КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (8), 2020
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2020.8.3448
УДК 004.056

Борсуковський Юрій Володимирович
кандидат технічних наук , професор кафедри інформаційної та кібернетичної безпеки
Київський університет імені Бориса Грінченка, Київ, Україна
ORCID: 0000-0003-1973-2386
Y.Borsukovskyi@kubg.edu.ua

ВИЗНАЧЕННЯ ВИМОГ ЩОДО ПОБУДОВИ КОНЦЕПЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ. ЧАСТИНА 3

Анотація. В даній статті розглянуто сучасні тренди кібербезпеки, безпосередньо пов'язані з цілями і завданнями зловмисників. Наведено оцінки глобальних технологічних ризиків, що обговорювались під час роботи Всесвітнього економічного форуму 2020. Розглянуто оцінки щодо росту негативного впливу елементів геополітичної напруженості на економічний потенціал технологій наступного покоління. Шахрайство з даними і кібератаки відносять до пріоритетних ключових ознак в оцінках найбільш ймовірних глобальних ризиків, а атаки на інформаційну інфраструктуру відносять до ризиків кібератак у рейтингу найбільш ймовірних ризиків. Прогнозується, що кібератаки все частіше будуть використовуватися в якості непрямих конфліктів між країнами, які прагнуть розширити свої сфери впливу. В таких умовах питання кібербезпеки не можуть бути другорядним, чи питаннями, які потрібно вирішувати при виникненні прямих кіберзагроз сучасним інформаційним системам, системам IoT та SCADA. Очевидно, що потрібно переосмислення підходів до створення та розвитку сучасних інформаційних технологій і питання кібербезпеки повинні розглядатися як складові елементи при створенні сучасних інформаційних систем із моменту їх винайдення, проектування, на всіх стадіях виробництва і підтримки. Переорієнтування розробників інформаційних систем на створення інтегрованих технологічних платформ із складовими елементам кібербезпеки вимагає вивчення та впровадження нових підходів до їх розроблення, а також напрацювання світовою спільнотою відповідних стандартів та протоколів, що дозволить забезпечити безпечне функціювання інформаційних систем у світовій павутині. Сформульовані подальші базові вимоги до складових елементів при розробці концепції інформаційної та кібернетичної безпеки в умовах гібридних загроз, а саме рекомендована організаційна структура служби інформаційної безпеки та основні принципи організації робіт і заходи управління щодо інформаційного та кібернетичного захисту. Визначені завдання служби інформаційної безпеки, надано перелік базових заходів щодо захисту інформації, сформульовані завдання, що повинні забезпечуватися технічною інфраструктурою, заходи управління інформаційною безпекою організаційного рівня, заходи управління інформаційною безпекою процедурного рівня, заходи управління інформаційною безпекою програмно-технічного рівня та інші принципи забезпечення інформаційної безпеки при розробці концепції інформаційної безпеки в умовах гібридних загроз.

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

1. ВСТУП

Постановка проблеми. В перших частинах [5, 6] були розглянуті визначення термінів, структура, загальні положення, опис об’єкта захисту, основні принципи забезпечення інформаційної безпеки щодо побудови концепції інформаційної безпеки в умовах гібридних загроз. Далі послідовно розглянемо рекомендовану організаційну структуру служби інформаційної безпеки та основні принципи організації робіт і заходи управління щодо інформаційного та кібернетичного захисту Організації [2-4].

ISSN 2663 - 4023

Аналіз останніх досліджень і публікацій.

