УДК 621.396 **Боярчук Р.М., Савченко В.А., Мацько О.Й., Новікова І.В.**
DOI: 10.31673/2409-7292.2020.010610

МОДЕЛЬ ТРАНСФОРМАЦІЇ НАЦІОНАЛЬНОЇ СИСТЕМИ КІБЕРБЕЗПЕКИ В УМОВАХ ДІЇ ГІБРИДНИХ ЗАГРОЗ

У статті розглядається підхід щодо формування робочого плану трансформації національної системи кібербезпеки України. Основний ідея наведеної методології базується на використанні комбінованої моделі оцінки ризику та досвіду попередніх трансформацій з урахуванням існуючих процесів управління в окремих організаціях. Застосування експертного підходу дозволяє встановити пріоритетність портфеля можливих ініціатив, вибираючи ті, які мають найвищий потенційний вплив стосовно необхідних інвестицій та зусиль. Особливості моделі полягають у її застосовності в умовах фінансових та часових обмежень щоб забезпечити ефективне використання ресурсів компаній та дієвість рекомендацій. У результаті застосування моделі передбачається одержання плану з комплексом заходів, які слід здійснити для зменшення ризику порушення безпеки як для окремого підприємства, так і для національної системи в цілому.

Ключові слова: Кібербезпека, кібератака, трансформація, гібридні загрози, ризик

Вступ

На сьогодні Кібербезпека є тією актуальною проблемою, якій приділяється значна увага як серед ІТ-фахівців, так і серед широкої громадськості. Переважно це пов’язано зі зростаючою небезпечністю кібератак та їх наслідків, які вважаються одним з 5-ти найбільш серйозних глобальних ризиків поряд з надзвичайними природними явищами та катастрофами [1]. Аналіз динаміки втручання у кіберпростір свідчить, що кількість атак щороку збільшується на 34 % [2], а їх потужність на сьогодні може охоплювати сотні країн одночасно, як було у випадку WannaCry, Petya та ін. [3].

Периметр кібербезпеки типової організації є достатньо значним і потребує багато зусиль для організації ефективного захисту, у той час як для зловмисника достатньо лише одних “незачинених дверей” щоб проникнути у систему. Крім того, середній час виявлення ознак атаки може сягати декількох місяців [4], а багато атак довгий час залишаються взагалі непоміченими. Усе це ще більш ускладнюється у випадку організації безпеки групи підприємств державного сектору, який включає тисячі об’єктів, захист яких повинен координуватися та контролюватися централізовано.

Безпека критичної інфраструктури України забезпечується системою, до якої, за низкою документів 2015 – 2017 р.р. входять органи державного управління та силові структури, у складі яких за останні роки розгорнуто цілу мережу профільних центрів безпеки та реагування на різноманітні кіберінциденти. Причинами низки APT-атак, спрямованих на збір інформації з обмеженим доступом та виведення з ладу об’єктів критичної інфраструктури України були і здебільшого залишаються використання переважною більшістю українських державних організацій неліцензійного програмного забезпечення та низький рівень безпеки внутрішніх інформаційно-комунікаційних мереж на підприємствах та в організаціях, що належать до об’єктів критичної інфраструктури [5].

Загальний рівень фінансування заходів кібербезпеки на рівні держави постійно збільшується [6], проте їх розпорошеність та неузгодженість часто приводить до нераціонального використання коштів, що, само по собі не призводить до підвищення безпеки і відкриває додаткові можливості зловмисникам для подальших атак. Цьому також сприяє прогрес у нових технологіях. Так, Internet of Things (IoT), який передбачає підключення до 2023 року до 20 мільярдів пристроїв [7], створює умови для доступу через Google-подібні пошукові системи, такі як SHODAN, до будь-яких корпоративних мереж. Такі сервіси можуть мати доступ до сотень тисяч IoT-пристроїв, більшість з яких працює з незмінними паролями за замовчуванням та не передбачає жодних оновлень прошивки [8]. Як передбачається, зловмисні дії і у подальшому будуть націлені на енергетичні компанії та стратегічні підприємства країни, що вимагає передбачення та адекватного планування заходів захисту, в т.ч. і економічних.

Традиційно планування трансформації системи кібербезпеки держави у відповідності до поточних викликів та нових загроз здійснюється вищим керівництвом системи кібербезпеки (рівень Національного координаційного центру кібербезпеки), які часто у процесі роботи вирішують багато інших поточних питань. У такому випадку довготривалі стратегічні рішення можуть бути знівельовані або недооцінені з точки зору дії довготривалих загроз. Тому така система розгляду та ухвалення рішень потребує додаткового контролю з боку системи вищого рівня (РНБО України) з акцентом на доцільності фінансування тих чи інших програм та заходів.

