УДК 004.056
DOI: 10.31673/2409-7292.2022.015660

Букет Д.А.

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ЗА ДОПОМОГОЮ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ

У представленій роботі розглядається питання удосконалення організаційних заходів із захисту інформації шляхом розроблення концепції системи захисту інформації задля побудови комплексної системи захисту інформації (КСЗІ) на підприємстві. Це дасть змогу покращити та збільшити рівень захищеності, що забезпечується КСЗІ на підприємстві, та допоможе віднайти оптимальне рішення щодо побудови КСЗІ для різних підприємств та організацій. Також стаття описує різні методи, засоби та підходи захисту інформаційних ресурсів. Виходячи з цього, було визначено організаційні та програмно-технічні міри захисту як найефективніші. На основі цих досліджень було розроблену концепцію системи захисту інформації для побудови КСЗІ для підприємства.

Ключові слова: інформаційна безпека, методи забезпечення інформаційної безпеки, кібербезпека, комплексна система захисту інформації.

Вступ

Захист інформації у діяльності сучасного підприємства – один з основних напрямків, який вимагає проведення постійного аналізу якості засобів і методів захисту, що застосовуються, а також їх оперативної зміни та вдосконалення. Необхідність забезпечення безпеки, захищеності комерційної інформації та конфіденційних даних диктується умовами сучасного ринку. У зв'язку з бурхливим розвитком інформаційних технологій та технічних засобів система захисту інформації підприємства стає вразливою і як наслідок підприємству може бути завдано економічної шкоди. Проблеми захисту інформації виникають у зв'язку з масовим створенням та поширенням інформаційних систем. Аналіз та дослідження даної проблематики показують [1]:

якщо підприємство допускає витік понад 20% важливої внутрішньої інформації, то воно у 60 випадках із 100 стає банкрутом;

93% підприємств, що втратили доступ до власної інформації на термін більше 10 днів, припиняють займатися діяльністю (причому половина з них заявила про свою неспроможність негайно).

Тому постає питання, як з максимальною ефективністю забезпечити інформаційну безпеку на підприємстві? У часи такого стрімкого технологічного розвитку у світі вже майже не лишилось компаній та організацій, які так чи інакше не були б пов’язані з кіберпростором. Такі швидкі тенденції прогресу породжують багато не лише позитивних, а й негативних наслідків, одними з яких є велика кількість різноманітних загроз, наприклад, кібератак. Тому все більше уваги і ресурсів приділяється впровадженню та забезпеченню кібернетичної та інформаційної безпеки.

Мета роботи – огляд та аналіз методів захисту інформації з метою створення концепції комплексної системи захисту для підприємства.

Основні засади комплексної системи захисту інформації

Аналізуючи деякі існуючі публікації [2 с. 89-94, 3 с. 29-33], у яких зокрема розглядаються способи та підходи до захисту інформації, все ж постає питання який з методів є найефективнішим.

Методи інформаційної безпеки. Загалом будь-яка система захисту та управління кібербезпекою в інформаційних системах повинна базуватись на трьох основних критеріях: доступність інформації (можливість використовувати інформацію згідно встановленим правилам), цілісність інформації (здатність інформації зберігатись в незмінному вигляді, без права на модифікацію неавторизованими користувачами), конфіденційність інформації (стійкість до спроб несанкціонованого доступу до інформації, збереження конфіденційності при її використанні) [4, с. 12-13]. Вибір способів, за допомогою яких буде гарантуватись інформаційна безпека, відбувається в залежності від особливостей та сфери діяльності

організації. В основному у середовищі інформаційної безпеки виокремлюють наступні методи захисту: організаційні (управлінські), програмно-технічні, правові та методи мережевої безпеки [4, с. 14].

Проте оптимальним варіантом може бути комплексне застосування кількох базових методів. Тобто створення, реалізація, введення в експлуатацію з подальшим управлінням та вдосконаленням системи захисту інформації. Для підвищення рівня захищеності інформації, різні засоби захисту (апаратні, програмні, фізичні, організаційні тощо) повинні використовуватись одночасно і під централізованим керуванням. Це передбачається створенням комплексної системи захисту інформації від несанкціонованого доступу.

Комплексна система захисту інформації. КСЗІ – сукупність організаційних та інженерно-технічних заходів, спрямованих на забезпечення захисту інформації від розголошення, витоку та несанкціонованого доступу [5].