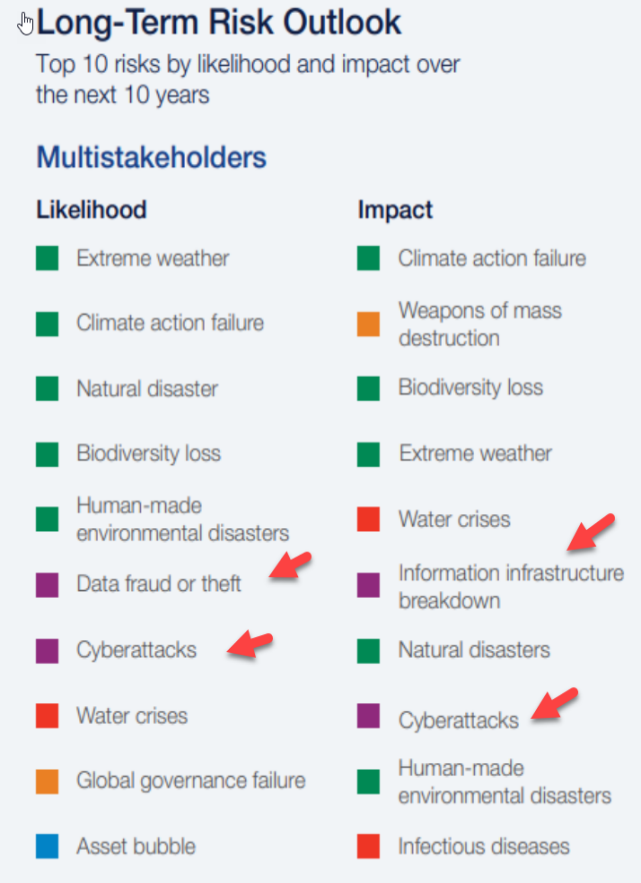

Рис. 1

У звіті про оцінки глобальних технологічних ризиків 2020, що були підготовлені до 50-го ювілейного Всесвітнього економічного форуму (ВЕФ) [1], обговорювались питання щодо розвитку нових технологій, таких, наприклад, як квантові обчислення, і як вони можуть трансформувати людські життя та світову економіку. Наряду із цим, світова спільнота повинна уже зараз прораховувати ті ризики щодо розвитку нових технологій, які вони принесуть в світову економіку, зробивши суспільство ще більш уразливим до кібератак.

Геополітична напруженість додатково буде негативно впливати на економічний потенціал технологій наступного покоління. Шахрайство з даними і кібератаки присутні як ключові ознаки в десятці найбільш ймовірних глобальних ризиків (шостий і сьомий відповідно), а інформаційна інфраструктура відноситься до пріоритетних ризиків кібератак у десятці найбільш ймовірних ризиків (шостий і восьмий відповідно) – Рис.1 – Рис. 3. Крім того, 76,1% респондентів очікують, що ризики кібератак збільшаться у 2020, що робить їх п'ятими за рейтингом найвищих ризиків у світі [1, 7, 8, 9].

За оцінками експертів, основні тенденції кібербезпеки в 2020 році будуть наступними [7, 14]:

Гібридні кібернетичні загрози (кібер-холодна війна) будуть посилюватися. Кібератаки все частіше будуть використовуватися в якості непрямих конфліктів між країнами, які прагнуть розширити свої сфери впливу.

Подальший розвиток і використання досягнень штучного інтелекту. Вибори в США у 2016 році ознаменувалися початком поширення підроблених новин на основі штучного інтелекту. Політичні кампанії виділяли ресурси на створення спеціальних команд, які організовували і поширювали неправдиві історії, щоб підірвати рейтинги своїх супротивників. Оскільки світ готується до великих виборів повсюдно в 2020 році, то можна очікувати, що такі методи знову будуть повторюватися.