Метою цієї статті є запропонувати модель трансформації національної системи кібербезпеки, яка грунтується на процесах планування з урахуванням потенційних гібридних загроз об'єктам критичної інфраструктури України.

Виклад основного матеріалу

1. Планування трансформації системи кібербезпеки

При підвищенні рівня загрози чи ускладненні потенційних кібератак компанії, як правило, вимушені збільшувати витрати на захист своїх ресурсів. За підрахунками аналітиків світові витрати на кібербезпеку у 2019 році склали 124 млрд дол. США, що на 12.4 % більше, ніж у 2018 році [9]. Однак збільшення витрат не обов'язково призводить до покращення рівня безпеки, оскільки заходи безпеки можуть мати різну ефективність. Традиційна кібербезпека окремої організації зосереджена переважно на контролі виробничих процесів. Але при організації масштабних заходів безпеки для багаточисленних об'єктів інфраструктури, що є характерним для національного рівня, необхідно звертати увагу і на інші аспекти, включаючи організаційні (організаційна структура окремого підприємства) або характер управління (ролі та обов'язки персоналу).

Переважна більшість видатків на кібербезпеку орієнтована на розгортання брандмауерів, систем запобігання вторгненням чи систем ідентифікації та контролю доступу, але, як часто буває, стандартні рішення часто не враховують особливості окремих підприємств та вплив цих особливостей на загальну систему кібербезпеки як підприємства, так і національної [10]. У такому середовищі трансформація системи національної кібербезпеки у якості відправної точки повинна враховувати наявний стан заходів безпеки в організаціях. Залежно від цього, у процесі трансформації необхідно буде відшукати баланс між технічними та організаційними заходами, які слід впроваджувати. Крім того, слід досягти балансу між довгостроковими та короткостроковими заходами щоб досягти максимуму результату при захисті від поточних загроз та закласти основу для загроз майбутніх.

Визначення базового підходу. Ключовий аспектом, необхідним для побудови ефективного плану трансформації системи кібербезпеки, – це повне розуміння поточного стану та характеру загроз як для для системи в цілому, так і для окремих її елементів. Це може бути досягнуто за допомогою двох різних підходів, залежно від наявної інформації щодо окремих елементів системи кібербезпеки [11]. Перший – ризикоорієнтований підхід, заснований на застосуванні моделей ризику, які базуються на більш детальній оцінці загроз, уразливості та наслідків і мають ймовірнісну основу. Це вимагає достатньо потужних зусиль щодо побудови окремих моделей і зазвичай зустрічається лише в розвинених організаціях з чітко відрегульованими виробничими процесами. Другий – це підхід, орієнтований на досвід і є більш поширеним завдяки легшій його реалізації. Він має певні обмеження, оскільки часто залежить від досвіду експертів, якого може не бути при протидії новим викликам та загрозам.

Ризикоорієтований підхід. Підхід на основі ризику – це методологія, яка вимагає від організації чітко визначати та оцінювати ризики, які їм загрожують. Це розуміння використовується для того, щоб зосередити зусилля та ресурси на вирішенні першочергових заходів щодо найвищих ризиків та реалізації належного захисту для інших ризиків. Для реалізації такого підходу у системі національної кібербезпеки необхідно створити та вести перелік потенційних загроз, уточнювати поточний стан уразливих об'єктів у мережевому

середовищі та розгорнути систему централізованого контролю за технологічними процесами критично важливих підприємств. Крім того, необхідно мати уявлення до яких наслідків можуть призвести ті чи інші дії зловмисників для того, що б можна було обчислити матеріальний збиток у випадку успішної реалізації атаки

$$\text{Ризик} = \text{Загрози} \times \text{Уразливості} \times \text{Наслідки} \quad (1)$$

У формулі (1) “загрози” та “уразливості” мають ймовірністну міру і означають ймовірність атаки на конкретний об’єкт інфраструктури та ймовірність успішної її реалізації відповідно. “Наслідки” виражаються, як правило, у матеріальній формі (грошових одиницях), що дозволяє в цілому оцінювати ризик у грошовій формі. Порівняння різноманітних заходів, які б знижували уразливість системи чи наслідки реалізації атаки дає змогу створити план трансформації, який би орієнтувався на максимальне зменшення ризику.

Емпіричний підхід. Підхід, орієнтований на досвід (емпіричний) є більш поширеним, хоча інколи і менш ефективним, оскільки залежить від рівня компетенції експертів. Ідея емпіричного підходу полягає у експертній оцінці ступеня захищеності окремого процесу, підрозділу чи організації в цілому та її стійкості до впливу кібератаки. Як правило використовуєтья 5-ти чи 10-ти бальна шкала, за якою ранжується захищеність об’єкта чи ефективність засобів захисту. Практична реалізація цього методу може бути достатньо широкою – як правило застосовуються опитувальники різних груп персоналу, які надають відповіді. При цьому таке оцінювання дозволяє визначити пріоритетні області, які потребують негайного вдосконалення.

