https://www.sworldjournal.com/index.php/swj/article/view/swj09-01-025
DOI: 10.30888/2663-5712.2021-09-01-025

УДК 004.056

DEFINING REQUIREMENTS TO DEVELOP INFORMATION SECURITY CONCEPT N HYBRID THREATS CONDITIONS. PART 4

ВИЗНАЧЕННЯ ВИМОГ ЩОДО ПОБУДОВИ КОНЦЕПЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ. ЧАСТИНА 4

Borsukovskyi Y.V. / Борсуковський Ю. В.
c.t.s., as.prof. / к.т.н., доц.
ORCID ID 0000-0003-1973-2386
Haidur H.I. / Гайдур Г. І.
d.t.s., prof. / д.т.н., проф.
ORCID ID 0000-0003-0591-3290
State University of Telecommunications, Kyiv, Ukkraine, Solomenska street, 7. 03110
Державний університет телекомунікацій, Київ, Україна, вул. Солом'янська, 7, 03110

Анотація. *В роботі розглянуто базові елементи, щодо формування окремих розділів концепції інформаційної безпеки бізнес-структур та державних організацій. Сформульовані вимоги щодо визначення подальших складових елементів при розробці концепції інформаційної та кібернетичної безпеки в умовах гібридних загроз, а саме рекомендований розподіл відповідальності і порядок взаємодії щодо питань інформаційної безпеки та порядок класифікації інформації що захищається. Визначений перелік робіт щодо захисту інформації, організаційні міри щодо забезпечення інформаційної безпеки, шляхи контролю захищеності інформаційних активів, порядок запобігання, виявлення, реагування та розслідування порушень інформаційної безпеки. Визначено порядок класифікації інформації, що захищається, надано орієнтовний перелік інформаційних активів, які повинні бути класифіковані та внесені до переліку інформації з обмеженим доступом.*

Ключові слова: *загрози, ризики, класифікація, кібербезпека, стратегія, концепція.*

Вступ

В перших частинах публікацій [4-6] були розглянуті визначення термінів, структура, загальні положення, опис об'єкта захисту, основні принципи забезпечення інформаційної безпеки, організаційна структура служби інформаційної безпеки, організація робіт щодо захисту інформації, а також заходи управління інформаційною безпекою щодо побудови концепції інформаційної безпеки в умовах гібридних загроз. Далі розглянемо рекомендований розподіл відповідальності і порядок взаємодії щодо питань інформаційної безпеки та порядок класифікації інформації що захищається [1-3,7].

Аналіз останніх публікацій

Геополітична напруженість та глобальні технологічні ризики продовжують негативно впливати на економічний потенціал технологій наступного покоління і призводять до серйозних інцидентів як в глобальному бізнесі так і в сфері персональних даних. Тільки в 2019-2021 ми бачимо значний ріст інформаційних та кібернетичних загроз, реалізація яких призводять до значних фінансових збитків. Згадаємо тільки найгучніші події 2021 року - Європейське агентство лікарських препаратів (EMA) заявило, що хакери опублікували в мережі дані про ліки і вакцини від COVID-19, що отримані ними в кінці 2020 року – акції Pfizer впали в ціні на 2,2%, витік даних з американського сайту

знайомств MeetMindful - 2,28 млн були опубліковані в загальному доступі на хакерському форумі, що містили не тільки реальні імена і профілі на Facebook, але і такі конфіденційні дані, як електронна пошта та адреса проживання, атака на нафтопровід Colonial Pipeline, який на 45% забезпечує пальним Східне узбережжя США – заплачений викуп в 5 млн.дол. США (частину викупу вдалось повернути завдяки роботі спецслужб) та інші інциденти подібного характеру. Все це загальні тенденції успішних реалізацій ризиків сучасного технологічного суспільства [8].

Результати дослідження

Розподіл відповідальності і порядок взаємодії. Відповідальним за розробку заходів і контроль над забезпеченням захисту інформації є керівник служби інформаційної безпеки (СлІБ) Організації.

