систем. Кроме того, крайне важно иметь соответствующие контакты внутри компании, с операторами транзита, а также с поставщиками услуг защиты от DDoS-атак.

Список использованных источников:

1. DoS-атака [Электронный ресурс]. – URL: https://ru.wikipedia.org/wiki/DoS-%D0%B0%D1%82%D0%B0%D0%BA%D0%B0
2. Что такое DDoS-атака [Электронный ресурс]. – URL: https://aws.amazon.com/ru/shield/ddos-attack-protection/
3. Защита от DDoS [Электронный ресурс]. – URL: https://www.xelent.ru/services-additional/zashchita-ddos/
4. DDoS-атака – что это такое? [Электронный ресурс]. – URL: https://ddos-guard.net/ru/terminology/attacks/ddos-ataka
5. Способы защиты от DDoS-атак [Электронный ресурс]. – URL: https://timeweb.com/ru/community/articles/sposoby-zashchity-ot-ddos-ataki-1

Ключові слова: DDoS, DDoS-атака, захист від DDoS-атак.
Ключевые слова: DDoS, DDoS-атака, защита от DDoS-атак.
Keywords: DDoS, DDoS attack, DDoS attack protection.

Научный руководитель: *к.т.н., доцент Соколов А. В.*

Саніцька Інна Валеріївна
Національний університет «Одеська юридична академія»,
студентка 4 курсу факультету кібербезпеки
та інформаційних технологій

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ

Інформаційна безпека – це такий стан захищеності інформаційної інфраструктури, включаючи також комп'ютери та інформаційно-телекомунікаційну інфраструктуру і інформацію, що в них знаходиться, який також забезпечує сталий розвиток особистості, суспільства і держави.

На сьогодні в Україні немає чітко врегулювання вимог до Інформаційної безпеки на підприємствах. При цьому є вимоги які ставляться до компаній, які працюють з персональними даними громадян Європейського союзу відповідно до вимог General data protection regulation (GDPR), та деяких інших нормативних актів.

Останні тенденції нормотворення, зокрема, проект Постанови НБУ «Про затвердження Положення про кіберзахист та інформаційну безпеку в платіжних системах та системах розрахунків», окремі норми Закону України «Про основні засади забезпечення кібербезпеки України» та деякі інші, вказують на те, що в близькому майбутньому нас чекає чітке законодавче регулювання з жорсткими вимогами до Політик інформаційної безпеки підприємств.

Не випадково питання інформаційної безпеки вже давно входять до головних пріоритетів практично всіх великих компаній. Останнім часом більше керівників середнього і малого вітчизняного бізнесу починають усвідомлювати реальну небезпеку ризиків, пов'язаних з інсайдерською інформацією, системами її обробки і співробітниками, що беруть участь у цьому процесі [1].

Інформація може бути будь-якою, як інформація про вашу компанію, вашу особисту інформацію, ваші конфіденційні дані на вашому комп'ютері чи мобільному телефоні тощо.

Але це не єдине пояснення, яке дають нам науковці, адже інформаційна безпека – це порятунок життя організацій по всьому світі. Людей, які працюють у цій галузі, можна вважати та називати лікарями комп'ютерної системи.

Ми не можемо недооцінювати вплив кібератак, які можуть призвести до втрати даних, витоку особистої інформації, втрати часу та розповсюдження вірусів в організаціях.

Безпека – це сфера, яка може створити або в іншому випадку знищити компанію. Дуже важливо в організаціях тримати конфіденційну цифрову інформацію та захищати технічні системи від вірусів та хакерів [2].

Компанії впроваджують інформаційну безпеку з широкого кола причин. Основні цілі, як правило, пов'язані із забезпеченням конфіденційності, цілісності та доступності інформації про саму компанію.

Багато людей досі не мають уявлення про важливість інформаційної безпеки та її реалізації для організації. Багато менеджерів мають хибне уявлення про те, що інформація в їх комп'ютерах повністю захищена і не містить жодних загроз. На жаль, це є зовсім не так. Важливо відмовитись від переконання, що комусь неможливо проникнути у ваші особисті дані, чи дані вашої організації, оскільки компанія вживає заходів для захисту своєї інтелектуальної власності.

З розвитком технологій кібератаки швидко еволюціонують і будь-яка організація, яка має шляхи подолання наслідків кібератак, може не впоратись з хвилею нової атаки [3].

Нехтуючи інформаційною безпекою, вся компанія знаходиться в серйозній небезпеці, оскільки її дані та інформація від клієнтів та ділових партнерів знаходяться під загрозою. Кібератака може спричинити серйозні проблеми та незліченну шкоду бізнесу.

Американський політик Джо Енн Девіс зазначав: «Оскільки країна все більше покладається на електронне зберігання та зв'язок інформації, обов'язково потрібно, щоб уряд вносив відповідні зміни до наших законів про інформаційну безпеку». З цим важко не погодитись, адже через відсутність захисту інформаційних систем багато «успішних» атак були спрямовані на такі компанії.

Втрати у великих компаніях внаслідок кібератак часто викликають більш шокуючі суперечки навіть щодо кількості вкраденої інформації. Невеликі компанії, в такому випадку, чекає закінчення їх бізнесу та фінансових проблем, що призведуть до банкрутства установи.

Для багатьох організацій інформація є їх найважливішим надбанням, тому її захист є надзвичайно важливим.

