УДК 004.056
DOI: 10.31891/2219-9365-2021-68-2-4

КУПЕРШТЕЙН Л. М., ДУДАТЬЄВ А. В.,
ВОЙТОВИЧ О. П., ЯСІНСЬКА Я. О.
Вінницький національний технічний університет

МОДЕЛЬ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЛЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

У статті запропоновано підхід щодо створення політики інформаційної безпеки (ПІБ) об'єкта інформаційної діяльності, яке відноситься до об'єктів критичної інфраструктури. Шляхом логіко-ймовірнісного моделювання досліджено рівень поточного стану кібербезпеки досліджуваного об'єкта. Проведене ранжування дозволили виявити найбільш значущі загрози, що у свою чергу, дозволило розробити адекватну політику інформаційної безпеки.

Ключові слова: критична інфраструктура, політика інформаційної безпеки, загроза інформаційної безпеки, експертна оцінка ризиків.

LEONID KUPERSHTEIN, ANDREY DUDATYEV
OLESIA VOITOVYCH, YANA YASINSKA
Vinnytsia National Technical University

INFORMATION SECURITY POLICY MODEL FOR CRITICAL INFRASTRUCTURE OBJECTS

The approach to creating an information security policy of information object, which belongs to the critical infrastructure is proposed in the article. The safety status analysis of the critical infrastructure (the primary health care center) shows it to be sufficiently low. To quantify the object security, a logical-probabilistic model, which takes into account the threats of categories: confidentiality, integrity, accessibility is developed. The level of the current state of studied object cybersecurity is investigated by logical-probabilistic modeling. The ranking allows identifying the most significant threats and, as a result, allows developing an information security policy that legislates the current requirements and capabilities of the investigating object. The purpose of the security policy is to ensure that the critical infrastructure is protected from possible threats types e.g. internal, external, accidental, and intentional. The basic principles of security policy are as follows: protection against breaches of confidentiality, integrity, availability of critical information resources; responsibility introduction of officials on providing cyber protection of the critical infrastructure; periodic training of employees on information security; ensuring the functioning and prevention of disturbances in the operation of the critical infrastructure facility; delimitation of user access rights; minimization of privileges; responding to the security incident. The rules and policy recommendations implementation help to organize the advanced secure operation of the critical infrastructure and reduce the risks of typical threats and leaks of critical information. It is significant to maintain the continuity of information security processes to keep it up to date due to the possibility of new threats and channels of information leakage.

Keywords: critical infrastructure, information security policy, information security threat, expert risks assessment

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями

В сучасному світі інформаційні технології набувають все більшого поширення, що не оминуло й галузь охорони здоров'я. Актуальність теми полягає у тому, що цифровізація у галузі медицини не тільки поліпшила медичні послуги, але й принесла за собою небезпечний побічний ефект такий, як збільшення ризиків кібербезпеки та інформаційної безпеки (ІБ) в цілому. Відома велика кількість випадків, коли саме медична інформація була викрадена чи виставлена для загального доступу, так, за деякими джерелами, галузь охорони здоров'я є лідером за витоками інформації [1]. Це не в останню чергу пов'язано з тим, що медична інформація має високу ціну на чорних ринках, і відкриває можливості для подальших маніпуляцій. Тому постає необхідність у забезпеченні безпеки в галузі охорони здоров'я, а саме: забезпечення її цілісності, доступності та конфіденційності. У відповідності до НД ТЗІ 1.4 - 001-2000 «Типове положення про службу захисту інформації в автоматизованих системах» [2] ПІБ повинна базуватись на принципах системності, комплексності, неперервності захисту, достатності механізмів і заходів захисту та їхньої адекватності загрозам, гнучкості керування системою захисту, простоти і зручності її використання, відкритості алгоритмів і механізмів захисту, якщо інше не передбачено окремо.

Для забезпечення заданого рівня захищеності досліджуваного об'єкта, необхідно виконати його аналіз, в першу чергу ідентифікувати інформаційні ресурси, які потребують захисту, а також оцінити їх ризики, у випадку ефективної реалізації загроз на ці ресурси [3]. На основі проведеного оцінювання можна визначити, на які аспекти варто захист та створити правила, рекомендації, вимоги тощо.

Для забезпечення заданого рівня захищеності досліджуваного об'єкта, необхідно виконати його аналіз, в першу чергу ідентифікувати інформаційні ресурси, які потребують захисту, а також оцінити їх ризики, у випадку ефективної реалізації загроз на ці ресурси [3].На основі проведеного оцінювання можна визначити, на які аспекти варто акцентувати захист та створити правила, рекомендації, вимоги тощо.

