МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДНУ “ІНСТИТУТ МОДЕРНІЗАЦІЇ ЗМІСТУ ОСВІТИ”
ЄВРОПЕЙСЬКИЙ УНІВЕРСИТЕТ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
АСОЦІАЦІЯ НАВЧАЛЬНИХ ЗАКЛАДІВ УКРАЇНИ
ПРИВАТНОЇ ФОРМИ ВЛАСНОСТІ
ГО «АСОЦІАЦІЯ СПЕЦІАЛІСТІВ КІБЕРБЕЗПЕКИ»

АКТУАЛЬНІ ПИТАННЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

Матеріали

IX Міжнародної науково-практичної конференції

30 березня 2023 р.

Київ
Європейський університет
2023

УДК: 004(063)

Редакційна колегія:
Тимошенко О. І. – ректор, доктор філософських наук, професор
Скляренко О. В. – кандидат фізико-математичних наук, доцент
Невзоров А.В. – кандидат технічних наук, доцент
Яровий Р.О. – кандидат технічних наук

Відповідальні секретарі:
доц. Скляренко О.В., Милашенко В.М.

Актуальні питання забезпечення кібербезпеки та захисту інформації: Матеріали IX Міжнарод. наук.-практ. конф., Київ, 30 березня 2023 р. / Редкол.: О. І. Тимошенко та ін. – К.: Вид-во Європейського університету, 2023. – 122 с.

Збірник містить матеріали IX Міжнародної науково-практичної конференції «Актуальні питання забезпечення кібербезпеки та захисту інформації».

Матеріали друкуються за редакцією авторів

© Європейський університет, 2023

ЗМІСТ

КІБЕРБЕЗПЕКА ТА ШТУЧНИЙ ІНТЕЛЕКТ У КОНТЕКСТІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ПІДПРИЄМНИЦТВА У ВІЙСЬКОВИЙ ЧАС

Тимошенко О.І.,
д.ф.н., професор,
ректор ПВНЗ «Європейський університет»
Гаврилюк О.В.,
д.е.н, професор,
професор кафедри менеджменту та інноваційного провайдингу,
ПВНЗ «Європейський університет»

Підприємництво складає невід'ємну частину життєдіяльності будь-якої країни. Його стабільний стан та безпека функціонування детермінують успішність соціально-економічного, технологічного, інноваційного та інформаційного розвитку суспільства. Умови воєнного часу вносять ряд особливостей у здійснення підприємницької діяльності. Зокрема, втрата ринків, постачальників і фізичних активів, зменшення можливостей працевлаштування, зміна мотивації виробників і поведінки споживачів, зростання цін на багато видів сировини, енергії, напівфабрикатів та транспортних послуг, порушення ланцюжків поставок тощо потребують від компаній визначення джерел потенційної економії та ранжування пріоритетів розвитку (у т.ч. за рахунок оцифрування).

Військові конфлікти кардинально трансформують підходи до забезпечення безпеки підприємницької діяльності, війна з росією потребує урахування нових реалій – діджиталізації економіки, боротьби з кіберзагрозами, використанні нових інноваційних технологій та штучного інтелекту. Серйозні збої в бізнесі можуть виникнути через широкий діапазон тригерів, що пов'язані з кібернетичною діяльністю, включаючи зловмисні атаки злочинців чи хакерів, витік інформації, людський фактор або відмовою техніки.

Даний виступ буде сконцентровано на вирішенні наступних завдань:

– висвітленні нових умов підприємництва у військовий час;

– окресленні можливостей забезпечення безпеки бізнес-діяльності за допомогою використання інноваційних технологій;

– формулюванні рекомендацій щодо використання штучного інтелекту в оптимізації функціонування підприємств в умовах війни.

Війна в Україні генерувала велику невизначеність у функціонуванні багатьох підприємств, через що останнім вкрай важко оцінити її наслідки. Згідно даних міжнародної консалтингової компанії KPMG, 41% підприємств досі не можуть оцінити вплив війни на свій бізнес, 46% очікують падіння продажів, 47% – скорочення доходів, 80% вважають, що війна негативно

позначиться на подальшому розвитку компанії, 40% побоюються, що негативні наслідки триватимуть понад три роки [4]. Усе це виступає вагомою причиною для переоцінки стратегій, методів та процесів управління ризиками з метою максимально ефективного функціонування в умовах невизначеності.

Війна відбувається не лише на фізичному фронті, а й в інформаційно-інноваційному полі. Одна з найбільших і впливових у світі страхова компанія Allianz SE (Німеччина) з-поміж глобальних ризиків поточного 2023 року вдруге за два роки поспіль на першому місці ранжувала кіберризики – в результаті масштабних кібератак у поєднанні з проблемами, що викликані прискоренням цифровізації та переходом великої кількості підприємств, персоналу та населення на дистанційну працю [1]. Інша глобальна консалтингова фірма – Control Risks – що спеціалізується на ідентифікації ризиків у сфері політики та бізнесу, ранжувала кіберризики на другому місці серед інших загроз підприємництву [5]. У звіті Світового економічного форуму про Глобальні ризики 2023 наголошено, що проблеми кібербезпеки складають постійне занепокоєння [6]. До найбільш поширених видів кіберзагроз належать DDoS та DoS-атаки; фішингові розсилки з вірусними файлами або посиланнями; злом акаунтів для отримання доступу до особистих і корпоративних даних; шкідливе програмне забезпечення, що приховує файли та блокує доступ до них; віруси-вимагачі; несанкціоновані входи в інтернет-банкінг; витік конфіденційної інформації та персональних даних тощо. Успішна реалізація цих загроз здатна завдати дошкульних ударів будь-якому бізнесу, населенню і державі.

Сьогодні кіберзагрози вийшли далеко за рамки хакерських атак і витоку даних. Хакери дедалі більше орієнтуються як на цифрове, так і на фізичне постачання ланцюгів, які надають можливість одночасно атакувати кілька цілей. Постійно зростаючі можливості кіберзлочинців змушують компанії акцентувати пильну увагу на ризиках, яким можуть піддатися їхні об’єкти критичної інфраструктури, такі як інтелектуальні технології, системи подачі води та електроенергії. Особливу стурбованість потенційні кібератаки викликають у підприємств сфери торгівлі й комунікаційних технологій, а також малого та середнього бізнесу.

З початком російської агресії Україна стала ціллю чисельних кібератак, що спрямовані на державні установи критичної інфраструктури, приватний бізнес і населення. Протидіяти їм реально за рахунок посилення кібербезпеки і використання штучного інтелекту (ШІ).[1] Останній може обробляти великі

[1] Штучний інтелект не можна розглядати в якості панацеї вирішення усіх проблем безпеки підприємництва. По-перше, сам може бути використаний з ворожими намірами, по-друге, не виключена імовірність його переходу в некерований стан. Стурбованість з приводу останнього була висловлена Ілоном Маском та багатьма поважними бізнесменами 29 березня 2023 р.; вони закликали тимчасово припинити його розробку [2]. Про небезпеку використання ChatGPT у спробах фішингу, дезінформації та кіберзлочинності попередив і Європол 28 березня 2023 р. [3].

обсяги даних та ідентифікувати тенденції й патерни, які здатні вказувати на майбутні зміни в економічній і політичній ситуації. Вважається можливим сформулювати напрями убезпечення підприємництва в умовах війни за допомогою ШІ:

1. Розробка системи моніторингу, яка відстежуватиме зміни в політичній та економічній кон'юнктурі й попереджатиме підприємців про гіпотетичні ризики та загрози, сприяючи прийняттю більш виважених рішень про свої інвестиції та стратегії розвитку.

2. Прогнозування майбутніх тенденцій на ринку з попереднім реагуванням на них. Аналіз економічної динаміки, даних про виробництво, споживання, експорт та імпорт дасть змогу виявити ризики та зміни в економіці. Наприклад, ШІ може допомогти визначити, які товари є стратегічно важливими, і оцінити ризики у їх виробництві або постачанні.

3. Оптимізація бізнес-процесів з використанням роботизованих систем призведе до зменшення кількості помилок під час прийняття рішень.

4. Використання систем захисту даних та кібербезпеки допоможе запобігти витоку конфіденційної інформації, виявити появу кібератак або незвичайну активність персоналу, спрямовану на витік конфіденційної інформації, порушення безпеки та блокування/обмеження доступу до конфіденційної інформації за рахунок використання алгоритму розпізнавання обличь та інших технологій ідентифікації авторизованих користувачів.

5. Співпраця з федеральними та регіональними органами влади дозволить отримувати інформацію про зміни політичної та економічної кон'юнктури, у т.ч. відстежувати зміни в урядовій політиці, оцінювати нові регулюючі норми та закони, щоб попередити про можливі ризики та оперативно приймати усвідомлені рішення.

6. Розробка антикризових планів/стратегій на основі алгоритму збереження бізнесу у разі виникнення загроз та катастрофічних подій.

Впровадження і розвиток цифрових технологій в бізнес-організаціях супроводжується посиленням/диверсифікацією загроз та реальних наслідків кібератак. У військовий час кожне підприємство мусить функціонувати у режимі підвищеної готовності та заздалегідь оцінити вразливість своїх критичних сервісів до кіберінцидентів та технологічних збоїв аби запобігти негативних наслідків від атак зловмисників. Мінімізації негативних наслідків останніх і сприятиме посилення кібербезпеки. На повістці денній також виступає покращення нормативно-законодавчого забезпечення кібербезпеки підприємництва. Бізнес потребує юридичної підтримки, оскільки регулювання кібербезпеки в Україні є фрагментарним. Регулятивні норми розкидані в багатьох законах та підзаконних актах і власнику бізнесу часто складно самостійно знайти потрібну інформацію для захисту в разі кіберінциденту.

Список використаних джерел:

1. Allianz Risk Barometer 2023. URL: https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2023-Appendix.pdf.

2. Elon Musk among experts urging a halt to AI training. URL: https://www.bbc.com/news/technology-65110030.
3. Europol sounds alarm about criminal use of ChatGPT, sees grim outlook. URL: https://www.reuters.com/technology/europol-sounds-alarm-about-criminal-use-chatgpt-sees-grim-outlook-2023-03-27/.
4. The Economic Impact of the Russia-Ukraine War. URL: https://kpmg.com/de/en/home/insights/2022/05/the-economic-impact-of-the-russia-ukraine-war.html#:~:text=As%20a%20result%20of%20the,lasting%20longer%20than%20three%20years.
5. Top Risks 2023. URL: https://www.controlrisks.com/riskmap/top-risks.
6. The Global RisksReport 2023. URL: https://www.weforum.org/reports/global-risks-report-2023/digest/.

ВИКОРИСТАННЯ СТЕГАНОГРАФІЇ В СУЧАСНИХ КІБЕРАТАКАХ

Арделян І.С.,
магістрант факультету інформаційних систем та технологій,
ПВНЗ «Європейський університет»

У сучасну епоху інформаційних технологій Інтернет є важливою частиною спілкування та обміну інформацією. Надання конфіденційної інформації та встановлення прихованих зв'язків викликає великий інтерес здавна. Безпека інформації, що передається по відкритому каналу, стала фундаментальною проблемою, тому конфіденційність і цілісність даних необхідні для захисту від несанкціонованого доступу та подальшого використання. Криптографія та стеганографія є двома популярними методами забезпечення безпеки. Криптографія кодує повідомлення, щоб воно не було зрозумілим, і генерує зашифрований текст. Стеганографія – це практика надсилання даних у прихованому форматі, тому сам факт надсилання даних маскується. Слово стеганографія є поєднанням грецьких слів στεγανός (steganos), що означає «прикритий, прихований або захищений», і γράφειν (graphein), що означає «письмо». На відміну від криптографії, яка приховує зміст секретного повідомлення, стеганографія приховує сам факт передачі повідомлення. Поняття стеганографії вперше було введено в 1499 році, але сама ідея існує з давніх часів [3].

Кодування секретних повідомлень у цифрових зображеннях є найпоширенішим з усіх методів у цифровому світі. Це пояснюється тим, що він може використовувати переваги обмеженої потужності зорової системи людини. Майже будь-який простий текст, зашифрований текст, зображення та будь-який інший носій, який можна закодувати в бітовий потік, можна приховати в цифровому зображенні. З безперервним зростанням високої потужності графіки в комп'ютерах і дослідженнями стеганографії на основі зображень ця галузь продовжуватиме розвиватися дуже швидкими темпами [1].

Стеганографія активно розвивалася протягом 20-го століття, як і стегоаналіз, або практика визначення факту передачі прихованої інформації на носії [2]. По суті, стегоаналіз – це практика атаки на стегосистеми. Однак, сьогодні з'являється нова небезпечна тенденція: стеганографія все частіше використовується хакерами, які створюють шкідливі програми та інструменти кібершпигунства. Більшість сучасних рішень для захисту від зловмисного програмного забезпечення практично не забезпечує захисту від стеганографії, а будь-який носій, на якому можна таємно переносити корисне навантаження, становить потенційну загрозу. Він може містити дані, викрадені шпигунським програмним забезпеченням, зв'язок з шкідливою програмою або нове шкідливе програмне забезпечення.

Щоб запобігти кібератакам на основі стеганографії, необхідно переконатися, що співробітники не активують приховане зловмисне програмне забезпечення (наприклад, відкривши фотографію чи дозволивши макроси в документах MS Office), і, як другу лінію захисту, виявлення мережевої активності, викликаної шкідливим програмним забезпеченням.

Сегментація та відокремлення мережі: однією з ключових структурних змін, яку мають запровадити всі промислові організації, є збереження розділення взаємодії між операційною та IT-мережами за допомогою брандмауерів та DMZ (demilitarized zones).

Людська/соціальна інженерія: ця діяльність передбачає навчання співробітників тому, що таке стеганографічні та фішингові атаки, на що слід звернути увагу в підозрілих електронних листах, а також процедури звітування в IT-відділ; деякі організації фактично проводять тренування із запобігання фішингу для вищих посад і навіть карають працівників за недотримання правил безпеки використання електронної пошти.

Виявлення за допомогою IDS (Intrusion Detection System): хоча файли, що містять приховане шкідливе програмне забезпечення, не завжди можна виявити до активації людиною, системи виявлення вторгнень (IDS), здатні виявляти дрібні зміни в поведінці мережі, які вказують на запуск і розповсюдження шкідливого програмного забезпечення, як-от підключення до сервера хостингу, який раніше не використовувався, відкриття нових зовнішніх з'єднань та/або незвичні шаблони трафіку даних.

Як висновок, можна відзначити сильний позитивний тренд: все більше і більше розробників шкідливого програмного забезпечення починає використовувати стеганографію, у тому числі для приховування комунікації з командним центром і для завантаження модулів. Це дає результат, адже процедури аналізу контейнерів дуже технічно високонавантажені, отже більшість захисних рішень не можуть собі дозволити обробляти всі об'єкти, які потенційно можуть бути заповненими шкідливою інформацією.

Однак, рішення є і воно засноване на комбінуванні різних способів аналізу, високошвидкісних предетектів, дослідженні метаданих потенційно заповненого контейнера і т.п.. Використання даного способу дозволяє

співробітнику служби інформаційної безпеки своєчасно дізнатися про можливу таргетовану атаку на систему, та/або ексфільтрацію даних з неї.

Список використаних джерел:

1. Neetha Francis, Information Security using Cryptography and Steganography. URL: https://www.ijert.org/information-security-using-cryptography-and-steganography
2. Global cybersecurity alliance, Rise of Steganography OT Cyberattacks URL: https://gca.isa.org/blog/the-rise-of-steganography-based-ot-cyberattacks
3. Стеганографія URL: https://uk.wikipedia.org/wiki/Стеганографія

УДОСКОНАЛЕННЯ МОДЕЛІ ЗАГРОЗ КІБЕРБЕЗПЕКИ НА ПІДПРИЄМСТВІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Божаткін С.М.[1], Пасюк Б.Б.[2], Гусєва-Божаткіна В.А.,[3]
[1]ст. викладач кафедри КТІБ
[2]аспірант
[3]ст. викладач кафедри ПЗАС,
Національний університет кораблебудування імені адмірала Макарова,
Україна, м. Миколаїв

На сьогоднішній день складається така ситуація, що кіберпростір разом з іншими фізичними просторами визнано одним з можливих театрів військових дій, тому спроможність держави захищати національні інтереси в ньому розглядається як важлива складова кібербезпеки України. Станом на сьогодні, спостерігається зростання інтенсивності міждержавного протиборства і розвідувально-підривної діяльності стосовно підприємств критичної інфраструктури, а особливо, – підприємств оборонного комплексу держави.

Система безпеки інформаційних систем не будується сама по собі. Вона базується на моделях загроз і моделі порушника. Сама модель загроз – це документ, в якому перелічені та описані можливі загрози інформаційній безпеці організації/підприємства, ймовірність реалізації і наслідки їх дії.

Сама загроза – це недолік або місконфігурація в системі безпеки (через недостатню обізнаність спеціаліста з кібербезпеки, наприклад), якими можуть скористатися зловмисники. Наявність загрози не означає неминучий можливий витік інформації: це говорить про те, що у зловмисників є теоретична можливість несанкціонованого доступу до персональних даних підприємства або певних програмних чи апаратних систем.

Як і будь-який нормативний документ, модель загроз будується за певною структурою: титульний аркуш, список термінів, визначень і скорочень, змісту, основної частини і додатків.

Для створення такої моделі необхідно проаналізувати дані, отримані при аудиті інформаційної системи підприємства. Це допоможе виявити слабкі місця системи; зрозуміти, що буде їй загрожувати; звідки може прийти загроза

і якими засобами її можливо буде нейтралізувати або заздалегідь запобігти її виявленню.

Загрози визначаються при обробці даних. У моделі необхідно визначити й прописати, ким або чим вони можуть бути викликані:

– фізичною особою;
– шкідливим програмним забезпеченням;
– витоком інформації технічними каналами зв'язку;
– з'явитися при проектуванні великих електронних пристроїв ненадійними виробниками (т.зв. апаратні закладки);
– при спеціальному або електромагнітному впливі.

Джерела загроз – розділ, який також необхідно відобразити в моделі. Ними можуть стати зовнішній або внутрішній порушники, вірус або програмно-апаратна закладка на рівні мікропроцесора цифрового виробу.

При побудові моделі загроз визначається рівень цільової захищеності інформаційної системи (ІС). Це глобальний параметр, який визначається одноразово і не змінюється в залежності від загрози (лише у випадку ремасштабування ІС). Наступним кроком виділяються актуальні загрози і виключаються зайві – ті, які не несуть для системи шкоди. Загрози, що не були виключені, вносяться до моделі з описом.

Автори [1] та [2] представляють моделі загроз у вигляді списку можливих вразливостей інформаційної системи (виду DoS, DDoS, сніфінг, підміна заголовків пакетів чи HTML-запитів і т.д.), однак об'єкти критичної інфраструктури підлягають набагато ретельнішій перевірці і розроблювана модель має бути певною мірою більш деталізована.

Спочатку визначимось з моделлю порушника безпеки інформації на підприємстві. Для цього підійде типова модель, зображена на рисунку 1.

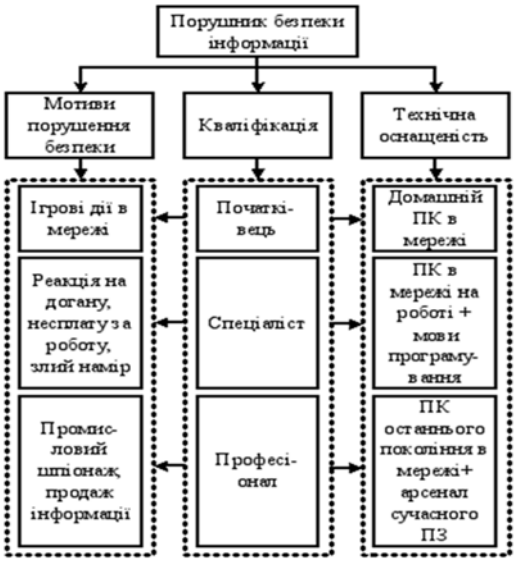

Рис.1. Модель порушника

Варто зазначити, що Європейський Союз визначає критичну інфраструктуру як системи, які мають важливе значення для підтримки

життєво важливих соціальних функцій. Пошкодження критичної інфраструктури, її руйнування або порушення в результаті стихійних лих, тероризму, злочинної діяльності або зловмисної поведінки, може істотно негативно вплинути на безпеку ЄС і добробут громадян.

Простоювання такого підприємства у разі хакерської атаки або недбальства з боку співробітників або відповідального за кібербезпеку тягнуть за собою можливі «простої» підприємства або ж повну зупинку його діяльності.

Для складання повної деталізованої моделі загроз кібербезпеки на підприємстві критичної інфраструктури необхідно враховувати так звану модель “Cyber Kill Chain” (розроблена оборонною організацією Lockheed Martin), що представляє собою 7 послідовних рівнів (кроків), які зловмисник проходить для реалізації «зламу» інформаційної системи жертви (рис. 2).

