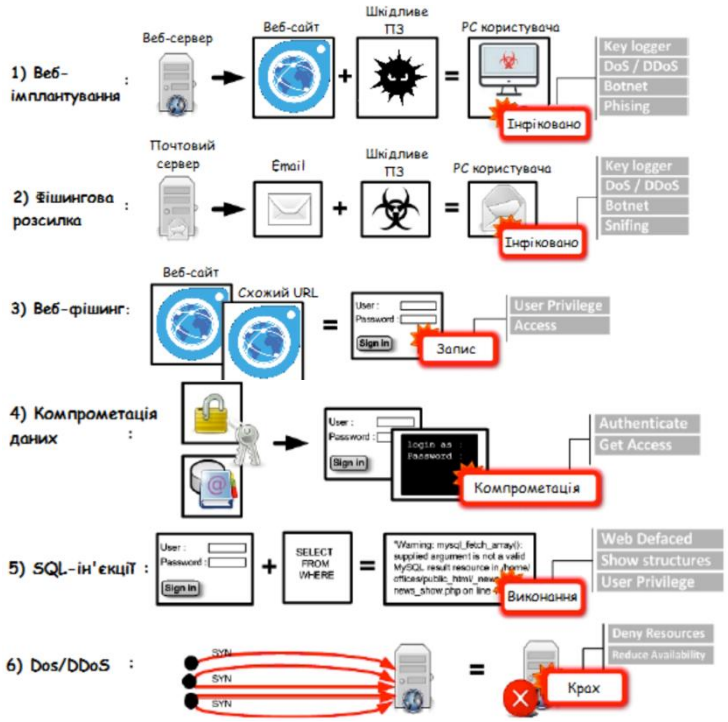

Рис. 2 Основні види кібернетичних атак

експлуатація веб-вразливостей, яка використовується в двох основних сценаріях – при атаці безпосередньо на сайт та подальшого його використання і для проникнення в корпоративну мережу компанії через її веб-ресурси. При цьому, кожний четвертий веб-ресурс є уразливим до “*впровадження операторів SQL*” (так званих SQL-ін’єкцій – мітка 5);

DOS/DDOS-атака (мітка 6), яка передбачає надсилання багатьох запитів на сервер за короткий проміжок часу, тим самим збільшивши завантаження сервера і зменшивши пропускну здатність мережі, що призводить до унеможливлення використання ресурсів або послуг уповноваженими користувачами.

Щоб зламати систему будь-якої організації незалежно від її масштабів і сфери діяльності, хакери використовують цілі стратегії нападу, які складаються здебільшого з п’яти кроків (і майже повністю переплітаються з основними етапами проведення тестування на проникнення), це: розвідка, сканування, встановлення контролю, організація доступу та управління системою, знищення або заплутування слідів кібернетичного нападу, при цьому, використовуючи щойно згадані види атак [2, 12].

Прикладом порушення інформаційної безпеки є подія 27 липня 2017 року, коли відбулася наймасштабніша в історії України кібератака, деякі ЗМІ класифікують її як кібертеракт: відбулося інфікування великої кількості комп’ютерів різних організацій через програму бухгалтерського обліку Me.Doc комп’ютерним вірусом під назвою Petya.A (або mbr locker 256 – вірус-шифрувальник). У списку організацій, які зазнали шкоди, – найбільші банки (включаючи НБУ); комунальні та енергетичні підприємства; підприємства інфраструктури (в т.ч. Укрзалізниця); провідні оператори мобільного зв’язку; автозаправні станції; поштові компанії (Укрпошта, Нова Пошта та ін.); ЗМІ; влада та державні підприємства (Кабінет міністрів України, ГСЧС, ЧАЕС та ін.).

Глобальна статистика, зібрана компанією Cisco у 2017 р., свідчить про таке: уразливості (“дири”) в сучасних системах захисту уможливлюють до 65 % кіберінцидентів; людський фактор – критичне (якщо масштабувати його до кількості та ступеня складності кіберзагроз) зниження рівня грамотності користувачів – до 48 % інцидентів; 55 % організацій

нездатні встановити причину інциденту; середній час встановлення такої причини в сучасній індустрії ІБ та кібербезпеки складає 100 днів [13].

