Отже, потрібно завжди дотримуватись певних правил що до користування особистими даними в кіберпросторі, щоб не попасти в тенета злочинців, і не стати їх жертвою.

У випадку, якщо ви все ж стали жертвою, необхідно відразу звернутись до найближчого відділу поліції або зателефонувати 102. Потрібно зібрати інформацію, яка підтверджує факти вчинення проти вас шахрайських дій: квитанції з банку про проведення грошових операцій, чеки про оплату, роздруківки оголошень, посилання на сайт тощо.

Зверніться до адміністратора сайту з метою блокування сторінки шахрая, а також зателефонуйте в банк, через який було здійснено платіжні операції, повідомте, що переказ здійснено на картку шахрая.

Після притягнення винної особи до кримінальної відповідальності, ви можете звернутись до суду з вимогою відшкодування матеріальної та моральної шкоди.

Згідно із частиною першою статті 1212 Цивільного кодексу України особа, яка, набула майно або зберегла його у себе за рахунок іншої особи (потерпілого) без достатньої правової підстави (безпідставно набуте майно), зобов`язана повернути потерпілому це майно. Особа зобов'язана повернути майно і тоді, коли підстава, на якій воно було набуте, згодом відпала [2].

Тому в ситуації, коли ви в інтернеті перерахували кошти шахраям, дієвим способом захисту може бути звернення до суду з позовом про повернення безпідставно набутих коштів до власника банківського рахунку, на який було здійснено зарахування коштів.

Список використаних джерел

1. Як не стати жертвою шахраїв в інтернеті та що робити, якщо ви потрапили у пастку. Офіційний сайт Міністерства юстиції. URL: https://minjust.gov.ua/m/yak-ne-stati-jertvoyu-shahraiv-v-interneti-ta-scho-robiti-yakscho-vi-potrapili-u-pastku (27.04.2023)

2. Цивільний кодекс України. Законодавство України – офіційний сайт Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/435-15#Text (27.04.2023).

Одержано 01.05.2023

УДК 313

ЗІНЧЕНКО Даніїл Анатолійович,
слухач магістратури факультету № 3
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0002-8089-0511;

МАКАРОВА Олена Павлівна,
кандидат психологічних наук, доцент,
старший викладач кафедри педагогіки та психології факультету № 3
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0002-5480-5942

АНАЛІЗ РИЗИКІВ І СТРАТЕГІЙ ЗАХИСТУ ВІД КІБЕРАТАК У СУЧАСНОМУ ЦИФРОВОМУ СВІТІ

У сучасному цифровому світі, де комп'ютери та інтернет використовуються в усіх сферах життя, виникає все більше ризиків внаслідок кібератак. Кібератаки можуть завдати значних збитків як фізичним, так і юридичним особам. Тому дуже

важливо розуміти, які ризики існують та які стратегії можуть бути використані для захисту від кібератак.

На мою думку кібербезпека є надзвичайно важливим аспектом сучасного цифрового світу, оскільки залежність суспільства від технологій швидко зростає. Ризики кібератак зростають разом з кількістю зав'язків та пристроїв, що з'єднуються з Інтернетом, тому вивчення цієї проблеми є надзвичайно важливим. Кібератаки можуть мати різноманітні наслідки для компаній та організацій, включаючи крадіжку конфіденційної інформації, віруси, шифрування файлів та вимагання викупу, порушення роботи систем, втрату фінансових коштів та інше. Ризики також можуть мати негативний вплив на репутацію компанії та втрату довіри клієнтів [1].