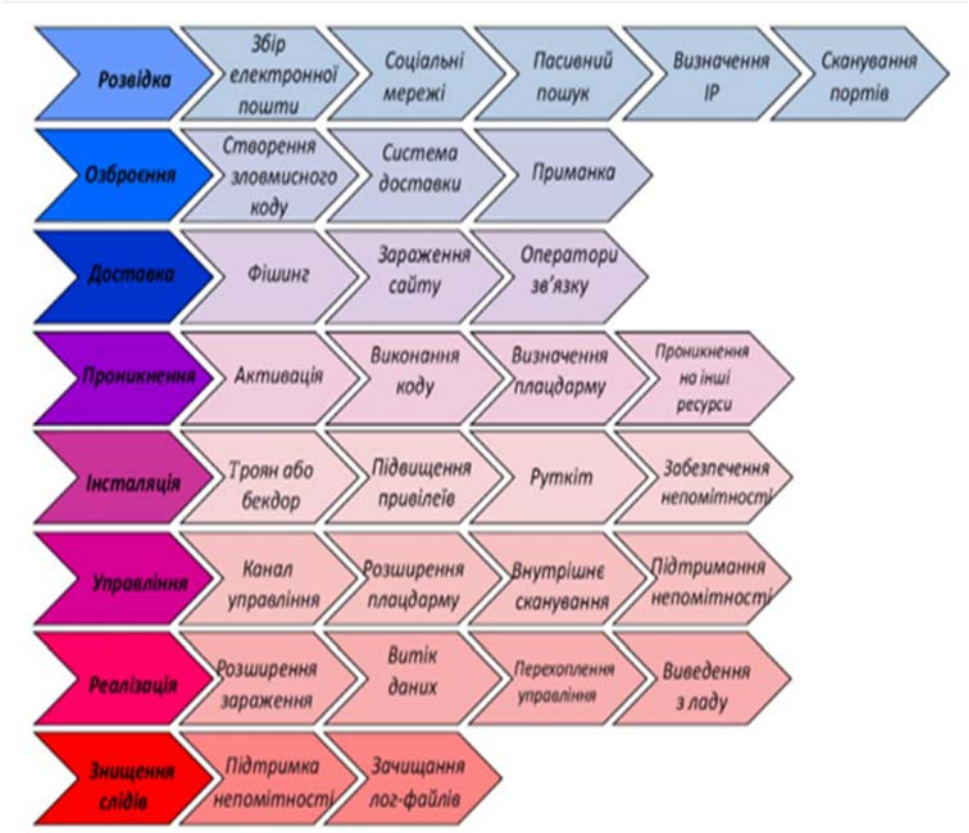

Рисунок 2. Модель Cyber Kill Chain

Враховуючи вищесказане, визначимо критерії, за якими буде побудовано модель загроз кіберзахисту підприємства критичної інфраструктури:

- етап моделі “Cyber Kill Chain”;
- вид загроз на даному етапі;
- типові інструменти зловмисника на даному етапі;
- точки входу зловмисника на даному етапі (можливі прогалини в безпеці);

– актор небезпеки (особа або відділ, руками яких можна виконати вхід до інформаційної системи) на даному етапі;
– механізм реалізації зловмисних дій на даному етапі;
– превентивні дії (інструкції) системного адміністратора або відповідального за кіберзахист підприємства на даному етапі;
– нинішній рівень реалізації превентивних дій на підприємстві за етапом моделі «Cyber Kill Chain».

Рекомендована модель є універсальною та може використовуватись на будь-якому підприємстві критичної інфраструктури України.

Список використаних джерел:

1. *О.О. Ільїн, С.О. Сєрих, В.В. Вишнівський* «Аналіз уразливості інформаційного ресурсу вищого навчального закладу та класифікація загроз інформаційної безпеки». http://journals.dut.edu.ua/index.php/dataprotect/article/view/1414
2. *О.Я. Матов, В.С. Василенко* «Модель загроз у розподілених мережах». http://dspace.nbuv.gov.ua/bitstream/handle/123456789/7538/09-Matov.pdf

МЕТОДИ ЗАХИСТУ ЦИФРОВИХ ЗОБРАЖЕНЬ

Букатов Д.В.,
викладач кафедри математичних дисциплін та інноваційного проектування,
Романенко О.І.,
асистент кафедри математичних дисциплін та інноваційного проектування,
ПВНЗ «Європейський університет»

Захист цифрової інформації є надзвичайно важливим у світі, де цифрові зображення, аудіо та текстові файли використовуються в різних сферах життя, а вірогідність їхнього підроблення або зламу зростає. Враховуючи це, виникає постійна потреба у розробці та застосуванні ефективних методи захисту інформації. Особливо це важливо у сферах розробки та створення візуально-цифрового контенту.

У постійно зростаючій цифровій економіці зображення, зазвичай, зберігаються у цифровому форматі, що робить їх вразливими до неправомірних дій різного типу, особливо, якщо вони зберігаються на інтернет ресурсах.

Для захисту цифрових зображень є різноманітні методи, такі як шифрування, обмеження доступу, водяні знаки, навмисне зменшення роздільної здатності зображень та інші. Також для захисту цифрових зображень можна використовувати техніки обмеження доступу, такі як системи авторизації та аутентифікації, щоб забезпечити контроль доступу до зображень та обмежити можливість несанкціонованого доступу до них.

Нейромережеві підходи та методи машинного навчання також можуть бути застосовані до захисту цифрових зображень. Наприклад, застосування нейронних мереж для виявлення змін колірних діапазонів та інших форм маніпулювання зображеннями дозволяє виявляти спроби підробки цифрових зображень [1,2].

В художній індустрії фахівці можуть використовувати різноманітні методи та інструменти для захисту своїх цифрових зображень. Одним з таких методів є водяний знак, який використовується для захисту авторських прав та вказання належності зображення до конкретного автора. Водяний знак може бути розміщений на зображенні в будь-якому місці, зазвичай, це буває в нижньому куті або центрі зображення, і може бути нанесений вручну або за допомогою спеціальних програм.

Іншим методом захисту є техніка блокування копіювання, що дозволяє обмежити можливість копіювання зображень без дозволу автора. Ця техніка може бути реалізована за допомогою вбудованих обмежень в програмах для перегляду та завантаження зображень або шляхом застосування спеціальних налаштувань функціоналу сайту.

Ще одним методом захисту є використання техніки цифрового підпису, який дозволяє забезпечити автентичність зображення та встановити авторство. Цей метод передбачає використання спеціального ключа для підпису зображення, який дозволяє перевірити його автентичність та встановити автора.

Також, дуже важливо проводити регулярну перевірку мережі на наявність незаконного використання зображень та вжиття заходів щодо їх вилучення.

Загалом, ефективний захист цифрових зображень вимагає використання різноманітних технік та підходів, включаючи шифрування, системи авторизації та аутентифікації, а також методи машинного навчання.

Список використаних джерел:

А. М. Ковальчук, Н. Д. Лотошинська “Шифрування і дешифрування півтонових та кольорових зображень” // Вісник Національного університету "Львівська політехніка". Комп’ютерні системи та мережі. – 2018. – № 905. – С. 82-87.

В. В. Зоріло “Алгоритм виявлення малого розмиття цифрового зображення” // Сучасна спеціальна техніка. – 2014 – № 2(37). – С. 103-109.

ВИКЛИКИ У СФЕРІ НАДАННЯ ПУБЛІЧНИХ ІНФОРМАЦІЙНИХ ПОСЛУГ В УМОВАХ ВІЙНИ В УКРАЇНІ

Бурак М.П.,
магістрант факультету інформаційних систем та технологій,
Пашорін В.І.,
к.т.н., професор,
завідувач кафедри інформаційних систем,
програмування та кібербезпеки
ПВНЗ «Європейський університет»

Перед повномасштабним вторгненням та з початком воєнних дій в Україні обсяг та потужність кібератак зросла у декілька разів. Масові кібератаки проти державних структур України та бізнесу були протягом січня та лютого 2022 року, і, особливо, в ніч з 23 на 24 лютого. Кіберзлочинці планували ці атаки, з метою обмежити роботу стратегічних об'єктів. За даними Держспецзв'язку у період з середини лютого до початку березня 2022 року українські організації зазнали близько 2800 кібератак (для порівняння – у 2021 році кібератак було 2200)[1].

Через війну у 2022 році не працювали Державний земельний кадастр та Державний реєстр речових прав на нерухоме майно, правочини щодо купівлі-продажу земельних ділянок та зміна власника/користувача земельної ділянки не здійснювалися. Станом на даний момент ці сервіси відновили свою роботу із змінами. Також у 2023 році Держгеокадастр розпочинає тестування геопорталу Державного картографо-геодезичного фонду України за допомогою порталу «Дія» для відновлення системи оформлення прав оренди земельних ділянок сільськогосподарського призначення та вдосконалення законодавства з питань охорони земель, це забезпечувало б приймання, облік, зберігання, аналіз і оброблення матеріалів та даних, що надходять на зберігання, в електронному вигляді [4].

Банки виявилися операційно стійкими, вони щодня майже безперебійно надавали послуги клієнтам у тих регіонах, де це було безпечно для працівників та клієнтів. Із середини червня працювало вже близько 85% банківських відділень країни.

На перших тижнях війни Єдиний державний реєстр не працював, тобто нові бізнеси не реєстрували.

Ключовим фактором є те, що після початку вторгнення країни-агресорки в Україну, низка державних інституцій приховали частину публічної інформації, у тому числі, у формі відкритих даних про свою роботу, закрили держреєстри та призупинили інформування про свою роботу.

Основною причиною цього стали міркування безпеки, хоча, далеко не для всіх даних підходить таке пояснення, і в деяких випадках їх закривали з інших міркувань. Така політика суттєво погіршила прозорість роботи

державних органів та органів місцевого самоврядування, а громадяни втратили оперативний доступ до відкритих даних, які становлять значний суспільний інтерес.

Закритість держреєстрів та відкритості доступу до суспільно важливих даних призводить до корупції, відсутності звітності та відповідальності, і, найголовніше, – до втрати довіри до ключових державних інституцій.

В умовах війни це руйнівні наслідки, оскільки війна не стала перепоною для корупції, а прихованість публічної інформації створила підґрунтя для її поширення.

Список використаних джерел:

1.Кібербезпека бізнесу під час війни: https://mklegalservice.com/tpost/k123zz39h1-kberbezpeka-bznesu-pd-chas-vini
2. Гаряча агрополітика: https://agropolit.com/news/23952-v-ukrayini-vidnoviv-robotu-derjavniy-zemelniy-kadastr
3. Економічна правда: https://www.epravda.com.ua/news/2022/03/31/684991/
4. Державна служба України з питань геодезії, картографії та кадастру: https://land.gov.ua/derzhgeokadastr-rozpochynaye-testuvannya-geoportalu-derzhavnogo-kartografo-geodezychnogo-fondu-ukrayiny/
5.НБУ: https://bank.gov.ua/ua/news/all/finansova-sistema-uspishno-protistoyit-viklikam-viyni---zvit-pro-finansovu-stabilnist
6.Доступ до правди: https://dostup.pravda.com.ua/news/publications/hromadskist-vymahaie-vidkryty-reiestry-ta-ponovyty-dostup-do-publichnoi-informatsii-zaiava

ОРГАНІЗАЦІЯ ЗАХИСТУ ІНФОРМАЦІЇ

Вдовіна О.В.,
викладач вищої категорії,
Дніпровський фаховий коледж залізничного транспорту
та транспортної інфраструктури

На сьогоднішній день задача захисту інформації в комп’ютерних системах є актуальною внаслідок широкого розповсюдження таких систем, більш частого використання комп’ютерних мереж, завдяки яким й передаються значні обсяги інформації.

Політика безпеки комп’ютерних систем представляє набір правил та рекомендацій, які являють собою інструкції спрямовані на захист, розподіл та керування процесом захисту інформації у комп’ютерних мережах. Політика безпеки представляє собою регламент ефективного використання засобів захисту комп’ютерних мереж, а також вона охоплює усі процедури процесу забезпечення безпеки користування комп’ютерною мережею та усіма її складовими, вона охоплює всі особливості процесу обробки інформації та контролює й забезпечує захист даних, у будь-яких ситуаціях, котрі виникають під час користування і застосування системи.

Політика безпеки реалізується за допомогою адміністративних, організаційних, фізичних мір та програмно-технічних засобів і на цьому базується система захисту даних. Кожна комп'ютерна система має свою власну політику безпеки, вона має індивідуальний характер та залежить від технології обробки інформації і застосованих у даному випадку технічних та програмних засобів обробки інформації. В залежності від способу керування доступу до даних кожної конкретної системи будується індивідуальна політика безпеки даної системи та визначається порядок доступу до об'єктів використовуємих у системі. Існує два види політики безпеки (ПБ), а саме: виборча або дискреційна ПБ та повноважна або мандатна ПБ.

У чому полягають відмінності вище названих політик безпеки? Виборча політика безпеки заснована на способі керування доступом до елементів комп'ютерної системи і полягає у виборчому способі керування. Дане керування доступом до елементів мережі базується на тому, що адміністратор конкретної мережі задає безліч алгоритмів та правил дозволених дій у мережі. Виборча політика безпеки загалом використовується у комп'ютерних мережах комерційного сектора, завдяки тому, що її реалізація відповідає вимогам, які пред'являють комерційні організації завдяки розмежувальному доступу та підзвітності, але вона ще має прийнятну вартість для даного сектору попиту.

Повноважна політика безпеки заснована на повноважному способі керування доступом, котрий характеризується наявністю правил надання доступу, які описані як атрибути безпеки суб'єктів та об'єктів даної комп'ютерної системи.

Чим більше важливий об'єкт, тим вищою буде його мітка конфіденційності, тому об'єкти з найвищими мітками конфіденційності інформації суб'єктів вважаються самими захищеними.

Основним призначенням мандатної політики безпеки є саме встановлення алгоритмів доступу суб'єктів системи до об'єктів з різноманітними рівнями конфіденційності інформації, а також застереження витоку інформації з верхнього рівня на нижній і попередження проникнення з нижніх рівнів на верх.

Наряду з вище охарактеризованими виборчою (дискреційною) політикою безпеки та повноважною (мандатною) політикою існують політика безпеки інформаційних потоків, політика ізольованого програмного середовища та ролева політика безпеки.

Сутність політики безпеки інформаційних потоків полягає у головній ролі адміністратора мережі, котрий повинен визначити які інформаційні потоки, котрі відбуваються у мережі ведуть до витоку інформації, а які працюють в межах регулювання потоків мережі та є "легальними" й не ведуть до витоку інформації. І виникає необхідність розробки правил, які повинні керувати інформаційними потоками у системі. Звичайне керування інформаційними потоками застосовується або в межах повноважної чи виборчої політики, доповнює їх та сприяє підвищенню надійності системи захисту.

Ролева політика безпеки основана на охарактеризованих вище мандатній та дискреційній політиці, але вона є цілком самостійною, та відповідно до політики ролевого розмежування доступу права доступу до об'єктів та суб'єктів формуються згідно з їх ролями. Межі застосування рольової політики безпеки це мережеві операційні системи, великі системи керування базами даних та інше.

Якщо характеризувати політику безпеки у повному обсязі, неможливо не сказати про ще одну політику безпеки, а саме про політику ізольованого програмного середовища. Дана політика відповідає про порядок взаємодії між суб'єктами комп'ютерної системи по заздалегідь прописаним алгоритмам і правилам, така взаємодія унеможливлює будь-яку модифікацію параметрів системи, а також зміну алгоритму взаємодії. Тобто усі виникаючі інформаційні потоки комп'ютерної мережі поділяються на два типи, це потоки, які підлягають фільтрації та ретельній перевірці й потоки, так звані легальні, котрі не фільтруються й вважаються потоками легального доступу.

Робота з даними потоками, організація та керування ними, є базовими складовими, на яких базується загалом система захисту комп'ютерних мереж. Адже під системою захисту комп'ютерних мереж розуміють сукупність правових, моральних, етичних норм, а також адміністративних й організаційних застосувань, фізичних і програмно-технічних засобів, котрі спрямовані на запобігання та виявлення загроз у комп'ютерні мережі (КМ) з метою мінімального отримання збитків від витоку інформації.

Етапи системи захисту під час її будови є наступними:

– збір інформації щодо можливих погроз КМ;

– аналіз погроз для конкретної КМ;

– створення структури моделі майбутньої мережі;

– реалізація системи захисту КМ;

– супровід системи захисту КМ.

Перераховані міри безпеки комп'ютерних мереж можна розглядати як послідовність бар'єрів або рубежів захисту інформації. Для того щоб добратися до інформації, що захищається, потрібно послідовно перебороти усі перелічені рубежі.

Список використаних джерел:

1. О.М. Гапак, С.І. Балога Підручник з курсу «Захист інформації в комп'ютерних системах» призначено для студентів інженерно-технічного факультету ДВНЗ «УжНУ» спеціальності 123-«комп'ютерна інженерія».

СУЧАСНІ РЕАЛІЇ КІБЕРВІЙНИ: ВИКЛИКИ, ЗАГРОЗИ ТА ВПЛИВ НА ЕКОНОМІКУ

Вілянський А.В.,
Чайко В.В.,
аспіранти,
ПВНЗ «Європейський університет»

У світі постійно відбуваються конфлікти, але останнім часом їх характер змінився. Традиційні війни на землі, в повітрі та на морі поступово замінюються на новий вид конфлікту – кібервійну. Кібервійна – це використання комп'ютерних систем та мереж для здійснення атак та контратак в межах конфлікту [1]. Вона може бути проведена державами або приватними суб'єктами з метою здійснення шкідливих дій на об'єктах критичної інфраструктури, керуванням електронною поштою, відстеженням спілкування та іншими способами.

Історія кібервійни починається з ранніх днів розвитку комп'ютерів, коли хакери використовували свої навички для вторгнення до комп'ютерних систем задля отримання конфіденційної інформації. Однак, з часом, ці дії стали більш масштабними та організованими, що призвело до появи кібернетичних війн. Першими країнами, які розпочали активно використовувати кібервійну, стали США та Ізраїль. Згодом, багато інших країн також почали залучатися до кібервійни, зокрема Китай, Іран, Північна Корея та росія.

Необхідно відмітити, що росія відома своїми активними діями в кіберпросторі та використанням кіберзброї в політичних конфліктах. Так, російська федерація була звинувачена у втручанні в політичні процеси інших країн, зокрема в США, Франції, Німеччині та інших країнах.

Найбільш відомим прикладом втручання росії є її вплив на вибори президента США 2016 року. російські хакери викрали електронну пошту кандидата від Демократичної партії та опублікували ці дані в Інтернеті. Це призвело до скандалу та спричинило зростання популярності кандидата від Республіканської партії [2].

Також росія вдалася до використання кіберзброї під час широкомасштабного військового вторгнення в Україну. Російські хакери були звинувачені у викраденні конфіденційної інформації, використанні шпигунських програм та інших методів, щоб зламати системи безпеки.

У світлі таких дій росії, було прийнято кілька міжнародних документів, які закликають до заборони використання кіберзброї та встановлюють міжнародні норми в цій сфері. Зокрема, у 2015 році Організація Об'єднаних Націй прийняла документ "Кібербезпека та інформаційна безпека", а у 2018 році Європейський Союз прийняв Загальний регламент з захисту даних.

Проте, міжнародні норми та угоди не є достатньою гарантією безпеки в кіберпросторі. Розробка ефективних механізмів захисту від кібернападів

потребує більш широкої співпраці між державами, науковими установами та приватним сектором. Також важливо забезпечити країну кваліфікованими кадрами в галузі кібербезпеки та надавати відповідну якісну освіту, здійснюючи необхідну підготовку для молодих людей.

Крім того, потрібно звернути увагу на зміну національних політик у сфері кібербезпеки. Деякі держави, зокрема росія та Китай, активно пропагують концепцію "національного суверенітету в кіберпросторі", яка передбачає обмеження свободи мережевої діяльності та контроль за даними.

Така політика може спричинити загрозу світовій стабільності та безпеці. Водночас, деякі країни, зокрема США та певні європейські країни, прагнуть підвищити рівень кібербезпеки та захисту від кіберзагроз шляхом залучення приватного сектору та активного застосування новітніх технологій.

Незалежно від національної політики, важливо, щоб усі держави розуміли та приймали відповідальність за свої дії в кіберпросторі. Кібербезпека повинна стати пріоритетом національної та міжнародної безпеки, і усі зацікавлені сторони повинні співпрацювати, щоб забезпечити безпеку в цьому просторі.

Одним з найбільш серйозних наслідків кібервійни є її вплив на економіку.

Кібератаки можуть призвести до серйозних фінансових втрат для компаній та держав. Компанії, які стали жертвами кібератак, можуть втратити значну кількість грошей на відновлення своїх систем та втрату даних. Крім того, кібератаки можуть призвести до витоку конфіденційної інформації, такої як персональні дані користувачів або важлива корпоративна інформація, що, в свою чергу, може потягнути за собою значні фінансові витрати, штрафи, втрату довіри клієнтів та т.ін.

Крім цього, кібератаки на державні інформаційні системи можуть мати серйозні наслідки для економіки країни. Наприклад, кіберзлочинці можуть зруйнувати критичну інфраструктуру, таку як електроенергетика, транспортні мережі та фінансові системи, які є необхідними для ефективної роботи економіки. Це може призвести до значного зменшення продуктивності та збільшення втрат коштів.

Зараз все більше країн усвідомлюють серйозність проблеми кібербезпеки та вживають заходи для захисту своїх інформаційних систем. Однак, кібератаки продовжують бути серйозною загрозою для економіки та безпеки країн у всьому світі, тому необхідно додавати ще більше зусиль для запобігання їхнього поширення.

У світі, де все більше процесів переходять до цифрового простору, кібербезпека є важливим аспектом національної та міжнародної безпеки. Кібервійни можуть мати негативні наслідки для економіки, інфраструктури та політичної стабільності, тому важливо розуміти цю проблему та діяти, щоб зменшити ризики виникнення кіберзагроз. Тільки через спільні зусилля та співпрацю національних та міжнародних громадських організацій, урядів та

приватного сектору можна забезпечити безпеку в кіберпросторі та запобігти негативним наслідкам від кібернападів.

Список використаних джерел:

1. Електронний ресурс: https://uk.wikipedia.org/wiki/Кібервійна
2. Ellen Nakashima (14 червня 2016). Russian government hackers penetrated DNC, stole opposition research on Trump. Washington Post. URL: https://web.archive.org/web/20190522235639/https://www.washingtonpost.com/world/national-security/russian-government-hackers-penetrated-dnc-stole-opposition-research-on-trump/2016/06/14/cf006cb4-316e-11e6-8ff7-7b6c1998b7a0_story.html?utm_term=.3529ef522129

ОГЛЯД ПРОГРАМНИХ ЕМУЛЯТОРІВ ТА СИМУЛЯТОРІВ ДЛЯ ПОБУДОВИ ПРАЦЕЗДАТНИХ МОДЕЛЕЙ МЕРЕЖІ

Виноградова В.В.,
курсантка ІІ курсу
Харківського національного університету внутрішніх справ,
Світличний В.А.,
кандидат технічних наук, доцент
доцент кафедри протидії кіберзлочинності факультету № 4
Харківського національного університету внутрішніх справ

У сучасному світі мережеві технології стали невід'ємною частиною бізнес-процесів та повсякденного життя людей. З цього приводу, для вивчення, тестування та розробки мережевих рішень необхідні інструменти, що дозволяють побудувати працездатні моделі мережі. Програмні емулятори та симулятори є корисними інструментами для побудови працездатних моделей мережі. Вони дозволяють розглядати різні сценарії роботи мережі, експериментувати з різними налаштуваннями та алгоритмами та визначати найкращі підходи для побудови ефективної мережі. Вони дозволяють імітувати фізичні компоненти мережі, такі як маршрутизатори, комутатори та інші мережеві пристрої, та досліджувати їх роботу в різних умовах [1]. Такі емулятори зазвичай забезпечують високу точність моделювання, але можуть вимагати значних обчислювальних ресурсів.

