Глухенький С.О. магістрант, гр. ІСТм-19-1
Науковий керівник: Лобанчикова Н.М., канд. техн. наук, доц.
Державний університет «Житомирська політехніка»

НЕОБХІДНІСТЬ РОЗРОБКИ СИСТЕМИ АНАЛІЗУ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ І МЕРЕЖАХ

Розвиток нових інформаційних технологій, загальна комп'ютеризація і різке збільшення кількості інформаційно-комунікаційних систем і мереж (ІКСМ) сьогодні призводять до того, що інформаційна безпека стає провідним питанням більшості компаній. Фактор безпеки інформаційних ресурсів і послуг при розробці та експлуатації сучасних ІКСМ грає першорядну роль. При організації систем захисту потрібно керуватися рядом принципів, що забезпечать якісний захист і протидію від існуючих загроз.

В основі інформаційної безпеки лежить діяльність по захисту інформації – забезпечення її конфіденційності, доступності та цілісності, а також недопущення будь-якого доступу сторонньої особи до інформації, що захищається. Зараз, не дивлячись на те, що в більшості організацій документація досі базується на паперових документах, спостерігається неухильне зростання числа ініціатив по впровадженню цифрових технологій на підприємствах, що тягне за собою залучення фахівців з інформаційної безпеки, як правило, собі в штат. В їх завдання входить убезпечити всі технології від шкідливих кібератак, найчастіше націлених на викрадення важливої конфіденційних відомостей або на перехоплення управління внутрішніми системами організації.

Щодо загроз безпеці, то їх у загальному вигляді визначають як сукупність чинників та умов, що створюють небезпеку певному об’єкту. Загрозу розглядають як родову ознаку безпеки (можливість чи неминучість виникнення соціальних, природних або техногенних явищ із прогнозованими, але неконтрольованими небажаними подіями, що можуть статись у певний момент часу в межах певної території, спричинити смерть людей чи завдати шкоди їхньому здоров’ю, призвести до матеріальних і фінансових збитків тощо) [1]. Небезпеку ж науковці вважають якісним станом – безпекою на її нульовому рівні.

Саме через це в 2018 році в Євросоюзі введений в дію Загальний регламент щодо захисту даних (англ. General Data Protection Regulation, GDPR), що вимагає від кожної організації в будь-який момент часу на усіх ділянках власної діяльності або ланцюга поставок, продемонструвати, які персональні дані і для яких цілей є в наявності, як вони обробляються, зберігаються і захищаються. При чому ці відомості повинні бути надані не тільки в ході перевірок уповноваженими органами, а й на вимогу приватної особи – власника цих даних.

Дотримання такого комплексу дій вимагає від компанії значних затрат коштів і ресурсів. І хоча в порядкування обробки персональних даних передбачає в довгостроковій перспективі поліпшення інформаційної безпеки, в короткостроковому плані ризики організації помітно зростають.

Найбільше зміна, яке відбудеться в організації після імплементації GDPR, буде не поява нових правил і політик, а перегляд ставлення до персональних даних та їх захист, а саме: компанії відчують більшу відповідальність за збір, обробку та зберігання даних; розробка продукту або сервісу буде починатися з продумування і оцінки впливу і ризиків для даних вже до, а не після релізу; кожен співробітник, який має доступ до персональної інформації буде обізнаний про правила і тому буде вже усвідомлено піклуватися про збереження персональних даних, тим самим дотримуючись базових правил щодо їх захисту.

На превеликий жаль необхідно констатувати, що на сьогодні не у всіх ІКС вирішено проблему захисту даних. Причин тому декілька – від відсутності належного фінансування та матеріально-технічного забезпечення до недооцінки відповідальними особами важливості захисту інформації. Інформаційна безпека, як сфера зайнятості, значно зазнала розвитку в останні роки. У цій галузі з’явилось безліч професійних спеціалізацій, наприклад, таких, як безпека мереж і пов'язаної інфраструктури, захист програмного забезпечення та баз даних, аудит інформаційних систем, планування безперервності бізнесу, виявлення електронних записів і комп'ютерна криміналістика тощо.

Таким чином, на основі проведеного аналізу сучасних інформаційно-комунікаційних систем, та загроз пов’язаних із ними – можемо зробити висновок, що разом із зростаючим попитом ІКСМ збільшується кількість загроз та ризиків. Тому доцільне впровадження систем захисту інформації, але наразі маємо велику нестачу кваліфікованого персоналу в цій області. В наслідок чого, розробка системи аналізу захищеності інформації в інформаційно-комунікаційних системах і мережах, яка буде допомагати перевірити ступінь безпеки ІСТМ без залучення спеціально навчених працівників, є необхідною.

Список використаних джерел:

1. Грайворонський М. В., Новіков О. М. Г14 Безпека інформаційно-комунікаційних систем. — К.: Видавнича група ВНУ, 2009. — 608 с.