державою органами та службовими особами у регламентованих законодавством процедурних межах і процесуальному порядку.

Список використаної літератури

1.Колодій А.М., Олійник А.Ю. Права людини і громадянина в Україні: Навч. посіб. К.: Юрінком Інтер, 2004. - 336 с.

2. Конституційне право України: підручник / В.Ф. Погорілко, В.Л. Федо- ренко. 2-ге вид., переробл. К.: Прав. єдність, 2010. 432 с.

3. Кириченко Ю.В. Актуальні проблеми конституційно-правового регулювання прав, свобод та обов'язків людини і громадянина в Україні в контексті європейського досвіду. Монографія. Київ : Центр учбової літератури, 2017. 538 с.

4. Майданник О.О. Конституційне право України: Навч. посіб. К. : Алерта, 2011. 380 с.

Ронська О.Г.
к.е.н, доцент кафедри безпеки та правоохоронної діяльності,
Західноукраїнський національний університет
Ронський В.О.
ст. гр ПРт-11
Західноукраїнський національний університет

ФОРМУВАННЯ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ ЯК ОСНОВНОГО СПОСОБУ ПРОТИДІЇ ВНУТРІШНІМ ЗАГРОЗАМ

Сучасний етап розвитку суспільства характеризується зростаючою роллю інформаційної сфери, що представляє собою сукупність інформації, інформаційної інфраструктури, суб'єктів, здійснюють збір, формування, розповсюдження і використання інформації, а також системи регулювання виникаючих при цьому суспільних відносин.

В Україні, на жаль, жодна з гілок влади не приділяє належної уваги підготовці до входження в інформаційне суспільство. Поки не існує ні окремого органу виконавчої влади, що створює і проводить інформаційну політику, ні, тим більше, єдиного владного органу, який міг би об'єднати всі функції, пов'язані із забезпеченням інформаційної безпеки, реалізація яких в даний час розосереджена між службою безпеки, службою охорони, службою з технічного та експортного контролю, Міністерством оборони, Міністерством зв'язку.

Наукові дослідження, спрямовані на підвищення ефективності управління підприємством на основі формування системи інформаційної безпеки, здатної забезпечити узгодженість і ефективність дій між організаційними, технологічними, технічними, правовими та економічними факторами при створенні необхідного рівня інформаційної безпеки, є актуальними. Тому невипадково питання інформаційної безпеки вже давно входить до числа головних пріоритетів менеджменту всіх великих національних і світових компаній, а останніми роками все більше число керівників середнього і малого бізнесу починають усвідомлювати реальну небезпеку ризиків, пов’язаних з інсайдерською інформацією [1, с. 138]. Дія інсайдерів в середньому завдає більшої шкоди, ніж середня атака зовнішнього хакера на корпоративну мережу. А це разом з частотою внутрішніх витоків інформації робить цю загрозу найсерйознішою для бізнесу.

Нажаль, завжди більшої уваги надавалося зовнішнім загрозам, і замовчувалася загроза внутрішніх небезпек. Останнім часом з'являється все більше публікацій про домінуючу значущість внутрішніх загроз серед усіх загроз інформаційної безпеки. Проте термінологія, що саме вважати внутрішніми загрозами, а що зовнішніми, до сих пір не є достатньо визначеною. Наприклад, в науковій літературі США можна побачити, що під терміном «внутрішні загрози» мається на увазі, в числі інших,

несанкціонований доступ до документів і додатків з боку співробітників компанії [3, с. 21]. Всі типи інцидентів, пов'язані з використанням інформації або комп'ютера, до яких у співробітника немає доступу, американська термінологія відносить до внутрішніх загроз. З точки зору ж української термінології, ця загроза вважається зовнішньою, оскільки кошти її запобігання ті ж, що і засоби запобігання доступу до корпоративної інформації будь-яких відвідувачів офісу компанії - розподіл фізичного та інформаційного доступу.