Я вважаю для захисту від кібератак, компанії та організації повинні використовувати комплексну стратегію, яка включає різноманітні методи та технології. Основні стратегії захисту від кібератак включають захист мережі, захист пристроїв, шифрування даних та захист від соціальної інженерії. Ці стратегії використовують різні методи, такі як використання паролів та аутентифікація, оновлення програмного забезпечення, встановлення фаєрволів та антивірусного програмного забезпечення та інші. Оцінка ризиків та методи їх зменшення також є важливими підходами до забезпечення безпеки в Інформаційні технології-сфері. Оцінка ризиків допомагає ідентифікувати можливі загрози та найбільш вразливі місця в системі. Зменшення ризиків включає в собі прийняття заходів для запобігання можливим загрозам, такі як встановлення захисних програм, регулярне оновлення програмного забезпечення, проведення тренінгів з кібербезпеки для співробітників, а також створення плану дій у випадку кібератаки.

Крім того, у процесі аналізу ризиків, важливо визначити можливі загрози з боку зовнішніх і внутрішніх джерел, які можуть забезпечити несанкціонований доступ до конфіденційної інформації. Зовнішніми джерелами можуть бути хакери та зловмисники, які намагаються отримати доступ до інформації з метою викрадення грошей або знищення даних. Внутрішніми джерелами можуть бути співробітники, які можуть намагатися викрасти інформацію з метою перепродажу або використання для власної користі.

Найважливішою стратегією захисту від кібератак є постійна увага до кібербезпеки та виконання регулярних оновлень технологій та методів захисту. Крім того, важливо навчати співробітників правильному використанню програм та систем, а також розробляти плани дій у випадку кібератаки.

Далі, можна вивчити методи ідентифікації ризиків та оцінки їх впливу на організацію. Це можна зробити шляхом аналізу звітів про кібератаки, дослідження досвіду інших компаній та організацій, які були жертвами кібератак, а також проведення внутрішньої аудиту безпеки [4].

Далі, можна проаналізувати різні стратегії захисту від кібератак, такі як використання захисного програмного забезпечення, резервне копіювання даних, криптографічні методи захисту даних, а також стратегії мережевої безпеки. Важливо звернути увагу на методи навчання співробітників правильному використанню програм та систем, щоб зменшити ризик внутрішніх загроз [5].

Одним з основних методів захисту від кібератак є використання захисного програмного забезпечення. Це може бути антивірусне програмне забезпечення,

захист від шпигунського програмного забезпечення, файрволи, системи виявлення вторгнень та інші. Таке програмне забезпечення допомагає виявляти та блокувати потенційні загрози для інформаційної безпеки. Також важливим методом захисту від кібератак є резервне копіювання даних. Це дозволяє зберігати резервні копії важливих даних, щоб у разі кібератаки або іншої аварії відновити втрачені дані. Це можна робити за допомогою зовнішніх пристроїв зберігання даних або через хмарні сервіси зберігання даних. Однак, криптографічні методи захисту даних є ефективним способом захисту від кібератак. Застосування шифрування даних, підписів та інших методів криптографії дозволяє захистити дані від несанкціонованого доступу та забезпечити їх конфіденційність та цілісність [4].

Також важливим методом захисту від кібератак є навчання та підвищення культури кібербезпеки серед співробітників організації. Навчання співробітників щодо правильної поведінки в мережі, використання захисного програмного забезпечення та інших методів захисту від кібератак може значно зменшити ризики та захистити організацію від можливих кібератак. У сучасному цифровому світі, захист від кібератак є вкрай важливим аспектом діяльності будь-якої організації. Застосування захисного програмного забезпечення, резервне копіювання даних, криптографічні методи захисту даних, методи аутентифікації та авторизації користувачів, навчання та підвищення культури кібербезпеки серед співробітників є важливими аспектами захисту від кібератак. Правильне застосування цих методів допоможе запобігти можливим наслідкам кібератак та зберегти інформаційну безпеку організації. Для забезпечення надійного захисту від кібератак, важливо розробляти та використовувати стратегії захисту. Ці стратегії повинні включати в себе різноманітні методи та технології, які допоможуть забезпечити безпеку інформації та захистити її від можливих кібератак [3].