Моделювання оцінки ризиків

Поняття політики інформаційної безпеки використовується у низці стандартів та нормативних документів [4- 5]. Відповідно до статті 6 Закону України «Про основні засади забезпечення кібербезпеки України» медичні установи відносяться до об'єктів критичної інфраструктури тому ПІБ повинна відповідати Постанові КМУ №518 від 19.06.2019 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» [6, 7]. Відповідно до Постанови поняття ПІБ – це політика, яка визначає підхід підприємства/організації тощо, до правил, вимог, рекомендацій обмежень, які в свою чергу регламентують порядок дотримання та забезпечення ІБ. У Постанові визначені розділи, які повинна містити ПІБ: мета та основні принципи забезпечення захисту важливих активів, опис критичних операційних процесів, політика розмежування прав доступу, політика фізичної безпеки, політика управління обліковими записами, політика забезпечення безперебійної роботи об'єкта, політика управління інцидентами ІБ, політика мережевого захисту, політика проведення модернізації компонентів об'єкта, політика управління оновленнями, політика реєстрації та аудиту подій, політика використання електронної пошти, політика проведення внутрішнього аудиту інформаційної безпеки об'єкта, політика ознайомлення персоналу з ПБ, політика покарань в разі недотримання правил ПБ.

Для аналізу стану інформаційної безпеки медичної установи визначено цінні активи установи. За ДСТУ ISO/IEC 27005-2019 цінність активів оцінюється за 4-х бальною шкалою, де 1 означає, що при реалізації загрози, спрямованої на одну чи декілька послуг безпеки (конфіденційність, доступність, цілісність) відповідного активу не матиме жодних наслідків, 2 – незначні наслідки (втрати), 3 – значні наслідки, але з можливістю відновлення стану системи, 4 – може призвести повну зупинку усіх операційних процесів [8]. Ресурси досліджуваного об'єкта захисту поділяються на: інформаційні ресурси, критичні операції, персонал, медичне обладнання, носії інформації та апаратно-програмний комплекс.

Як досліджуваний об'єкт взято центр первинної медико-санітарної допомоги одного з райцентрів Вінницької області. Дана установа налічує 40 працівників. Будівля складається з двох поверхів та містить 37 кабінетів. Більшість кабінетів установи обладнані комп'ютерами. Площа даного об'єкту не обмежена парканом та не налічує системи відеоспостережень. Результати проведеного аналізу важливих активів установи та їх цінність наведені в таблиці 1.

Таблиця 1

Цінні активи установи

№	Назва ресурсу		Конфіденційність	Цілісність	Доступність	Цінність активу
1	Інформаційні ресурси	БД eHealth	4	4	4	4
2		Технологічний процес збору, обробки, зберігання та передачі інформації	4	2	2	4
3		Звіти в електронному вигляді	3	4	3	4
4		Паперові звіти	3	4	3	4
5		Паперові картки хворих	4	4	3	4
6		Паперові журнали ведення	3	3	3	3
7	Критичні операції	Прийом пацієнтів	4	-	-	4
8		Внесення мед. даних до БД	4	3	3	4
9		Наради	2	-	-	2
10	Персонал	Керівництво	4	2	2	4
11		Лікарі/Медичні сестри	3	1	2	3
12		Санітари	1	1	1	1
13		Бухгалтер	2	2	2	2
14	Мед. обладнання	Електрокардіограф	-	3	3	3
15		Пульсоксиметр	-	2	1	2
16		Флюрограф	-	3	2	3
17	Носії інформації	Флеш носії з ЕЦП працівників	3	2	2	3
18		Жорсткі диски	3	3	3	3
19		Паперова документація	3	2	2	3
20	Апаратно-програмний комплекс	Апаратне забезпечення	3	3	3	3
21		Програмне забезпечення	3	2	3	3

До складу апаратного комп'ютерного забезпечення медичного закладу входять 20 персональних

комп'ютерів на основі процесора Intel Celeron Dual Core J1800 з 4 ГБ ОЗП та 500 ГБ ПЗП, 2 ноутбуки Acer Extensa EX2540-39BD, 9 принтерів HP Laser JetPro M15a, 3 БФП Canon Pixma MG3640S з доступом по Wi-Fi, 2 телефонні апарати Panasonic KX-TS2352UAB, комутатор TP-LINK TL-SF1024D для організації локальної комп'ютерної мережі, бездротовий маршрутизатор TP-LINKArcher MR200 для доступу до глобальної мережі Інтернет. Топологія мережі в межах установи – "зірка". Доступ до мережі Інтернет надається місцевим провайдером на основі технології Ethernet на швидкості 100 Мбіт/с.

Медична установа підключена до електронної системи охорони здоров'я eHealth, яка забезпечує обмін медичною інформацією та реалізацію програми медичних гарантій населення. eHealth складається з центральної бази даних з віддаленим доступом до неї через клієнтське програмне забезпечення електронної медичної інформаційної системи (МІС) МедЕйр.

В інформаційних мережах підприємства відбувається обробка інформації, що підлягає захисту, зокрема, історії хвороби пацієнтів, персональні дані співробітників та пацієнтів, бухгалтерська та фінансова документація. Інформація обробляється на персональному комп'ютері під управлянням операційної системи Windows 10 20H1.

Проаналізувавши середовище користувачів виявлено, що не всі працівники є висококваліфікованими операторами ПК, хоч і проходили навчання по роботі із спеціалізованим програмним забезпеченням, в наслідок недостатньої кваліфікації в сфері інформаційних технологій медичних працівників є ризик ненавмисного порушення властивостей інформації або її втрати. Також присутній ризик навмисного порушення конфіденційності, доступності чи цілісності, оскільки не реалізовано моделі логічного розмежування доступу до інформації.