Фахівцями СлІБ здійснюються такі види робіт із захисту інформації:

1. Планування і реалізація організаційних заходів щодо забезпечення інформаційної безпеки (ІБ), включаючи:
   - Аналіз і управління інформаційними ризиками.
   - Розробку, впровадження, контроль виконання та підтримання в актуальному стані політик, керівництв, концепцій, процедур, регламентів та інших організаційно-розпорядчих документів щодо забезпечення ІБ.
   - Розробку планів заходів щодо підвищення рівня ІБ Bi3S Організації.
   - Навчання користувачів інформаційних систем Bi3S Bi3S Організації, з метою підвищення їх обізнаності в питаннях ІБ.
2. Контроль захищеності ІТ інфраструктури Організації від загроз ІБ шляхом:
   - Проведення аудиту безпеки активів інформаційної системи (ІС) Організації.
   - Контролю виконання правил затверджених політик безпеки адміністраторами та користувачами корпоративної мережі.
   - Контролю доступу до мережевих ресурсів.
3. Запобігання, виявлення, реагування та розслідування порушень ІБ шляхом:
   - Аналізу і моніторингу журналів аудиту критичних компонентів корпоративної мережі, включаючи активне мережеве обладнання, МЕ, сервери, робочі станції і т.п.
   - Моніторингу мережевого трафіку з метою виявлення мережевих атак.
   - Контролю процесу створення нових облікових записів користувачів і надання доступу до ресурсів корпоративної мережі.
   - Опитування користувачів і адміністраторів інформаційних систем.
   - Впровадження та експлуатації спеціалізованих програмних і програмно-технічних засобів захисту інформації.
   - Координації діяльності всіх структурних підрозділів Організації по підтримці режиму допустимих ризиків ІБ.
4. У розробці та погодженні організаційно-розпорядчих та нормативних

документів щодо захисту інформації, включаючи складання переліків інформаційних активів підлягають захисту, також беруть участь наступні підрозділи Організації:

- Служба безпеки.
- Служби ІТ.
- Юридичний департамент.
- Відділ кадрів.
- Функціональні підрозділи, в яких обробляється інформація і яка потребує захисту.

5. Кваліфікаційні вимоги, що пред'являються до співробітників підрозділів, що відповідають за забезпечення ІБ, містяться в посадових інструкціях. Фахівці повинні проходити регулярну перепідготовку і навчання.

6. Надання, зміна, скасування і контроль доступу до ресурсів корпоративної мережі проводиться співробітниками ЗВТ виключно за затвердженими СлІБ заявками відповідно до політики управління доступом до ресурсів мережі Організації.

7. Співробітники ЗВТ відповідають за здійснення налаштування параметрів безпеки серверів і робочих станцій корпоративної мережі відповідно до затверджених корпоративними стандартами, що визначають необхідні рівні забезпечення безпеки для різних структурних і функціональних компонентів корпоративної мережі. СлІБ відповідає за розробку відповідних специфікацій і рекомендацій по налаштуванню параметрів безпеки, а також за здійснення контролю їх виконання.

8. Створення зовнішніх підключень корпоративної мережі до мережі Інтернет та інших зовнішніх мереж, надання співробітникам Організації віддаленого доступу до корпоративної мережі та організація VPN-каналів зв'язку здійснюється співробітниками служби ІТ з дотриманням вимог інформаційної безпеки, що визначаються політикою управління інформаційною безпекою при взаємодії з мережею Інтернет та політикою забезпечення безпеки віддаленого доступу до корпоративної мережі Організації.

9. При взаємодії зі сторонніми організаціями у випадках, коли співробітникам цих організацій надається доступ до ІзОД або до ІС Організації, з цими організаціями має бути укладена службою ІТ угода про конфіденційність і угода про дотримання режиму ІБ при виконанні робіт в ІС Організації. Підготовка типових варіантів цих угод здійснюється СлІБ спільно з юридичним департаментом.

Порядок класифікації інформації що захищається

Класифікуються категорії інформаційних активів, що містять інформацію з обмеженим доступом (ІзОД), і які підлягають захисту в Організації:

- ✓ Відомості, що становлять конфіденційну інформацію Організації.
- ✓ Відомості, що становлять комерційну таємницю Організації.
- ✓ Відомості, що становлять інформацію для службового користування Організації.
- ✓ Персональні дані співробітників Організації.

- ✓ Конфіденційна інформація (включаючи строго конфіденційну інформацію, комерційну таємницю, інформацію для службового користування і персональні дані), що належить третій стороні.
- ✓ Дані, критичні для функціонування ІС Організації і роботи бізнес підрозділів.