ISSN 2663 - 4023

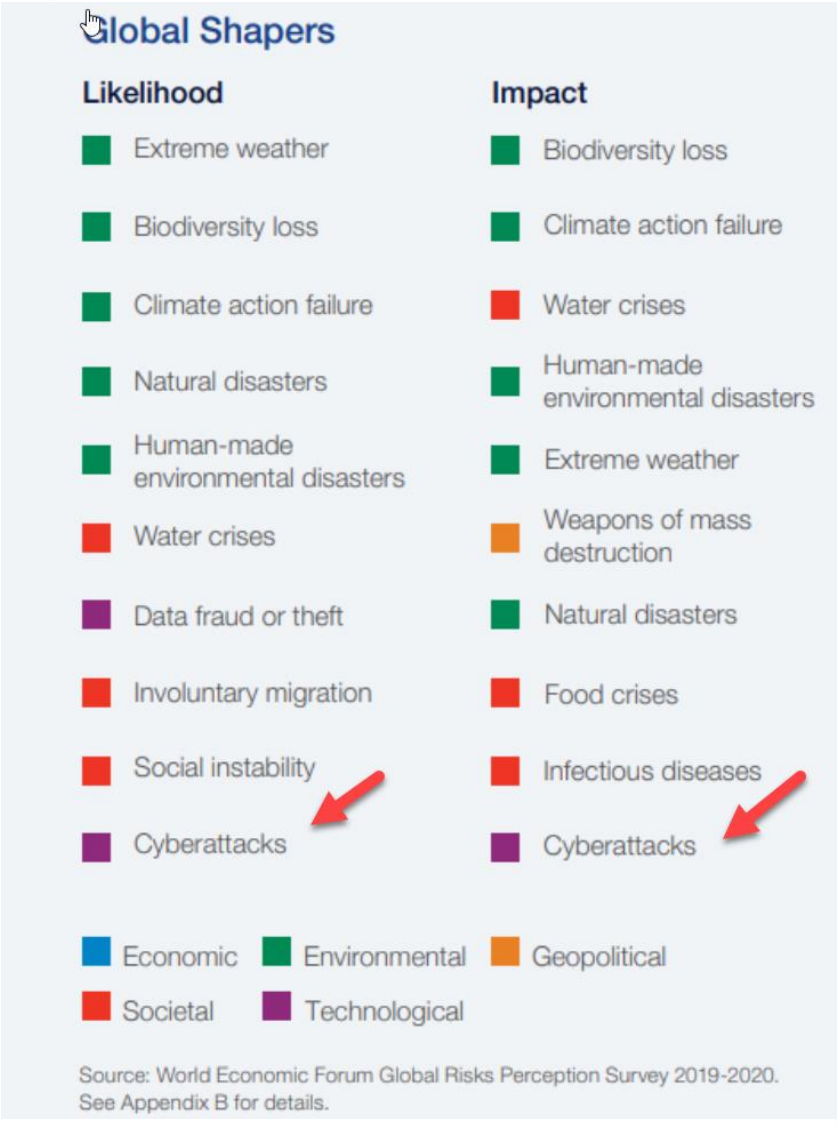

Рис. 2

Засоби зв'язку будуть використовуватися з більш наступальними цілями. Уявлення про те, що зв'язаність створює нові бойові ландшафти, підтверджується напрямками, що активно розвиваються у сфері сьогоднішніх і завтрашніх кібератак. Наприклад, в 2019 році зафіксований ріст на 50% зловмисних програм в мобільному банкінгу в порівнянні із 2018. Очевидно, що те, що використовується спільнотою найчастіше, може стати найбільш пріоритетним вектором в загальному ландшафті кібератак.

Розробки 5G мереж і впровадження пристроїв інтернету речей (IoT) будуть підвищувати вразливість до атак. У міру розгортання мереж 5G використання підключених пристроїв IoT різко прискориться. Це значно підвищить вразливість мереж до великомасштабних, багатовекторних кібератак п'ятого покоління.

Організації переосмислять свій підхід до хмарних технологій. Організації вже широко використовують хмарні сервіси для виконання більшості своїх робочих завдань, але рівень розуміння питань інформаційної безпеки в хмарі залишається низьким. Фактично, питання інформаційної безпеки стають запізнілою думкою при розгортанні хмарних технологій.

ISSN 2663 - 4023

В таких умовах питання кібербезпеки не можуть бути другорядними, чи питаннями які потрібно вирішувати при виникненні прямих кіберзагроз сучасним інформаційним системам Організації. Очевидно, що потрібно переосмислення підходів

Рис. 3

до створення та розвитку сучасних інформаційних технологій і питання інформаційної та кібербезпеки повинні розглядатися як складові елементи при створенні інформаційних систем, IoT та автоматизованих систем управління виробництвом, починаючи з моменту їх винайдення, проектування та на всіх стадіях виробництва і підтримки.

На думку Голови правління Fortinet Кена Се (Ken Xie) для досягнення такої інтеграції потрібно вирішити чотири фундаментальних завдання [7]:

1) **Забезпечити обмін інформацією в режимі реального часу.** Темпи розвитку цифрового світу продовжують експоненціально зростати. Щоб не відставати, фахівці з кібербезпеки повинні швидко реагувати на загрози і слабкі місця в системі інформаційної безпеки, перш ніж кіберзлочинці завдадуть удар.
2) **Забезпечити широке співробітництво в області кібербезпеки.** Ефективна кібербезпека повинна ґрунтуватися на принципах глибокої і широкої співпраці. Якщо організації або держави не будуть вчитися один у одного, то одні і ті ж атаки будуть без значних затрат знищувати існуючі структури кіберзахисту.
3) **Забезпечити створення і просування спільного бачення інтегрованої кібербезпеки.** Лідери державного і приватного секторів повинні взяти на себе зобов'язання створити спільне бачення ключових питань у розвитку кібербезпеки. Це бачення повинно бути орієнтовано не тільки на поточний ландшафт загроз, але і враховувати прогнози на можливі дії кіберзлочинців.
4) **Забезпечити використання інтегрованих технологічних платформ.** Для забезпечення кібербезпеки потрібні додаткові обчислювальні потужності.

Інформаційні технологічні платформи повинні мати та надавати цю додаткову обчислювальну потужність для забезпечення функціювання технологічних платформ безпеки. Такі інтегровані і керовані безпековими ризиками технологічні платформи повинні мати здатність розподіляти робочі навантаження за рівнями системи. Орієнтована на безпеку інтегрована технологічна платформа повинна оцінювати ризики кожного шляху в мережі і направляти трафік по найшвидшому і безпечному шляху. Очевидно, що при таких підходах всі мережеві пристрої повинні обмінюватися інформацією про швидкість і ризики для кожного мережевого шляху.

Переорієнтування розробників інформаційних систем на створення інтегрованих технологічних платформ із складовими елементам кібербезпеки вимагає вивчення та впровадження нових підходів до їх розроблення, а також напрацювання світовою спільнотою відповідних стандартів та протоколів, що дозволить забезпечити безпечне функціювання інформаційних систем у світовій павутині. Актуальність цих питань добре підтверджується опублікованим IC3 FBI США аналізом фінансових збитків від кіберзлочинів за 2019 рік [13].

2. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

2.1. Організаційна структура служби інформаційної безпеки

Для формалізації поняття можемо визначити термін «служба інформаційної безпеки» як керівний орган корпоративного управління інформаційною безпекою. Іншими словами – особа чи група осіб, яка відповідає за результативність та відповідність функціювання системи, яка забезпечує спрямованість та контрольованість дій з інформаційної безпеки Організації [10].