Наступним кроком після проведеного аналізу об'єкта захисту, є ідентифікація основних загроз інформаційної безпеки установи [9], яка може здійснюватися двома підходами: статистичним або експертним. Оскільки в більшості випадків статистика загроз відсутня або недостатня, доцільно проводити ідентифікацію загроз з використанням експертного підходу [10]. Експертні оцінки формалізуються за допомогою теорії нечітких множин, що дозволяє визначити найбільш точну вірогідність виникнення події. Формалізація експертних оцінок передбачає два етапи: – фазифікацію (розмиття) та дефазифікацію (отримання найбільш достовірного значення). Етап дефазифікації був виконаний методом центру ваги [11]:

$$\widetilde{X} = \frac{\sum_i x_i \cdot \mu_i}{\sum_i \mu_i} \quad , \tag{1}$$

деx_i – оцінка експерта,μ_i- значення функції належності.

У наступній нечіткій множині, для прикладу, наведена експертна оцінка виникнення загрози у формі – «близько 0,02»:

$$\{0{,}95|0{,}018;\ 1|0{,}02;\ 0{,}98|0{,}022\}.$$

Представлена нечітка множина формалізує експертну оцінку, що дозволяє виконати процеси дефазифікації.

Для наведеної множини етап дефазифікації виглядає

$$\widetilde{X} = \frac{0{,}018 \cdot 0{,}95 + 0{,}02 \cdot 1 + 0{,}022 \cdot 0{,}98}{0{,}95 + 1 + 0{,}98} = 0{,}02\,.$$

Всі можливі загрози для даного об'єкта захисту та їх ймовірності виникнення, що були отримані експертним шляхом) представлені в таблиці 2.

Після ідентифікації усіх негативних факторів для даної установи, що впливають на інформаційні ресурси об'єкта захисту, і, відповідно, на його загальний стан інформаційної безпеки, визначається інтегральний показник їх впливу. Для цього розроблена логіко-ймовірнісна модель, яка подана у вигляді «дерева подій», фрагмент якого представлено на рис. 1. Для отримання загальної оцінки, наприклад, ймовірності виникнення несанкціонованого доступу до інформаційних ресурсів центр первинної медико-санітарної допомоги, шляхом порушення правил ІБ, необхідно визначити порушення інформаційної безпеки окремо за кожним критерієм (конфіденційність, цілісність, доступність та спостережність) [12].

Таблиця 2

ISSN 2219-9365

Загрози інформаційної безпеки установи

№	Загроза	Оцінка експерта	№	Загроза	Оцінка експерта
1	Пожежа	0,02	20	Корисливий інтерес працівників	0,07
2	Повінь	0,01	21	Неналежна мотивація дотримання правил ПБ	0,13
3	Троянська програма	0,11	22	Неповне ознайомлення працівників з правилами ПБ	0,1
4	Хробак	0,07	23	Недостатня кваліфікація працівників	0,12
5	Вірус	0,08	24	Інсайдер	0,06
6	Шпигунське ПЗ	0,05	25	Переналаштування медичного обладнання	0,03
7	Перехоплення даних через Wi-Fi	0,1	26	Деактивація медичного обладнання	0,07
8	Перехоплення даних через шкідливе ПЗ(ШПЗ)	0,09	27	Відсутність журналу безпеки	0,13
9	Фішинг	0,12	28	Несанкціонований доступ до системи	0,06
10	Вішинг	0,06	29	Випадкові помилки працівників	0,14
11	Підбір даних методом грубої сили	0,14	30	Навмисні помилки працівників	0,06
12	Підбір даних за словником	0,08	31	Атака на відмову в обслуговуванні	0,04
13	Підслуховування за допомогою технічних засобів	0,04	32	Мережеві несправності	0,08
14	Фізичне підслуховування	0,09	33	Збій електроенергії	0,09
15	Відкритий доступ до приміщень з комп'ютерами	0,13	34	Викрадення апаратного забезпечення	0,05
16	Відкритий доступ до приміщень з паперовими носіями	0,13	35	Поломка апаратного забезпечення	0,09
17	Незаблоковані комп'ютери при завершені роботи з ними	0,15	36	Неналежне ведення журнал безпеки	0,08
18	Зберігання чутливої інформації на видному місці	0,18	37	Видалення записів з журналу безпеки	0,05
19	Неналежне розмежування прав доступу	0,21	38	Збій програмного забезпечення	0,1

На рис. 1 наведена гілка, яка формалізує причинно-наслідкові зв'язки порушення конфіденційності.
.