Як приклад, система кіберзахисту державних інформаційних ресурсів і об'єктів критичної інфраструктури на об'єктах моніторингу України в період з 1 по 7 липня 2020 року зафіксувала 45,03 тис. кіберінцидентів, що на 21,4% більше в порівнянні з попереднім тижнем. Згідно з повідомленням Держспецзв'язку України, переважна більшість зафіксованих підозрілих подій стосується виявлення спроб мережевого сканування (52%), нестандартних протоколів або подій (24%), виявлення мережевого шкідливого ПО (11%), веб-атак (8%) і спроб отримання прав адміністратора (4%). Основна кількість інцидентів стосується поширення шкідливого ПЗ (73% загальної кількості) та фішингу (26%).

З метою протидії кібератакам створюються операційні цетри безпеки (*SOC*), які є ключовою частиною сучасних систем кіберзахисту ІТС. Операційні центри безпеки (*SOC*) за допомогою операторів (офіцерів) безпеки та/або засобів управління інформацією і подіями безпеки (*SIEM*) з різним ступенем автоматизації реалізують протидії атаці [15, 16]:

1) спостереження у реальному часі за допомогою сенсорів безпеки за подіями в корпоративному сегменті кіберпростору;

2) формування за допомогою сенсорів безпеки інформації про події безпеки, її збір і нормування в єдиному центрі оперативної обробки;

3) аналіз подій і прийняття рішення про наявність кібератаки (інциденту кібербезпеки);

4) визначення вразливостей, що сприяли атаці, прийняття рішення про протидію та реалізація цього рішення за допомогою актуаторів безпеки (виконавчих пристроїв системи захисту, засобів захисту).

Формування інформації про поточні події безпеки в ІТС здійснюється за допомогою використання індикаторів компрометації (*indicators of compromise, IOCs*). Це цифрові (бітові) послідовності (сигнатури), що є ознаками небезпечного трафіку або обчислювального процесу. Повідомлення про інциденти (події) безпеки формуються сенсорами безпеки (*security sensors, SS або засоби IDS*) на основі *IOCs*.

В рамках підсистеми протидії атакам можливо виділити послідовність дій, яка регулярно повторюється появою кожної атаки:

отримання SOC за допомогою сенсорів безпеки інформації про події в ІТС;

аналіз подій в SOC і прийняття рішення про наявність кібератаки;

прийняття рішення про протидію атаці і реалізація цього рішення за допомогою актуаторів безпеки.

Такий регулярний порядок дій дозволяє представити процеси протидії атакам у вигляді траєкторії поведінки керованої (кібернетичної) системи. У такій системі, назвемо її кібернетичної системою оперативного захисту (*Cybernetic Operational Protection System, COPS*), можна виділити наступні компоненти:

об'єкт управління (*Management Object, MO*) – це ІТС, яку необхідно захистити;

підсистема управління захистом (*Protection SubSystem, PSS*), яка складається з:

центру операцій безпеки (SOC); сенсорів безпеки (*security sensor, SS*) і актуаторів безпеки (*security actuator, SA*) – це процеси комп'ютерів, які відповідають за формування інформації про події безпеки і реалізацію інформації про керуючий вплив на ІТС;

каналів прямого зв'язку від SS до SOC (*Forward Link, FL*) і зворотного зв'язку від SOC до актуаторів SA (*Return Link, RL*) – це комп'ютерна мережа, що забезпечує обмін інформацією між центром управління SOC і об'єктом управління ІТС.