Основними цілями КСЗІ є:

захист законних інтересів підприємства від протиправних дій;

не допустити розкрадання фінансових та матеріально-технічних засобів;

захистити від розголошення, витоку та несанкціонованого доступу до службової інформації

не допустити порушення роботи технічних засобів забезпечення виробничої діяльності, включаючи інформаційні технології.

КСЗІ є глобальною концепцією безпеки та основою для безпеки інфраструктури підприємства загалом. КСЗІ є універсальним підходом щодо встановлення безпеки та основною концепцією для безпеки інфраструктури підприємства загалом. Необхідність побудови КСІ визначається вимогами нормативних документів у сфері технічного та криптографічного захисту інформації або бажанням власника інформаційних ресурсів.

Організаційні методи захисту. Організаційні засоби захисту є обов’язковою частиною будь-якої КСЗІ, а програмно-технічні заходи впроваджуються в міру необхідності, виходячи з потреб, можливостей та стану захищеності інформації підприємства.

Організаційні міри захисту передбачають:

створення посадових інструкцій для працівників підприємства (користувачів системи) та обслуговуючого персоналу;

встановлення правил адміністрування інформаційної системи, обліку, зберігання, розповсюдження, знищення носіїв інформації, ідентифікації користувачів;

розробка плану дій у разі виявлення спроб несанкціонованого доступу до інформаційних ресурсів системи, виходу з ладу засобів захисту, виникнення надзвичайної ситуації;

навчання правилам інформаційної безпеки користувачів.

Програмно-технічні засоби захисту. Програмно-технічні міри захисту, що проводяться для захисту інформаційної інфраструктури підприємства, можуть включати використання захищених підключень, міжмережевих екранів, розмежування потоків інформації між сегментами мережі, використання засобів шифрування і захисту від несанкціонованого доступу. Також ефективним є застосування наступних систем: система виявлення вторгнень (IDS), система запобігання вторгнень (IPS), також UTM-системи та ін. У разі необхідності, в рамках проведення інженерно-технічних заходів, може здійснюватися установка в приміщеннях систем охоронно-пожежної сигналізації, систем контролю і управління доступом.

Комплексна система захисту інформації на підприємстві передбачає два види функцій:

функції, основною метою яких є створення механізмів захисту;

функції, що здійснюються з метою безперервного та оптимального керування механізмами захисту.

Створення концепції системи захисту інформації

Основною метою управління системою захисту на підприємстві є забезпечення максимально можливої ефективності використання ресурсів. Технологія управління має бути

побудована так, щоб забезпечувати ефективну обробку інформації для всіх функціональних підрозділів під час раціонального використання ресурсів сучасних засобів обчислювальної техніки та інформаційних технологій.

Особливе місце в сучасній системі захисту інформації на підприємстві мають інформаційні ресурси. Під інформаційними ресурсами розуміються документи та масиви документів в інформаційних системах підприємства.

Інформаційні ресурси підприємства схильні до різноманітних загроз. Для зниження загроз, вразливостей, ризиків для підприємства необхідний контроль та ефективне управління інформаційними ресурсами.

Питання розподілу, використання та захисту інформаційних ресурсів підприємства покладено на службу КСЗІ, яка формує стратегію потреб в інформаційних ресурсах, що оцінює поточний стан системи захисту інформації та ефективність використання інформаційних ресурсів.

На підприємстві захист інформаційних ресурсів зводиться до оптимізації методів захисту інформації, технічних засобів та її складу. Управління інформаційними ресурсами пов'язані з потужністю підприємства. Інформаційна потужність підприємства – синергетична характеристика, що описує рівень ефективності використання існуючих інформаційних активів для збільшення конкурентоспроможності підприємства з досягненням максимуму при:

повному використанні функціоналу та можливостей інформаційних систем,

організації інформаційних бізнес-рішень, адекватних завдань, що вирішуються підприємством [6].

Відповідно до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» [7]:

інформація, що є власністю держави, або інформація з обмеженим доступом має бути захищена шляхом побудови КСЗІ, та подальшим отриманням «Атестату відповідності», який видається Адміністрацією державної служби спеціального зв'язку та захисту інформації України за результатами проведення державної експертизи КСЗІ;

інша інформація може бути захищена за допомогою КСЗІ за бажанням її власника.

