Папуша К.А.
магістрантка,
Науковий керівник: **Гадецька З.М.**
кандидат технічних наук, доцент,
Черкаський національний університет
імені Богдана Хмельницького

КОМПЛЕКСНИЙ ЗАХИСТ КОРПОРАТИВНИХ МЕРЕЖ

На сьогоднішній день в сучасному економічному світі спостерігаємо стрімкий ріст глобалізації та комп'ютеризації. В зв'язку з цим, разом із безперервним розвитком інформаційних технологій з'являються нові способи втручання в роботу комп'ютерних систем. Існуючі традиційні механізми безпеки, реалізовані в брандмауерах, серверах аутентифікації, системах блокування доступу тощо є важливими інструментами для атаки. Для стабільної і безперервної роботи захищеної мережі та її побудови, необхідні інструменти, які здатні одночасно виявляти та блокувати атаки, та, що не менш важливо, запобігати їх появленню. Виходячи з вимог, що представлені для формування і функціонування захищеної комп'ютерної системи, в даній роботі будуть розглянуті сучасні методи захисту комп'ютерної системи та запропоновано новий підхід до захисту – адаптивний захист.

Розробка корпоративних систем інформаційної безпеки є важливим аспектом створення корпоративної мережі. Реалізація системи захисту здійснюється для запобігання несанкціонованому проникненню в інформацію, що обробляється автоматизованою системою. Передбачається, що існує «джерело інформації» та «одержувач інформації», а інформація передається через канали зв'язку.

Для зменшення неприпустимості або зменшення ймовірності загроз проводиться захист корпоративної мережі. Загрозою безпеці є вжиття будь-яких дій проти захисту об'єкта або пошкодження.

Система забезпечення безпеки інформації повинна мати наступну структуру і включати такі рівні [1]:

– рівень захисту автоматизованих робочих місць (АРМ);

– рівень захисту локальних мереж і інформаційних серверів;

– рівень захисту корпоративної мережі.

На рівні безпеки автоматичних робочих просторів користувачі операційної системи повинні бути ідентифіковані і автентифіковані. Доступ повинен контролюватись: дати доступ до товарів по матриці доступу, брати до уваги всі впливи, пов'язані з втіленням у життя реєстрації та доступ до журналів реєстрації. Необхідно гарантувати єдність програмного середовища регулювання і постійне випробування засобів захисту інформації. Рекомендовано гарантувати захист від несанкціонованого доступу за допомогою сертифіката захисту. Ці функції безпеки повинні підключати прилад до гнучких налаштувань і можливості до віддаленого управління.

Ступінь безпеки корпоративної мережі повинен забезпечувати єдність передачі інформації від джерела до отримувача, а також захищати від несанкціонованого розкриття інформації [2].

Наявні звичайні захисні механізми працюють лише у другій фазі атаки. Іншими текстами це метод заблокувати, а не обмежити атаку. Найчастіше він захищає від існуючих атак.

Вбудована система оборони інформації повинна працювати на всіх трьох фазах атаки. І на третьому, заключному рубежі забезпечення наступної безпеки найменш важливо, ніж на перших двох етапах. Оскільки тільки в цьому випадку можна оцінити шкоду, завдану «успішною» атакою, а також зробити кроки для знищення наступних наміру подібної атаки.

Адаптивна консервація – становлення нормальних приладів консервації. Він не ліквідує класичних практик, а розширює їх активні можливості на нові технології.

Адаптивна безпека мережі складається з трьох основних елементів:

– технології аналізу захищеності;

– технології виявлення атак;

– технології управління ризиками.

Засоби аналізу захищеності працюють на першому етапі здійснення атаки. Виявляючи і вчасно усуваючи вразливості, вони тим самим усувають саму можливість реалізації атаки, що дозволяє понизити витрати на експлуатацію засобів захисту. Системи аналізу захищеності проводять пошук вразливостей КМ на усіх чотирьох рівнях поступово, починаючи з мережевого.

Виявлення атак вважається ходом оцінки підозрілих вчинків, що здійснюються у корпоративній мережі. Виявлення атак реалізується за допомогою аналізу чи журналів реєстрації операційної системи та прикладного програмного забезпечення, чи мережевого трафіку у реальному часі. Складові виявлення атак, поміщені на вузлах або розділах мережі, розглядають різні дії, у яких кількості і використовують знайому вразливості. Методи виявлення атак працюють відразу на двох етапах здійснення атак – другому і третьому. Подібно до засобів аналізу безпеки способи виявлення атак ще працюють на всіх рівнях корпоративної мережі.

Використання моделі адаптивної безпеки мережі дозволяє контролювати практично всі ризики і вчасно відгукуватися на їх високоефективним методикою, що дозволяє не тільки прибрати вразливості, які можуть призвести до реалізації небезпеки, але і досліджувати умови, що призводять до їх появи. За допомогою цієї моделі можна зменшити зловживання в мережі, збільшити поінформованість користувачів, адмінів та інструкція компанії про заходи в мережі.

Список використаних джерел:

1. Биячуев Т.А. Безопасность корпоративных сетей. СПб. : СПб ГУ ИТМО, 2004. 161 с.

2. Кивиристи А.О. Адаптивная безопасность сети. *«КомпьютерПресс».* URL: http://www.compress.ru