При розробці моделі *COPS* використовується ряд тверджень, які дозволяють спростити графічний та математичний опис ситуації:

будь-які характеристики та стан системи інформаційних технологій (комп'ютерних пристроїв) можна представити у вигляді кінцевої множини двійкових одиниць (бітів);

інформація про будь-який стан будь-якого комп'ютерного пристрою, яка передається через мережу ІТС, може бути представлена також множиною бітів, як і сам стан;

роль сенсорів безпеки в ІТС виконують обчислювальні процеси, які передають інформацію про стан комп'ютерів ІТС через мережу за вказаною адресою;

роль актуатора безпеки в ІТС (керуючого елемента) виконують обчислювальні процеси, які на основі прийнятих команд від *SOC* запускають нові процеси, що виконують необхідні дії захисту.

Дані твердження дозволяють представити графічно дві суміжні фази *COPS* у вигляді наступної структури (див. рис. 3). В рамках цієї моделі, ІТС виступає в ролі об'єкта управління (*MO*). Операційний центр безпеки (*SOC*) – в ролі центру управління (*Control Center, CC*) кібернетичної системи. *I(ITSi:S*) – це інформація на сенсорах безпеки про поточний стан *ITSi* в рамках актуальної (поточної) фази *COPSi*. Дана інформація сформована і направлена до *SOC* сенсорами *SS*. На основі прийнятої інформації *SOC* приймає рішення про переведення системи інформаційних технологій в наступний стан *ITSi+1* і оформлює це рішення в вигляді команди *I(ITSi+1:SOC)*. Далі ця інформація надсилається до ІТС, де прийняте рішення реалізується за допомогою актуаторів безпеки *SA*: об'єкт управління переходить в наступний стан протидії атаці *ITSi+1*.

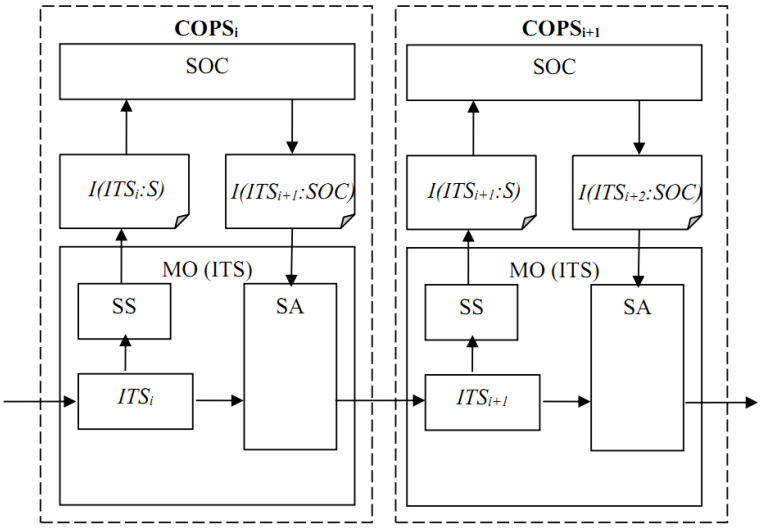

Рис. 3 Модель поведінки кібернетичної системи захисту в режимі протидії атаці

Процес управління в рамках *COPS* і поведінку самої *COPS* (перехід з однієї фази в іншу) може бути описаний наступною системою рівнянь:

$$\begin{cases} I(ITS_{i+1} : SOC) = F_{SOC}[I(ITS_i : SS)]; \\ ITS_{i+1} = F_A[ITS_i,\ I(ITS_{i+1} : SOC)], \end{cases} \quad (1)$$

де $I(ITS_{i+1} :SOC) = F_{SOC}[I(ITS_i :SS)]$ – це взаємозв'язок між командою на протидію з інформацією від сенсору безпеки (всі інформаційні об'єкти - кінцеві бітові множини);

$F_{SOC}[\cdot]$ – це оператор відображення, який на основі прийнятої інформації і по заданому правилу прийняття рішення формує команду про перехід в інший стан;

$F_A[.]$ – це оператор відображення, який на підставі прийнятої команди переводить об'єкт управління з одного стану в інший.