Симулятори, з іншого боку, дозволяють досліджувати поведінку мережі на більш високому рівні абстракції, не звертаючи уваги на конкретні фізичні компоненти. Вони дозволяють проводити експерименти з різними топологіями мережі та налаштуваннями без необхідності наявності фізичного обладнання.

Деякі з найпопулярніших програмних емуляторів та симуляторів для побудови працездатних моделей мережі включають в себе:

- Cisco Packet Tracer – програмний емулятор, що дозволяє моделювати мережі з використанням пристроїв Cisco.

- GNS3 – інструмент для побудови віртуальних мереж, що базуються на різних операційних системах та пристроях [2].
- NS-3 – симулятор мережі, що дозволяє досліджувати різні протоколи та топології мережі [3].
- OMNeT++ – інструмент для моделювання мережі з високою рівнем абстракції, що дозволяє досліджувати різні типи мереж та протоколів з використанням моделей з різними рівнями деталізації [4].
- Mininet – програмний емулятор мережі, що базується на ядрі Linux та дозволяє побудувати віртуальну мережу на одному комп'ютері [5].

Кожен з цих інструментів має свої переваги та недоліки, тому перед вибором конкретного інструменту варто ретельно розглянути його можливості та вимоги до обчислювальних ресурсів. Незважаючи на це, використання програмних емуляторів та симуляторів дозволяє значно зекономити час та кошти, що пов'язані з розгортанням фізичного обладнання, та дозволяє зосередитися на дослідженні різних аспектів мережі та її оптимізації.

Застосування програмних емуляторів та симуляторів є важливим етапом у процесі проектування та тестування мережі. Ці інструменти дозволяють відтворити та перевірити роботу мережі у різних умовах, що допомагає забезпечити її стабільну та надійну роботу. Використання програмних емуляторів та симуляторів дозволяє ефективно витрачати час та ресурси, уникати можливих проблем та забезпечувати високу якість мережі.

Список використаних джерел:

1. Software-Defined Networking: A Comprehensive Survey. *IEEE Xplore*. URL: https://ieeexplore.ieee.org/document/6994333 (date of access: 18.03.2023).
2. GNS3 website, URL: https://gns3.com/ (дата звернення: 18.03.2023).
3. nsnam. ns-3. *ns-3*. URL: https://www.nsnam.org/ (date of access: 18.03.2023).
4. OMNeT++ Discrete Event Simulator. *OMNeT++ Discrete Event Simulator*. URL: https://omnetpp.org/ (date of access: 18.03.2023).
5. Mininet website, URL: https://mininet.org/ (date of access: 18.03.2023).

ОСОБЛИВОСТІ ЗАХИСТУ ІНФОРМАЦІЇ ТА ПЕРСОНАЛЬНИХ ДАНИХ ЯК ВАЖЛИВІ КОМПОНЕНТИ ОСВІТНЬОГО ПРОЦЕСУ У НАВЧАЛЬНИХ ЗАКЛАДАХ

Волкова Н.М.,
викладач кафедри математичних дисциплін
та інноваційного проектування,
ПВНЗ «Європейський університет»

Інформаційна сфера, як системоутворюючий фактор життя суспільства, активно впливає на стан політичної, економічної, оборонної й інших складових національної безпеки.

Основою є інформаційні технології та інформація, яка в таких умовах стає товаром й основним продуктом виробництва та створення додаткової вартості. Зворотнім боком цієї "медалі" є тотальні незаконні зазіхання на чужу інформацію, що, в свою чергу, вимагає її захисту.

У сучасному світі відбувається безперервна боротьба за контроль над інформаційними потоками. Виграє той, хто не лише їх формує та вміє регулювати у своїх власних інтересах, але й здатний забезпечити цілісність свого інформаційного ресурсу України – і сфера освіти та виховання є однією з найважливіших у цьому сенсі.

Конфіденційна інформація – це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов [3].

Значна частина підприємств, установ та організацій усіх форм власності не забезпечують кіберзахист електронних інформаційних ресурсів, якими вони розпоряджаються, що призводить до порушень прав користувачів цифрових послуг та дискредитує процеси цифрової трансформації в державі.

Щодо законодавчою бази у країні інформація визначається як документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі [1,2,4].

Отже, з огляду саме на конкретний навчальний заклад потрібно вибудовувати відповідну інформаційну інфраструктуру, яка має включати в себе організаційні структури, що забезпечують функціонування і розвиток єдиного інформаційного простору (зокрема, збирання, обробку, збереження, поширення, пошук і передачу інформації). Забезпечувальну частину мають складати науково-методичне, інформаційне, лінгвістичне, технічне, кадрове, фінансове забезпечення. Це може починатися саме з вступної компанії – коли абітурієнт надає свої персональні дані, які зберігаються в його особистому кабінеті і протягом навчання доступ до нього будуть мати тільки адміністрація певних структур навчального закладу і дані зберігаються як його персональні

– наприклад, середній бал, особисті оцінки рівня знань та умінь, траєкторія навчального процесу, рейтинг навчання і таке інше.

Список використаних джерел:

1. Закон України. Про захист персональних даних (Відомості Верховної Ради України (ВВР), 2010, № 34, ст. 481). {Із змінами, внесеними згідно із Законами минулих редакцій та № 2494-IX від 29.07.2022}.
2. Кібербезпека України: Аналіз сучасного стану. Олена Трофименко, Юлія Прокоп, Наталія Логінова, Олександр Задерейко. DOI: 10.18372/24107840/21/13951. УДК 004.056.5:343.326 (045).
3. Рибальский О.В., Хахановський В.Г., Кудінов В.А. / Основи інформаційної безпеки та технічного захисту інформації. – Національна Академія Внутрішніх Справ, Київ – 2012. УДК 681.518 (075.8).
4. Стратегія кібербезпеки України (2021 – 2025 роки). Безпечний кіберпростір – запорука успішного розвитку країни. (Проєкт)

МАСКУВАННЯ ЧУТЛИВИХ ДАНИХ ЗА ДОПОМОГОЮ MICROSOFT SQL SERVER DYNAMIC DATA MASKING

Григорчук Р.О.,
магістрант факультету інформаційних систем та технологій,
Литвиненко Л.О.,
к.т.н., доцент кафедри інформаційних систем,
програмування та кібербезпеки
ПВНЗ «Європейський університет»

Захист конфіденційності даних є однією з головних проблем в інформаційній безпеці. За останні роки кількість випадків порушення конфіденційності даних значно зросла. За даними звіту Verizon Data Breach Investigations за 2021 рік, більшість витоків даних відбувається через кібератаки та зловживання привілеями. Більше 80% витоків включають особисті дані, такі як імена, адреси та ідентифікаційні номери [2-4].

Ці витоки даних можуть коштувати компаніям та організаціям мільйони доларів через втрату довіри клієнтів, витрати на відшкодування шкоди та штрафи від регуляторних органів. За даними IBM Security Cost of a Data Breach Report за 2020 рік, середня вартість одного витоку даних складає $3.86 мільйонів доларів, що є значною сумою для будь-якої компанії. Тому захист конфіденційності даних є надзвичайно важливою проблемою, яка потребує уваги та вирішення.

Dynamic Data Masking є одним із засобів захисту конфіденційних даних в SQL Server. Він дозволяє приховувати конфіденційні дані від користувачів, які не мають доступу до них, тим самим зменшуючи ризики їх порушення. Dynamic Data Masking має кілька переваг, таких як легкість використання, флексибільність та збереження продуктивності системи.

Далі більш детально розглянемо Dynamic Data Masking в SQL Server, надаючи приклади коду та результатів запитів. Розглянемо також визначення конфіденційності даних та ризики їх порушення.

Dynamic Data Masking – це технологія, яка дозволяє приховати чутливі дані в базі даних в режимі реального часу. Це означає, що можна змінювати відображення даних безпосередньо на сервері баз даних, щоб забезпечити захист від несанкціонованого доступу до чутливих даних.

Технологія Dynamic Data Masking працює шляхом зміни значень полів в запитах до бази даних, а не фактичної інформації в базі даних. Це означає, що користувачі можуть бачити тільки відображені значення, а не справжні дані.

Розглянемо приклад використання Dynamic Data Masking. Припустимо, що у нас є база даних з таблицею користувачів, і у цій таблиці є поле “Пароль”, яке містить чутливу інформацію. Якщо ми використовуємо Dynamic Data Masking, ми можемо забезпечити, щоб пароль був відображений тільки для авторизованих користувачів, тоді як для всіх інших користувачів буде відображено замінююче значення, наприклад, “********”.

Також, Dynamic Data Masking може бути корисним при передачі даних з бази даних до зовнішніх систем. Наприклад, якщо ви маєте додаток, який використовує дані з бази даних, ви можете використовувати Dynamic Data Masking для забезпечення захисту чутливої інформації або, якщо ви передаєте дані з бази даних в зовнішню систему.

Зважаючи на те, що Dynamic Data Masking реалізовано у SQL Server як вбудована функція, налаштування маскування в таблиці дуже просто. Ось декілька прикладів коду на T-SQL, які демонструють, як застосовувати механізм Dynamic Data Masking.

Приклад 1: Застосування маскування для стовпця з номером кредитної картки.

```
CREATE TABLE Customers
(
 CustomerID INT PRIMARY KEY,
 Name VARCHAR(100),
 CreditCardNumber VARCHAR(16) MASKED WITH
 (FUNCTION = ‘partial(0, "xxxx-xxxx-xxxx-", 4)’)
)
INSERT INTO Customers (CustomerID, Name, CreditCardNumber)
VALUES (1, ‘John Smith’, ‘1234-5678-9012-3456’)
```

У цьому прикладі використовується функція partial, яка маскує перші 12 символів стовпця з номером кредитної картки, замінюючи їх на рядок “xxxx-xxxx-xxxx-“.

Приклад 2: Застосування маскування для стовпця з датою народження.

```
CREATE TABLE Employees

(

 EmployeeID INT PRIMARY KEY,

 Name VARCHAR(100),

 BirthDate DATE MASKED WITH (FUNCTION = ‘year(2)’)

)

INSERT INTO Employees (EmployeeID, Name, BirthDate)

VALUES (1, ‘Jane Doe’, ‘1990-01-01’)
```

У цьому прикладі використовується функція year, яка маскує всі, крім останніх двох символів дати народження, замінюючи їх на нулі.

Результат запиту буде залежати від того, хто виконує запит та від його рівня доступу. Наприклад, якщо користувач має доступ до відкритих даних, він може отримати результат запиту без маскування, в той час як інші користувачі можуть отримати запит з маскуванням даних.

Отже, для прикладу 1 запит SELECT * FROM Customers поверне наступний результат:

CustomerID	Name	CreditCardNumber
1	John Smith	xxxx-xxxx-xxxx-3456

Як видно, номер кредитної картки був замаскований.

Для прикладу 2 запит SELECT * FROM Employees поверне наступний результат:

EmployeeID	Name	BirthDate
1	Jane Doe	19-01-01

Як видно, рік народження був маскований, лишивши тільки останні два символи.

Отже, маскування даних дозволяє зберігати конфіденційні дані безпечними, дозволяючи контролювати рівень доступу користувачів до цих даних.

Налаштування Dynamic Data Masking дуже просте і може бути використане з будь-якою таблицею бази даних. Для отримання додаткової інформації про функції маскування в SQL Server можна звернутися до офіційної документації Microsoft [1].

Таблиця з основними функціями маскування

Функція маскування	Опис	Приклад
default	Замінює значення стовпця на NULL	Salary FLOAT MASKED WITH (FUNCTION = ‘default()’)
email	Замінює частину тексту від символу @ до кінця на *	Email VARCHAR(100) MASKED WITH (FUNCTION = ‘email()’)
partial	Замінює певну кількість символів на *	CreditCardNumber VARCHAR(16) MASKED WITH (FUNCTION = ‘partial(0, "****-****-****-", 4)’)
random	Замінює значення стовпця на випадкову послідовність	PhoneNumber VARCHAR(10) MASKED WITH (FUNCTION = ‘random(1)’)
custom string	Замінює значення стовпця на користувацький рядок	Address VARCHAR(100) MASKED WITH (FUNCTION = ‘custom("No Address Provided")’)

У підсумку, Dynamic Data Masking є потужним інструментом для захисту чутливої інформації в базі даних. Він може бути корисним для багатьох типів проектів, де є необхідність зберігати чутливі дані в базі даних, але потрібно забезпечити доступ до цих даних для обраних користувачів. Dynamic Data Masking дозволяє відображати дані, які потрібні користувачам, але приховувати справжні значення. Це забезпечує високий рівень захисту даних в базі даних, що особливо важливо у сферах, які працюють з чутливою інформацією, таких як медицина, фінанси, державні установи та інші.

Список використаних джерел:

1. Офіційна документація Microsoft про Dynamic Data Masking: https://docs.microsoft.com/en-us/sql/relational-databases/security/dynamic-data-masking?view=sql-server-ver15
2 Звіт Verizon Data Breach Investigations за 2021 рік: https://www.verizon.com/business/resources/reports/dbir/2020/introduction/
3. Звіт IBM Security Cost of a Data Breach Report за 2020 рік: https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/
4. Стаття на тему захисту конфіденційності даних від OWASP: https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html

КІБЕРБЕЗПЕКА МІЖНАРОДНИХ ФІНАНСОВИХ ОПЕРАЦІЙ

Гук П.В.,
аспірант,
ПВНЗ «Європейський університет»

В умовах, коли інформаційні технології з кожним днем відіграють все важливішу роль в нашому житті, звичні нам процеси оцифровуються, а інформаційні технології стрімко розвиваються і стають все доступнішими, а забезпечення кібербезпеки стає все більш актуальною задачею. Одним з особливо важливих є питання забезпечення кібербезпеки міжнародних фінансових операцій, адже недостатній захист може стати причиною значних втрат.

Фінансові транзакції можуть здійснюватися, як у випадку грошових платежів, так і у випадку руху капітальних ресурсів, наприклад, лізинг, кредит, франчайзинг [1].

Об’єктами фінансових операцій завжди є фінансові активи, такі як:

- національні гроші;
- цінні папери;
- дорогоцінні метали;
- нерухомість.

Також вирізняють наступні типи фінансових операцій.

- Операції з переказу грошей – всі форми та види розрахунків, а також трансфери;
- Операції з капіталом – операції спрямовані на керування капіталом в умовах різноманітних ризиків, а саме хеджування, іпотеки та застави;
- Інвестиційні операції – переміщення капіталу з метою приросту. До них належать: кредит, лізинг, траст, оренда, франчайзинг та інші, термін яких перевищує 180 днів;
- Спекулятивні операції – короткострокові операції з метою отримання вигоди, наприклад, операції своп, відсотковий та валютний арбітраж і т.ін.

Що ж стосується саме міжнародних фінансів, то сюди можна віднести фонди фінансових ресурсів, які утворилися внаслідок різноманітних міжнародних економічних відносин. В організаційному плані – це сукупність банків, бірж, міжнародних фінансових інституцій, міжнародних та регіональних фінансово-кредитних установ, саме через які може здійснюватися рух світових фінансових потоків.

Суб'єктів в таких операціях можна поділити на національних, тобто держава, підприємство, громадяни та наднаціональних, а саме, міжнародні організації і фінансові інституції.

В залежності від простору функціонування міжнародні фінанси поділяють на наступні категорії:

- національно-державні, тобто такі, які не залучають іноземних суб'єктів та не виходять за межі держави;
- міжнародні – тобто транснаціональні та міждержавні кредитно-фінансові відносини.

В свою чергу, здійснити міжнародні фінансові операції можна наступними каналами:

- валютні операції;
- купівля-продаж товарів;
- операції з цінними паперами;
- зарубіжні інвестиції;
- перерозподіл частки національного доходу у формі внесків до міжнародних організацій та допомоги бідним країнам.

З вище описаного можна зробити висновок, що існує декілька об'єктів міжнародних фінансових відносин, які можуть стати ціллю кібератак. Різноманітні канали здійснення цих операцій часто підпадають під юрисдикцію декількох суб'єктів, що, в свою чергу, породжує можливості атаки на проміжних суб'єктів.

На сьогодні існують такі способи забезпечення кібербезпеки [2]:

- Регулювання кібербезпеки на законодавчому рівні. Тобто створення законодавства, яке б допомогло врегулювати відносини між суб'єктами фінансових операцій всередині держави та визначати наслідки у випадку їх порушення.
- Формування політик для керування взаємодії інституцій, які дають змогу суб'єктам фінансових операцій сформувати процеси, які будуть стійкими до кібератак.
- Формування стандартів для регулювання кібербезпеки, які можуть регулювати захищеність каналів фінансових операцій.
- Визначення державою суб'єктів загроз та вживання заходів для її нейтралізації.
- Інвестування в кібербезпеку підприємств, а саме, застосування технологій для захисту самого підприємства, а також шифрування каналів проведення фінансових операцій.

- Інвестування в наукові дослідження, пов’язані з оцінкою загроз, які існують і можуть виникнути в найближчому майбутньому та розробкою засобів для протидії ним.

Як бачимо, існує досить багато способів захисту фінансових операцій, але вони досить не ефективні самі по собі, а можуть дати результат лише при комплексному застосуванні, так як регулюють окремі аспекти кібербезпеки фінансових відносин.

Список використаних джерел:

1. Зайцева І.Ю. Міжнародні фінанси: Навч. посібник. – Харків: УкрДАЗТ, 2015. – 311 с.
2. Кращі практики управління кібербезпекою. URL: *https://www.undp.org/sites/g/files/zskgke326/files/migration/ua/Report_on_Cybersecurity_04.pdf*

ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ В БАНКАХ

***Гущак О.М.*[1]**
***Коцун В.І.*[2]**
[1]к. т. н., доцент кафедри математики та комп’ютерних дисциплін
[2]к. т. н., доц., завідувач кафедри математики та комп’ютерних дисциплін,
Львівська філія ПВНЗ «Європейський університет»

Ще з початку епідемії COVID-19 як українці, так і увесь світ були змушені приймати нові виклики, навчатися жити в новому, дистанційному форматі. Обмеження через поширення вірусу торкнулися усіх сфер життя. Співробітники багатьох підприємств, компаній, фірм були вимушені працювати поза межами офісів та своїх постійних місць роботи. Вони користувалися домашніми інтернет-мережами, підключалися з пристроїв, які, на відміну від корпоративних, не були належним чином захищені. Величезна кількість даних опинилася без належного захисту. З часом ми певним чином призвичаїлися до нових умов користування, але з початком повномасштабного вторгнення російської федерації всі українські державні сайти, банківські сервіси, системи та інфраструктура зазнали величезної кількості ворожих кібератак та збоїв [1].

Почалися атаки на сайти Верховної Ради України, Кабінету Міністрів України, Міністерства закордонних справ України, Служби безпеки України, Міністерства оборони України, Міністерства України з питань реінтеграції тимчасово окупованих територій, ПриватБанку, Ощадбанку та великої кількості інших установ [2].

Сучасні форми гібридних війн демонструють залучення інформаційних атак на серйозні вірусні програми на сервери державного та

транскорпораційного рівня, які серйозно підривають політичну та економічну стабільність у країні та регіоні загалом [3].

Загалом, кібератаки націлені на приховане викрадення важливої інформації, ймовірно, для надання росії стратегічної переваги на полі бою. Все це відбувається для того, аби здійснити психологічний тиск на громадян, дестабілізувати ситуацію всередині країни, посіяти паніку та хаос, паралізувати засоби комунікації та зв'язку у державі. Такого роду атаки стали можливими лише через те, що не був забезпечений надійний та досконалий захист інформаційних ресурсів такої важливої сфери діяльності держави, як національна кібербезпека [6].

Від рівня зрілості комплексу кібербезпеки, її інфраструктури та безвідмовності залежать безпечна робота та захист інформаційних даних підприємств, особливо фінансової установи

Комп'ютерна безпека – це сукупність проблем у галузі телекомунікацій та інформатики, пов'язаних з оцінкою і контролюванням ризиків, що виникають при користуванні комп'ютерами та комп'ютерними мережами і розглядуваних з точки зору конфіденційності, цілісності і доступності.

Закон України «Про основні засади забезпечення кібербезпеки України» дає таке визначення: «кібернетична безпека (кібербезпека) – це стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі; кібернетичний простір (кіберпростір) – це середовище, яке виникає в результаті функціонування на основі єдиних принципів і за загальними правилами інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем» [4].

Кібербезпека, без жодних сумнівів, в умовах воєнного стану є одним із стратегічних напрямків розвитку банку. За кібернетичну безпеку відповідальна не тільки служба інформаційних технологій, але й фінансова установа загалом. Від організаційної ефективності системи захисту інформації та загалом цілого комплексу дій і професіоналізму персоналу зокрема залежить захист персональних даних клієнтів, їх обробка та зберігання, конфіденційність проведення банківських операцій [7].

Дбаючи про свою репутацію та враховуючи ризики для бізнесу банки старанно відслідковують за оновленнями щодо кібербезпеки, можливими загрозами та слідують настановам з питань безпеки, які висуває міжнародна спільнота та Національний банк України [5]/. Так, відповідно до постанови НБУ №95 від 28.09.2017 про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України, зокрема, мова йде про необхідність фільтрації трафіку центрів обробки даних, АТ «Кредобанк» придбав обладнання та програмне забезпечення для побудови безвідмовного рішення для захисту серверів процесингу. Оскільки раніше банк вже відбудував мережеву інфраструктуру цифрових-центрів на базі архітектури Cisco ACI, оптимально задовольнити його потреби в питаннях якості та відповідності вимогам безпеки трафіку вдалося рішенню Cisco Firepower 4110 NGIPS Applianc

Для захисту серверів процесингу АТ «Кредобанк» систему було розгорнуто на двох майданчиках. Обрані міжмережеві екрани слугують сервісними пристроями для фабрики ACI. Основна задача обладнання полягає в інспектуванні трафіку, перенаправлення якого відбувається засобами тієї ж таки фабрики ACI. Самі міжмережеві екрани реалізовані, як окремі логічні пристрої у режимі multi-instance на гіпервізорах Firepower 4110. Технологія «failover» дозволила об'єднати усі міжмережеві екрани в одну логічну систему. Інтерфейси керування платформами, самими міжмережевими екранами та інтерфейси для failover – усі підключені до класичної мережі, а керування цими пристроями здійснюється з існуючої системи FMC.