В ГОСТ 45.127-99 дано наступне визначення цього терміну - служба інформаційної безпеки (англ. Service of infosecurity) - організаційно-технічна структура системи забезпечення інформаційної безпеки, що реалізує вирішення певної задачі, спрямованої на протидію тій чи іншій загрозі інформаційної безпеки [11].

Дуже часто виникає питання підпорядкування Служби інформаційної безпеки в організаційній структурі Організації. На практиці найчастіше використовується дві схеми підпорядкування СлІБ – службі безпеки Організації або директору служби ІТ.

СлІБ, як частина служби безпеки. Одна із схем, що найбільш часто зустрічається. Логіка зрозуміла – питання безпеки, значить в підпорядкування до служби безпеки. З очевидних мінусів - різні напрямки, що практично не перетинаються. Керівництво служби безпеки Організації, як правило, колишні поліцейські, військові або співробітники СБ. Вони не знають специфіки і завдань ІТ та ІБ, а звідси витікають значні проблеми в комунікаціях та прийнятті рішень щодо питань інформаційної безпеки. Ці питання ускладнюються ще й тим, що керівництво служби безпеки повинно комунікувати із керівництвом ІТ, а це призводить до повного нерозуміння один одного. Як результат - мале фінансування СлІБ , опір будь-яким нововведенням. Із позитивних моментів – великі повноваження служби безпеки Організації, що дозволяє оперативно отримувати інформацію і прискорювати прийняття рішень.

СлІБ, як частина служби ІТ. Тут зразу виникає конфлікт інтересів. Один із напрямків роботи СлІБ це, зокрема, контроль за виконанням ІТ правил, приписів і регламентів. Очевидно, що керівництво ІТ не буде зацікавленим виносити недоліки в роботі ІТ на розгляд вищого керівництва. Як результат – фінансування по залишковому

принципу, ігнорування впровадження нових технологій безпеки. Із позитивних моментів – швидке впровадження нових систем, оскільки всі виконавці під рукою, прозора інтеграція систем інформаційної безпеки в інфраструктуру ІТ.

Ідеальна схема - це підпорядкування СлІБ першій особі – керівнику Організації (Правлінню або Наглядовій раді). Але така схема вимагає від першої особи виділення часу на комунікації із керівником СлІБ і необхідності вникати в питання управління інформаційною безпекою. Із позитивних моментів – окремий бюджет СлІБ, швидке прийняття необхідних рішень.

Для всіх варіантів, при обґрунтуванні місця СлІБ в структурі Організації треба враховувати те, що СлІБ безпосередньо прибуток не приносить і при розробці інвестиційних планів потрібно обґрунтовувати вигоду від нереалізованих ризиків. А чим більше ланок при узгодженні цих питань, тим важче і довше вони вирішуються, що є неприпустимим в умовах сучасних кіберзагроз.

Враховуючи вищесказане та усталені схеми управління, що прийняті в Організаціях, рекомендується вибирати компромісну схему, коли СлІБ одночасно підпорядковується першій особі і керівнику служби безпеки Організації – Рис. 4. Це дозволяє, на даному етапі управлінського розвитку Організацій, уникати частини конфліктів і забезпечувати швидкі комунікації з вищим керівництвом Організації в процесі оперативного управління системою інформаційної безпеки Організації.

Рис. 4. Рекомендований варіант підпорядкованості СлІБ

Відділи ІБ бізнес-підрозділів Організації адміністративно, функціонально і методично, у даній фукціональній схемі, підпорядковуються керівнику СлІБ Організації.

Служба ІТ та структурні бізнес-підрозділи Організації підпорядковуються керівнику СлІБ в частині питань інформаційної безпеки. CISO (Chief Information Security Officer) - керівник служби інформаційної безпеки несе головну

відповідальність за розробку і реалізацію політики безпеки компанії відповідно до реалізованих бізнес-процесів компанії і пріоритетного забезпечення питань неперервності бізнесу в частині питань інформаційної безпеки [3, 12].

На керівника СлІБ покладаються такі ключові завдання [12]:

- розробка політики в області ІБ, включаючи стандарти, процедури, регламенти, керівництва;
- розробка принципів класифікації інформаційних потоків і управління ними;
- аналіз ризиків, їх оцінка і прийняття;
- забезпечення персоналу всіх підрозділів настановами та знаннями по виконанню політики в області ІБ, організація відповідного навчання та інструктування;
- консультування менеджерів компанії і виконавчого персоналу в межах їх компетенції з питань інформаційних ризиків і захисту від них;
- узгодження всіх політик і регламентів з тим, щоб вони були успішно впроваджені на всіх рівнях компанії;
- діяльність у складі робочих груп або експертних рад, які оцінюють ризики при впровадженні нових технологій, модернізації виробництва, формуванні планів технічного оновлення чи інших змін бізнесу. Включення аспектів ІБ на всі етапи даних проектів;
- «Сполучна ланка» між службою якості і відділом ІТ/автоматизації з правом перевірки внутрішніх звітів служби якості;
- спільна робота зі службою безпеки в частині, що стосується їх обох, наприклад, науково-дослідні роботи (НДДКР) або пропускна система (бейджі, пропуски), розслідування інцидентів безпеки;
- спільна робота зі службою персоналу в частині, що стосується перевірки деяких даних при найму на роботу;
- в разі криз або надзвичайних подій в області захисту інформації брати участь разом з топ-менеджментом в управлінні кризовою ситуацією;
- забезпечення менеджменту компанії регулярними оглядами стану інформаційної безпеки, звітами про впровадження політики;
- інформаційна підтримка топ-менеджменту про зміни в законодавстві та технічні новинки, що мають відношення до інформаційної безпеки.