2. Формування варіантів плану

Після початкової оцінки поточного стану системи національної кібербезпеки наступний крок включатиме порівняння окремих ризиків або показників експертних оцінок з моделлю всіх потенційних варіантів розвитку подій та заходів щодо захисту, які можуть бути рекомендовані. Це дозволить визначити, які дії і для якого сценарію необхідні, а також те, яким заходам слід надати найбільшого пріоритету, враховуючи існуючі обмеження.

Визначення базової моделі поведінки. Для визначення усього можливого переліку потенційних заходів необхідно визначити базову модель поведінки яка б включала операції та заходи захисту стосовно окремих підприємств з урахуванням їх особливостей. Найбільш очевидним вибором для такої моделі є загально визнані міжнародні та галузеві стандарти, такі як ISO 27001 та 27002, або NIST Cybersecurity Framework (CSF).

Визначення пріоритетності заходів. Вибравши базову модель необхідно розробити широкий спектр початкових заходів (ініціатив), який охоплював би декілька можливих сценаріїв, в яких може опинитися система національної кібербезпеки. Зразок набору ініціатив може включати в себе наступне:

інформування користувачів зі зворотним зв’язком у реальному часі;

встановлення спільного бачення та місії функції кібербезпеки відповідно до профілю діяльності підприємств та організацій;

запровадження необхідних рішень щодо управління мережевим доступом для об’єктів критичної інфраструктури.

Модель включає такі елементи для кожного з видів діяльності у базовому портфелі:

дієвий опис можливого розвитку подій (сценарії);

сфери кібербезпеки, на які діяльність системи захисту впливатиме найбільше;

оцінка часу, необхідного для впровадження заходів захисту;

послідовність/пріоритетність в межах кожної групи заходів локально (згідно з логікою заходів) та глобально (на основі загального впливу та взаємозалежності);

два індикатори високого рівня: що вважати «швидкою перемогою» (протягом місяця) або «довгостроковим починанням», та як здійснювати контроль впровадження;

орієнтовний вплив на початковий показник самооцінки після завершення усіх робіт;

маркери контролю окремих кроків для відслідковування поточного стану активності.

Поєднання вхідних даних та варіантів ініціатив призведе до того, що кожній діяльності буде присвоєно відповідний пріоритет у залежності від ступеня зменшення ризику чи покращення показника експертних оцінок. Це дозволяє врахувати той факт, що не кожному елементу необхідно досягти максимально можливого потенціалу зменшення ризику чи експертних оцінок задля ефективного використання ресурсів організацій та системи кіберзахисту в цілому.

3. Узагальнення та коригування плану трансформації

Завершальним етапом після завершення формування заходів та встановлення їх пріоритетності є коригування результатів та розробка рекомендацій таким чином, щоб зробити їх актуальними та корисними для системи національної кібербезпеки взагалі. Один із способів зробити це – встановити певні обмеження, щоб бажаний план був актуальним та реалістичним. Наприклад, якщо оцінити окремий елемент системи у 10 разів більше, ніж він є у дійсності, то будь-яка рекомендація щодо посилення захисту у подальшому не буде сприйматися серйозно і, тим більше, не буде реалізована. Однак, якщо визначити перелік першочергових дій, які були б найкращими у межах бюджетних обмежень, то це створило б міцне підгрунтя для швидкого подальшого розвитку системи кібербезпеки. По-друге, також важливо навести графічне подання плану трансформації з легкодоступними деталями, що буде мати вирішальне значення і дозволить виконавцям швидко зрозуміти суть діяльності.

Обмеження. Діяльність кожного підприємства у будь-який момент часу обумовлюється умовами середовища з різними обмеженнями та особливостями. Відтак, для формування дієвих рекомендацій необхідно враховувати наступні особливості організації:

розмір компанії та її роль у загальній системі кібербезпеки;

виділений бюджет підприємства на кібербезпеку;

розмір групи забезпечення кібербезпеки;

кількість сил та засобів, які можна задіяти одночасно;

потенційно-можливе зниження ризику (%) або покращення показника експертних оцінок (балів).

Зміни в організаціях за цими критеріями ще до початку трансформації дозволять досягти цільового стану усієї системи меншими зусиллями. Однак, іноді це не потрібно, оскільки необхідно спочатку зрозуміти наслідки того, що відбудеться після першої ітерації, перш ніж приступити до коригування усього плану.