Однією з основних стратегій захисту від кібератак є принцип захисту в глибину. Цей принцип передбачає застосування декількох шарів захисту, що забезпечує більшу надійність та захист системи від можливих атак. Наприклад, це може бути застосування мережевих брандмауерів, антивірусних програм, систем виявлення вторгнень та інших методів захисту [5].

Ще однією важливою стратегією захисту від кібератак є планування реагування на інциденти. Важливо мати готовість до можливих кібератак та мати розроблений план дій у разі виявлення кібератаки. Цей план повинен включати в себе кроки з усунення наслідків кібератаки та відновлення роботи системи після інциденту [2].

Також давайте розглянемо основні стратегії кібербезпеки в Україні:

Формування нової якості національної системи кібербезпеки потребує чіткого та зрозумілого визначення стратегічних цілей, що мають бути досягнуті протягом періоду реалізації цієї Стратегії.

Для формування потенціалу стримування (С) необхідним є досягнення таких стратегічних цілей:

ціль С.1. Дієва кібероборона;

ціль С.2. Ефективна протидія розвідувально-підривній діяльності у кіберпросторі та кібертероризму;

ціль С.3. Ефективна протидія кіберзлочинності;

ціль С.4. Розвиток асиметричних інструментів стримування.

Для набуття кіберстійкості (К) необхідним є досягнення таких стратегічних цілей:

ціль К.1. Національна кіберготовність та надійний кіберзахист;

ціль К.2. Професійне вдосконалення, кіберобізнане суспільство та науково-технічне забезпечення кібербезпеки;

ціль К.3. Безпечні цифрові послуги.

Для вдосконалення взаємодії (В) необхідним є досягнення таких стратегічних цілей:

ціль В.1. Зміцнення системи координації;

ціль В.2. Формування нової моделі відносин у сфері кібербезпеки;

ціль В.3. Прагматичне міжнародне співробітництво[1].

Отже, захист від кібератак та кібербезпека є дуже важливими проблемами у сучасному світі, де все більше інформації зберігається в електронному вигляді та передається через мережу Інтернет. Ризики кібератак постійно зростають, атаки стають більш складними та витонченими, тому необхідно вживати дієвих заходів для забезпечення надійного захисту від них.

Основними чинниками, які впливають на ефективність захисту від кібератак, є розуміння ризиків, належне планування та впровадження стратегій захисту, а також постійне оновлення програмного забезпечення та систем безпеки. Важливо також мати розроблений план дій у разі виявлення кібератаки та забезпечувати підготовку спеціалістів з кібербезпеки для виявлення та запобігання можливих кібератак.

Список використаних джерел

1. Архіпов В.О., Пєтухов А.Ю., Коваленко В.В. Кібербезпека: навчальний посібник. Київ. ВЦ "Академія" 2017. 382 с.

2. Зінченко Д.А. Віктимологічні особливості злочинності неповнолітніх Злочинність і протидія їй в умовах війни: глобальний, регіональний та національний виміри : зб. тез доп. наук.-практ. конф. (м. Вінниця, 12 квіт. 2023 р.) / МВС України, Харків. нац. ун-т внутр. справ ; Кримінол. асоц. України ; Наук. парк «Наука та безпека». Вінниця : ХНУВС. 2023. С. 88-91.

3. Макрова О.П. Інформаційні технології в юридичної діяльності як один з напрямків підвищення її ефективності. 25 років становлення Сумської філії Харківського національного університету внутрішніх справ: славетна історія та горизонти майбутнього: матеріали Міжнародної науково-практичної конференції / Сумська філія Харківського національного університету внутрішніх справ. Суми: Видавничий дім «Ельдорадо». 2020. 424 с.

4. Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління Тези доповідей дванадцятої міжнародної науково-технічної конференції Том 1: секції 1-4 Баку – Харків – Жиліна. 2022.

5. https://www.ncs.gov.ua/

Одержано 25.04.2023