На службу ІБ Організації покладаються такі завдання:

- управління інформаційною безпекою та забезпечення відповідності нормативним вимогам;
- оцінка операційних ризиків Організації в частині ІБ;
- стратегічне планування розвитку ІБ Організації;
- вибір групових рішень в сфері ІБ Організації;
- забезпечення класифікації ІзОД;
- контроль за безпекою корпоративної мережі Організації;
- централізований моніторинг і запобігання несанкціонованого доступу до ІзОД;
- управління доступом до ІС Організації;
- контроль виконання стратегічної програми розвитку ІБ бізнес-підрозділами Організації;
- розробка політик і стандартів ІБ Організації;
- моніторинг подій безпеки та реагування на інциденти;
- узгодження планів розвитку і стандартів Організації з Наглядовою радою Організації.

На відділи ІБ бізнес-підрозділів Організації покладаються такі завдання:

- контроль впровадження і експлуатації систем ІБ в бізнес-підрозділах;
- управління системами ІБ в бізнес-підрозділах;
- контроль рівнів доступу до конфіденційної інформації, внесення пропозицій щодо доповнення або зміни переліку відомостей, що становлять ІзОД Організації;
- контроль за безпечною експлуатацією ІС і АСУТП;
- реагування на нештатні ситуації в ІБ;
- моніторинг і розслідування інцидентів на місцевому рівні;
- тренінг користувачів з питань ІБ.

Ці завдання можуть бути базовими при розробці організаційної структури СлІБ та формулюванні її завдань.

2.2. Організація робіт щодо захисту інформації

Організація і проведення робіт по забезпеченню ІБ Організації при її обробці технічними засобами визначаються цією Концепцією, діючими державними і міжнародними стандартами, а також іншими нормативними та методичними документами Організації.

Організація робіт по забезпеченню впровадження та підтримки працездатності засобів ІБ покладається на керівника ЗВТ (ІТ), що здійснює експлуатацію і супроводження ІС Організації, а методичне керівництво і контроль над ефективністю передбачених заходів захисту інформації - на керівника СлІБ.

Експлуатація ІС Організації здійснюється в повній відповідності до затвердженої організаційно-розпорядчої та експлуатаційної документації, з урахуванням вимог і положень, викладених у відповідних розділах політики безпеки.

Комплекс заходів щодо захисту інформації в Організації включає в себе наступні заходи:

- призначення ролей і розподіл відповідальності;
- розробка, реалізація, впровадження і контроль виконання планів заходів, політик безпеки та інших документів щодо забезпечення ІБ;
- підготовка користувачів і технічних фахівців до вирішення проблем, пов'язаних із забезпеченням ІБ;
- проектування, розгортання і вдосконалення технічної інфраструктури СУІБ;
- аудит ІБ Організації.

Технічна інфраструктура СУІБ призначена для вирішення наступних завдань:

- захист кінцевих точок;
- захист від руткітів і прихованих загроз;
- захист серверів;
- моніторинг і захист конфігурацій і цілісності файлів;
- захист віртуальних середовищ;
- захист мобільних пристроїв;
- захист баз даних;
- захист електронної пошти;
- забезпечення безпеки роботи з Веб;
- захист мережі і міжмережевих з'єднань;
- захист від мережевих вторгнень, DOS / DDOS атак;

- захист даних від втрати і витоків;
- сканування вразливостей серверів, кінцевих станцій і баз даних;
- сканування вразливостей веб додатків;
- аналіз та управління ризиками ІБ;
- збір та управління інцидентами ІБ (SIEM);
- неперервне оцінювання відповідності стандартам і нормативним актам.