Інформаційна взаємодія між компонентами системи на мережевому рівні відбувається за допомогою використання протоколів на базі відкритих стандартів, що входять до протоколу IP. А інформаційний обмін між системами відбувається через єдине інформаційне середовище, використовуючи стандартні протоколи обміну даних із забезпеченням необхідної кількості оптичних каналів зв'язку між пристроями. В результаті розроблені технічні рішення забезпечують функціонування системи безперервно, в цілодобовому режимі, 365 днів на рік. Система забезпечує високу ступінь готовності, спроектована з відсутністю єдиних точок відмови для критичних, з точки зору функціонування, елементів. Підвищення безвідмовності забезпечується наступними засобами:

– використання високонадійного обладнання;

– дублювання і резервування ліній зв'язку;

– дублювання і резервування критичних для роботи системи в цілому програмних, програмно-апаратних та апаратних засобів.

Для забезпечення інформаційної безпеки на міжмережевих екранах були налаштовані наступні політики безпеки:

– політика фільтрації трафіку від/до мережі процесингу на рівні L4-L7. Ця політика була перенесена із існуючого контексту міжмережевого екрану ASA для мережі процесингу. IPS політика для мережі процесингу;

– політика фільтрації на базі переліків потенційно-небезпечних FQDN/адрес, що динамічно завантажуються.

Як результат, АТ «Кредобанк» отримав комплексну систему для захисту серверів процесингу на платформі Cisco Firepower 4110 NGIPS Appliance, до складу якої було включено якісне відмовостійке обладнання, програмне забезпечення, яке відповідає ІТ та бізнес-вимогам установи. Кредобанк вже багато років демонструє високопрофесійний підхід до організації ІТ-інфраструктури та комплексу безпеки, завжди працює відповідно до європейських стандартів та згідно з ними підтримує на безпечному рівні свої системи та інфраструктуру. Банк приділяє максимальну увагу захисту фінансової інформації та веде активну роботу як всередині установи, розвиваючи власну інфраструктуру, так і зовнішню.

Отже, щоб вберегти підприємство від кіберзагроз необхідно:

1. Інвестувати у найпростіші способи захисту. Найпопулярнішими методами кібератак російських військових хакерів є:

– фішингові розсилання, внаслідок яких вони можуть отримати облікові дані для доступу до інформаційних систем;

– розсилання шкідливого програмного забезпечення, яке спрямоване на викрадення даних або знищення інфраструктури;

– використання відомих вразливостей.

2. Мінімізувати ризик кібератак завдяки дотриманню правил кібергігієни, відповідальному ставленню до політики використання паролів та вчасному оновленню програмного забезпечення.

3. Вивчати слабкі місця кіберзахисту установи та укріплювати їх. Хакери постійно здійснюють розвідувальні операції в Україні, знаходять найслабші місця у захисті компаній та атакують через них. Не існує на 100% захищених систем.

4. Пам’ятати, що безпека підприємства залежить від кожного працівника. Хакери можуть атакувати установу і через співробітників, викравши їхні дані.

5. Пам’ятати, що фізична безпека користувачів критичної інформаційної інфраструктури така ж важлива, як і захист їхніх облікових записів. Російські хакери можуть використовувати облікові дані користувачів, які перебувають на тимчасово окупованих територіях. Компанії, особливо з-поміж критичної інфраструктури, мають усвідомлювати, що фізична безпека їхніх працівників – це також інвестиція в їхній кіберзахист [8].

Державні органи, урядові організації спільно з українськими компаніями з кібербезпеки і провідними світовими виробниками рішень запровадила ешелонований кіберзахист для держави та бізнесу [4].

Список використаних джерел:

1. Щодо кібератак на сайти державних органів. Офіційний веб-сайт Державної служби спеціального зв’язку та захисту інформації України. URL: https://cip.gov.ua/ua/news/shodo-kiberatak-na-saiti-derzhavnikh-organiv

2. Щодо кібератаки на сайти військових структур та державних банків. Офіційний веб-сайт Кабінету Міністрів України. URL: https://www.kmu. gov.ua/news/shchodo-kiberataki-na-sajti-vijskovih-struktur-ta-derzhavnih-bankiv

3. Закон України «Про основні засади забезпечення кібербезпеки України»: Закон від 05.10.2017 № 2163-19. Відомості Верховної Ради. 2017. № 45. Ст. 403.

4. Закон України «Про Державну службу спеціального зв’язку та захисту інформації України»: Закон України від 23.02.2006 № 3475-15. Відомості Верховної Ради України. 2006. № 30. Ст. 258.

5. Постанова НБУ №95 від 28.09.2017 Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України URL:https://bank.gov.ua/ua/legislation/Resolution_28092017_95

6. *Дубов Д. В.* Кіберпростір як новий вимір геополітичного суперництва: монографія. Київ: НІСД, 2014. 328 с. URL: https://niss.gov.ua/sites/default/ files/2015-02/Dubov_mon-89e8e.pdf

7. Завгородня Ю. В. Кібербезпека як інноваційний захист у політичному просторі України. Вісник НТУУ «КПІ». Політологія. Соціологія. Право. 2021. № 4 (52). URL: http://visnyk-psp.kpi.ua/article/view/248130/245405
8. Комітет з питань цифрової трансформації інформує як посилити кіберзахист підприємствам та установам Інформаційне управління Опубліковано 15 квітня 2022 URL: https://www.rada.gov.ua/news/razom/221800.html

ФОРМУВАННЯ НАВИЧОК ФІКСАЦІЇ ДЕСТРУКТИВНОЇ ДЕЗІНФОРМАЦІЇ В КІБЕРПРОСТОРІ ПІД ЧАС ЗАНЯТЬ ДЛЯ СТУДЕНТІВ СПЕЦІАЛЬНОСТІ «КІБЕРБЕЗПЕКА»

Давиденко А.,
д.т.н., пров.наук.співр. відділу математичного
та економетричного моделювання
Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова
Висоцька О.,
к.т.н.,доцент кафедри комп'ютеризованих систем захисту інформації
Національного авіаційного університету
Потенко О.,
мол.наук.співр. відділу математичного та економетричного моделювання
Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова

Проблема виявлення, моніторингу та фіксації російської дезінформаційної діяльності має політичні, організаційні та технологічні аспекти. Як своєчасно виявити, зафіксувати дезінформацію та передбачити наслідки для попередження її руйнівного впливу? Від якості вирішення цих питань залежить перемога або поразка, як мінімум, на інформаційному фронті. Суспільство України має унікальні властивості самоорганізації, але цілеспрямованість та наполегливість дій має пряму залежність від інформаційного впливу та від частоти його випадкової або навмисної дезінформації. Основи кібергігієни мають впроваджуватися в суспільство через навчання. Студентство, молодь, школярі в першу чергу вразливі, тому мають бути залучені до процесу виявлення дезінформації з метою отримання імунітету до її впливу.

Попередній досвід авторського колективу пов'язано з міжнародним впровадженням технологій захисту інформації на базі штучного інтелекту[1], а саме, механізмів автентифікації користувачів автоматизованих систем обробки критичної інформації на базі штучних нейронних мереж [3]. Головною особливістю при цьому є використання спеціально адаптованих штучних нейронних мереж [4] для реалізації біометричних механізмів. Найчастіше це розпізнавання обличчя користувача та його стиль роботи на клавіатурі. Викладацький досвід підтверджується багаторічної практикою викладання в провідних навчальних установах України та методичних публікаціях [2].

На останніх курсах бакалаврату студенти технічного напряму мають достатній досвід використання інформаційних технологій але їм потрібна чітка фіксація проблемі протидії дезінформації, тому є актуальною задача розробки практичних лабораторних робіт з вияву російської дезінформації.

Розробка лабораторних робіт за тематикою виявлення, моніторинг та фіксація російської дезінформаційної діяльності для здобувачів вищої освіти ОС «Бакалавр» спеціальності 125 «Кібербезпеки» буде сприяти залученню молоді безпосередньо до процесу протидії російській дезінформаційній діяльності. Наявність закордонних студентів в групах, які навчаються в рамках навчального курсу Incident Management in Cyberspace (НАУ), робіть процес протидії більш публічним та незалежним.

Досвід 2022 року показав, що розглядати тільки технологічні аспекти процесу виявлення, моніторингу та фіксації російської дезінформаційної діяльності недостатньо. Потрібне навчання студентів навичкам пошуку, аналізу та збереження фейкової інформації, яке включає ручну процедуру пошуку з акцентом на пошук першоджерела інформації, визначення головних напрямів інформаційної атаки та вивчення характерних рис та методів розповсюдження фейкової інформації. Також потрібне набуття навичок своєчасної фіксації дій. Не менш важливим етапом є навчання студентів навичкам копіювання інформації зі збереженням її автентичності. Це копіювання в вигляді дзеркала веб-сайту з обов'язковою фіксацією дати копіювання, адреси. Забезпечення цілісності копії, наприклад хешування та накладення цифрового підпису. Надійне збереження знайденої інформації в хмарному або грід середовищі.

Але, крім отримання цих важливих навичок, необхідно коригувати сприйняття осіб, які навчаються. Стандартною помилкою студентів під час виконання лабораторних робіт, є помилки при ідентифікації інформаційної атаки. По-перше фіксація вторинного джерела дезінформації, по-друге студенти не завжди відрізняють кібер вплив від інформаційного. Тому в цьому році були запропоновані додаткові лабораторні роботи, які наочно показують цю різницю.

Важливим аспектом при проведенні лабораторних робіт є розуміння факту, що інформація – це зброя, використання якої, потребує особливої обережності. Намагаючись довести фейковість інформації, не можна розкривати критичну інформацію (наприклад ЗСУ має тільки х-літаків, а рф говорить, що знищила на сто більше чим існує насправді). Нажаль, невдала спроба протидії може спричинити більше шкоди, ніж сама фейкова інформація. Тому важливими є фактори самоцензури та усвідомлення наслідків розголошення інформації. Перші місяці війни добре навчили нас, що застосування інформаційних технологій, без розуміння, що саме вони роблять, веде до незворотних втрат.

Розробка навчально-методичних матеріалів, їх практична апробація та формування групи фахово підготовленої молоді, вмотивованої на виявлення,

моніторинг та фіксацію російської дезінформаційної діяльності, є основними результатами.

Список використаних джерел:

1. Vysotska Olena, Davydenko Anatolii, «Dodatkowe uwierzytelnianie uprawnionych użytkowników według geometrii ich twarzy w systemach informatycznych wykorzystujących technologię single sign-on», XI edycja Konferencji «Inżynier XXI wieku», Part of the Monograph «Przetwarzanie, transmisja i bezpieczeństwo informacji» (10 grudnia 2021), Bielsko – Biała, Polska, 2021, S. 257-268. DOI: https://doi.org/10.53052/9788366249868.27
2. Ю.Є. Хохлачова, В.М. Кінзерявий, В.В. Погорелов, А.М. Давиденко Управління проектами захисту інформації. Лабораторний практикум для здобувачів вищої освіти ОС «Бакалавр» спеціальності 125 «Кібербезпека». – К.: НАУ, 2022. – 84 с.
3. Vysotska O., Davydenko A. Keystroke Pattern Authentication of Computer Systems Users as One of the Steps of Multifactor Authentication. Advances in Intelligent Systems and Computing, 2020, 938, p. 356–368
4. Патент UA 150034 U; G06N 3/04; Базовий елемент для побудови нейронної мережі, здатної адаптуватися / Давиденко А.М.; Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України. – заяв. u 2021 04761, 20.08.2021 р. – Опубл. 22.12.2021, Бюл. № 51.

АНАЛІЗ КІБЕРЗАГРОЗ НА ПОЧАТКУ РОКУ

Демидов З.Г.,
старший науковий співробітник
науково-дослідної лабораторії
з проблем інформаційних технологій
та протидії злочинності у кіберпросторі,
Хлестков О.В.,
старший науковий співробітник
науково-дослідної лабораторії
з проблем інформаційних технологій
та протидії злочинності у кіберпросторі,
Харківський національний університет внутрішніх справ

Зловмисники часто використовують поштові розсилки для поширення шкідливого програмного забезпечення (ПЗ). Кількість виявлених у поштовому трафіку вкладень більшою мірою залежить від активності та наполегливості атакуючих і меншою – від дій користувачів: у цій статистиці реєструється факт виявлення листа, що містить шкідливе вкладення, а не спроба його запуску користувачем. Оскільки масові розсилки шкідливого ПЗ відбуваються хвилями, на великому проміжку часу кількість спрацювань поштового компонента то зростає, то падає, хоча має неяскраво виражений висхідний тренд.

У березні цього року захисні рішення компаній виявили рекордну кількість шкідливого програмного забезпечення у поштовому трафіку користувачів – понад 19 мільйонів спрацьовувань. Щоб визначити причину цього зростання, було проаналізовано, які саме файли зробили найбільш значний внесок. Як з'ясувалося, березневий пік у сукупній кількості виявленого шкідливого програмного забезпечення збігся зі збільшенням числа шкідливих офісних документів.

Якщо кількість шкідливих виконуваних файлів, виявлених у поштовому трафіку в березні, збільшилася приблизно на 14% відносно лютого, то кількість шкідливих документів за той же період зросла приблизно вдвічі і виявилася майже на три з половиною мільйони більше, ніж у середньому з травня 2022 року до лютого 2023-го. Тобто саме розсилки з документами спричинили березневий пік.

Розглянемо докладніше, які шкідливі файли розповсюджували поштою у перші майже три місяці 2023 року. Оцінюючи розподілу файлів ми використовуємо поняття «платформи» – середовища, у якому виконується шкідливий програмний код. За цей період в поштовому трафіку було зафіксовано ВПЗ для приблизно п'ятдесяти різних платформ. Розглянемо декілька найпоширеніших із них.

Перше місце ділять платформи, що відносяться до PE-файлів, та скрипти, що виконуються, такі як JavaScript і VisualBasicScript. В обох випадках як вкладення до листа розсилаються файли, що виконуються. Це найбільш простий спосіб атаки, і незважаючи на те, що багато поштових клієнтів і шлюзів блокують такі листи або забороняють запуск таких вкладень, зловмисники продовжують його масово використовувати – майже в половині випадків з 60 мільйонів шкідливе ПЗ в пошті являло собою звичайний PE-файл, що виконується.

На другому місці опинилися шкідливі офісні документи – на них припало близько чверті всіх спрацювань поштових компонентів захисних рішень із початку цього року. За цей період рішення виявили близько 1,9 мільйонів унікальних файлів цього типу. Останні кілька років зловмисники активно використовують офісні програми під час проведення масових атак на користувачів. Зараз розсилання шкідливих офісних документів – це один із основних способів зараження пристрою жертви.

Далі йде платформа Multi – переважно це спрацювання хмарної технології детектування UrgentDetectionSystem. Також сюди потрапляє мультиплатформне шкідливе програмне забезпечення.

Потім у списку йде різне програмне забезпечення: PDF-файли, файли на мові Java, ярлики і т. д., що демонструє широкий спектр засобів, що використовуються зловмисниками.

Тепер подивимося на конкретні загрози, з якими найбільше користувачів зіткнулося. Оскільки офісні документи становлять значну частку шкідливих вкладень, ми відзначимо найпоширеніші загрози цього.

Можна виділити дві групи загроз, що використовують офісні програми: документи, що експлуатують різні вразливості в офісному ПЗ (експлойти) [1], а також документи, що містять шкідливі.

Найчастіше зловмисники намагаються експлуатувати щодо старих вразливостей 2017–2018 років: CVE-2018-0802 та CVE-2017-11882. В обох випадках експлуатація полягає у підготовці атакуючими спеціальних конструкцій, що викликають переповнення стека при обробці в редакторі формул з офісного пакету, що дозволяє виконати в системі довільний код. Обидві вразливості виправлені вже кілька років тому, але, як бачимо, ними все ще активно намагаються скористатися. Зазначимо однак, що хоча в масових атаках поширені старі вразливості, в цільових атаках для зловмисників привабливішими виглядають нещодавно виправлені вразливості та вразливості нульового дня.

До другої групи документів відносяться ті, в яких шкідливі дії здійснюються не внаслідок експлуатації вразливостей, а за рахунок виконання офісним програмним забезпеченням макросів VBA або Excel, що містяться в документі. Зловмисники можуть поєднувати різні макроси в одному документі, обфузувати їх та використовувати додаткові техніки, наприклад, завантаження шаблонів. У більшості випадків документи з макросами завантажують на комп’ютер користувача основне корисне навантаження – інше ВПЗ, яке може належати до будь-якої родини і, відповідно, нести в собі будь-яку функціональність (бекдори, банери, шифрувальники і т.п.). Останнім часом найчастіше такі документи завантажують ВПО сімейства Emotet [2] і є основним способом поширення цієї, можливо, найактуальнішої загрози останніх років – документи, що містять характерні макроси і які детектуються як Trojan.MSOffice.Emotet.gen. Проте зловмисники використовують офісні документи, як вектор розповсюдження далеко не лише цієї родини. Наприклад, цей спосіб застосовується і для розсилки IcedID і Qbot. Також документи з макросами регулярно використовують у цільових атаках, наприклад угрупуванням ScarCruft.

Можна також виділити ще один тип шкідливих документів, що статистично менш поширений і тому не потрапив у TOP 15 поштових загроз. Такі документи не містять експлойти та макроси, але вимагають від користувача виконати якусь дію – наприклад, перейти на посилання в документі, що веде на шкідливий або фішинговий сайт.

Найчастіше поштові компоненти захисних рішень виявляли шкідливі документи в Італії, В’єтнамі та Мексиці. Загалом атаки такого типу відбуваються по всьому світу, у всіх регіонах.

Розсилка шкідливих файлів офісних форматів є одним із найбільш поширених серед зловмисників способів зараження в останні роки, причому вже звично велика кількість таких атак продовжує зростати. Шкідливі документи використовуються, як у масових розсилках «навмання», так і у цільових атаках.

Для захисту від атак через електронну пошту, зокрема з використанням шкідливих документів, компаніям рекомендується:

• використовувати надійне захисне рішення на рівні поштового шлюзу, так і на робочих станціях;

• встановлювати необхідні оновлення безпеки для офісного програмного забезпечення, щоб знизити ризик експлуатації вразливостей зловмисниками;

• навчати працівників правилам інформаційної безпеки, регулярно проводити тренінги, у тому числі, присвячені безпечному поводженню з електронною поштою.

Звичайним користувачам рекомендується з підозрою ставитись до посилань і вкладень у листах, особливо якщо вони прийшли з незнайомої адреси.

Список використаних джерел:

1. Експлойт https://uk.wikipedia.org/wiki/%D0%95%D0%BA%D1%81%D0%BF%D0%BB%D0%BE%D0%B9%D1%82
2. Що таке шкідливе програмне забезпечення Emotet і як його видалити з Mac (2021) https://blog.webtech360.com/uk/macos/%D1%89%D0%BE%D1%82%D0%B0%D0%BA%D0%B5-%D1%88%D0%BA%D1%96%D0%B4%D0%BB%D0%B8%D0%B2%D0%B5%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BD%D0%B5%D0%B7%D0%B0%D0% B1%D0%B5%D0%B7%D0%BF%D0%B5%D1%87%D0%B5%D0% BD%D0%BD%D1%8F-emotet-%D1%96-%D1%8F%D0%BA-%D0%B8%D0%BE%D0%B3%D0%BE%D0%B2%D0%B8%D0%B4%D0%B0%D0%BB%D0%B8%D1%82%D0%B8-%D0%B7-mac-2021/77700407

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ У ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ

Діденко О.В.,
курсант ІІ курсу
Харківського національного університету внутрішніх справ
Світличний В.А.,
кандидат технічних наук, доцент,
доцент кафедри протидії кіберзлочинності факультету № 4
Харківського національного університету внутрішніх справ

Побудова інформаційного суспільства є стратегічною метою провідних держав світу: США, Японії, Канади, а також країн-учасниць Європейського Союзу. Розуміючи актуальність та важливість розвитку інформаційної сфери як запоруки конкурентоспроможності, дедалі більше країн обирають аналогічну стратегію, зокрема і Україна.

За даними міжнародного рейтингу конкурентоспроможності держав у цифровому середовищі – World Digital Competitiveness Ranking, Україна в 2021 році посіла 54 місце. Порівняно з 2020 роком показник покращився на чотири

позиції. Підсумкова рейтингова система розраховується на основі трьох показників: якість освіти та науки («Знання»); регуляторне середовище, фінансовий капітал у ІТ-галузі, стан інтернету та комунікаційних технологій («Технології»); рівень готовності використання цифрової трансформації («Готовність») [1].

Нова галузева програма інформатизації системи МВС та ЦОВВ зосереджена на розбудові публічних сервісів єдиної інформаційної системи МВС, упровадженні та модернізації національних електронних інформаційних ресурсів як складових ЄІС МВС, створенні інноваційної інфраструктури органів системи МВС, підвищенні довіри і безпеки при використанні ІКТ, створенні в новостворених функціональних підсистемах ЄІС МВС [2] комплексних систем захисту інформації та вжитті заходів із забезпечення кіберзахисту цих систем, подальшій структуризації законодавчих та нормативно-правових документів сфери інформатизації органів системи МВС.