Питання аналізу загроз і ризиків є визначальним при побудові ефективної системи захисту інформації. Однак, за

оцінками фахівців, лише не більше 5% підприємств використовують власні методики аналізу ризиків, що дозволяють виконувати кількісний аналіз та оптимізацію підсистеми інформаційної безпеки. Водночас дії внутрішніх порушників, такі як недбалість співробітників, крадіжки інформаційних ресурсів та IT-устаткування, фінансові й інші види шахрайства з використанням інформаційних систем і ресурсів тощо, набагато рідше стають предметом уваги при розв'язанні проблем інформаційної безпеки у випадку, якщо вони розглядаються у відриві від загальних завдань забезпечення економічної безпеки.

Впровадження інформаційної безпеки в організації може захистити технологію та інформаційні активи, які вона використовує, запобігаючи, виявляючи та реагуючи на внутрішні та зовнішні загрози.

Для підтримки стратегії інформаційної безпеки організації важливо підвищити обізнаність персоналу з питань інформаційної безпеки за допомогою тренінгів та семінарів. Організаціям також потрібно дотримуватися своїх політик захисту інформації та регулярно їх переглядати, щоб задовольнити вимоги безпеки.

Можливі загрози та вразливості повинні бути оцінені та проаналізовані. Це означає встановлення та впровадження контрольних заходів та процедур для мінімізації ризику та проведення аудиту для оцінки ефективності контролю [4].

Існує три основні цілі, які захищені інформаційною безпекою:

1. Конфіденційність – запобігає доступу несанкціонованих користувачів до інформації для захисту конфіденційності інформаційного вмісту. Порушення конфіденційності можуть відбутись через помилки під людським впливом, навмисне обмін даними або зловмисний вхід.

2. Цілісність –забезпечує достовірність та точність інформації. Втрата цілісності може статися, коли інформація не захищена від умов навколишнього середовища, не передана належним чином цифрова інформація або коли користувачі вносять несхвалені зміни.

3. Доступність – забезпечує авторизованим користувачам надійний доступ до інформації. Доступність забезпечується за допомогою безперервності процедур доступу, резервного копіювання або копіювання інформації, а також технічного обслуговування та мережевих з'єднань.

Погіршення на підприємстві таких параметрів інформації, як конфіденційність, цілісність, доступність, вірогідність тощо, може призвести до досить негативних наслідків: збоїв у функціонуванні систем управління технологічними процесами й іншими критичними системами; розголошення відомостей, що становлять комерційну й інші види таємниць; порушення вірогідності фінансової документації; несанкціонованого доступу до персональних даних фізичних осіб тощо.

Найбільш зацікавленими сторонами в безпеці організації є клієнти, які не хочуть, щоб їхні дані були виставлені неналежним чином та всезагальний огляд.

Деякі фактори ризику, які можуть залишитися непоміченими, – це застаріле обладнання, незахищені мережі, неправильна конфігурація та навіть відсутність підготовки працівників. Також існує кілька помилок, які можуть підірвати конфіденційність інформації в компаніях.

Наявність ІТ-відділу, підготовленого до захисту інформації, сьогодні є фундаментальним. Уже існують різні засоби інформаційної безпеки, які дозволяють уникнути серйозних проблем та забезпечити цілісність та конфіденційність інформації, що, зрештою, є першим бажанням компаній. Інформація буде безпечною лише тоді, коли користувачі та ІТ-фахівці будуть діяти відповідно, створюючи найкращі способи уникнути майбутніх ризиків [5].

Нарешті, обізнаність щодо інформаційної безпеки організації є дуже важливою практикою для всіх середніх та великих компаній. Це захистить дані компанії, запобігаючи загрозам та будь-яким вразливостям.

Один з найважливіших девізів наукової фантастики говорить «майбутнє зараз», але це майбутнє, яке кожен зобов'язаний будувати.

Це просте повідомлення, але таке, що вимагає відданості підприємців визнанню безпеки як необхідного фактора у винаході майбутнього. Особливої уваги потребує реальне втілення заходів щодо забезпечення інформаційної безпеки, які мають стати основою для формування та реалізації інформаційної політики підприємства, захисту інформації від внутрішніх та зовнішніх загроз.

Список використаних джерел:

1. Сорокін О. Л. Інформаційна безпека та її складові: проблеми визначення кон- цепту. *Держава та право*. 2014. No8. С. 18–22.

2. Ніколаєв В., Остапович Г., Костицька І. та ін. Правове регулювання інформаційної безпеки у сфері підприємницької діяльності. К., 2002. С. 19–25

3. Шубіна О. В. Державна інформаційна безпека: проблеми визначення концепту. *Держава та права*. 2014. No3. С. 26–31.

4. Information Security Requirements: Your Obligations & Considerations, Published by Stephanie Baskerville June 10, 2020 Режим доступу: https://www.proserveit.com/blog/information-security-requirements

5. Караулов О. Н. Захист комп'ютерної інформації з точки зору міжнародного права. *Вісник Української академії державного управління при Президентові України*. 2014. No11. С. 53–63.

Ключові слова: Інформація, інформаційна безпека, кібератака, організація, економіка, компанія

Ключевые слова: Информация, информационная безопасность, кибератака, организация, экономика, компания

Keywords: Information, information security, cyber attack, organization, economy, company

***Науковий керівник**: д. фіз.-мат. н., професор Василенко М. Д.*