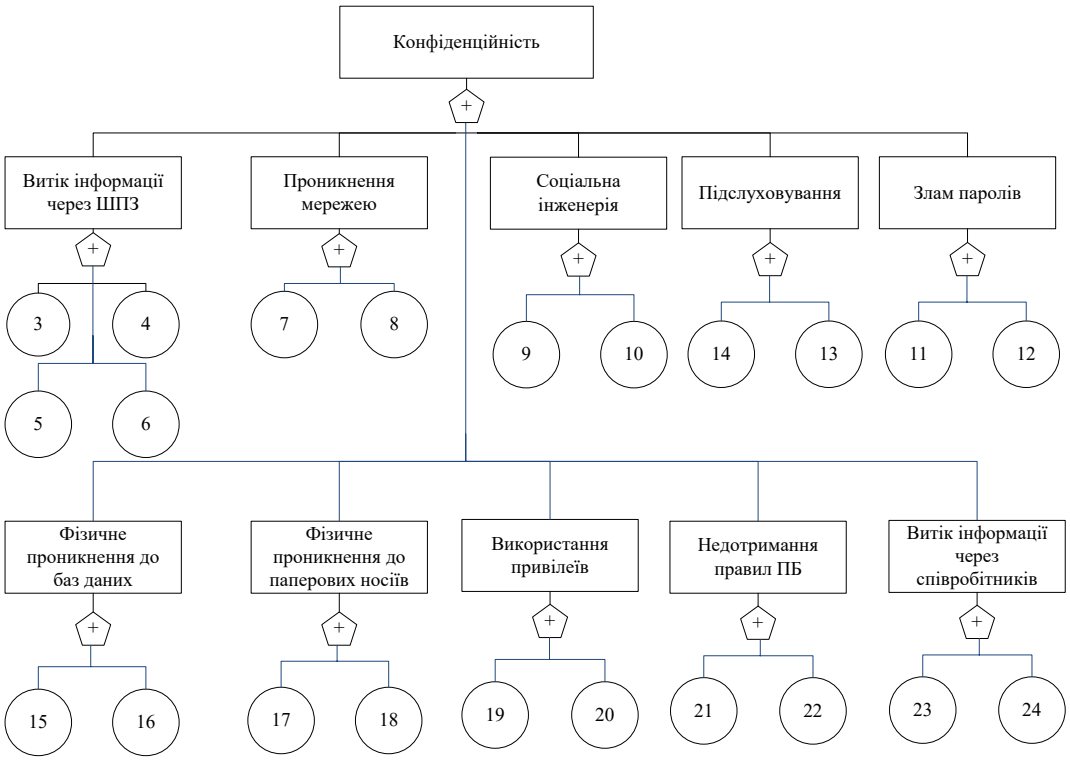

Рис. 1. Гілка «Конфіденційність» логіко-ймовірнісної моделі

За умови незалежних базових подій, для аналізу наведеної моделі, використовується вираз (2), якщо події зв'язані логічною функцією «І» та вираз (3), якщо події зв'язані виразом функцією «АБО».

$$P = \prod_{j=1}^{k} P_j \quad , \tag{2}$$

$$P = 1 - \prod_{j=1}^{k} (1 - P_j), \tag{3}$$

де P_j – ймовірність виникнення j-тої події, які є причинами появи вихідної події, k– кількість подій, що впливають на появу вихідної події.

Результатом оцінювання рівня захищеності об'єкту захисту є визначення не лише загального стану ІБ, але й впливу кожного фактору на цей стан. Цей вплив визначається за допомогою ранжування.

Для визначення значущості подій, як проміжних, так і базових, що виникають на об'єкті захисту, використано (4).

$$R_i = P - P_i, \tag{4}$$

де P – ймовірність появи головної події, P_i – ймовірність появи головної події за умови вилучення i-ої події.

Усі результати розрахунків ймовірностей проміжних подій наведено в таблиці 3.

Таблиця 3

Ймовірності проміжних подій для гілки «Конфіденційність»

№	Назва проміжної події	Ймовірність	№	Назва проміжної події	Ймовірність
1	Витік інформації через ШПЗ	0,27	6	Фізичне проникнення до баз даних	0,26
2	Проникнення мережею	0,18	7	Фізичне проникнення до паперових носіїв	0,28
3	Соціальна інженерія	0,17	8	Використання привілеїв	0,01
4	Підслуховування	0,21	9	Недотримання правил ПБ	0,22
5	Злам паролів	0,12	10	Витік інформації через співробітників	0,17

Результати ранжування загроз для гілки «Конфіденційність» наведено у таблиці 4.

Таблиця 4

Ранжування загроз для гілки «Конфіденційність»

№	Назва загрози	Ранг	№	Назва загрози	Ранг
1	Зберігання конфіденційної інформації на видному місці	1	12	Підбір даних методом грубої сили	4
2	Корисливий інтерес працівників	2	13	Перехоплення за допомогою ШПЗ	4
3	Незаблоковані комп'ютери	3	14	Троянськапрограма	5
4	Фізичне підслуховування	3	15	Вішинг	5
5	Неналежна мотивація дотримання правил ПБ	3	16	Підслуховування за допомогою спеціальних засобів	5
6	Відкритий доступ до приміщень з комп'ютерами	3	17	Неналежне розмежування прав доступу	5
7	Фішинг	3	18	Інсайдер	5
8	Недостатня кваліфікація працівників	3	19	Вірус	5
9	Відкритий доступ до приміщень з паперовими носіями	4	20	Хробак	5
10	Перехоплення через Wi-Fi	4	21	Підбір даних за словником	5
11	Неповне ознайомлення з правилами ПБ	4	22	Шпигунське ПЗ	5

Аналіз, аналогічний наведеному, проводиться для інших гілок, які формалізують порушення доступності, цілісності та спостереженості. Через обмеження обсягу статті дані результати не наводяться.