Розглянемо обидва підходи докладніше. Для цього наведемо приклад, який ілюструє різницю в підходах до класифікації. Припустимо, співробітник, який працює з конфіденційною інформацією, відійшов на час від комп'ютера, не заблокувавши його, а в цей час колега по кабінету записав на флеш-накопичувач дані, з якими працював співробітник. За класифікацією американських науковців, це реалізація внутрішньої загрози, так як зловмисник знаходився всередині компанії. З точки зору класифікації - реалізувалася загроза зовнішня, так як зловмисник не мав службового доступу до даних і порушив не правила зберігання інформації, а правила поділу доступу до інформації.

Правильно класифікувавши потенційного порушника, співробітники підрозділу інформаційної безпеки підприємства можуть спрогнозувати поведінку порушника при неможливості здійснення спроби передачі інформації. На практиці можна скористатися класифікацією, яка умовно виділяє п'ять основних типів порушників [2]:

- Необережність. (вони порушують правила зберігання конфіденційної інформації, діючи з кращих намірів. Найчастіші інциденти з такими порушниками - винос інформації з офісу для роботи з нею вдома, у відрядженні і т. д., З подальшою втратою носія або доступом членів сім'ї до цієї інформації. Незважаючи на добрі наміри, збиток від таких витоків може бути нітрохи не меншим, ніж від шпигунів);

- Маніпуляція. (маніпуляції використовуються для отримання обманним шляхом персональної інформації користувачів - паролів, персональних ідентифікаційних номерів, реквізитів кредитних карт і адрес);

- Саботажники (це співробітники, які прагнуть завдати шкоди підприємству через особисті мотиви. Найчастіше мотивом такої поведінки може бути образа через недостатню оцінку їх ролі на підприємстві. Його метою є нанести шкоду, а не викрасти інформацію);

- Нелояльні (це співробітники, які вирішили змінити місце роботи та намагаються забрати максимально можливу кількість доступної інформації для використання у своїй подальшій роботі);

- Порушники, мотивовані ззовні (до цього типу співробітників відносять спеціально влаштованих на роботу працівників для викрадення інформації, і завербованих, тобто співробітників, спочатку лояльних, але згодом підкуплених).

Проведення навчання персоналу - обов'язкова міра, яка повинна входити в комплексну програму забезпечення інформаційної безпеки. Іншими організаційними заходами захисту від витоків інформації є розробка і чітке дотримання загальної корпоративної політики інформаційної безпеки, в яку обов'язково має входити розмежування прав. Тобто кожен співробітник повинен мати доступ тільки до тієї інформації, яка йому необхідна для роботи. Третя міра захисту є вже технічною. Мова йде про спеціалізоване програмне забезпечення, яке покликане забезпечити безпеку даних від внутрішніх загроз. Це програмне забезпечення здатне контролювати витік інформації через інтернет і електронну пошту, вести протоколи роботу всіх користувачів з конфіденційними даними і повинна мати ще ряд незамінних функцій, в тому числі і сигнал тривоги при настанні потенційно небезпечної події. Тільки повний набір всіх перерахованих заходів здатний надійно

захистити підприємство від витоку важливої інформації і, відповідно, зберегти її репутацію та кошти. Запропонована політика інформаційної безпеки може служити моделлю для підприємств широкого спектру спеціалізації при створенні їх власної політики інформаційної безпеки.

Список використаних джерел

1. Бурячок В.Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби [Підручник] / В.Л. Бурячок, Г.М Гулак, В.Б. Толубко. – К. : ТОВ «СІК ГРУП УКРАЇНА», 2015. – 449 с.

2. Сороківська О.А. Інформаційна безпека підприємства: нові загрози та перспективи / О.А. Сороківська, В.Л. Гевко // Економічні науки: Вісник Хмельницького національного університету 2010. – № 2. – Т. 2. – С. 32–35.

3. Литвинов В.В. Моделювання та аналіз безпеки розподілених інформаційних систем: навч. пос. [для студ. спец. 121 «Інженерія програмного забезпечення»] / В.В. Литвинов, В.В. Казимир, І.В. Стеценко та ін. – Чернігів: Чернігів. нац. технол. ун-т, 2016. – 254 с.