Формування плану. У результаті застосування моделі повинен з’явитися часовий графік (діаграма), що пропонує перелік рекомендованих заходів, складених в послідовності з оцінкою трудовитрат (людино-годин), необхідних для його виконання. План може бути модифікований на основі використання раніше встановлених обмежень, які застосовуються в конкретній організації (підприємстві). Запропонований підхід до планування повинен бути систематизованим на основі ранжування заходів за багатьма параметрами, щоб встановити логічну послідовність заходів. Крім того, план має містити алгоритми для деталізованого планування за кожним з аспектів діяльності конкретного підприємства. Додаткова складність полягає в тому, що розробникам потрібно діяти в умовах невизначеності, яка залежить від часу, оскільки на початок планування достатньо складно визначити тривалість окремих заходів. За можливості, при достатньо великому наборі зразків для подальшої автоматизації процесу та покращення якості виводу може бути використаний алгоритм машинного навчання. Однак, при використанні лише ручного процесу планування валідація плану є ключовим фактором для забезпечення високої якості планування [12].

Такий алгоритм роботи може бути використаний як безпосередньо для планування на високому рівні трансформації національної системи кібербезпеки, так і для розробки планів для конкретних організацій та підприємств, зокрема критичної інфраструктури держави. На стадії деталізованого планування до плану можуть вноситись додаткові коригування.

Висновки

Кібербезпека на сьогодні залишається однією з найбільш актуальних проблем національного масштабу. Удосконалення та трансформація системи національної кібербезпеки на сьогодні неможливі без цілісного розуміння масштабів та обсягів діяльності системи з застосуванням класичних методів, які є надто абстрактними та теоретичними. Ефективне удосконалення загальнонаціональної системи кібербезпеки можливе лише на основі поєднання ризико-орієнтованого та емпіричного підходів з урахуванням моделей діяльності окремих елементів системи. Передбачається, що деталізована розробка описаної методології та формування окремих елементів моделі дозволять скоротити час і зусилля на вирішення проблеми трансформації, особливо в умовах жорстких часових та ресурсних обмежень.

Перелік посилань

1. World Economic Forum (WEF), 2019. The Global Risks Report 2019, 14th Edition. Geneva, Switzerland. http://www3.weforum.org/docs/WEF_Global_Risks_ Report_2019.pdf.
2. Трофименко О. Кібербезпека України: аналіз сучасного стану / Олена Трофименко, Юлія Прокоп, Наталія Логінова, Олександр Задерейко // Захист інформації, Том 21, №3, липень-вересень 2019. – С. 150–157.
3. Картер О. У 2019 році зареєстровано більше 300 кіберінцидентів, пов'язаних з атаками на сайти органів влади України // Українські національні новини. Четвер, 23 січня 2020. https://www.unn.com.ua/uk/exclusive/1848123-u-2019-rotsi-zareyestrovano-bilshe-300-kiberintsidentiv-povyazanikh-z-atakami-na-sayti-organiv-vladi-ukrayini
4. Data Breach Investigations Report, 10th Edition, USA. Verizon, 2017. http://www.verizonenterprise.com/verizon-insightslab/dbir/tool/
5. Гібридні загрози Україні і суспільна безпека. Досвід ЄС і східного партнерства. Аналітичний документ. М.Гончар, А.Чубик, С.Жук, О.Чижова, Г.Максак, Ю.Тищенко, О.Зварич // Київ, 2018. – 106 с.
6. Шипілова Ю. Правова база української кібербезпеки: загальний огляд і аналіз / Юлія Шипілова // Міжнародна фундація виборчих систем в Україні, 2019. – 36 с.
7. Ericsson Mobility Report with Middle East and Africa Appendix, November 2017. https://www.ericsson.com/assets/local/mobilityreport/documents/2017/ericsson-mobility-reportnovember-2017-middle-east-and-africa.pdf
8. Rot A., Blaicke B., 2017. Internet of Things security. Selected threats and protection methods on the example of manufacturing systems, Publishing House of Czestochowa Technical University, Czestochowa, Poland.
9. Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019, United States. // Gartner Inc., 2018. https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartnerforecasts-worldwide-information-security-spendingto-exceed-124-billion-in-2019
10. Choi J., Kaplan J., Krishnamurthy, C., Lung, H. Hit or myth? Understanding the true costs and impact of cybersecurity programs. 2017. https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/hitor-myth-understanding-the-true-costs-and-impact-ofcybersecurity-programs
11. Rot A., Blaicke B. Towards Automated Modelling of Large-scale Cybersecurity Transformations: Potential Model and Methodology / Artur Rot a and Bartosz Blaicke // ICEIS 2019 – 21st International Conference on Enterprise Information Systems. – P. 345–350.

Кольцов М., Аушев Є. Пропозиції до політики щодо реформування сфери кібербезпеки в Україні сфери кібербезпеки в Україні (Policy Paper) / Кольцов Михайло, Єгор Аушев // Лабораторія законодавчих ініціатив. – Грудень, 2017. – 32 с.

Надійшла: 09.01.2020 Рецензент: д.т.н., професор Вишнівський В.В.