Ефективність правоохоронної діяльності значною мірою залежить від якості інформаційної підтримки, тому інформаційні технології знаходять широке застосування у діяльності правоохоронних органів. Необхідно відмітити, що в МВС України протягом років накопичено чималий досвід використання різноманітних інформаційних систем оперативно-розшукового та інформаційно-довідкового призначення. Департаментом інформатизації МВС України створена та постійно удосконалюється система інформаційного забезпечення, яка виконує підтримку практичної діяльності органів та підрозділів Національної поліції щодо забезпечення запобігання кримінальним правопорушенням, їх виявлення, припинення, розкриття і розслідування, розшуку осіб, які вчинили кримінальні правопорушення, надає багатоцільову статистичну, аналітичну та довідкову інформацію, допомагає при розв’язані інших завдань боротьби зі злочинністю. Серед найбільш потужних складових зазначеної системи необхідно відмітити інформаційно-телекомунікаційну систему «Інформаційний портал Національної поліції України» [3] (інформаційні підсистеми «Факт (ЄО)», «Кримінальні провадження», «Кримінальна статистика», «Адмінпрактика», «Custody Records», «Атріум», «Особа», «Номерна річ», «Розшук», «Пізнання», «Гарпун», «Розслідування», «Слід», «Поліцейські Операції», «Зброя-Арсенал», «Воєнний Злочинець», «Зброя-Схрон»), «Єрдр», «Наіс», «Аркан», «Цунамі» [4]. Практика боротьби зі злочинністю переконливо свідчить не тільки про суттєву, а в багатьох випадках пріоритетну роль системи інформаційного забезпечення МВС України як ланки, що значно зумовлює ефективність роботи всієї системи правоохоронних органів України.

Серед найбільш актуальних напрямів удосконалення інформаційних технологій у правоохоронній діяльності на сучасному етапі можна виділити:

1. Використання технології «Big data». Інформаційна методика «Big data» полягає в обробці гігантських та постійно наростаючих масивів даних та отриманні результатів які людина взмозі сприйняти (наприклад, GPS-сигнали

від автомобілів, інформація про транзакції банків та ін.), що відкриває великі можливості для її застосування в різних галузях правоохоронної діяльності.

2. Використання технології «Deep learning». Глибокі нейронні мережі – це один із найпопулярніших підходів до створення різних систем штучного інтелекту у наш час. Успішність їх застосування обумовлена тим, що мережа автоматично виділяє з множини даних важливі ознаки, необхідні для вирішення задачі. Ця можливість актуальна для вдосконалення правоохоронної діяльності.

3. Застосування методів нечітких множин прийняття оптимального юридичного рішення. Наприклад, вибір виду кримінального покарання або вибір запобіжного заходу в рамках попереднього розслідування може базуватися на застосуванні методу аналізу ієрархій, що є складовою математичної теорії нечітких множин.

На підставі вищезазначеного можна зробити висновок, що в умовах зростаючої комп'ютеризації суспільства, у тому числі і правоохоронних органів, головною метою освітнього процесу є надання курсантам, студентам, слухачам вузів МВС України, працівникам правоохоронних органів держави таких спеціальних знань, умінь та практичних навичок з інформатики та обчислювальної техніки, інформаційного забезпечення правоохоронних органів, які б склали міцний фундамент подальшого засвоєння і ефективного використання ними комп'ютерної техніки та сучасних інформаційно-комунікаційних технологій у своїй оперативно-службовій діяльності.

Список використаних джерел:

1. Світовий рейтинг конкурентоспроможності. URL: https://www.imd.org/centers/world-competitiveness-center/rankings/world-digital-competitiveness/ (дата звернення: 26.02.2023).
2. Інформатизація системи МВС. URL: https://mvs.gov.ua/uk/ministry/projekti-mvs/informatizaciya-sistemi-mvs-ukrayini (дата звернення: 26.02.2023).
3. Про затвердження Положення про інформаційно-телекомунікаційну систему «Інформаційний портал Національної поліції України»: наказ МВС України від 03.08.2017 № 676 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/z1059-17 (дата звернення: 26.02.2023).
4. Про роль інформаційних технологій та їх забезпечення в діяльності органів внутрішніх справ україни. URL: http://www.spilnota.net.ua/ua/article/id-3577/ (дата звернення: 26.02.2023).

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ВІЙСЬКОВИХ ДІЙ ТА БЕЗПЕКИ НАЦІЇ

Желновач І.О.,
курсант ІІ курсу
Харківського національного університету внутрішніх справ
Світличний В.А.,
кандидат технічних наук, доцент,
доцент кафедри протидії кіберзлочинності факультету № 4
Харківського національного університету внутрішніх справ

У сучасному світі використання штучного інтелекту (ШІ) набуває все більшого значення у різних галузях діяльності, зокрема у військовій сфері. Використання ШІ може допомогти підвищити ефективність військових дій та забезпечити більш високий рівень безпеки нації. Однак, використання ШІ військовими потребує пильної уваги до етичних та юридичних питань. У цій роботі будуть розглянуті можливості та обмеження використання ШІ для підвищення ефективності військових дій та безпеки нації.

Однією з основних можливостей використання ШІ у військовій сфері є забезпечення ефективності військових дій. ШІ може допомогти військовим командирам приймати рішення на основі аналізу великої кількості даних, що збираються в ході військових операцій. Наприклад, ШІ може аналізувати супротивника, прогнозувати його дії та рекомендувати оптимальні варіанти дій для перемоги в бою.

Ще однією можливістю використання ШІ є автоматизація військових процесів, що дозволяє зменшити час на їх виконання та збільшити точність. Наприклад, ШІ може виконувати завдання з контролю за дронами або використовуватись для пілотування безпілотних літальних апаратів. Це дозволяє зменшити ризики для життя військових пілотів та забезпечити більш точне виконання завдань.

Також ШІ може використовуватись для аналізу інформації, що надходить з датчиків та розвідувальних засобів. Наприклад, ШІ може аналізувати відео– та фотоматеріали, що надходять з безпілотників, та виявляти потенційні загрози для військових об’єктів [1].

Однак, використання ШІ військовими також має свої обмеження та виклики. Одним з найбільших обмежень є етичні та юридичні питання. Використання ШІ може призвести до появи нових видів зброї, які можуть виявитись смертоносними та непередбачуваними. Це може призвести до порушення прав людини та міжнародного гуманітарного права.

Також використання ШІ може призвести до втрати контролю над ситуацією. Наприклад, якщо системи ШІ розгорнути на бойовому полі, то

може виникнути ситуація, коли системи вже не можуть бути контрольовані та відключені, що може призвести до непередбачуваних наслідків.

За використанням ШІ військовими стоїть велика відповідальність, що потребує пильної уваги до етичних та юридичних питань. ШІ може допомогти підвищити ефективність військових дій та забезпечити більш високий рівень безпеки нації, але лише за умови ретельної розробки та впровадження етичних та юридичних стандартів. Крім того, важливо розробляти та вдосконалювати системи контролю та моніторингу, щоб забезпечити можливість своєчасного виявлення та припинення непередбачуваних наслідків використання ШІ [2].

Окрім того, важливо вести активну роботу зі створенням міжнародних стандартів та правил використання ШІ в військовій сфері. Такі стандарти мають бути прийняті на міжнародному рівні та повинні бути юридично зобов'язуючими для всіх країн.

Нарешті, важливо враховувати соціальні та етичні аспекти використання ШІ. Необхідно проводити відкриту дискусію з громадськістю та експертами щодо можливостей та обмежень використання ШІ в військовій сфері. Тільки в такий спосіб можна забезпечити використання ШІ на благо нації та не створювати нових загроз для людства.

Отже, використання ШІ в військовій сфері є однією з перспективних технологій, що може допомогти підвищити ефективність військових дій та забезпечити більш високий рівень безпеки нації. Однак, використання ШІ має свої обмеження та виклики, що потребують уважного вивчення та розробки відповідних етичних та юридичних стандартів. Важливо забезпечити відкриту дискусію з громадськістю та експертами щодо можливостей та обмежень використання ШІ в військовій сфері та враховувати соціальні та етичні аспекти використання цієї технології.

Список використаних джерел:

1. Allies and Artificial Intelligence: Obstacles to Operations and Decision-Making // вебсайт. URL: https://repositories.lib.utexas.edu/bitstream/handle/2152/81858/TNSRVol3Issue2Lin-Greenberg.pdf?sequence=2&isAllowed=y (дата звернення: 01.03.2023)

2. ArtificialIntelligence and National Security// вебсайт. URL: https://www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf (дата звернення: 02.03.2023)

ПРАКТИЧНІ АСПЕКТИ ЗАХИСТУ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ І ДАНИХ

Ісаєв Я.С.,
Скляренко О.А.,
аспіранти,
ПВНЗ «Європейський університет»

Кібербезпека почала активно розвиватися у 1970-х роках, коли комп'ютерні системи стали використовуватися ширше та з'явилися вразливі місця в безпеці. Перші антивірусні програми були розроблені у 1980-х роках [1], а у 1990-х Інтернет приніс нові виклики кібербезпеці. На початку 2000-х років кібератаки стали все більш масовими та шкідливими, що призвело до створення Департаменту внутрішньої безпеки та Національного центру кібербезпеки та інтеграції комунікацій. Сьогодні кібербезпека є головним пріоритетом, постійно розробляються нові технології та стратегії для покращення захисту від кібератак.

Захист програмного забезпечення та даних у програмному забезпеченні вимагає багаторівневого підходу. Нижче наведено кілька практичних порад щодо захисту програмного забезпечення та даних.

- Методи безпечного кодування: розробники повинні дотримуватися методів безпечного кодування, щоб запобігти вразливостям, якими можуть скористатися зловмисники. Це включає належну перевірку введених даних, обробку помилок і керування паролями.
- Регулярні оновлення та виправлення: програмне забезпечення слід регулярно оновлювати за допомогою виправлень безпеки та виправлень для усунення відомих вразливостей.
- Шифрування [2]. Щоб запобігти несанкціонованому доступу, конфіденційні дані мають бути зашифровані, як під час передачі, так і під час зберігання. Необхідно використовувати надійні алгоритми шифрування, такі як AES або RSA.
- Безпека мережі. Щоб захистити програмне забезпечення та дані від зовнішніх загроз, необхідно запровадити такі заходи безпеки мережі, як брандмауери, системи виявлення/запобігання вторгненням і віртуальні приватні мережі (VPN).
- Автентифікація та авторизація: потрібно реалізувати багатофакторну автентифікацію, політику паролів і мінімальний доступ для користувачів. Це допоможе запобігти несанкціонованому доступу та переконатися, що користувачі є тими, за кого себе видають.

- Тестування та оцінка: необхідно проводити регулярне тестування безпеки та оцінку програмного забезпечення та даних, щоб виявити та усунути будь-які вразливості чи недоліки.
- План реагування на інциденти: створення плану реагування на інциденти допоможе швидше реагувати на інциденти безпеки та мінімізувати вплив на програмне забезпечення та дані.

Ці методи є лише деякими з багатьох, які можна використовувати для захисту програмного забезпечення та даних у програмному забезпеченні. Важливо пам’ятати, що безпека – це безперервний процес, який потребує постійного моніторингу та вдосконалення.

Існує кілька сучасних криптографічних і стеганографічних засобів захисту інформації, кожен з яких має свої сильні і слабкі сторони. Наведемо деякі з них.

- Постквантова криптографія [3] – це тип криптографічного алгоритму, розробленого для захисту від атак квантових комп’ютерів. Це досить важливо, оскільки очікується, що квантові комп’ютери зможуть зламати багато поточних криптографічних алгоритмів, які використовуються сьогодні.
- Гомоморфне шифрування – це форма шифрування, яка дозволяє виконувати обчислення із зашифрованими даними без необхідності їх попереднього розшифрування. Може бути корисним у ситуаціях, коли конфіденційні дані потрібно проаналізувати або обробити, але дані неможливо розшифрувати через проблеми конфіденційності.
- Блокчейн [4] – технологія розподіленої книги, яка використовує криптографічні методи для забезпечення безпеки та конфіденційності. Найчастіше ця технологія асоціюється з криптовалютою, але її також можна використовувати для інших додатків, таких як цифрова ідентифікація та керування ланцюгом поставок.
- Стеганографія зі штучним інтелектом. Стеганографія – це практика приховування інформації в інших даних, таких як зображення чи аудіофайли. З появою штучного інтелекту та машинного навчання методи стеганографії стали більш досконалими, що ускладнило виявлення прихованих даних зловмисникам.
- Квантовий розподіл ключів (QKD) – це техніка, яка використовує квантову механіку для безпечного розподілу криптографічних ключів. QKD теоретично незламний, що робить його дуже безпечним засобом зв’язку.

Криптографічні та стеганографічні засоби захисту інформації корисні для забезпечення конфіденційності, цілісності, автентичності та

неспростовності конфіденційної інформації. Вони захищають від таких атак як прослуховування, перехоплення та підробка даних. Ці інструменти є важливим компонентом сучасної інформаційної безпеки та використовуються для безпечного зв'язку, цифрових платежів і зберігання даних.

Список використаних джерел:

1. Core War: Creeper & Reaper, URL: https://web.archive.org/web/20140502001343/http://corewar.co.uk/creeper.htm
2. What Is Cryptography in Cyber Security: Types, Examples & More. URL: https://blog.rsisecurity.com/what-is-cryptography-in-cyber-security/
3. Post-Quantum Cryptography. URL: https://csrc.nist.gov/projects/post-quantum-cryptography
4. Blockchain For Beginners: What Is Blockchain Technology? URL: https://blockgeeks.com/guides/what-is-blockchain-technology/

КРИПТОГРАФІЧНІ ЗАСОБИ ЗАХИСТУ ДОДАТКІВ ДЛЯ МОБІЛЬНИХ ПРИСТРОЇВ ПІД УПРАВЛІННЯМ ОПЕРАЦІЙНОЇ СИСТЕМИ ANDROID

Казаков В.І.,
магістрант факультету інформаційних систем та технологій,
Панченко О.І.
викладач кафедри інформаційних систем,
програмування та кібербезпеки,
ПВНЗ «Європейський університет»

Мобільні пристрої стали досить розповсюдженими у сучасному житті, а операційна система Android є однією з лідерів ринку. Користувачі використовують їх для різноманітних дій, таких, як банківські операції, спілкування та багатьох інших. Програми, зазвичай, збирають значну кількість особистої інформації, такої, як контакти, повідомлення, дані про місцезнаходження та історію веб-перегляду. Використання мобільних пристроїв і надалі продовжує зростати, внаслідок чого безпека додатків стала критичною проблемою. Тому часто розробники використовують криптографічні засоби для захисту особистих даних.[1, 4]

Криптографія – це практика захисту зв'язку та даних від стороннього втручання з використанням кодів та шифрів. Варто зазначити, що це не є панацеєю і все ще існують потенційні вразливості, якими можуть скористатися зловмисники. Через поганий захист вони можуть отримати доступ до зашифрованих даних, тому для користувачів дуже важливо захистити свої пристрої надійними паролями або біометричною аутентифікацією, щоб запобігти несанкціонованому доступу.

У програмах для Android розробники можуть застосовувати систему Android Keystore, яка дозволяє зберігати дані в захищеному контейнері. Її можна використовувати для створення, зберігання та використання криптографічних ключів у додатку, гарантуючи, що вони та інформація залишаться в безпеці і захищені від атак [2].

Ще одним важливим аспектом криптографії в мобільних програмах є використання безпечних протоколів зв'язку, таких, як Transport Layer Security (TLS). TLS забезпечує безпечний канал для передачі даних між додатками та серверами, захищаючи від перехоплення та несанкціонованого доступу. Розробники повинні переконатися, що протокол TLS реалізовано правильно та оновлено до останніх виправлень безпеки.

Також є інші заходи безпеки, які програмісти можуть застосувати для захисту даних користувача в мобільних додатках [3]. Наприклад, можна використовувати безпечне сховище, таке, як зашифровані бази даних для зберігання конфіденційної інформації про користувачів. Разом з тим потрібно використовувати методи безпечного кодування, щоб уникнути вразливостей, таких, як впровадження SQL та атаки переповнення буфера. Крім того, система дозволів Android надає можливість користувачам контролювати доступ додатків до персональної інформації, тому розробникам необхідно належним чином реалізувати її, а користувачам – ретельно перевіряти дозволи, які запитують програми.

Для підвищення безпеки мобільних додатків програмісти повинні дотримуватись передових методів безпечного кодування та регулярно тестувати програми на наявність вразливостей. Існує багато інструментів для перевірки безпеки своїх програм, наприклад, такі як Mobile Security Framework (MobSF) та Android Debug Bridge (ADB).

Безпека додатків має важливе значення, особливо в умовах щоденного використання мобільних пристроїв у повсякденному житті. Криптографія є хорошим інструментом для захисту особистих даних і розробники повинні використовувати її у своїх програмах. Однак, важливо розуміти, що це лише частина комплексних заходів, тому потрібно застосовувати цілісний підхід до безпеки додатків, щоб мінімізувати ризики атак і витоків даних.

Список використаних джерел:

1. Безпека мобільних додатків. Посібник з тестування мобільної безпеки. URL: https://owasp.org/www-project-mobile-security-testing-guide
2. Документація для розробників. Система Android Keystore. URL: https://developer.android.com/training/articles/keystore
3. Документація для розробників. Огляд дозволів. URL: https://developer.android.com/guide/topics/permissions/overview
4. Методи та алгоритми криптографії. URL: https://searchsecurity.techtarget.com/definition/cryptography

МІСІЇ, ЦІЛІ ТА ЗАВДАННЯ ЩОДО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ТА КІБЕРСТІЙКОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ ВІЙНИ

Когут Ю.І.,
к.ю.н., Генеральний директор,
Консалтингова компанія «СІДКОН»

Під час ведення військових дій критична інфраструктура держави стає однією з основних цілей супротивника. Під час повномасштабної війни, яку веде росія проти України, критична інфраструктура України зазнає шкоди як від фізичних руйнувань, так і в кібербпросторі. Для досягнення високого рівня кібербезпеки та кіберстійкості критичної інфраструктури як важливої складової національної безпеки держави, місії, цілі та завдання забезпечення безпеки критичних об'єктів мають бути визначені на національному рівні. Необхідно, щоб керівництво будь-якої держави розуміло та реалізовувало програму розробки політики забезпечення кібербезпеки та кіберстійкості до кіберзагроз критичної інфраструктури – Національну програму захисту критичної інфраструктури.

Для досягнення цих цілей необхідно розробити бачення, місії, цілі та завдання щодо створення та підтримки кібербезпеки та кіберстійкості об'єктів критичної інфраструктури.

1) Стратегічний напрямок зусиль щодо створення та підтримки кібербезпеки та кіберстійкості критичної інфраструктури залежить від загального бачення основних цілей, які мають бути досягнуті: критична інфраструктура захищена та стійка, рівень уразливості щодо об'єктів критичної інфраструктури дуже низький, мінімізовані можливі наслідки ідентифікованих та деструктивних кіберзагроз, ефективно та оперативно відбувається реагування на кіберризики та кіберзагрози щодо критичної інфраструктури та її відновлення за результатами викриття цих ризиків та загроз.

2) Місія/завдання щодо забезпечення кібербезпеки та кіберстійкості критичної інфраструктури.

Зміцнення кібербезпеки та кіберстійкості критичної інфраструктури через управління кіберризиками здійснюється партнерами за критичною інфраструктурою – державою та приватним сектором як власником об'єктів критичної інфраструктури – шляхом спільних і комплексних дій.

Від бачення місії щодо забезпечення кібербезпеки та кіберстійкості критичної інфраструктури залежить досягнення цілей, які є стратегічним напрямком, на якому має бути зосереджена вся критична діяльність для забезпечення кібербезпеки та кіберстійкості об'єктів критичної інфраструктури.

3) Цілі щодо забезпечення безпеки та стійкості критичної інфраструктури:

- оцінити та проаналізувати кіберзагрози, вразливі місця та вплив на критичну інфраструктуру, що, у свою чергу, також необхідно для оцінки діяльності з управління кіберризиками щодо об'єктів критичної інфраструктури;
- захистити критичну інфраструктуру від техногенних, природних і кібернетичних загроз шляхом зменшення ризиків, враховуючи витрати та вигоди від інвестування в забезпечення безпеки об'єктів критичної інфраструктури;
- підвищити критичну стійкість критичної інфраструктури шляхом мінімізації несприятливих наслідків інцидентів за допомогою превентивного планування та заходів пом'якшення.

4) Ключові пріоритетні завдання щодо забезпечення безпеки та стійкості критичної інфраструктури:

- зміцнювати партнерські відносини щодо управління об'єктами критичної інфраструктури;
- вводити інновації в управлінні ризиками критичної інфраструктури;
- зосередитися на результатах управління ризиками щодо об'єктів критичної інфраструктури.

Отже, зниження вразливостей критичної інфраструктури та підвищення її кібербезпеки та кіберстійкості є однією з головних цілей будь-якої держави. Це забезпечить належний рівень їх захисту та, наскільки це можливо, суттєво зменшить негативні наслідки від збоїв на життєдіяльність суспільства та його громадян.

Наприклад, більшість із 35 країн-учасниць Організації економічного співробітництва та розвитку врахували трансформації з ризиками та «ландшафтом» криз, що спостерігалися в останнє десятиліття, та спрямували свої зусилля на реформування системи управління кризами, щоб адаптуватися до свого нового контексту. Однак кризи продовжують розвиватися, кидаючи виклик навіть найбільш інноваційним і надійним системам захисту критичної інфраструктури в розвинених країнах світу. Відбувається процес зміни типів і видів криз, з якими сьогодні стикаються держави в процесі забезпечення безпеки об'єктів критичної інфраструктури в умовах глобалізації та цифровізації економічних і соціальних процесів у світі.

Національні зусилля щодо зміцнення кібербезпеки та кіберстійкості критичної інфраструктури залежать від здатності власників критичної інфраструктури приймати обґрунтовані управлінські рішення з урахуванням ризиків при розподілі обмежених ресурсів як для повсякденних, так і для кризових операцій. Тому управління ризиками, яке має стати наріжним питанням національної програми захисту критичної інфраструктури України, є актуальним як на державному, так і на місцевому рівнях. Безпека та стійкість критичної інфраструктури на цих двох рівнях залежить від створення та підтримки надійних партнерських відносин між бізнес-спільнотою та

державою, місцевою владою та громадськими організаціями. Необхідність координації між цими партнерами у сфері управління ризиками критичної інфраструктури також підкреслює серйозні проблеми державного управління об'єктів критичної інфраструктури.

