УДК 303.7
Петелін Д.Д.[1], Зайко Т.А.[2]
[1]студ. гр. КНТ-118 НУ «Запорізька Політехніка»
[2]канд. техн. наук, доц. НУ «Запорізька Політехніка»

ФІЗИЧНІ ЗАСОБИ ПІДВИЩЕННЯ ЦИФРОВОЇ БЕЗПЕКИ

В останні роки багато компаній добре усвідомили необхідність управління цифровою безпекою підприємства. Ефективне управління питаннями цифрової безпеки набуває все більшого значення для компаній по мірі їх зростання і просування на нові ринки товарів і послуг. Клієнтам важливо знати, що дотримується конфіденційність їхніх персональних і ділових даних. Інвесторам необхідна впевненість в тому, що бізнес та інформаційні активи компанії захищені. Ділові партнери очікують, що компанія буде функціонувати без збоїв, які можуть бути викликані помилками в роботі інформаційних систем, навмисними або ненавмисними діями персоналу, шкідливим програмним забезпеченням та іншими факторами.

Управління цифровою безпекою – це комплекс заходів, які ґрунтуються на підході, що враховує бізнес-ризики, призначені для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення інформаційної безпеки.

Побудова ефективної системи управління цифровою безпекою – це не разовий проект, а комплексний процес, спрямований на мінімізацію зовнішніх і внутрішніх загроз при обліку обмежень на ресурси та час.

Для побудови ефективної системи цифрової безпеки необхідно спочатку описати процеси діяльності. Потім слід визначити поріг ризику – рівень загрози, при якому вона потрапляє в процес управління ризиками. Потрібно побудувати таку систему цифрової безпеки, яка забезпечить досягнення заданого рівня ризику.

Фізичні види порушень включають фізичне пошкодження апаратних засобів автоматизованих систем, ліній зв'язку і комунікаційного устаткування, крадіжки або несанкціоноване ознайомлення з вмістом носіїв інформації, що зберігаються в неналежних місцях, розкрадання носіїв інформації, відмови апаратних засобів та ін.

Як же запобігти фізичним видам порушень? Фізичні засоби захисту – це засоби, необхідні для зовнішнього захисту засобів обчислювальної техніки, територіїта об'єктів на базі ПК, які спеціально призначені для створення фізичних перешкод на можливих шляхах проникнення і доступу потенційних порушників до компонентів інформаційних систем та інформації, що захищаються.

До законодавчих засобів захисту відносяться законодавчі акти, які регламентують правила використання і обробки інформації обмеженого доступу і встановлюють заходи відповідальності за порушення цих правил.

Найпростіший і надійний спосіб захисту інформації від загроз несанкціонованого доступу (НСД) - режим автономного використання ПК одним користувачем у спеціально виділеному приміщенні при відсутності сторонніх осіб. У цьому випадку роль замкненого контуру захисту виконує виділене приміщення, а фізичний захист- вікна, стіни, підлога, стеля, двері. Якщо стіни, стеля, підлога і двері міцні, підлога не має люків, які з'єднуються з іншими приміщеннями, вікна і двері обладнані охоронною сигналізацією, то стійкість захисту буде визначатись технічними характеристиками охоронної сигналізації при відсутності користувача в неробочий час.

У робочий час, коли ПК працює, можливий витік інформації каналами побічного електромагнітного випромінювання. Для усунення такої загрози здійснюються спеціальні дослідження щодо апаратих засобів та їх випромінювання, основним змістом яких є атестування та категорування засобів і об'єктів електронно-обчислювальної техніки (ЕОТ) з видачею відповідного дозволу на експлуатацію. Крім того, двері приміщення повинні бути обладнані механічним або електромеханічним замком. У деяких випадках, коли відсутня охоронна сигналізація, на період тривалої відсутності користувача ПК для підвищення безпеки доцільно системний блок і машинні носії інформації зберігати в сейфі. Використання в деяких

ЕОМ у системі вводу-виводу BIOS апаратного паролю, що блокує завантаження і роботу ПК, не зовсім надійно забезпечує захист від загроз НСД, оскільки при відсутності на корпусі системного блоку механічного замка та самого власника-користувача апаратна частка BIOS-носія паролю може бути замінена на іншу таку ж, оскільки вузли BIOS уніфіковані, але вже з відомим значенням паролю. Саме тому механічний замок, що блокує вмикання і завантаження ПК є найбільш ефективним заходом у цьому випадку.

Спектр сучасних фізичних засобів захисту дуже широкий. До цієї групи засобів захисту належать також різні засоби екранування робочих приміщень та каналів передачі даних.

Можна зробити висновок, що інформацію слід захищати не тільки від внутрішніх загроз, а також і від зовнішніх.