Проведений розрахунок запропонованої моделі показав, що ймовірність загального порушення інформаційної безпеки установи дорівнює 0,96. Це означає, що установа є незахищеною та потребує негайного підвищення рівня безпеки. Результати ранжування дозволили виявити найбільш критичні загрози, що в свою чергу дозволить запропонувати ефективну ПІБ, яка врахує результати проведеного моделювання.

Політика безпеки

Далі наводиться загальна політика інформаційної безпеки середнього рівня, яка є базою для розробки ІБ нижнього рівня, до якої входять регламенти робіт, керівництва по адмініструванню, інструкції з експлуатації окремих сервісів інформаційної безпеки.

Мета та основні принципи забезпечення захисту критичних активів

Метою ПБ є забезпечення захисту об'єкта критичної інфраструктури (ОКІ) від можливих видів і типів загроз (внутрішніх, зовнішніх, випадкових і навмисних). Основі принципи забезпечення безпеки полягають у такому: захист від порушення конфіденційності, цілісності, доступності критичних інформаційних ресурсів; впровадження відповідальності посадових осіб щодо забезпечення кіберзахисту ОКІ; періодичне навчання працівників з інформаційної безпеки; забезпечення функціонування та недопущення порушення в роботі ОКІ; розмежування прав доступу користувачів; мінімізація привілеїв; реагування на виникнення надзвичайних ситуацій.

Опис критичних операційних процесів

Критичними операційними процесами медичної установи є: прийом пацієнтів, занесення медичних даних пацієнтів до БД eHealth, наради керівництва.

Політика затвердження відповідальних осіб

Відповідальність за забезпечення безпеки ОКІ покладається на керівництво центра первинної медико-санітарної допомоги. Керівництво повинно впровадити посаду спеціаліста з інформаційної безпеки, на якого покладаються такі обов'язки: підтримка функціонування інформаційних ресурсів ОКІ, налаштування механізмів безпеки, зокрема міжмережевого екрану, автентифікації та авторизації усіх працівників, що мають доступ до ОКІ, встановлення захисту від шкідливого програмного забезпечення та підтримка його в актуальному стані, налаштувати систему відеоспостереження, виконувати необхідні налаштування мережі, забезпечувати регулярне резервне копіювання даних та інші задачі. При виборі відповідальної особи слід надавати перевагу особам з фаховою освітою і досвідом роботи в області ІБ. Ця посада повинна бути підпорядкована безпосередньо керівнику центра первинної медико-санітарної допомоги.

Політика розмежування прав доступу

Необхідно виділити три ролі користувачів, а саме: перша – звичайні працівники (лікарі та медичні сестри, що вносять відомості до системи eHealth), друга – адміністрація (головний лікар, начальник медичної частини, головна медична сестра, що мають право переглядати всі відомості та право підпису), третя – системні адміністратори (спеціаліст з ІБ, що має право налаштовувати систему, встановлювати права доступу та привілеї, застосовувати спеціалізоване ПЗ із забезпечення безпеки). Доступи до конфіденційної паперової інформації визначають спеціалістом з ІБ з узгодженням керівництва.

Політика фізичної безпеки

Для забезпечення фізичної безпеки необхідно встановити захисні решітки на вікна в кабінетах, в яких використовується критичне апаратне забезпечення, медичне обладнання та конфіденційні дані в фізичному вигляді установи, встановити паркан по межі території медичної установи.

Необхідно встановити охоронну сигналізацію по всій будівлі центру, таким чином, щоб при несанкціонованому проникненні сторонніх осіб до будівлі подавався сигнал диспетчеру служби охорони. Необхідно встановити систему відеоспостереження зовнішньої території та внутрішнього приміщення, а саме не менше ніж чотири відеокамери ззовні та чотири всередині.

Працівники центру повинні закривати кабінет на ключ, якщо в приміщенні відсутні працівники. Працівники центру повинні блокувати свої робочі комп'ютери при відсутності потреби у ньому, також необхідно встановити автоматичне блокування комп'ютера при його невикористанні більше 10 хвилин. Працівники центру повинні дотримуватись правил «чистого столу» та «чистого екрану».

Політика управління обліковими записами

Для кожного працівника необхідно створити окремий обліковий запис з певним набором прав, який визначається роллю, до якої належить цей працівник. Кожен працівник повинен виходити з облікового запису після використання комп'ютера.

Необхідно налаштувати парольну політику в ОС Windows, а саме: ведення журналу паролів з встановленням кількості збережених паролів в 10 записів, встановлення максимального терміну дії пароля в 30 днів та мінімальної довжини паролю в 12 символів. Політика використання паролів повинна включати такі вимоги до пароля: містить хоча б одну цифру, містить хоча б один спеціальний символ, містить, як великі так і малі літери, не містить імені облікового запису користувача або будь-які інші дані, що ідентифікують користувача (прізвище, дата народження і т. п.). Налаштувати політику блокування облікового запису на 5 хвилин після трьох неправильних спроб введення паролю з повідомленням спеціаліста з ІБ.