Перші п'ять категорій інформації представляють собою відомості обмеженого поширення, для яких в якості основної загрози безпеці розглядається порушення конфіденційності інформації шляхом розкриття її вмісту третім особам, які не допущені в установленому порядку до роботи з цією інформацією.

До останньої категорії «критичних» даних, відносяться інформаційні ресурси Організації, порушення цілісності або доступності яких може привести до збоїв функціонування ІС або бізнес підрозділів Організації.

Предметом захисту ІзОД є все, властиві бізнесу Організації особливості і деталі комерційної діяльності, ділові зв'язки, закупівля сировини і товарів, відомості про постачальників, передбачуваного прибутку, методики встановлення цін і ін.

В першу чергу до ІзОД відносяться:

- Відомості за структурою і власників.
- Відомості щодо забезпечення загальної безпеки.
- Відомості, що становлять комерційну таємницю.
- Відомості, що містять персональні дані.
- Відомості фінансового і економічного характеру.
- Знання і досвід в області реалізації продукції і послуг.
- Відомості про кон'юнктуру ринку, маркетингові дослідження.
- Відомості щодо зовнішньої діяльності та взаємовідносинам.
- Відомості про виробничі процеси.
- Аналіз конкурентоспроможності продукції та послуг.
- Інформація про споживачів, замовників і посередників.
- Банківські відносини, кредити, позики, борги.
- Знання найбільш вигідних форм використання грошових коштів, цінних паперів, акцій, капіталовкладень.
- Зведені бухгалтерські та фінансові звіти.
- Передбачувані обсяги комерційної діяльності, матеріали договорів (умови, реалізація, порядок передачі продукції).
- Списки клієнтів і ділове листування.
- Ціни і розцінки, форми і види розрахунків.
- Відомості про системи автоматизації, зв'язку і технічних засобах і т.д.

Правила віднесення інформації до категорій інформації з обмеженим доступом та порядок роботи з документами, складовими ІзОД, визначаються положенням про інформацію з обмеженим доступом і порядком захисту інформаційних активів в Організації, що повинен бути розроблений і затверджений керівництвом Організації.

Підходи до вирішення проблеми захисту інформації в Організації, в

загальному вигляді, зводяться до виключення неправомірних або необережних дій з відомостями, що відносяться до інформації обмеженого поширення, а також з інформаційними ресурсами, які є критичними для забезпечення функціонування бізнес процесів Організації. Для цього в Організації виконуються наступні заходи:

- Визначається порядок роботи з документами, зразками виробами та ін., що містять інформацію з обмеженим доступом.
- Розробляються правила класифікації інформації, що дозволяють відносити її до різних видів відомостей, що містять ІзОД, і визначати ступінь її критичності для Організації.
- Встановлюється коло осіб і порядок доступу до подібної інформації.
- Розробляються заходи щодо контролю поводження з документами та даними, що містять ІзОД.
- У трудові договори з працівниками включаються зобов'язання про нерозголошення відомостей, що містять ІзОД, і визначаються санкції за порушення порядку роботи з ними і за їх розголошення.

Форма підписки про нерозголошення ІзОД повинна міститися в трудовому договорі, який підписується усіма співробітниками Організації при прийомі на роботу.

Захист конфіденційної інформації, що належить третій стороні, здійснюється на підставі договорів, що укладаються Організацією з іншими бізнес-структурами.

Персональні дані працівника - інформація, необхідна роботодавцю у зв'язку з трудовими відносинами і що стосується конкретного працівника.

Відповідно до чинного законодавства, захист персональних даних працівника від неправомірного їх використання або втрати повинна бути забезпечена роботодавцем за рахунок його коштів в порядку, встановленому законом.

Відповідно до чинного законодавства при передачі персональних даних працівника роботодавець повинен дотримуватися таких вимог:

– Здійснювати передачу персональних даних працівника в межах однієї організації відповідно до локальних нормативних актів організації, з яким працівник повинен бути ознайомлений під розписку.

– Дозволяти доступ до персональних даних працівників тільки спеціально уповноваженим особам, при цьому зазначені особи повинні мати право отримувати тільки ті персональні дані працівника, які необхідні для виконання конкретних функцій.

Відповідно до чинного законодавства особи, які винні в порушенні норм, що регулюють отримання, обробку та захист персональних даних працівника, несуть дисциплінарну, адміністративну, цивільно-правову або кримінальну відповідальність відповідно до чинних законів.