Отримані результати графічної і математичної формалізації дозволяють математично представити процес протидії кібератакам *(Protection Process,* траєкторія поведінки *COPS)* у вигляді множини :

$$PP=\{COPSi\},\ i=1,\ ...,\ I. \quad (2)$$

де, *PP* – це кінцева множина, що складається з кінцевих підмножин *COPSi* (відповідних фаз кібернетичної системи оперативного захисту);

I(ITSi+1 :SOC) = [ITSi, I(ITSi :SS), I(ITSi+1 :SOC)] – підмножина *(COPSiPP),* що складається з кінцевих бітових наборів (множин). Дві суміжні фази *COPS* пов'язані між собою системою рівнянь (1);

i – номер поточної фази *ITC; I* - кількість фаз управління захистом*, i=1, …, I.*

За допомогою такої математичної формалізації вдалося представити процеси протидії атакам в системі захисту у вигляді послідовності фаз кібернетичної системи. Кожна фаза – це послідовність регулярно повторюваних дій, які можна назвати процедурами захисту. Часові межі кожної фази визначаються моментами детектування подій безпеки. Під новим станом слід розуміти зміни в ІТС, що впроваджуються актуаторами безпеки (*засобами IDS*) на основі команд від *SOC* (відповідей на події безпеки). В рамках розробленої моделі (див. рис. 3) представлений формалізований опис взаємодії процесів розвідки кіберзагроз та процесів протидії кібератакам. Процеси розвідки кіберзагроз є первинними для виконання процесів протидії атакам (інформація про *IOCs* потрібна для сенсорів безпеки (засобів *IDS).*

В межах розглянутих аспектів (рівнів взаємодії) доцільно визначити наступні задачі вдосконалення інформаційної та кібернетичної безпеки ОКІ:

Розробка та прийняття необхідних нормативних документів, а саме:

Переліку об’єктів критичної інфраструктури держави;

Плану заходів щодо реалізації Стратегії кібербезпеки України;

Протоколу спільних дій основних суб’єктів забезпечення кібербезпеки, суб’єктів кіберзахисту та власників (розпорядників) об’єктів критичної інформаційної інфраструктури під час попередження, виявлення, припинення кібератак та кіберінцидентів.

Організаційне узгодження діяльності суб’єктів забезпечення інформаційної та кібернетичної безпеки об’єктів критичної інфраструктури, а саме:

розробка відомчих документів щодо визначення вимог до кіберзахисту ОКІ;

визначення повноважень посадових осіб (введення підрозділів), відповідальних за забезпечення інформаційної та кібернетичної безпеки;

визначення порядку ведення та використання державного реєстру кіберінцидентів.

Технічне (технологічне) забезпечення інформаційної та кібернетичної безпеки об’єктів критичної інфраструктури:

створення систем (підсистем) забезпечення безпеки ОКІ згідно вимог нормативних та відомчих документів;

визначення показників забезпечення інформаційної та кібернетичної безпеки об’єктів критичної інфраструктури;

адаптація (розробка) засобів управління інформацією і подіями безпеки (*SIEM*) відповідним вимогам;

формалізація підходів керування ОКІ з врахуванням вимог відомчих документів (на прикладі вимог визначених) [11].

Висновки. Управління інформаційною та кібернетичною безпекою об’єктів критичної інфраструктури ґрунтується на знаннях про стан об’єктів управління, стан середовища функціонування і про впливи, які відбуваються. Ефективну інформаційну та кібербезпеку можливо забезпечити лише шляхом комплексної реалізації низки правових, організаційних, технічних, наукових заходів, кадрового та ресурсного забезпечення на національному та відомчому (з врахуванням особливостей та специфіки діяльності в основних сферах діяльності держави) рівнях. В статті розглянуто становлення сфери забезпечення кібербезпеки в Україні та її імплементація зі сферами захисту інформації та інформаційної безпеки. Визначено задачі вдосконалення інформаційної та кібернетичної безпеки об’єктів критичної інфраструктури. Подальші дослідження доцільно спрямувати на адаптацію математичного апарату для оцінювання вимог кіберзахисту та кібербезпеки, які визначені у [8, 11] з метою повноцінного врахування визначених організаційних та технічних аспектів функціонування об’єктів критичної інфраструктури, а також реагування на атаки в режимі реального часу.