Загалом можна виділити дві основні категорії вразливостей інформаційної системи: людський фактор користувача цієї системи та незахищеність чи несправність роботи програмного та системного забезпечення. Тому при проектуванні системи захисту потрібно обов’язково враховувати це, будуючи її за двома напрямками.

На основі розглянутих досліджень було розроблену наступну концепцію системи захисту (рис. 1).

Створена концепція – це система, що складається з комплексу заходів, націлених на виявлення та запобігання атакам, і побудована на двох основних принципах: організаційні та програмно-технічні міри захисту.

Організаційними мірами є захист інформації шляхом регулювання за допомогою організаційних заходів доступу до всіх ресурсів інформаційної системи. Програмно-технічні міри захисту можуть включати в себе такі рішення як система виявлення вторгнень (IDS), система запобігання вторгнень (IPS), UTM-системи і т. д.

Робота такої комплексної системи складається з трьох основних етапів: запобігання (до атаки), реагування (під час атаки) та відновлення (після атаки). За допомогою цієї системи можна оптимально та ефективно забезпечити впровадження та управління інформаційною безпекою на підприємстві.

Перспективи застосування. Матеріали даної статті можна використовувати для створення тактик забезпечення безпеки інформаційних систем. За допомогою розробленої концепції системи захисту можна розгорнути оптимальну КСЗІ для будь-якого підприємства чи організації.

Основною метою подальшої роботи буде формування та детальна розробка кожного елемента КСЗІ, на основі розглянутої концепції. Також буде проведено аналіз ефективності

запропонованого комплексу із заходів для захисту інформації після тестового впровадження. Після чого буде визначено оптимальність як створеної концепції системи захисту, так і побудованої на ній КСЗІ, що дасть змогу вдосконалити дану розробку.

Рис. 1. Концепція системи захисту інформації для створення КСЗІ

Висновки

Отож, проблема інформаційної безпеки є дійсно важливою та потребує постійного пошуку нових рішень захисту, адже світ змінюється, і кіберзлочинці відповідно

вдосконалюють способи вчинення атак. Оскільки вірогідність того, що загрози у кіберпросторі можуть повністю припинитись, є мінімальною, то основна задача – вміти приймати запобіжні заходи: правильно створювати, впроваджувати та контролювати систему, яка допомагає керувати інформаційною безпекою.

Проаналізувавши ситуацію в інформаційному просторі, яка склалась на даний час, можна зробити висновки, що забезпечення захисту інформації на сучасних підприємствах є однією з ключових тенденцій, яка потребує постійне проведення нових досліджень та знаходження дієвих та ефективних засобів та мір захисту, та вдосконалення тих методів, що вже використовуються.

У даній статі було досліджено методи, засоби та підходи захисту інформаційних ресурсів. Було описано найефективніші міри захисту: організаційні та програмно-технічні. Також було розглянуто доцільність та необхідність застосування КСЗІ на підприємствах, враховуючи реалії сьогодення. На основі цих досліджень було розроблену концепцію системи захисту інформації для побудови КСЗІ для підприємства.

Перелік посилань

1. Хайретдинов Р.Н. Комплексная методика оптимизации затрат на создание корпоративной системы защиты информации: дисс. канд. экон. наук … по спец. 08.00.05. – Москва, 2011. – 189 с.
2. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання: монографія / А.Ю. Нашинець-Наумова. – Київ: Видавничий дім «Гельветика», 2017. – 168 с.
3. Інформаційна безпека держави: навч. посіб. для студ. спец. 6.170103 «Управління інформаційною безпекою», 125 «Кібербезпека»/ В.І. Гур'єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2018. – 166 с.
4. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка.— К.: ДУТ, 2015.— 288 с.
5. Домарєв В.В. Безопасность информационных технологий. Методология создания систем защиты. - К.: ТИД Диа Софт, 2002.— 688 с.
6. Абросимов В.К., Канев С.А. Информационная мощность компании // Бизнес-информатика, №3(13), 2010.
7. Про захист інформації в інформаційно-телекомунікаційних системах [Електронний ресурс]: закон України від 05.07.1994 № 80/94-ВР. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/80/94-вр.

Надійшла: 22.01.2022 Рецензент: д.т.н., професор Кожухівський А.Д.