В організації повинен бути документально оформлений «Перелік відомостей, що становлять ІзОД». Всі працівники повинні бути ознайомлені з цим переліком в частині що їх стосується.

Відповідальність за визначення та включення до «Переліку відомостей, що

становлять ІзОД» відомостей, які становлять інформацію з обмеженим доступом, несуть керівники підрозділів в частині яка їх стосується.

Відповідальність за підтримання в актуальному стані зведеного «Переліку відомостей, що становлять ІзОД» несе керівник СлІБ.

Зрозуміло, що вимоги які сформульовані вище носять орієнтовний та рекомендаційний характер і в кожному конкретному порядку повинні формулюватися та уточнюватися відповідно до результатів оцінки ризиків конкретної Організації.

Висновки та перспективи подальших досліджень

Сучасні тренди кібербезпеки безпосередньо пов'язані з цілями і завданнями зловмисників.

Очевидно, що статистика росту числа успішних кіберзлочинів однозначно вимагає узагальнення кращих світових практик в визначенні шляхів ефективної та своєчасної протидії сучасним інформаційним та кібернетичним загрозам. Всі ці міри повинні бути орієнтовані в першу чергу на створення політик управління інформаційною безпекою, що відповідають сучасним викликам в галузі захисту інформації, а також і на підвищення обізнаності працівників Організації та працівників СлІБ щодо виникнення таких загроз та порядку застосування процедур оперативної протидії їм, якщо вони можуть нести значні фінансові збитки та можуть бути реалізовані в Організації тим чи іншим шляхом.

Враховуючи вищесказане, подальші дослідження варто зосередити на таких складових частинах концепції політики ІБ як:

- формуванні вимог щодо побудови моделі загроз безпеці інформаційним активам організації;

- формуванні вимог щодо побудови моделі порушника безпеки систем ІТ та ІКБ.

Література

1. Борсуковський Ю.В., Борсуковська В.Ю., Бурячок В.Л. «Напрямки формування політик кібербезпеки для державного, банківського та приватного секторів», Modern Methodologies, Innovations, and Operational Experience on the Field of Technical Science: Conference proceedings, December 27-28, 2017, Radom, Republic of Poland, с. 8-11

2. Борсуковська В.Ю., Борсуковський Ю.В. «Безперервність бізнесу: новий тренд або необхідність», Економіка. Менеджмент. Бізнес. - 2017, №2(20), с.48-52

3. Борсуковський Ю.В., Бурячок В.Л., Борсуковська В.Ю. «Базові напрямки забезпечення кібербезпеки державного та приватного секторів», Сучасний захист інформації, - 2017, № 2(30), с. 85-89

4. Борсуковський Ю.В. «Визначення вимог щодо побудови концепції інформаційної безпеки в умовах гібридних загроз. Частина 1», Кібербезпека, освіта, наука, техніка, - 2019, №1(5), с. 61-72

5. Борсуковський Ю.В. «Визначення вимог щодо побудови концепції інформаційної безпеки в умовах гібридних загроз. Частина 2», Кібербезпека,

освіта, наука, техніка, - 2019, №2(6), с. 112-121

6. Борсуковський Ю.В. «Визначення вимог щодо побудови концепції інформаційної безпеки в умовах гібридних загроз. Частина 3», Кібербезпека, освіта, наука, техніка, - 2020, №4(8), с. 34-48

7. ДСТУ ISO/IEC 27000:2015. Інформаційні технології. Методи захисту. Система управління інформаційною безпекою (ISO/IEC 27000:2014 IDT).

8. Hackers Breached Colonial Pipeline Using Compromised Password. Режим доступу: https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password. [Перевірено: 21 вересня 2021]

Abstract. *The article considers the basic elements of the formation of separate sections of the concept of information security of business structures and government organizations. The article provides the further requirements for the definition of further components in the development of the concept of information and cyber security in the context of hybrid threats, namely the recommended division of responsibilities and the order of interaction on information security and the order of classification of protected information. The list of works on information protection, organizational measures to ensure information security, ways to control the security of information assets, the procedure for prevention, detection, response and investigation of information security violations are defined. The order of classification of the protected information is defined, the approximate list of the information assets which should be classified and included in the list of the information with limited access is given.*

Keywords: *threats, risks, classification, cyber security, strategy, concept.*

Стаття відправлена 22.09.2021 р.