2.3. Заходи управління інформаційної безпекою

1) Заходи управління інформаційною безпекою організаційного рівня

- СУІБ реалізується шляхом поєднання заходів організаційного та програмно-технічного рівнів.
- Організаційні заходи складаються із заходів адміністративного рівня і процедурних заходів захисту інформації.
- Основою заходів управління інформаційною безпекою адміністративного рівня, тобто заходів, що вживаються керівництвом Організації, є політика безпеки. Під політикою безпеки розуміється сукупність документованих управлінських рішень, спрямованих на захист інформації та асоційованих з нею активів.
- Політика безпеки визначає стратегію Організації в області ІБ, а також ту міру уваги і кількість активів, яку керівництво вважає за доцільне виділити.
- Політика безпеки Організації визначається цим документом, а також іншими нормативними та організаційно-розпорядчими документами Організації, що розробляються на основі цієї Концепції. До числа таких документів належать:
  - політика і методологія управління ризиками інформаційної безпеки;
  - політика інвентаризації інформаційних активів;
  - процедури застосування превентивних і коригуючих заходів;
  - антивірусна політика;
  - парольна політика;
  - політика управління доступом до ресурсів корпоративної мережі;
  - правила управління інформаційною безпекою при роботі користувачів в корпоративній мережі;
  - політика управління інформаційною безпекою при взаємодії з мережею інтернет;
  - політика забезпечення безпеки віддаленого доступу до корпоративної мережі;
  - політика резервного копіювання та відновлення даних;
  - політика аудиту інформаційної безпеки;
  - регламенти роботи служб адміністрування корпоративної мережі;
  - регламенти роботи з мобільними пристроями і з цифровими носіями конфіденційної інформації;
  - план забезпечення безперервності бізнесу і процедури аварійного відновлення;
  - процедура реагування на інциденти, пов'язані з порушенням інформаційної безпеки;

- положення про конфіденційність, інструкція щодо забезпечення режиму конфіденційності та перелік конфіденційних відомостей;
- інші організаційно-розпорядчі документи.

2) Заходи управління інформаційною безпекою процедурного рівня

- До процедурного рівня відносяться заходи безпеки, що реалізуються людьми. Виділяються наступні групи процедурних заходів, спрямованих на забезпечення інформаційної безпеки:
  - управління персоналом;
  - фізичний захист;
  - підтримка працездатності;
  - реагування на порушення режиму безпеки;
  - планування відновлювальних робіт.
- В рамках управління персоналом для кожної посади повинні існувати відповідність кваліфікаційним вимогам по інформаційної безпеки. До посадових інструкцій повинні входити розділи, що стосуються безпеки. Кожного працівника потрібно навчити заходам безпеки теоретично і відпрацювати виконання цих заходів практично.
- Безпека комп'ютерної системи залежить від оточення, в якому вона працює. Необхідно вжити заходів для захисту будівель і прилеглої території, що підтримує інфраструктуру, і самих комп'ютерів.
- При розробці СУІБ передбачається адекватна реалізація заходів фізичного захисту офісних будівель і інших приміщень, що належать Організації, за наступними напрямками:
  - фізичне управління доступом;
  - протипожежний захист;
  - захист підтримуючої інфраструктури;
- Передбачається також адекватна реалізація наступних напрямків підтримки працездатності:
  - підтримка користувачів;
  - підтримка програмного забезпечення;
  - конфігураційне управління;
  - резервне копіювання;
  - управління носіями;
  - документування;
  - регламентні роботи;
- Програма безпеки повинна передбачати набір оперативних заходів, спрямованих на виявлення і нейтралізацію порушень режиму безпеки. Важливо, щоб в подібних випадках послідовність дій була спланована заздалегідь, оскільки заходів потрібно буде вживати термінових і скоординованих.
- Реакція на порушення режиму безпеки переслідує дві головні цілі:
  - блокування порушника і зменшення нанесеної шкоди;
  - недопущення повторних порушень.
- У Організації повинен бути черговий співробітник, доступний 24 години на добу, що відповідає за реакцію на порушення. Всі повинні знати координати чергового співробітника і звертатися до нього при перших ознаках небезпеки.

- Планування відновлювальних робіт і проведення періодичних навчань дозволяє підготуватися до аварій, зменшити шкоду від них і зберегти здатність до функціонування хоча б у мінімальному обсязі.
- Механізми контролю, які є важливими для Організації з юридичної точки зору, включають в себе:
  - захист даних з обмеженим доступом;
  - охорону документів організації;
  - права на інтелектуальну власність.
- Відповідно до міжнародного стандарту ISO 17799 ключовими також є такі механізми контролю:
  - політика інформаційної безпеки;
  - розподіл відповідальності за забезпечення інформаційної безпеки;
  - навчання та тренінги з інформаційної безпеки;
  - інформування про інциденти безпеки;
  - управління безперервністю бізнесу.

3) Заходи управління інформаційною безпекою програмно-технічного рівня

- Програмно-технічні засоби захисту розташовуються на наступних рівнях (рубіжах):
  - захист зовнішнього периметра корпоративної мережі;
  - захист внутрішніх мережевих сервісів і інформаційних обмінів;
  - захист серверів і робочих станцій;
  - захист мережевих і комутаційних пристроїв;
  - захист SCADA, IoT систем;
  - захист WiFi мереж;
  - захист системних активів і локальних додатків на серверах і робочих станціях.
- На програмно-технічному рівні виконання захисних функцій в ІС здійснюється наступними сервісами безпеки:
  - ідентифікація / аутентифікація;
  - розмежування доступу;
  - протоколювання / аудит;
  - екранування та сегментація;
  - тунелювання;
  - шифрування;
  - контроль цілісності;
  - контроль захищеності;
  - управління.
- На зовнішньому рубежі розташовуються засоби виявлення шкідливої активності і контролю захищеності. Далі йдуть міжмережеві екрани, що захищають зовнішні підключення. Вони, разом із засобами підтримки віртуальних приватних мереж, що об'єднуються з міжмережевими екранами, утворюють периметр безпеки, що відокремлює корпоративну систему від зовнішнього світу.
- Сервіс активного аудиту (як і управління) повинен бути присутнім у всіх критично важливих компонентах і, зокрема, в захисних. Це дозволить швидко виявити атаку, навіть якщо з яких-небудь причин вона виявиться успішною.