Політика управління інцидентами ІБ

Керівництво ОКІ повинно повідомляти про інциденти в ІБ відповідно до законодавства. Необхідно розробити і затвердити формальну процедуру повідомлення про події в області ІБ, а також процедуру реагування на події ІБ. Процедуру реагування на інциденти повинен розробити спеціаліст з ІБ. Необхідно створити механізми, що дозволяють оцінювати і відслідковувати типи інцидентів, їх масштаб і пов'язані з ними витрати. Необхідно передбачити моніторинг систем, повідомлень та вразливостей для виявлення інцидентів ІБ. Всі співробітники повинні бути ознайомлені з процедурою повідомлення про інциденти ІБ, а в їх обов'язки повинна входити максимально швидка передача інформації про подію спеціалісту з ІБ.

Політика мережевого захисту

Захист від ШПЗ

Необхідно використовувати засоби захисту від ШПЗ та зловмисного коду, в першу чергу, спеціалізовані програмні засоби, до складу яких входять евристичні аналізатори.

Необхідно встановити ліцензійне антивірусне програмне забезпечення із автоматичним оновленням баз. Антивірусне ПЗ повинне бути встановленим в режимі постійного захисту на усі робочі місця працівників та сервер. Антивірусне програмне забезпечення забороняється відключати.

Усе ПЗ повинно встановлюватись тільки спеціалістом з ІБ, працівникам забороняється встановлювати будь-яке ПЗ самостійно. Усе програмне забезпечення повинно бути виключно ліцензійним.

Необхідно обмежити технічну можливість підключення до робочих станцій працівниками мобільних телефонів, зовнішніх накопичувачів інформації, модемів, використання дисководів та USB-портів. Необхідно налаштувати міжмережевий екран, так щоб вихід в Інтернет був тільки для обмежених сервісів.

Безпека бездротового зв'язку

Заборонено використовувати для передачі інформації, що потребує захисту відповідно до законів України, бездротові засоби зв'язку технологій Wi-Fi та Bluetooth.

При необхідності передачі відкритої інформації необхідно дотримуватись політики використання технології Wi-Fi. Необхідно обмежити зону покриття бездротової мережі, для цього виконати рівневіддалене (центральне) розташування антени. Постійно виконувати доступне оновлення ПЗ маршрутизатора. Змінити пароль від маршрутизатора за замовчуванням на більш стійкий, що містить не менше 12 символів та включає в себе великі та малі літери, символи та цифри. Пароль необхідно періодично змінювати. Рекомендовано відключити DHCP та використовувати статичні IP-адреси, або ж при використані DHCP обмежити кількість IP-адрес у пулі DHCP. Необхідно налаштувати шифрування даних (обрати алгоритм шифрування WPA2-AES).

Необхідно помістити користувачів бездротових мереж до демілітаризованої зони та налаштувати міжмережеві екрани таким чином, щоб до таких користувачів застосовувались правила як для віддалених користувачів.

Необхідно вимкнути наступні опції: віддалене управління, віддалене оновлення, які потенційно можуть скомпрометувати ПЗ, ping.

Необхідно налаштувати системи виявлення вторгнень для бездротових мереж.

Мережа центру

Необхідно сегментувати мережу, а саме: розбити її на чотири підмережі, за функціональними обов'язками, що виконуються, де перша підмережа використовується для адміністрації, друга – для бухгалтерії, третя – для спеціаліста з ІБ та четверта для решти користувачів. Для сегментації мережі необхідно використати технології віртуальних локальних мереж та міжмережевого екранування.

Необхідно заключити договір з провайдерами інтернет, з урахуванням вимог щодо забезпечення інформаційної безпеки об'єкта критичної інфраструктури.

Політика проведення модернізації компонентів об'єкта

За модернізацію компонентів ОКІ повинен відповідати спеціаліст з ІБ, який визначає необхідність проведення модернізації, в тому числі за планом.

Політика реєстрації та аудиту подій

Політика реєстрації та аудиту подій повинна фіксувати всі події, що стосуються безпеки, а саме: вхід і вихід суб'єктів доступу, запуск і завершення програм, видача друкованих документів, спроби доступу до ресурсів, що захищаються, зміна повноважень суб'єктів доступу, зміна статусу об'єктів доступу тощо.

Спеціаліст з ІБ повинен проводити моніторинг журналу безпеки не рідше як один раз на день. Необхідно налаштувати системи активного аудиту подій в мережі.

Політика використання електронної пошти

Забороняється використовувати електронну пошту (ЕП) для відправки незашифрованої спеціальним ПЗ (дозволеним на ОКІ) конфіденційної інформації. Забороняється використовувати службову ЕП в особистих або благодійних цілях, які не пов'язані з функціоналом установи. Забороняється відкривати сумнівні файли від незнайомих відправників, а також переходити за підозрілим посиланнями у тексті листа. Забороняється розкривати непублічну інформацію установи без необхідності в листах, які йдуть за межі установи та пересилати паролі електронною поштою у відкритому вигляді. Рекомендується використання двофакторної автентифікації для доступу до поштово облікового запису.