Список використаних джерел:

1. Crowley, Bo Julie, Greg Honan, Richard Kuzma, David Michelson, Jacqueline Parziale, Kathryn Reed, Ryan Solis, Tom Wester, and William Wright. Defense Playbook for Campaigns. Edited by Casey Corcoran and Allison Lazarus. Paper, Belfer Center for Science and International Affairs, Harvard Kennedy School, March 2020.
2. Cyber defence. URL: https://www.nato.int/cps/en/natohq/topics_78170.htm.
3. Вейтас М. В. Лукашенко М. І. Кібертероризм: тенденції розвитку та механізми протидії. Науковий огляд. 2018. № 4 (47). URL: https://naukajournal.org/index.php/naukajournal/article/viewFile/1545/1625.
4. *Ткачук Н. А.* Актуальні кіберзагрози сучасного безпекового середовища. Міжнародний науковий журнал «Інтернаука». Серія: «Юридичні науки». 2018. № 7. URL: https://www.inter-nauka.com/uploads/public/15381330973208.pdf.
5. Україну атакує новий вірус-здирник XData. URL: https://ua.112.ua/suspilstvo/ukrainu-atakuie-novyi-virus-vymahach-xdata-391325.html.

ГЛОБАЛІЗАЦІЯ КІБЕРЗЛОЧИННОСТІ: СУЧАСНІ ВИКЛИКИ ТА ЗАГРОЗИ ЦИФРОВІЙ ЕКОНОМІЦІ І БІЗНЕСУ

Колодінська Я.О.,
викладач кафедри математичних дисциплін
та інноваційного проектування,
ПВНЗ «Європейський університет»

У сучасному світі кіберзлочинність стала однією з найбільш актуальних проблем в галузі інформаційної безпеки. Її масштаби постійно збільшуються, а глобалізація кіберзлочинності стала суттєвим викликом для правоохоронних органів і організацій по всьому світу.

Кіберзлочинність – це злочини, які вчиняються за допомогою комп'ютерів або мережі Інтернет [1]. За даними Ради національної безпеки і оборони (РНБО), у 2020 році в Україні зафіксували близько 1 мільйон випадків кіберзагроз [2].

Однією з основних причин глобалізації кіберзлочинності є широке використання інтернету та його технологій в усьому світі. Це дає злочинцям можливість здійснювати кібератаки з будь-якої точки світу на будь-яку організацію. Окремі особи можуть стати жертвами кіберзлочинності через віруси, шахрайство, фішинг, хакерські атаки, вимагання викупу за збереження даних та інші злочинні дії віддалених злочинців. Наприклад, кіберзлочинці можуть використовувати соціальні мережі, щоб здобути особисту інформацію

про людей, яку потім можна використовувати для шахрайства або злочинів, пов'язаних з ідентичністю. Організації також є частою мішенню кіберзлочинців, особливо великих компаній і урядових установ. Зловмисники можуть використовувати кібератаки, щоб здобути конфіденційну інформацію, вимагати викуп, знищити дані або пошкодити інфраструктуру компанії. Ці атаки можуть спричинити серйозні фінансові втрати та нанести шкоду репутації компанії.

Крім того, кіберзлочинність може впливати на цілі країни або регіони. Наприклад, вірус WannaCry, який заразив мільйони комп'ютерів у 150 країнах у 2017 році, призвів до зупинки роботи багатьох організацій та підприємств по всьому світу.

Ще один з гучних випадків витоку персональних даних стався у 2016 році, коли компанія Uber повідомила про витік даних своїх користувачів та водіїв. Зловмисники отримали доступ до даних більше ніж 57 мільйонів користувачів та водіїв компанії, включаючи імена, адреси електронної пошти, номери телефонів та номери реєстрації автомобілів. Цей випадок став прикладом того, як важливо захищати персональні дані та нагадуванням про те, що жодна організація не є надійною в питаннях захисту персональних даних своїх користувачів та клієнтів [3].

Боротьба з кіберзлочинністю на глобальному рівні є викликом для правоохоронних органів та урядів по всьому світу. Щоб захистити країни, організації та їхніх клієнтів, необхідно вкладати зусилля в розробку та впровадження захисних технологій та програм. Ось кілька шляхів, якими можна боротись з кіберзлочинністю у глобальному масштабі:

1. Міжнародна співпраця. Країни мають співпрацювати між собою, обмінюватися інформацією та досвідом у боротьбі з кіберзлочинністю. Наприклад, держави можуть створювати спільні комісії для обговорення проблем кіберзлочинності та розробки міжнародних стандартів для боротьби з цим явищем.

2. Розробка міжнародних законів. Міжнародні організації можуть сприяти розробці міжнародних законів та норм, що регулюють поведінку в кіберпросторі. Наприклад, створення міжнародної конвенції про кіберзлочинність та забезпечення кібербезпеки.

3. Підвищення кваліфікації фахівців з кібербезпеки. Компанії та уряди можуть інвестувати у навчання фахівців з кібербезпеки задля їхньої подальшої ефективної боротьби з кіберзлочинністю. Також важливо залучати до боротьби з кіберзлочинністю молодь та створювати умови для її розвитку в цій сфері.

4. Розвиток технологій. Компанії, держави та міжнародні організації мають інвестувати у розвиток технологій, які допоможуть виявляти та запобігати кіберзлочинності. Наприклад, розробка інтелектуальних систем виявлення вторгнень та ризиків в комп'ютерних мережах може допомогти забезпечити більш ефективний захист від кіберзлочинності.

Усі наведені вище шляхи захисту інформації мають бути розглянуті та враховані при розробці стратегій боротьби з кіберзлочинністю у глобальному

масштабі. Щоб забезпечити кібербезпеку на глобальному рівні, необхідно вживати комплексні заходи, які будуть враховувати технічні, соціальні та культурні аспекти кібербезпеки. Тільки шляхом спільної роботи держав, організацій та громадськості можна забезпечити ефективний захист від кіберзлочинності та зберегти цифрову безпеку у глобальному масштабі.

Список використаних джерел:

1. Електронний ресурс: https://uk.wikipedia.org/wiki/Інформаційні_злочини
2. Електронний ресурс: https://ms.detector.media/kiberbezpeka/post/25227/2020-08-07-v-ukraini-v-2020-rotsi-zafiksuvaly-1-milyon-kiberatak-rnbo/
3. Kate Conger, Kevin Roose. Uber Investigating Breach of Its Computer Systems – The New York Times – Sept. 16, 2022, Section B, Page 3. URL: https://www.nytimes.com/2022/09/15/technology/uber-hacking-breach.html

РЕАЛІЗАЦІЯ ФУНКЦІОНАЛУ КІБЕРЗАХИСТУ ЗА ДОПОМОГОЮ PYTHON

Комиса Ю.О.,
старший викладач
Фахового коледжу бізнесу та аналітики,
Національна академія статистики,
обліку та аудиту, м. Київ

Сканери портів є корисними інструментами для мережевих адміністраторів і спеціалістів із безпеки (1), оскільки вони дозволяють їм ідентифікувати відкриті порти на комп’ютері чи мережевому пристрої та визначати служби, які працюють на цих портах. Їх можна використовувати для перевірки безпеки мережі, а також для пошуку вразливостей, якими можуть скористатися хакери.

Налаштування середовища розробки включає в себе наступні етапи:

1. Встановлення Python на персональний комп’ютер:

2. Підключення бібліотеки socket (2, 3): ця бібліотека забезпечує доступ до інтерфейсу сокета. Вона використовується для створення та керування сокетами в сканері портів.

3. Підключення бібліотеки argparse (2, 3): ця бібліотека використовується для аналізу аргументів командного рядка. Це дозволяє вказати спеціальні діапазони сканування та інші параметри під час запуску сканера портів із командного рядка.

4. Підключення бібліотеки time (2, 3): ця бібліотека надає функції для роботи з часом і датами. Вона використовується для того, щоб додати затримку між скануваннями, щоб уникнути перевантаження цільового пристрою.

Наступним етапом після налаштування середовища розробки є реалізація основних функцій сканера портів.

По-перше, була визначена функція під назвою scan_port, яка приймає хост і порт як аргументи. Ця функція відповідає за спробу підключення до вказаного порту на цільовому хості та повернення статусу порту (відкритий чи закритий). Усередині функції був створений об'єкт socket за допомогою функції socket.socket та встановлені відповідні параметри сокета за допомогою setsockopt. Далі відбувалася спроба підключитися до порту методом connect. Якщо підключення вдалось, функція повертає повідомлення про те, що порт відкрито. Якщо це не вдається, він повертає повідомлення про те, що порт закрито. Потім функція перевіряється на кількох різних хостах і портах, щоб перевірити, чи вона працює правильно.

Функція scan_port було реалізовано в декількох варіаціях:

1. Перевірка вхідних даних: додана можливість перевірки введених користувачем даних. Наприклад, є можливість переконатися, що хост є дійсною IP-адресою або доменним іменем, а порт є дійсним цілим числом у дозволеному діапазоні (1–65535).

2. Форматування виводу: додані параметри для налаштування виводу сканера. Реалізована можливість дозволити користувачеві вказати формат виводу (наприклад, CSV, JSON або спеціальний формат) або включити додаткові деталі у вивід (наприклад, назву служби та версію для відкритих портів).

3. Настроюваний діапазон сканування: додана можливість дозволити користувачеві вказати настроюваний діапазон портів для сканування замість сканування всіх 65535 портів. Це можливо зробити за допомогою бібліотеки argparse для аналізу аргументів командного рядка.

4. Паралельне сканування: оптимізація роботи сканера портів. Запуск сканування паралельно можливий за допомогою бібліотек threading або multiprocessing. Це дозволяє сканувати декілька портів одночасно, зменшуючи загальний час, необхідний для завершення сканування.

У роботі на декількох рівнях розглянуто реалізацію сканера портів з використанням мови програмування Python. Робота надає чітке розуміння того, як працюють сканери портів, а також може бути використана в якості посібника для створення власного спеціального інструмента відповідно до потреб конкретного користувача.

Список використаних джерел:

1. Що таке сканування портів? https://spy-soft.net/skanirovanie-portov/
2. Mark Summerfield. Programming in Python3: A Complete Introduction to the Python Language, 2nd Edition, Addison-Wesley Professional, 2009, – 609 с.
3. Matthew Wilkes. Advanced Python Development, APress Media, 2020, – 503 с.

ІНФОРМАЦІЙНА БЕЗПЕКА – ЕЛЕМЕНТ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Корляков Б.О.,
курсант ІІ курсу
Харківського національного університету внутрішніх справ
Світличний В.А.,
кандидат технічних наук, доцент,
доцент кафедри протидії кіберзлочинності факультету № 4
Харківського національного університету внутрішніх справ

Інформаційна безпека є складним процесом, який включає в себе багато елементів. Основні з них – це технічний захист, криптографія, кібербезпека, захист від шпигунства, правове регулювання та підготовка кадрів. Кожен з цих елементів має велике значення у забезпечення інформаційної безпеки в сучасному світі. Розглянемо кожен з них докладніше [1]:

1. Технічний захист – це комплекс заходів, спрямованих на захист інформаційних ресурсів від несанкціонованого доступу, втручання та знищення. Технічний захист включає у себе застосування антивірусного програмного забезпечення, файрволів, систем виявлення вторгнень та інших заходів.
2. Криптографія – це наука про забезпечення конфіденційності та цілісності інформації шляхом застосування шифрування та дешифрування. Криптографічні методи застосовуються для захисту конфіденційної інформації від несанкціонованого доступу.
3. Кібербезпека – це комплекс заходів, спрямованих на захист інформаційних систем та мереж від кібератак та кіберзлочинів. До заходів кібербезпеки належать контроль доступу, моніторинг мережі, захист від вірусів та шкідливих програм, резервне копіювання даних та інші.
4. Захист від шпигунства – це комплекс заходів, спрямованих на захист інформації від збору та розголошення інформації нелегітимними особами. До таких заходів належать контроль за працівниками, захист документів та інформації від крадіжки, захист від внутрішньої шпигунської діяльності.
5. Правове регулювання – це система нормативних актів та законодавства, які регулюють використання інформації та забезпечують її захист від несанкціонованого доступу та використання. Правове регулювання перед усім пов’язане з визначенням прав та обов’язків у сфері інформаційної безпеки, а також з встановленням механізмів їх захисту.

У сфері інформаційної безпеки важливо, щоб правове регулювання було чітким та прозорим, щоб кожен користувач мав змогу знати свої права та

обов’язки [2]. Для цього в Україні прийнято низку нормативних актів, що регулюють цю сферу, зокрема:

- Закон України "Про захист персональних даних", який встановлює правила збору, зберігання та використання персональних даних громадян;
- Закон України "Про кібербезпеку", який встановлює правила захисту інформації від кібератак та злочинних дій в мережі Інтернет;
- Закон України "Про інформацію", який встановлює правила розповсюдження, зберігання та захисту інформації;
- Закон України "Про державну таємницю", який встановлює правила зберігання та захисту державної таємниці.

Крім цього, в Україні діє ряд підзаконних актів, які деталізують та уточнюють положення законів та встановлюють механізми їх реалізації [3]. Також існують міжнародні документи, які регулюють сферу інформаційної безпеки, зокрема Конвенція про кіберзлочинність та Рекомендації Ради Європи щодо захисту персональних даних.

Також існують також національні стандарти та рекомендації щодо інформаційної безпеки, які розробляються та впроваджуються в Україні. Наприклад, Національний стандарт з інформаційної безпеки (НДСЗІБ), який містить вимоги до захисту інформації на різних рівнях її конфіденційності. Також в Україні діють різноманітні програми та проекти, спрямовані на підвищення рівня інформаційної безпеки в різних сферах життя. Наприклад, програма "Е-Україна", яка передбачає впровадження електронних послуг та створення безпечної інформаційної інфраструктури.

Висновки. Для ефективного забезпечення інформаційної безпеки в Україні необхідно забезпечити правове регулювання, вдосконалити технічний захист, криптографію та кібербезпеку, захистити від шпигунства, а також забезпечити високий рівень підготовки кадрів у цій сфері. Для цього необхідно вдосконалювати законодавчу базу та проводити широкомасштабну інформаційно-освітню роботу серед населення та органів влади.

Список використаних джерел:

1. Концепція національної безпеки України. Затверджена Указом Президента України від 26.05.2015 № 287/2015 // URL:hhttps://www.president.gov.ua/documents/2872015-19238 (дата звернення: 04.03.2023).
2. Закон України "Про основні засади забезпечення кібербезпеки України" від 5.07.2018 р. № 246-IX. // вебсайт. URL: https://zakon.rada.gov.ua/laws/show/246-19 (дата звернення: 04.03.2023).
3. Безпека інформаційних технологій: Монографія / Коваленко В.І., Свєтлов О.А., Євтушенко І.О. та ін.; за заг. ред. Коваленка В.І. – К.: НДУ, 2013. – 360 с.

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ДЛЯ ГЕНЕРУВАННЯ МАТРИЦЬ ШИФРУВАННЯ

Коцун В.І.[1]
Засадна Х.О.[2]
[1]к. т. н., доц., завідувач кафедри математики та комп'ютерних дисциплін,
[2]к. ф.-м. н., доцент кафедри математики та комп'ютерних дисциплін,
Львівська філія ПВНЗ «Європейський університет»

Сфера застосування криптографії за останній період значно розширилася і означає не лише забезпечення таємної передачі повідомлень між двома отримувачами, але і методи перевірки цілісності повідомлень, визначення відправника/одержувача (автентифікація), цифрові підписи, інтерактивні підтвердження доступу та безпечні технології комунікації, тощо. Тобто можна стверджувати, що криптографія необхідна для тієї інформації, котра потребує захисту. Зазвичай така інформація має містити таємницю, чи має бути захищеною від зловмисника, секретною, конфіденційною [1, 2]. Тому, в більшості випадків, такі напрями як генерування даних та освоєння класичних методів захисту інформації є першими кроками у вивченні криптографії, на що і звертається увага в цій роботі.

На сьогодні існує велика кількість криптографічних алгоритмів, варіативність яких базується як на певних наборах загальних характеристик, так і на певних принципах і механізмах їх роботи. Надійність цих алгоритмів також не є однаково визначеною: існують такі алгоритми, які здатні пройти усі умови захисту та такі, що не гарантують та не можуть забезпечити жодного захисту в реальних умовах. Поясненням такого факту є питання складності проектування дійсно надійного криптографічного алгоритму. Крім того, очевидно, показник надійності є залежним від часу та доволі відносним – велика кількість алгоритмів, які розроблялися раніше та які підтвердили свою надійність, є зараз або ненадійними, або забезпечують невідповідний до реалій рівень надійності. Саме з цих причин важливим є врахування тенденцій розвитку інформаційних технологій, факторів ринку, актуальних стандартів, а також інші фактори, що потенційно можуть знизити стійкість та надійність криптографічного алгоритму в майбутньому.

В даній роботі розглянуто метод використання дискретних методів для генерування матриць шифрування. На основі аналізу існуючих методів генерування даних та послідовностей побудовано формалізований алгоритм для генерування послідовностей та наборів даних.

Запропоновано набір дискретних методів, які можуть вдосконалити, оптимізувати та раціоналізувати проаналізовані методи генерування числових послідовностей. Здійснено аналіз існуючих криптографічних систем, які використовують вищезгадані набори даних для шифрування та дешифрування блоків інформації.

За результатами проведеного аналізу планується розроблення веб-застосування, яке дасть можливість генерувати матриці шифрування з використання дискретних методі та з врахуванням користувацьких потреб. Отримані результати дають підставу для подальших досліджень із використання методів генерування, опрацювання та перетворення даних і їх використання в криптографічних системах.

Список використаних джерел:

1. Ковальчук А. Підвищення стійкості системи RSA при шифруванні зображень // Технічні вісті. – 2009. – № 1-2. – С. 70-71.
2. Красиленко В.Г. Матричні Афінні шифри для створення цифрових підписів на текстографічні документи / В.Г. Красиленко, С.К. Грабовляк // Системи оброблення інформації: зб. наук. пр. – Х.: ХУПС, 2011. – Вип. 7 (97). – С. 60-63.

ВИКОРИСТАННЯ СПЕЦІАЛЬНИХ ЗНАНЬ ТА МЕТОДІВ ПРИ РОЗСЛІДУВАННІ КІБЕРЗЛОЧИНІВ

Левченко С.В.,
старший викладач кафедри інформаційних систем,
програмування та кібербезпеки
Ткачук Е.Р.,
студентка Фахового бізнес-коледжу,
ПВНЗ «Європейський університет»

В останні роки галузь кібербезпеки, в умовах гібридної війни, фіксувала значну кількість хакерських атак, дані атаки безпосередньо загрожували національній безпеці держави. У даних умовах, кожен такий злодій ,який здійснює атаку, стає бойовою одиницею і його інструментом є злами й кібератаки. Війна в інформаційному просторі може завдавати не меншої шкоди, ніж війна на полі бою. Розуміючи цей факт, потрібно оптимізувати кримінальне та кримінально-процесуальне законодавство, при цьому удосконалити методи та способи притягнення до кримінальної відповідальності осіб, які здійснюють правопорушення.

Інформаційна безпека в Україні регулюється нормативними документами, зокрема указом Президента України від 25 лютого 2017 року, а також Указом Президента України від 26 серпня 2021 року № 447/2021 в яких введено в дію Рішення Ради національної безпеки й оборони України від 14 травня 2021 року Про Стратегію кібербезпеки України.

У цей час, не дивлячись на те, що існують нормативні документи, правила й інші вимоги, як показує практика, основна маса держслужбовців не володіють спеціальними знаннями, які потрібні для розслідування кіберзлочинів. Під кіберзлочином ми розуміємо протизаконні дії, які вчиняються з використанням комп’ютерної техніки та мережі Інтернет. До них

відносяться шахрайство в Інтернеті, крадіжка особистих даних, вірусні атаки, DDoS-атаки на сервери, розсилання спаму, крадіжка інтелектуальної власності, кібершантаж, піратство програмного забезпечення, інтернет-булінг, поширення дитячої порнографії та інші. Додаючи до вищенаведеного, зазначимо, що більшість держслужбовців – особи, яким понад 40-50 років і, в нинішніх умовах, спираючись на свої знання, вони не можуть в повному обсязі оцінити та розібрати більшість нюансів при розслідуванні даного виду злочинності.

За даними Національної поліції України, кількість кіберзлочинів у 2020 році зросла на 28% порівняно з попереднім роком. Водночас за даними дослідження, проведеного компанією "KPMG в Україні", понад 70% компаній в Україні зазнали кібератак за останній рік, а в середньому втрати від кіберзлочинів становлять 2,2 мільйона доларів.

У своїй боротьбі з кіберзлочинністю, поліція України залучає спеціалістів з кібербезпеки та комп’ютерної техніки для допомоги у розслідуванні кіберзлочинів. Крім того, в Україні існує декілька навчальних закладів, які пропонують спеціалізовані програми з кібербезпеки та інформаційної безпеки, що допомагають підготувати фахівців для роботи в цій галузі. Поліція в Україні веде боротьбу з кіберзлочинами за допомогою різних методів, серед яких можна виділити наступні.

1. Створення підрозділів із залученням спеціалістів у галузі кібербезпеки: у поліції України створено спеціалізовані підрозділи, такі як Департамент кіберполіції, Спеціальна служба з інформаційної безпеки та кіберзахисту тощо, які займаються виявленням та розслідуванням кіберзлочинів.

2. Моніторинг безпеки: поліція використовує спеціалізовані програмні засоби для моніторингу мереж та виявлення підозрілої активності.

3. Співпраця з іншими країнами та міжнародними організаціями: поліція співпрацює з міжнародними організаціями, такими як Інтерпол, Європол та інші, а також з правоохоронними органами інших країн, для виявлення та розслідування кіберзлочинів.

4. Розробка законодавства: в Україні розроблено законодавство, що регулює кіберзахист та кібербезпеку. Також створено національний центр кібербезпеки, який забезпечує координацію дій у галузі кібербезпеки.

5. Навчання та підвищення кваліфікації: поліція проводить навчання та тренінги для своїх співробітників з питань кібербезпеки та кіберзахисту.

Беручи до уваги всі фактори, можемо констатувати: залучення спеціаліста є важливою складовою розслідування кіберзлочинів, оскільки такі злочини часто потребують глибоких знань у сфері комп’ютерної технології та інформаційної безпеки.

Спеціаліст, який займається розслідуванням кіберзлочинів, повинен мати розуміння технічних аспектів кібербезпеки, а також знати особливості різних видів кіберзлочинів, щоб здійснювати розслідування та встановлювати винних осіб.