- Управління доступом також має бути присутнім на всіх сервісах, функціонально корисних і інфраструктурних. Доступу повинна передувати ідентифікація і аутентифікація суб'єктів доступу (користувачів і процесів).
- Засоби шифрування і контролю цілісності інформації, що передається по каналах зв'язку, доцільно виносити на спеціальні шлюзи, де їм може бути забезпечено кваліфіковане адміністрування.
- Останній рубіж утворюють засоби пасивного аудиту, які допомагають оцінити наслідки порушення безпеки, знайти винного, з'ясувати, чому успіх атаки став можливим.
- Розташування засобів забезпечення високої доступності визначається критичністю відповідних сервісів або їх компонентів.

Зрозуміло, що все вищевказане є орієнтовним і повинно уточнюватися та доповнюватися при розробці концепції інформаційної безпеки кожної окремої Організації. З врахуванням наданих експертами ВЕФ оцінок та постійний тренд росту успішних реалізацій кібернетичних складових в питаннях геополітичних відносин, питання гібридизації загроз і використання їх для досягнення тих чи інших цілей повинно виноситись в основу розробки стратегій захисту організацій державного та приватного сектору.

3. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Сучасні тренди кібербезпеки безпосередньо пов'язані з цілями і завданнями зловмисників. Як і раніше, атаки хакерів спрямовані на великі компанії, промислові системи та інші критичні інфраструктури. Сюди відносяться також і атаки, що безпосередньо фінансуються державами. Вже є приклади успішних атак, що були реалізовані через так званий ланцюжок поставок, що ще більше ускладнює процеси ідентифікації такого типу атак на ранніх стадіях.

Тільки за даними Центру розгляду скарг на кіберзлочини (IC3) FBI США, що були опубліковані у звіті «2019 Internet Crime Report», за 2019 рік збитки фізичних осіб і компаній склали близько 3,5 млрд. доларів США.

Очевидно, що ріст ефективності кіберзлочинів однозначно вимагає розробки та використання сучасних технологій та кращих світових практик в питаннях раннього оповіщення та обміну інформацією про нові загрози на державному рівні. Однак всі ці міри будуть неефективними, якщо управління власною інформаційною безпекою не буде відповідати динамічно-виникаючим загрозам та новим ризикам, що ними породжуються, апробованим підходам та кращим світовим практикам протидії їм.

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

- визначенні базових факторів, що впливають на розподіл відповідальності і порядок взаємодії при забезпеченні інформаційної та кібербезпеки.

- створенні та впровадженні типових політик, процедур та інструкцій щодо розробки порядку класифікації інформаційних активів державних і приватних структур;

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

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] The Global Risks Report 2020. [Електронний ресурс]. Режим доступу: http://bit.ly/2SIV9FX. [Перевірено: 17 лютого 2019]
[2] 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
[3] Борсуковська В.Ю., Борсуковський Ю.В. «Безперервність бізнесу: новий тренд або необхідність», Економіка. Менеджмент. Бізнес. - 2017, № 2(20), с. 48-52
[4] 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
[5] 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 https://doi.org/10.28925/2663-4023.2019.5.6172
[6] 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 https://doi.org/10.28925/2663-4023.2019.6.112121
[7] Про кіберзагрози в Давосі. [Електронний ресурс]. Режим доступу: http://bit.ly/2V5cbj9. [Перевірено: 17 лютого 2019]
[8] World Economic Forum report discusses the Wild Wide Web. [Електронний ресурс]. Режим доступу: http://bit.ly/2PctdbA. [Перевірено: 17 лютого 2019]
[9] These are the top risks facing the world in 2020. [Електронний ресурс]. Режим доступу: http://bit.ly/2SKBCoJ. [Перевірено: 17 лютого 2019]
[10] ДСТУ ISO/IEC 27000:2015. Інформаційні технології. Методи захисту. Система управління інформаційною безпекою (ISO/IEC 27000:2014 IDT).
[11] ОСТ 45.127-99. Система забезпечення інформаційної безпеки взаємопов'язаної мережі зв'язку РФ. Терміни та визначення. [Електронний ресурс]. Режим доступу: http://bit.ly/39OOa3Z. [Перевірено: 17 лютого 2019]
[12] Ірина Муравйова. Новий погляд на службу інформаційної безпеки компанії. [Електронний ресурс]. Режим доступу: http://bit.ly/38Jp6eN. [Перевірено: 17 лютого 2019]
[13] 2019 Internet Crime Report. [Електронний ресурс]. Режим доступу: http://bit.ly/2vNs2Zi. [Перевірено: 17 лютого 2019]
[14] These will be the main cybersecurity trends in 2020. [Електронний ресурс]. Режим доступу: http://bit.ly/2HEfV3d. [Перевірено: 17 лютого 2019]