Політика проведення внутрішнього аудиту інформаційної безпеки об'єкта

Керівництво центру повинно ініціювати проведення внутрішнього аудиту не рідше одного разу на рік. Внутрішній аудит ІБ, що виконується спеціалістом з ІБ, повинен включати: аналіз загроз та оцінка ризиків ІБ відповідно до ДСТУ ISO/IEC 27005, оцінку поточного рівня захисту інформаційної системи (ІС) об'єкта, виявлення вразливих місць в ІС, встановлення відповідності ІС існуючим стандартам в сфері ІБ, розробка рекомендацій щодо підвищення ефективності існуючих засобів і механізмів захисту та щодо впровадження нових.

Проведення внутрішнього аудиту проводиться позачергово при зміні структури центру, при зміні ІТ-інфраструктури, при виникненні нових вимог до ІБ (нові стандарти, зміни законодавства).

Політика ознайомлення персоналу з ІБ

Спеціаліст з ІБ повинен провести інструктаж щодо загальних правил та рекомендацій збереження інформаційної безпеки працівниками. Ролі та обов'язки щодо забезпечення безпеки інформаційних ресурсів, описані відповідно до ПБ центру, повинні бути доведені до співробітника при працевлаштуванні і внесені в його посадові обов'язки, куди повинні входити як загальні обов'язки щодо реалізації і підтримки політики безпеки, так і конкретні обов'язки щодо захисту ресурсів та виконання конкретних операцій, пов'язаних з безпекою.

Усі прийняті на роботу співробітники повинні схвалити і підписати свої трудові договори, в яких встановлюється їх відповідальність за порушення ІБ. У договір має бути включено згоду співробітника на проведення контрольних заходів з боку установи з перевірки виконання вимог ІБ, а також зобов'язання щодо нерозголошення конфіденційної інформації. У договорі повинні бути описані заходи, які будуть прийняті в разі недотримання співробітником вимог ІБ. Обов'язки щодо забезпечення ІБ повинні бути включені до посадових інструкцій кожного співробітника установи. Керівництво установи повинно вимагати від всіх співробітників прийняття заходів безпеки відповідно до встановленої ПБ. Всі співробітники повинні проходити періодичну підготовку в галузі ІБ. При звільненні всі надані співробітнику права доступу до ресурсів інформаційної системи повинні бути видалені. При зміні трудових відносин видаляються тільки ті права, необхідність в яких відсутня в нових відносинах.

Політика покарань в разі недотримання правил ПБ

Порушення ІБ тягнуть за собою відповідальність, встановлену законом. Спеціаліст з ІБ несе відповідальність за всі дії, що здійснені від імен системного облікового запису, за виключенням якщо було доведено факт несанкціонованого використання цих облікових записів не з його вини. До працівників, які порушили вимоги політики безпеки, повинні застосовуватись заходи дисциплінарного стягнення згідно з чинним законодавством.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі

У ході дослідження було проведено аналіз стану безпеки об’єкта критичної інфраструктури - центра первинної медико-санітарної допомоги, який виявився досить низьким. Для кількісної оцінки захищеності об’єкту розроблено логіко-ймовірнісну модель, яка враховує загрози чотирьох категорій: конфіденційність, цілісність, доступність та спостережність. За результатами моделювання розроблено загальну політику інформаційної безпеки середнього рівня досліджуваного медичного закладу. Дотримання та імплементація правил та рекомендацій політики дозволить організувати ефективне захищене функціонування закладу та знизити ризики реалізації типових загроз та витоків критичної інформації. Запропоновану політику безпеки можна використати як базу для її деталізації на більш низьких рівнях управління у вигляді більш чітких настанов, регламентів, рекомендацій та керівництв. При цьому важливим є періодичний моніторинг стану інформаційної безпеки для підтримки його в актуальному стані через можливість появи нових загроз та каналів витоку інформації.

Література

1. Утечки данных в медицинских учреждениях[Електронний ресурс]. – Режим доступу: http://www.tadviser.ru/index.php/Статья:Утечки_данных.

2. Техническая защита информации [Електронний ресурс]. – Режим доступу: https://tzi.com.ua/polozhennya-pro-sluzhbu-zaxistu-nformacz.html.

3. Хохлачова Ю. Політика інформаційної безпеки об’єкта/ Ю. Хохлачова // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2012.– №2(24). – С. 23-29. [Електронний ресурс]. – Режим доступа: https://ela.kpi.ua/bitstream/123456789/8581/1/24_p23.pdf

4. Куперштейн. Л.М. Дослідження політики інформаційної безпеки у розрізі нормативної документації / Л.М. Куперштейн, Я.О. Ясінська // Тези XLIX науково-технічної конференції підрозділів ВНТУ, м. Вінниця, 18-29 травня 2020 р. - С. 1226-1228.[Електронний ресурс]. – Режим доступу:https://conferences.vntu.edu.ua/public/files/1/vntu_2020_netpub.pdf.

5. ЛужецькийВ.А. Основи інформаційної безпеки / В.А. Лужецький, А.Д. Кожухівський, О.П. Войтович. Вінниця: ВНТУ, 2013. – 221 с.