Спеціаліст може виконувати різні завдання в процесі розслідування кіберзлочинів, такі як:

- Відновлення втраченої інформації
- Аналіз даних з комп'ютерів та інших пристроїв
- Проведення кіберекспертизи
- Виявлення слабких місць в системі безпеки
- Встановлення способу вчинення кіберзлочину

Залучення спеціаліста є важливою складовою розслідування кіберзлочинів, оскільки це може допомогти підвищити ефективність розслідування та допомогти забезпечити належну кібербезпеку в майбутньому.

Список використаних джерел:

1. Виступ експертів-учасників круглого столу «Український досвід: кібер та інформаційна безпека» [Електронний ресурс]: https://www.radiosvoboda.org/a/29656549.html
2. Указ президента України №47/2017 Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»
3. Указ президента України №447/2021 Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України"
4. Кібербезпека в Україні: стан, проблеми, перспективи / за ред. В.М. Бугая, О.М. Яцишина. – К.: Ін-т держави і права ім. В.М. Корецького НАН України, 2019. – 400 с.
5. Кібербезпека: сучасні виклики та загрози / за ред. А.В. Семенюки, Є.В. Калашнікової, В.І. Вергелеса. – К.: НАДУ, 2017. – 260 с.
6. Кібербезпека в Україні: стан та перспективи розвитку / І.В. Страшко, О.А. Кузик. – К.: Ін-т держави і права ім. В.М. Корецького НАН України, 2018. – 280 с.

РЕЗУЛЬТАТИ ДОСЛІДЖЕНЬ ДЖЕРЕЛ УСНОЇ ІСТОРІЇ ЩОДО ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИХ ОПЕРАЦІЙ РФ ПРОТИ УКРАЇНСЬКИХ ВІЙСЬКОВОСЛУЖБОВЦІВ

Легкодух В.В.,
ад'юнкт штатний науково-організаційного відділу
Національна академія сухопутних військ
імені гетьмана Петра Сагайдачного

Важливим елементом гібридної війни російської федерації проти України в період 2014–2021 рр. є інформаційно-психологічні операції, у тому числі – здійснювані через засоби мобільного зв'язку. Починаючи з 2014 р. війська інформаційних операцій у складі збройних сил (ЗС) рф неодноразово використовували мобільні телефони та мобільний зв'язок як засіб здійснення тиску на українських військовослужбовців. Однією з основних та найбільш доступних для ворога форм інформаційно-психологічного впливу на

військовослужбовців ЗСУ через засоби мобільного зв'язку є розсилка повідомлень деморалізуючого характеру.

Метою дослідження є визначення форм та методів впливу російської пропаганди на військовослужбовців ЗСУ в період АТО (ООС).

Дослідження здійснене на основі результатів опитування особового складу Національної академії сухопутних військ імені гетьмана Петра Сагайдачного у грудні 2022 року та охопило військовослужбовців, які брали безпосередню участь у АТО (ООС). Всього в опитуванні взяло участь 162 особи, з них 41 людина (25,3% від загальної кількості) вказали, що вони отримували СМС-повідомлення пропагандистського характеру від російської сторони. З них 17 осіб (28%) вказали, що отримували СМС погрозливого характеру, ще 15 осіб (25%) відповіли, що отримували СМС зі спробами залякування. 18% військовослужбовців серед опитаних отримували повідомлення із закликали скласти зброю та здатися, 16% військових отримували СМС, у яких дискредитувалися ЗСУ. У 10% випадків з виявлених у ході дослідження СМС-повідомлення від ворога містили пропозиції переходу на сторону ЗС рф, а також по 2% припадає на пропозиції співпраці та спроби приниження військових ЗСУ. Відповідно, частіше військовослужбовці ЗСУ протягом виконання завдань у зоні АТО (ООС) отримували СМС-повідомлення пропагандистського характеру зі спробами погроз та залякування зі сторони ворога.

При цьому, важливим є також співвідношення мобільних операторів, на які приходили такі СМС-повідомлення. Слід зауважити, що за даними аналітичного центру «BRDO»97% абонентів в Україна обслуговуються найбільшими українськими операторами мобільного зв'язку «Київстар», «Vodafone Україна» та «Lifecell», при цьому 48% абонентів користуються послугами оператора «Київстар», 36% – «Vodafone Україна» та лише 14% – послугами «Lifecell» (Investory News, 2020). Це частково пояснює й той факт, що серед опитаних найбільший відсоток (39%) вказали, що отримували пропагандистські СМС від ЗС рф на номери мобільного оператора «Київстар». На «Vodafone Україна» припадає 31,7% опитаних, тоді як «Lifecell» становить 17,1%. Ще 12,2% від загальної кількості опитаних припадає на мобільного оператора «МТС Україна».

Окрім СМС-повідомлень військовослужбовці, які брали участь в опитуванні, також вказали, що отримували повідомлення пропагандистського характеру у месенджерах, тобто через мережу Інтернет. Зокрема, з усіх опитаних такі повідомлення отримували 9 осіб (5,6%), при цьому частіше ці повідомлення надходили на такі месенджери як «Viber» та «Telegram», рідше – «Whats App» та «Facebook Messenger». Також 9 осіб (5,6%) вказали у опитуванні, що отримували коментарі пропагандистського характеру в соціальних мережах – зокрема, у «Facebook», «Instagram», «ВКонтакті» та на платформі «YouTube».

Іншим способом здійснення інформаційно-психологічного впливу на українських військовослужбовців зі сторони рф та її пропагандистської

машини є внесення персональних даних військовослужбовців до таких сайтів, як «Трибунал ДНР» або «Антиукроп». Ці ресурси збирають дані під виглядом організації «трибуналу» та містять російську пропаганду про «нацистську Україну», «хунту», дискредитацію українських патріотичних організацій та вихваляння російських загарбників. При додаванні даних людини до бази додається цинічне позначення «живий/ліквідований». На сайті викладені фотографії, дати народження, телефони, міста та адреси проживання, паспортні дані поліцейських, військових ЗСУ та добровольчих батальйонів, державних службовців, СБУ тощо (Брадов, 2021, с. 98). Внесення персональних даних військовослужбовців до таких пропагандистських баз даних також є способом тиску, залякування військових, реалізуючи інформаційно-психологічний вплив на них. У ході опитування 12 осіб (7,4%) відповіли, що знаходили свої дані на сайті «Трибунал ДНР».

В цілому ж, описані способи здійснення інформаційно-психологічного впливу на військовослужбовців ЗСУ спрямовані на дестабілізацію морально-психологічного клімату серед захисників України, покликані посіяти сумніви, знизити бойовий дух військових. При цьому, реальної загрози такі інформаційно-психологічні атаки не несуть, залишаючись лише спробою маніпуляцій та залякування на психологічному рівні. Відтак, важливим є навчання військовослужбовців ЗСУ правильному реагуванню на подібні спроби деморалізації зі сторони ворога, формування у військових навичок інформаційної гігієни.

У ході опитування визначено, що більшість осіб, які отримували провокативні СМС-повідомлення, коментарі або знаходили свої дані на пропагандистських ресурсах ворога (всього 42 особи) доповідали про це командирові (47,6% випадків) або просто ігнорували такі повідомлення та не відповідали на них (50%). Лише у 2,4% отримувач провокативного повідомлення від ЗС рф відповідав на нього. При цьому військовослужбовці, які приймали участь в опитуванні, вказали як варіанти впливу отриманих провокативних та погрозливих повідомлень від ворога наступні: «позбувались операторів мобільного зв’язку», «ніякого впливу», «викликали сміх від того, як неграмотно написані повідомлення» або «не звертали уваги».

Відтак, дослідження показало, що протягом АТО (ООС) ЗС рф здійснювали інформаційно-психологічні операції проти військовослужбовців ЗСУ, послуговуючись засобами мобільного зв’язку та ресурсами мережі Інтернет. Частіше застосовувалися саме СМС-повідомлення, як спосіб інформаційно-психологічного впливу на українських військовослужбовців, при цьому такі повідомлення приходили на мобільні оператори «Київстар», «Vodafone Україна», «Lifecell» та «МТС Україна». У мережі Інтернет засобами психологічних атак на військовослужбовців ЗСУ стають популярні месенджери (переважно – «Viber» та «Telegram»), соціальні мережі (зокрема, «Facebook», «Instagram», «ВКонтакті»), а також пропагандистські веб-сайти зі збору персональних даних захисників України (наприклад, пропагандистський ресурс «Трибунал ДНР»).

Список використаних джерел:

1. *Брадов, В. В.* (2021). Формування мережевого інструментарію інформаційної війни (на прикладі агресії росії проти України). Держава та регіони. Серія: Соціальні комунікації. № 2. С. 96–103.
2. Investory News, (2020). Дослідження: Український ринок мобільного зв'язку за 10 років збільшився майже вдвічі. URL: https://investory.news/doslidzhennya-ukrainskij-rinok-mobilnogo-zvyazku-za-10-rokiv-zbilshivsya-majzhe-vdvichi/

СИСТЕМА БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ ТА АУТЕНТИФІКАЦІЇ

Лєвіна С.О.,
студентка 3-го курсу
Україно-американського університету Конкордія

В останнє десятиліття ми спостерігаємо значне зростання і розвиток цифрових технологій. Нам стали доступні тисячі сервісів і відкрилася безмежна кількість можливостей, які ми можемо випробувати не тільки не виходячи з дому, а й не встаючи з ліжка.

Будь-який розвиток супроводжується "побічними ефектами", які, на жаль, можна виправити тільки через певну кількість часу і не завжди з першої спроби. Так сталося і у випадку зі збереженням безпеки та даних користувачів в інтернеті. На жаль, не всі люди здобули достатню кількість знань про те, як захистити себе в мережі. Звісно, здебільшого у всіх присутні базові знання про захист у цифровому просторі, але зловмисники так само не сплять і вигадують дедалі більше і більше нових способів дістати інформацію. Одним із способів захисту інформації, а також полегшення використання технологій і розширення можливостей, стали біометрична ідентифікація та аутентифікація користувачів.

Аутентифікація та ідентифікація тісно пов'язані між собою поняття коли ми говоримо про кібербезпеку. Біометрична аутентифікація – це концепція забезпечення безпеки даних. Простими словами – це захід безпеки, за якого для надання доступу використовують фізичні характеристики людини, наприклад відбиток пальця або обличчя. Аутентифікація – це процедура перевірки автентичності заявленого користувача, процесу або пристрою. Щоб підбити підсумки вищесказаного і розкласти все "по поличках", спочатку відбувається процес ідентифікації (розпізнавання користувача за його ідентифікатором), а потім аутентифікація (процедура перевірки автентичності, доказ, що користувач саме той, за кого себе видає). Ідентифікатором користувача може слугувати відбиток пальця, обличчя, райдужна оболонка очей, ДНК і безліч інших індивідуальних даних людини.

Так, наприклад, офіційний державний вебпортал України "Дія", розроблений Міністерством цифрової трансформації України, використовує ці

методи для роботи. Державний застосунок "Дія" дає змогу всім українцям тримати свої документи у смартфоні. Серед документів, якими ви можете скористатися через "Дію" – паспорт формату ID-картка, закордонний паспорт, водійське посвідчення, студентський квиток, технічний паспорт на авто, пенсійне посвідчення тощо. Що ж означає використання цих методів у такій серйозній системі з усіма даними громадян на державному рівні? Звісно ж прогрес у захисті даних та одночасним полегшенням життів людей.

Процедура біометричної автентифікації проводиться в три етапи: спочатку електронно-аналітичний пристрій зчитує пред'явлену біометричну інформацію, потім обробляє отриманий сигнал, після чого проводить порівняння зі зразком із бази даних. Якщо показники збігаються, то електронно-аналітичний пристрій визнає пред'явника власником із правом доступу до об'єкта або користування ресурсом. Нажаль, хоча ця технологія може замінити необхідність створення довгих і складних паролів, під час її використання також виникає небезпека викрадення особистих даних.

Як підсумок, можна сказати, що однозначно у перерахованих вище методів є безліч переваг і недоліків і важлива усвідомленість користувача для забезпечення належного рівня безпеки кіберданих.

ДЕЯКІ ПИТАННЯ МЕРЕЖЕВОЇ БЕЗПЕКИ

Льогких Н.Д.,
курсант,
Григоренко К.В.,
старший викладач,
Черкаський інститут пожежної безпеки
імені Героїв Чорнобиля НУЦЗ України

Безпека мережі – це системна політика комп'ютерних мереж, яка забезпечує безпеку активів своєї організації, програмних та апаратних ресурсів. Термін мережева безпека також наголошує на моніторингу та контролі несанкціонованого доступу, неправильного використання та будь-яких небажаних змін у мережевій системі.

Найпоширеніший процес автентифікації, що практикується повсюдно, – це присвоєння користувачеві ексклюзивного ідентифікатора та пароля для автентифікації та доступу до ресурсів мережі.

Термін «безпека» включає як приватні мережі, так і мережі загального користування, такі як RTGS або NEFT, через Інтернет-банкінг.

Управління безпекою в будь-якій мережі, будь то загальнодоступна чи приватна, – це набір політик та рутинних процедур, реалізованих мережевою системою, щоб захистити свою мережу від несанкціонованого доступу, відмови в роботі комп'ютера, перебоїв у роботі тощо, відомий як управління мережевою безпекою. Також наголошується на цілодобовому моніторингу

мережі для запобігання атакам вірусів та будь-якого неправильного використання або модифікації в базі даних.

Найкращі способи управління безпекою – це використання передового антивірусного та антивірусного програмного забезпечення та постійне оновлення системи через регулярні проміжки часу.

Використання Інтернету різко зросло, оскільки іде постійний рух до повної цифровізації. Через збільшення використання Інтернету хакери та зловмисники також активізуються, і наша мережева система піддається більшій кількості вірусних атак.

В основному, необхідність мережевої безпеки полягає у виконанні, головним чином, двох завдань, перше – це захист інформації від будь-якого несанкціонованого доступу, а друге – забезпечення захисту даних, що зберігаються на ПК або ноутбуках, не тільки для окремої мережі, але і в спільній або загальнодоступній мережі.

Потреба в інформаційній безпеці базується на таких моментах:

- для захисту інформації від небажаного доступу;
- для захисту даних від будь-якої невідповідної затримки маршруту;
- для захисту даних від будь-яких небажаних поправок;
- для заборони певному користувачеві мережі надсилати будь-які листи;
- для захисту ПК від програмного забезпечення, яке в разі встановлення може зашкодити нашій системі, як це роблять хакери;
- для захисту системи від троянських коней, хробаків тощо, які можуть повністю знищити нашу систему.

Ми можемо захистити нашу мережеву систему різними способами, залежно від типу мережевої атаки.

Таким чином, існує безліч рішень:

1) антивірусне та антивірусне програмне забезпечення;
2) запобігання втраті даних (DLP);
3) безпека електронної пошти;
4) брандмауери;
5) мобільна безпека;
6) сегментація мережі;
7) веб-безпека;
8) безпека кінцевої точки;
9) контроль доступу;
10) віртуальна приватна мережа (VPN).

Основними параметрами для забезпечення безпеки в системі є:

1) налаштування надійних паролів;
2) встановлення брандмауера;
3) антивірусний захист;
4) оновлення;
5) захисні ноутбуки та мобільні телефони;

6) своєчасне резервне копіювання;
7) розумний серфінг на веб-сайтах;
8) безпечна конфігурація;
9) керування знімними носіями.

Таким чином, ми намагались дослідити необхідність мережевої безпеки, типи безпеки, ключові моменти для управління нею та як зробити мережеву систему імунітетом до всіх видів вірусних та троянських атак.

Список використаних джерел:

1. Ковальчук В. Н. Система інформаційної безпеки навчального комплексу: Методичний посібник. – Житомир: Вид-во ЖДУ ім. І. Франка, 2009. – 84 с.
2. Основи комп'ютерних мереж та Інтернету. – К. Видавнича група BHV, 2006. – 256 с.
3. Шпонтак І. М. Проблема, яку не варто недооцінювати / Шпонтак І. М., Павко І. Й. // Всеукраїнський науково-популярний журнал «Безпека життєдіяльності». – 2009. – №10. – с. 25-27.

ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ В УМОВАХ ВІЙНИ

Мазуренко Л.І.,
кандидат політичних наук,
доцент кафедри соціально-гуманітарних та
фундаментальних дисциплін
Інституту Військово-Морських Сил
Національного університету «Одеська морська академія»

Сучасне XXI століття в науковій літературі називають інформаційним. Інформація стає рушійною продуктивною силою суспільства. В умовах глобалізації та інтеграції країн, створення належних умов подолання кризових явищ у їхньому політичному та соціально-економічному розвитку є забезпечення інформаційної безпеки. О.С. Бодрук зазначає, що існує три основні підходи до визначення сутності поняття «інформаційна безпека»**:** складова національної безпеки; стан захищеності інформаційного середовища та національних інтересів від можливих загроз; стан системи, який здатний забезпечити цільові параметри безпеки [1].

Науковець В.С. Цимбалюк вважає, що інформаційна безпека України – це стан захищеності її національних інтересів у інформаційній сфері [3, с. 24]. На думку Л.О. Кочубея, інформаційна безпека характеризує стан захищеності життєво важливих інтересів, інформаційну озброєність держави, суспільства, особистості [2, с. 222].

Таким чином, на нашу думку, під інформаційною безпекою слід розуміти стан захищеності держави від дезінформації.

Можна стверджувати, що інформаційна безпека сьогодні виходить на перший план. Повномасштабне вторгнення Російської Федерації на територію України, знищення міст, сіл, мирних жителів, ми бачимо, як російські ЗМІ

висвітлюють викривлену інформацію про нібито «військову операцію», виправдовуючи свої дії та вказують на постійну небезпеку, яка йде від України.

А тому, можливою є загроза блокування правдивої інформації, негативного сприйняття населенням ролі Збройних Сил України, дій керівництва та владних структур, що в підсумку негативно може вплинути на здобуття перемоги в цій війні.

Інформаційна безпека є дуже важливою під час військових дій, адже неправильно подана чи помилкова інформація може змусити населення панікувати, вплинути на хід подій, прискорити внутрішню міграцію населення, погіршенню іміджу вищого військово-політичного керівництва, розпалювати недовіру до політиків, їх заяв і звернень, що може негативно впливати на ведення бойових дій, викликати психічні та фізичні захворювання, крім того, може завдати непоправної шкоди для всього результату військового конфлікту.

Отже, боротьба з поширенням подібної шкідливої інформації під час війни має істотне значення для перебігу воєнного конфлікту.

Головними шляхами розповсюдженню недостовірної інформації в умовах війни є: соціальні мережі; підроблені акаунти відомих людей, політиків, телерадіомовні канали; через особисті повідомлення або у спільних групах Viber, Telegram, WhatsApp та інших месенджерах.

Під час війни, коли на країну напали і вона потрапляє під численні інформаційні загрози, їх нейтралізація потребує проведення низки організаційно-правових заходів.

Основними напрямками поліпшення системи забезпечення інформаційної безпеки держави є:

• стратегічне стримування та припинення бойових дій та військових конфліктів, що можуть виникнути після зумисного застосування дезінформаційних технологій;

• поліпшення системи забезпечення інформаційної безпеки ЗСУ, інших військових формувань, включно з силами та засобами інформаційної протидії;

• прогнозування, виявлення та оцінка загроз, включаючи загрози ЗСУ в сфері інформації.

Нині інформація як зброя є доволі серйозним засобом ведення війни, так як її технологічна інноваційність, потужність та непримітність є небезпечними. Відповідно, інформаційна безпека України має базуватися на синхронізованих діях структур держави та громадянського суспільства. Під час війни суттєво зросла роль інформаційної культури як чинника підсилення опору дезінформаційній зброї громадянами та збереження державного суверенітету України.

Висновки. Нинішня війна добре демонструє, що інформація використовується і в якості зброї масового ураження. У зв’язку з цим потрібно побудувати ефективний механізм, котрий би гарантував інформаційну безпеку України, в основу якого, на нашу думку, важливо покласти такі складові: технічну – створити належну технічну базу функціонування інформаційної безпеки; політичну – державна політика повинна бути направлена на

забезпечення інформаційної безпеки; правову – оформлення всіх заходів інформаційної безпеки якісними нормативно-правовими актами.

Ефективно протидіяти інформаційній агресії видається, на нашу думку, можливим за рахунок залучення до цього процесу міжнародних організацій, інституцій та міжнародної спільноти загалом. Практика показує – кордонів для ведення інформаційної війни не існує.

Список використаних джерел:

1. *Бодрук О.С.* Структури воєнної безпеки: національний та міжнародний аспекти: монографія. К.: НІПМБ, 2001. 300 с.
2. *Кочубей Л.О.* Інформаційна безпека держави: інструменти захисту українського інформаційного поля (на прикладі особливостей інформаційно-комунікаційних технологій у сучасному Донбасі). *Наукові записки Інституту політичних і етнонаціональних досліджень імені І.Ф. Кураса*. 2015. Вип. 3. С. 220-237.
3. *Цимбалюк В.С.* Правове регулювання інформаційної безпеки в Україні: проблеми теорії та практики. *Адміністративне право і процес*. 2014. № 2(8). С. 22-30.

ОСНОВНІ ЗАГРОЗИ БЕЗПЕКИ ВІРТУАЛЬНОЇ ПРИВАТНОСТІ ТА ШЛЯХИ ЇХ ПОДОЛАННЯ

Маленко І.В.,
Чайка Т.О.,
магістранти факультету інформаційних систем та технологій,
ПВНЗ «Європейський університет»

В сучасному світі, коли Інтернет став необхідністю для більшості людей, безпека віртуальної конфіденційності стає все більш актуальною і важливою темою. Існує багато загроз, які можуть стати причиною крадіжки особистої інформації, втрати грошей, або навіть стануть причиною шантажу. Тут ми розглянемо основні загрози безпеки віртуальної приватності та методи їх запобігання.

Кібератаки – це одна з найбільш серйозних загроз, які можуть стати причиною витоку важливої інформації. Ці атаки можуть бути здійснені з використанням різноманітних методів, включаючи відправку шкідливих програм на комп’ютер, спам атак або підроблених веб-додатків, що намагаються зламати пароль користувача. В 2020 році збитки від наслідків витоку інформації приватних осіб та компаній в США склали 8,64 мільйонів $, що призводило до втрати доходів, простою в роботі та проблем з відновленням інформації. Для захисту від кібератак необхідно забезпечити надійність комп’ютерної мережі, встановити ПЗ для виявлення вірусів і шкідливих програм, використовувати складні паролі та організувати регулярне оновлення софту та операційної системи.