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (8), 2020
ISSN 2663 - 4023

Yurii V. Borsukovskyi (Borsukovskii)
PhD in technical sciences, professor of the Department of Information and cyber security
Borys Grinchenko Kyiv University, Ukraine
ORCID: 0000-0003-1973-2386
Y.Borsukovskyi@kubg.edu.ua

DEFINING REQUIREMENTS TO DEVELOP INFORMATION SECURITY CONCEPT N HYBRID THREATS CONDITIONS. PART 3

Annotation. This article provides the modern cybersecurity trends directly related to aim ant tasks of criminals. It reflect the assessment of global technological risks discussed at 2020 World Economic Forum. The article covers estimations on increase on negative impact of geopolitical sharpness elements on economic potential of next generation technologies. Data fraud and cyberattacks are considered as priority key indicators at assessment of the most possible global risks, and attacks at informational infrastructure are equal to the cyberattacks risks at the rating of the most possible risks. Forecast indicates that cyberattacks are the most likely to be used as indirect conflicts between countries which look forward to expand their range on influence. In such situation the cybersecurity issues can`t stay on the second place or be the issues which should be solved at existence of direct cyber threats to the modern informational systems, IoT systems and SCADA. Obviously, we should revise the approaches to creation and development of modern informational technologies and cybersecurity issues should be considered as constituent element in development of modern informational systems from the very moment of its initiation, projecting, and on all stages of production and support. Reorientation of informational system developers to creation of new integrated platforms with cybersecurity constituent elements demands the research and implementation of new approaches to its development, as well as engagement of the world community at elaboration of relevant standards and protocols, which ensure the secure functioning of informational systems at world net. The article provides the basic requirements to constituent elements at development of concept of informational and cyber security in conditions of hybrid threats especially provides recommendations on organizational structure for informational security department and general principles to organize the activities and controls on informational and cyber protection. The article defines tasks for informational security department, provides the list of basic actions to secure information, and formulates the tasks, which should be ensured by technical infrastructure, organizational, procedural and hardware and technical actions to manage the informational security, and other principles to ensure informational security in development of concept of informational security within the hybrid threats conditions.

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

REFERENCES (TRANSLATED AND TRANSLITERATED)

[1] The Global Risks Report 2020. [Online]. Available: http://bit.ly/2SIV9FX. [Accessed: 17 February 2020]
[2] Borsukovskii Y.V., Borsukovska V.Y., Buriachok V.L. «Directions for creation of informational security policies for the state, banking and private sectors», Modern Methodologies, Innovations, and Operational Experience on the Field of Technical Science: Conference proceedings, December 27-28, 2017, Radom, Republic of Poland, p. 8-11
[3] Borsukovska V.Y., Borsukovskii Y.V. «Business Continuity: new trend or necessity», Economy. Management. Business. - 2017, № 2(20), c. 48-52
[4] Borsukovskii Y.V., Buriachok V.L., Borsukovska V.Y. «Basic ways to ensure cyber security of state and private sectors», Modern Information Security, - 2017, № 2(30), c. 85-89
[5] Borsukovskyi Y.V., «Defining requirements to develop information security concept n hybrid threats conditions. Part 1», Cybersecurity: education, science, technique, - 2019, №1(5), p. 61-72 https://doi.org/10.28925/2663-4023.2019.5.6172

[6] Borsukovskyi Y.V., «Defining requirements to develop information security concept n hybrid threats conditions. Part 2», Cybersecurity: education, science, technique, - 2019, №2(6), p. 112-121 https://doi.org/10.28925/2663-4023.2019.6.112121
[7] On cyber threats at Davos. [Online]. Available: http://bit.ly/2V5cbj9. [Accessed: 17 February 2020]
[8] World Economic Forum report discusses the Wild Wide Web. [Online]. Available: http://bit.ly/2PctdbA. [Accessed: 17 February 2020]
[9] These are the top risks facing the world in 2020. [Online]. Available: http://bit.ly/2SKBCoJ. [Accessed: 17 February 2020]
[10] ISO/IEC 27000:2015. Information technology. Security techniques. Information security management systems. Overview and vocabulary (ISO/IEC 27000:2014 IDT).
[11] ОСТ 45.127-99. Система обеспечения информационной безопасности взаимоувязанной сети связи РФ. Термины и определения. [Online]. Available: http://bit.ly/39OOa3Z. [Accessed: 17 February 2020]
[12] Iryna Muravyova. New vision for company security service. [Online]. Available: http://bit.ly/38Jp6eN. [Accessed: 17 February 2020]
[13] 2019 Internet Crime Report. [Online]. Available: http://bit.ly/2vNs2Zi. [Accessed: 17 February 2020]
[14] These will be the main cybersecurity trends in 2020. [[Online]. Available: http://bit.ly/2HEfV3d. [Accessed: 17 February 2020]