6. Закон України «Про основні засади забезпечення кібербезпеки України». [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

7. Закон України «Про затвердження Загальних вимог до кіберзахисту об'єктів критичноїінфраструктури» [Електронний ресурс]. – Режим доступу:https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF.

8. ДСТУ ISO/IEC 27005:2019. Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки / Нац. стандарт України. – Вид. офіц. – [Чинний від 2019-11-01]. – Київ : ДП «УкрНДНЦ», 2019. – 76 с.

9. Куперштейн Л. Аналіз загроз інформаційної безпеки в медицині / Л. Куперштейн, О. Войтович, Я. Ясінська // Матеріали XII Міжнародної науково-практичної конференції ІОН-2020, 26-29 травня 2020 р. – С. 210-211.

10. ДудатьєвА.В. Оцінка ступеня ризику промислових аварій при нечітких вихідних даних / А.В.Дудатьєв, В.І.Роптанов // Вимірювальна та обчислювальна техніка в технологічних процесах. - 1997. - № 2. - С. 171 - 174.

11. РотштейнА.П. Интеллектуальные технологиии дентификации: нечеткие множества, нейронные сети, генетические алгоритмы / А.П. Ротштейн. Винница: Універсум-Вінниця, 1999. — 295 с.

12. ДудатьєвА.В. Розробка уніфікованих моделей системного проектування оптимальних систем захисту інформаційних ресурсів / А.В.Дудатьєв // Вісник ЧТУ. - 2008. - №1. - С. 3-8.

References

1. Utechky dannukh v medytsynskykh uchrezhdenyiakh [Elektronnyi resurs]. – Rezhym dostupu: http://www.tadviser.ru/index.php/Статья:Утечки_данных.
2. Tekhnycheskaia zashchyta ynformatsyy [Elektronnyi resurs]. – Rezhym dostupu: https://tzi.com.ua/polozhennya-pro-sluzhbu-zaxistu-nformacz.html.
3. Khokhlachova Yu. Polityka informatsiinoi bezpeky obiekta/ Yu. Khokhlachova // Pravove, normatyvne ta metrolohichne zabezpechennia systemy zakhystu informatsii v Ukraini. ¬– 2012. – №2(24). – S. 23-29. [Elektronnyi resurs]. – Rezhym dostupa: https://ela.kpi.ua/bitstream/123456789/8581/1/24_p23.pdf
4. Kupershtein. L.M. Doslidzhennia polityky informatsiinoi bezpeky u rozrizi normatyvnoi dokumentatsii / L.M. Kupershtein, Ya.O. Yasinska // Tezy XLIX naukovo-tekhnichnoi konferentsii pidrozdiliv VNTU, m. Vinnytsia, 18-29 travnia 2020 r. - S. 1226-1228. [Elektronnyi resurs]. – Rezhym dostupu: https://conferences.vntu.edu.ua/public/files/1/vntu_2020_netpub.pdf.
5. Luzhetskyi V.A. Osnovy informatsiinoi bezpeky / V.A. Luzhetskyi, A.D. Kozhukhivskyi, O.P. Voitovych. Vinnytsia: VNTU, 2013. – 221 s.
6. Zakon Ukrainy «Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy». [Elektronnyi resurs]. – Rezhym dostupu: https://zakon.rada.gov.ua/laws/show/2163-19#Text.
7. Zakon Ukrainy «Pro zatverdzhennia Zahalnykh vymoh do kiberzakhystu obiektiv krytychnoi infrastruktury» [Elektronnyi resurs]. – Rezhym dostupu: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF.
8. DSTU ISO/IEC 27005:2019. Informatsiini tekhnolohii. Metody zakhystu. Upravlinnia ryzykamy informatsiinoi bezpeky / Nats. standart Ukrainy. – Vyd. ofits. – [Chynnyi vid 2019-11-01]. – Kyiv : DP «UkrNDNTs», 2019. – 76 s.
9. Kupershtein L. Analiz zahroz informatsiinoi bezpeky v medytsyni / L. Kupershtein, O. Voitovych, Ya. Yasinska // Materialy XII Mizhnarodnoi naukovo-praktychnoi konferentsii ION-2020, 26-29 travnia 2020 r. – S. 210-211.
10. Dudatiev A.V. Otsinka stupenia ryzyku promyslovykh avarii pry nechitkykh vykhidnykh danykh / A.V. Dudatiev, V.I. Roptanov // Vymiriuvalna ta obchysliuvalna tekhnika v tekhnolohichnykh protsesakh. - 1997. - № 2. - S. 171 - 174.
11. Rotshtein A.P. Yntellektualnыe tekhnolohyy ydentyfykatsyy: nechetkye mnozhestva, neironnыe sety, henetycheskye alhorytmы / A.P. Rotshtein. Vynnytsa: Universum-Vinnytsia, 1999. — 295 s.
12. Dudatiev A.V. Rozrobka unifikovanykh modelei systemnoho proektuvannia optymalnykh system zakhystu informatsiinykh resursiv / A.V. Dudatiev // Visnyk ChTU. - 2008. - №1. - S. 3-8.