ЛІТЕРАТУРА

1. Методика оцінки кіберстійкості об’єктів критичної інфраструктури / Гончар С. Ф., Комаров М. Ю. // Безпека соціально-економічних процесів в кіберпросторі: матеріали

Всеукр. наук.-практ. конф. (Київ, 27 берез. 2019 р.). – Київ: Київ. нац. торг.-екон. ун-т, 2019. – с. 49.

2. Кібербезпека держави: час перезавантаження. Радіо Свобода 27 червня, 2017 [Електронний ресурс]. – Режим доступу: http://safe-city.com.ua/kiberbezpeka-derzhavy-chas-perezavantazhennya/.

3. Стратегія забезпечення кібербезпеки в гібридній війні [Електронний ресурс]. – Режим доступу: //lexinform.com.ua/dumka-eksperta/strategiya-zabezpechennya-kiberbezpeky-v-gibrydnij-vijni/].

4. Закон України "Про основні засади забезпечення кібербезпеки України". [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua /laws/show/2163-19.

5. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" (із змінами). [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94.

6. Указ Президента України "Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року №96/2016 "Про Стратегію кібербезпеки України".

7. Постанова Кабінету Міністрів від 23 серпня 2016 р. № 563 "Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави".

8. Постанова Кабінету Міністрів України від 19 червня 2019 р. № 518 "Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури".

9. Пентестінг як інструмент комплексної оцінки ефективності захисту інформації в розподілених корпоративних мережах. / Бурячок В.Л., Козачок В.А., Бурячок Л.В., Складанний П.М. // Сучасний захист інформації No3, 2015.

10. СОУ Н НБУ 65.1 СУІБ 1.0:2010. Настанова. Методи захисту в банківській діяльності. Система управління інформаційною безпекою. [Електрон. ресурс]: – Режим доступу: http://www.uk.xlibx.com/4yuridicheskie/ 1354389-1-sou-nbu-651-suib-10-2010-standart-organizacii-ukraini-nastanova-metodi-zahistu-bankivskiy-diyalnosti-siste.php.].

11. Постанова Правління Національного банку України від 28.09.2017 року № 95 "Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України" [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/v0095500-17.

12. Киричок Р.В., Тест на проникнення як імітаційний підхід до аналізу захищеності корпоративних інформаційних систем, Сучасний захист інформації №2(34), 2018. С. 53-58.

13. Гнатюк С. Л., Кібербезпека в умовах розгортання четвертої промислової революції (Industry 4.0): виклики та можливості для України. Київ, Національний інститут стратегічних досліджень, 2019 [https://niss.gov.ua/doslidzhennya/informaciyni-strategii/kiberbezpeka-v-umovakh-rozgortannya-chetvertoi-promislovoi].

14. Система кібербезпеки в Україні: реальність чи міф? Константин Корсун, 2018 [Електронний ресурс]. – Режим доступу: https://www.slideshare.net/.

15. Яковів І. Базова модель інформаційних процесів та поведінки системи кіберзахисту / Information Technology and Security. July-December 2019. Vol. 7. Iss. 2 (13) c.183 – 196.

16. Яковив И. Базовая модель информационных процессов управления и критерии безопасности кибернетической системы / Information Technology and Security. January-June 2015. Vol. 3. Iss. 1 (4) c.68-74.

17. Моделювання роботи адаптивної системи розпізнавання кібератак в умовах неоднорідних потоків запитів в модулях e-business / В. Лахно, Т. Петренко, М. Пирог // Безпека інформації. – 2016. – Т. 22, № 2. – С. 135-142. [Електронний ресурс]. – Режим доступу: http://nbuv.gov.ua/UJRN/bezin_2016_22_2_6.

18. Вдосконалення кіберзахисту інформаційних систем за рахунок адаптивних технологій розпізнавання кібератак / В.Лахно, А.Терещук, Т.Петренко //Захист інформації, Том 18, № 2, стор. 99 – 106.