Фішинг – це метод шахрайства, коли зловмисники використовують підроблені електронні листи, веб-сайти та інші методи для виманювання особистої інформації. Зловмисники можуть використовувати підроблені є-імейли від банків, інтернет-магазинів та інших компаній щоб спонукати користувачів надати свої особисті дані, такі як паролі, ПІБ, адреси, номер телефону, номери кредитних карток та інші дані.

Щоб захистити себе від фішингу, необхідно бути уважним при отриманні листів, перевіряти адресу відправника та веб-сайт, з якого вони прийшли, не відкривати підозрілі посилання та надавати особисту інформацію тільки на надійних сторінках з https-протоколом.

Крадіжка даних – ще одна серйозна загроза безпеки віртуальної конфіденційності. Зловмисники можуть використовувати шпигунське ПЗ, щоб отримати доступ до особистої інформації, такої як паролі та номери кредитних карток. Для захисту від крадіжки даних необхідно встановити ПЗ для виявлення та видалення шпигунських програм.

Загальні методи забезпечення віртуальної приватності.

Окрім захисту від конкретних загроз, існують загальні методи захисту, які допоможуть зменшити ризик витоку конфіденційної інформації в Інтернеті.

Один з таких методів – це використання складних та унікальних паролів для всіх онлайн-акаунтів. Пароль повинен містити букви, цифри, символи та бути довжиною не менше 12 знаків. Крім того, необхідно використовувати різні паролі для різних акаунтів.

Інший засіб – це використання ПЗ для захисту від вірусів та шкідливих програм. Існують безкоштовні та платні програми, які допоможуть виявляти та видаляти віруси та інші шкідливі програми з вашого комп’ютера.

Ще один варіант – це шифрування конфіденційної інформації перед надсиланням або збереженням на локальному диску. Шифрування забезпечує захист від несанкціонованого доступу до вашої інформації навіть у випадку, якщо зловмисник отримає доступ до вашого комп’ютера.

Важливо уникати використання публічних WI-FI мереж, особливо для передачі важливої інформації.

Нарешті, важливо забезпечувати регулярне оновлення ПЗ та операційної системи. Відсутність оновлень може призвести до появи нових вразливостей, через які зловмисники можуть отримати доступ до вашої інформації.

Отже, у світі, де все більше і більше даних зберігається в Інтернеті, захист даних стає все більш важливим. На сьогодні, існують різні методи для протидії загрозам, які допомагають зберегти конфіденційність в Інтернеті. Важливо пам’ятати про необхідність використання складних та унікальних паролів, встановлення ПЗ для захисту від вірусів та шкідливих програм, а також регулярне оновлення софту та операційної системи.

В цілому, забезпечення інформаційної безпеки – це складний процес, який вимагає уваги та певної кількості зусиль. Проте, вкладені зусилля будуть виправдані, коли йдеться про безпечну роботу в мережі.

Список використаних джерел:

1. Phishing. Types of phishing attacks. URL: ttps://www.cisco.com/c/en_in/products/security/email-security/what-is-phishing.html
2. What is cybersecurity? URL: https://www.ibm.com/topics/cybersecurity

ІНСАЙДЕРСЬКІ ЗАГРОЗИ У КІБЕРПРОСТОРІ

Маленюк М.Ю.,
курсант ІІ курсу,
Світличний В.А.,
кандидат технічних наук, доцент,
доцент кафедри протидії кіберзлочинності факультету № 4,
Харківський національний університет внутрішніх справ

Інсайдерські загрози – це шкідливі для організацій загрози, які випливають з людей всередині організацій, таких як працівники, що були працівники, підрядники або робочі партнери, у яких є інформація про методи безпеки всередині організацій, даних і комп'ютерних систем. Загроза може включати шахрайства, край конфіденційної та комерційної цінної інформації, права інтелектуальної власності, або саботаж комп'ютерних систем.

Інсайдер – це будь-яка особа, яка має або мала авторизований доступ або знання ресурсів організації, включаючи персонал, приміщення, інформацію, обладнання, мережі та системи. Приклади інсайдера можуть включати: Особа, якій організація довіряє, включаючи співробітників, членів організації та тих, кому організація надала конфіденційну інформацію та доступ. Особа, якій надано бейдж або пристрій доступу, який ідентифікує її як особу з регулярним або постійним доступом (наприклад, працівник або член організації, підрядник, постачальник, охоронець або ремонтник). Особа, якій організація надала комп'ютер та/або доступ до мережі. Особа, яка розробляє продукти та послуги організації; до цієї групи входять ті, хто знає секрети продуктів, які забезпечують цінність організації. Людина, яка має знання про основи організації, включаючи ціни, витрати, а також сильні та слабкі сторони організації. Особа, яка добре обізнана з бізнес-стратегією та цілями організації, їй довірено плани на майбутнє або засоби для підтримки організації та забезпечення добробуту її людей. У контексті державних функцій інсайдером може бути особа, яка має доступ до захищеної інформації, яка, якщо її зламано, може завдати шкоди національній та громадській безпеці. Що таке внутрішня загроза? Інсайдерська загроза – це можливість для інсайдера використовувати свій авторизований доступ або розуміння організації, щоб завдати їй шкоди. Ця шкода може включати зловмисні, самовдоволені або ненавмисні дії, які негативно впливають на цілісність, конфіденційність і доступність організації, її даних, персоналу або засобів. Зовнішні зацікавлені сторони та клієнти Агентства з кібербезпеки та безпеки інфраструктури (CISA) можуть вважати,

що це загальне визначення краще підходить і адаптується для використання в їхніх організаціях. Загрози безпеці зросли та стали складнішими в міру поширення практики роботи з дому та віддаленої роботи [1]. У результаті віддалена робота кардинально змінила пріоритети безпеки та змінила заходи безпеки. Ця зміна системи безпеки поставила перед командами безпеки нові виклики: Збільшення загальної кількості інцидентів безпеки через зміни поведінки та збільшення площі атаки Збільшення кількості фішингових атак Відсутність видимості кінцевих точок і серверів, не підключених до VPN Зміни в поведінці співробітників через ненормований робочий день, різні локації та зміни в поведінці веб-перегляду Збільшене використання додатків SaaS і відсутність видимості Керівники відділу інформаційної безпеки (CISO) повинні впоратися зі швидкими змінами в IT-безпеці, оскільки вона виходить за межі корпоративної мережі. Команда CISO повинна краще розуміти особливості поведінки своїх віддалених співробітників і наслідки віддаленої роботи для виявлення внутрішніх загроз, щоб ефективно захистити активи компанії. Щоб вирішити проблеми з віддаленою робочою силою, CISO повинні мати відповіді на такі запитання: Як ми можемо перевірити, що особа, яка входить у корпоративну віртуальну приватну мережу (VPN), є співробітником, а не зловмисником, який використовує вкрадені облікові дані? Як ми можемо перевірити, що аномальна поведінка працівника не є результатом віддаленої роботи? Як ми можемо допомогти убезпечити співробітників, які підключаються до відкритих і незахищених місць в Інтернеті, таких як кафе? Розуміючи поведінку віддалених співробітників, групи безпеки можуть виявляти ненормальну поведінку, яка може сигналізувати про компрометацію облікових даних або зловмисний намір [2]. Припустимо, зловмиснику вдається уникнути виявлення на периметрі та знаходиться всередині мережі організації. У цьому випадку групи безпеки повинні перевірити загрозу, шукаючи кілька скомпрометованих облікових даних або індикаторів зловживання. Команди безпеки можуть отримати індикатори внутрішньої загрози за допомогою багатьох методів, часто за допомогою машинного навчання. Ці методи можуть допомогти визначити, чи є доступ від законного працівника чи злодія облікових даних.

Висновки. Змоделюйте чіткі стандартні моделі активності та частоту для виявлення вихідного відхилення. Відхилення може вказувати на зловживання, навмисне чи випадкове. Відстежуйте спроби викрадання даних за кількістю спроб вихідного зв’язку або з’єднань за певний день. Якщо кількість вихідних повідомлень працівника зростає, це може запропонувати уважно стежити за обліковими даними цього користувача. Визначте великий, ненормальний обсяг передачі даних для певного працівника. Моніторинг передачі сукупних даних може запропонувати спрощену, але потужну індикацію раннього злому. Перевірте цілісність кінцевої точки на наявність підозрілих програм, які можуть свідчити про активність зловмисного програмного забезпечення. Виявляючи нові процеси або виконання додатків, ви можете стримати зловмисне програмне забезпечення та зменшити ризик безпеки організації.

Список використаних джерел:

1. Contributors to Wikimedia projects. Insider – Wikipedia. *Wikipedia, the free encyclopedia*. URL: https://uk.wikipedia.org (дата звернення: 01.03.2023).
2. What Is insider? URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/347 (дата звернення: 01.03.2023).

АСПЕКТИ КІБЕРБЕЗПЕКИ У ЦИФРОВОМУ УНІВЕРСИТЕТІ

Милашенко В.М.,
декан факультету
інформаційних систем та технологій,
Романенко М.Ю.,
студент факультету
інформаційних систем та технологій,
ПВНЗ «Європейський університет»

В основі стабільного життя та сталого розвитку людини і суспільства знаходяться загальнолюдські, національні, корпоративні та особисті цінності, які мають формувати підґрунтя для безпеки і стійкості на відповідних рівнях.

Сучасні реалії, зокрема, геополітичні трансформації, євроінтеграція, імперські амбіції, збройний терор держави-агресора, різкі зміни в житті значної частини людей у регіонах і країнах разом в комплексі створюють водночас як виклики та загрози так і можливості для розвитку суспільства. Враховуючи основні тренди є можливість моделювати основні напрями змін в економіці та освіті. Відповідно змінюється роль освіти у суспільстві.

Вища освіта спрямована на досягнення багатьох цілей, включаючи підготовку студентів до активного громадянства, до їх майбутньої кар'єри, підтримку їх особистого розвитку. Розширення доступу до вищої освіти надає можливість використовувати все більш різнорідний індивідуальний досвід. Відповідь на різноманітність і зростаючі очікування вимагає фундаментальних змін у її наданні. Це потребує більш студентоцентрованого підходу до навчання і викладання (включаючи гнучкі освітні траєкторії та визнання навичок та компетентностей, набутих поза формальними освітніми програмами) та створення умов для безпечного інформаційного навчального простору університетів, враховуючи їх важливе системне значення для суспільства. Університети – це спільноти тих, хто навчається, викладачів, випускників та широке коло партнерів. Вони об'єднані в мережі на місцевому, національному та міжнародному рівнях і розбудовують соціальні та професійні зв'язки в різних сферах.

Важливим чинником сьогодення є те, що запити з боку суспільства щодо освіти все більш активно реалізується шляхом створення різних навчальних спільнот різноманітних форматів. Серед європейських трендів є також формування освітніх екосистем у різних країнах. Екосистемний спосіб

функціонування підтримує більше різноманіття, за рахунок чого забезпечується стійкість при змінах.

Зростання діджиталізації та конективності в різних сферах підвищує ризики кібербезпеки і робить суспільство в цілому більш вразливим до кіберзагроз та підвищує небезпеки, з якими можуть стикатися фізичні особи, у тому числі студенти. Для пом'якшення згаданих ризиків потрібно постійно вживати всіх необхідних заходів для підвищення кібербезпеки, щоб забезпечити кращий захист від кіберзагроз мережевих та інформаційних систем, комунікаційних мереж, цифрових продуктів, послуг та пристроїв.

У світлі зростання викликів кібербезпеки, існує потреба в комплексному наборі заходів, створених на основі минулих дій і заходів для сприяння досягненню цілей, що взаємно посилюють одна одну. Існує потреба в додаткових зусиллях, спрямованих на підвищення обізнаності громадян, організацій та підприємств про питання, пов'язані з кібербезпекою. Крім того, оскільки інциденти підривають довіру до надавачів цифрових послуг та до єдиного цифрового ринку як такого, особливо серед споживачів, існує потреба в подальшому посиленні довіри шляхом розповсюдження у прозорий спосіб інформації про рівні безпеки продуктів, послуг та процесів ІКТ. Зростання довіри може бути досягнуто завдяки сертифікації та передбачатиме спільні вимоги до кібербезпеки і критерії оцінювання для національних ринків і секторів.

Кібербезпека є питанням не суто технологічним. Для неї має велике значення людська поведінка. Відповідно, необхідно всіляко просувати «кібергігієну», а саме: прості та планові заходи, які у разі їх впровадження та здійснення на регулярній основі громадянами, організаціями та підприємствами мінімізують вплив ризиків від кіберзагроз. Користувачі повинні володіти точною інформацією стосовно рівня надійності, стосовно якого було сертифіковано їхні продукти, послуги та процеси ІКТ. У той же час жоден продукт чи послуга ІКТ не є цілком кібербезпечними, тому потрібно просувати та пріоритизувати базові правила кібергігієни. Зважаючи на дедалі більшу доступність пристроїв Інтернету речей, може бути виділено низку добровільних заходів, за допомогою яких приватний сектор може посилювати довіру до безпеки продуктів, послуг ІКТ та процесів ІКТ.

Одним із ключових аспектів підвищення кіберстійкості конкретного навчального закладу, є впровадження політики безпеки на різних рівнях функціонування університету та структурних підрозділів. Для створення та практичного впровадження політик безпеки можна залучати безпосередньо команди студентів у різних формах навчальної діяльності. Також такі політики важливі при створенні спеціалізованих навчально-тренувальних центрів та кіберполігонів.

Таким чином, системний підхід до формування навичок, компетентностей і мікрокваліфікацій з кібербезпеки дозволяє створити екосистему суспільної кіберстійкості з провідною роллю університету.

Список використаних джерел:

1. Стандарти і рекомендації щодо забезпечення якості в європейському просторі вищої освіти (ESG). URL: ttps://www.britishcouncil.org.ua/sites/default/files/standards-and-guidelines_for_qa_in_the_ehea_2015.pdf
2. РЕГЛАМЕНТ ЄВРОПЕЙСЬКОГО ПАРЛАМЕНТУ І РАДИ (ЄС) 2019/881 від 17 квітня 2019 року про Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA). URL: https://zakon.rada.gov.ua/laws/show/984_024-19#Text

ПРОБЛЕМИ ОСВІЧЕНОСТІ ДЕРЖАВНИХ СЛУЖБОВЦІВ ТА ПРАЦІВНИКІВ ДЕРЖАВНИХ ПІДПРИЄМСТВ У СФЕРІ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ВІЙСЬКОВОЇ АГРЕСІЇ

Моновцов І.О.,
магістрант,
Львівська філія ПВНЗ «Європейський університет»

На думку українських фахівців із кібербезпеки у державі протягом 5 років гібридної війни зафіксована значна кількість хакерських атак, які безпосередньо загрожували національній безпеці держави. У 2014 році – DDoS-атаки і злам сайту Центральної виборчої комісії під час президентських виборів; у 2015 році – за допомогою програми Black Energy 3 було відключено близько 30 підстанцій «Прикарпаття обленерго»; у 2016 році – хакерська атака на внутрішні телекомунікаційні мережі Мінфіну, Держказначейства, Пенсійного фонду із знищенням критично важливих баз даних. DDOS-атака на сайт «Укрзалізниці», внаслідок чого протягом дня була повністю заблокована його робота; у 2017 році – хакерська атака за допомогою вірусної програми Petya, яка порушила роботу аеропорту «Бориспіль», «Укртелекому», ЧАЕС, «Укрзалізниці», Кабінету міністрів та найвпливовіших ЗМІ [1]. Крім того, експерт в галузі інформаційної безпеки Cisco Володимир Ілібман констатує, що із року в рік кількість атак та вірусів зростає. Якщо порівняти кількість штамів вірусів у 2016 та 2017 роках, то ця цифра виросла з 10 мільйонів до 100 мільйонів унікальних вірусів [2].

В Україні на найглобальнішому рівні було затверджено Доктрину інформаційної безпеки України, що затверджена указом Президента України від 25 лютого 2017 року [3] також Указом Президента України від 26 серпня 2021 року № 447/2021 введено в дію Рішення Ради національної безпеки і оборони України від 14 травня 2021 року Про Стратегію кібербезпеки України.

Однак, попри існування вищенаведених законодавчих «мастодонтів» подивимось на реальну ситуацію, що склалася на сьогоднішній день. Чи задавались ми запитанням, який відсоток державних службовців та звичайних працівників державних підприємств знає хоча б елементарні правила кібербезпеки?

Спираючись на власний досвід, який я почерпнув за десять років роботи в різних структурах та установах, можна навести ряд прикладів, які стосуються проблеми освіченості працівників у сфері кібербезпеки та інформаційної безпеки в умовах військової агресії. Не вдаючись у деталі проблеми прикладів низького рівня освіченості працівників виражено проявляються у функціонуванні:

- одного з найбільших та стратегічних підприємств України «Укрзалізниці»;
- закладах охорони здоров'я;
- закладах освіти;
- органах державної влади та місцевого самоврядування.

Проаналізовані мною проблемні ситуації в роботі даних установ, що стосуються кіберзахисту та інформаційної безпеки, наводять на той факт, що переважна більшість державних службовців та працівників критичної інфраструктури – це люди, яким 40 і більше років, що в кращому випадку є поколінням цих людей в період навчання яких на уроках інформатики викладали мову «С» та використання програми «Paint», що в реаліях сучасних вимог до кібербезпеки немає жодної практичної цінності. Я не звинувачую цих людей за їх неосвіченість у сфері інформаційної безпеки та кібербезпеки, а акцентую на незадовільному стані справ в освітньому аспекті щодо інформаційної безпеки.

У західних країнах світу значна увага приділяється освітньому аспекту забезпечення інформаційної безпеки (кібербезпеки) починаючи ще з молодших класів школи. Австралія у цьому питанні «пішла» ще далі започаткувавши вивчення основ кібербезпеки з 4-ох років. І це виправдано, адже дуже багато сучасних дітей вперше «знайомляться» із кіберпростором у віці 3-4-ох років.

На сьогодні в Україні існує проблема цифрової освіти. Шкільний курс «Основи інформатики» має адаптуватись під розвиток сучасних цифрових навичок та основ кібергігієни. У закладах післяшкільної освіти мають з'явитись обов'язкові предмети з кібербезпеки та кібергігієни, які поступово вирішуються на законодавчому рівні.

Я впевнений, що ті діти, що зараз навчаються в школі вже будуть на «голову вищі» за сучасне покоління в розумінні кібербезпеки і, в майбутньому, це не буде такою гострою проблемою. Але проблема кіберосвіченості державних службовців та освіченості з питань інформаційної безпеки потребує декілька іншого підходу, можливо, програми освіти для цього сегменту повинні розроблятися у співпраці з психологами задля урахування складності сприймання цієї інформації.

Також, рушійні зміни з питань цифровізації та кіберосвченості прийшли в Україну з появою Міністерства цифрової трансформації у 2019 році, яке, окрім іншого, проводить політику освіти населення у сфері цифрових технологій. Але з огляду на вищенаведені приклади рішення потрібні вже сьогодні і ця робота з освіти досі не добралася до досить великої кількості державних структур та підприємств.

Фахівці з кібербезпеки, включаючи державний сектор, знають про кожну з цих проблем, але в умовах військової агресії ці проблеми мають критичне значення та потребують негайного вирішення, адже в системі кіберзахисту завжди найслабшою ланкою є людина та людський фактор. В нашому випадку в умовах тотальної відсутності базових знань у державних службовців та працівників державних підприємств – це подвійна небезпека, тому цьому питанню повинно бути приділено більше уваги та прискорено його вирішення.

Список використаних джерел:

1. Виступ експертів-учасників круглого столу «Український досвід: кібер та інформаційна безпека» [Електронний ресурс]: https://www.radiosvoboda.org/a/29656549.html
2. Кількість хакерських атак в Україні за рік зросла вдесятеро. Аналітична стаття Уніан. [Електронний ресурс]: https://www.ukrinform.ua/rubric-technology/2418011-kilkist-hakerskih-atak-v-ukraini-za-rik-zrosla-vdesatero.html
3. Указ президента України №47/2017 Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»
4. Указ президента України №447/2021 Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України"
5. Стаття на веб-сайті антивірусного програмного забезпечення «ESET» «Розповсюдження шкідливого ПЗ через торрент» [Електронний ресурс] : https://eset.ua/ua/news/view/697/rasprostraneniye-vredonosnogo-po-cherez-torrent.

ЗАВАДОСТІЙКЕ КОДУВАННЯ У СИСТЕМАХ ПЕРЕДАЧІ ЦИФРОВОЇ ІНФОРМАЦІЇ

Невзоров А.В.,
к.т.н., доцент,
доцент кафедри математичних дисциплін та
інноваційного проектування
ПВНЗ «Європейський університет»

Управління правильністю передачі інформації виконується за допомогою завадостійкого кодування. Є коди, які виявляють помилки, і коригувальні коди, які ще й виправляють помилки. Перешкодозахищеність досягається за допомогою введення надмірності, додаткових бітів. У симплексних каналах зв’язку усувають помилки за допомогою коригуючих кодів. У дуплексних – досить застосування кодів, що виявляють помилки. Це основні методи, використовувані в інформаційних мережах.

Найпростішими способами виявлення помилок є контрольне підсумовування, перевірка на непарність. Однак вони недостатньо надійні, особливо за наявності безлічі помилок. Тому в якості надійних виявляючих кодів застосовують циклічні коди.

Завадостійкість – здатність системи здійснювати прийом інформації в умовах наявності перешкод в лінії зв'язку і спотворень у внутрішньо апаратних трактах. Завадостійкість забезпечує надійність і достовірність переданої інформації (даних). Ми будемо в основному розглядати двійкові коди. Двійкові дані передаються між обчислювальними терміналами, літальними апаратами, супутниками і т. д.

Передача даних в обчислювальних системах чутлива до малої частки помилку, тому що одиночна помилка може істотно порушити процес обчислень.

Найбільш часто помилки з'являються в ПВВ, шинах, пристроях пам'яті. ПВВ містять велику кількість елементів, помилки обумовлюються старінням елементів, погіршенням якості електричних з'єднань, розфазуванням сигналів. Значна частина помилок припадає на ВП, внаслідок відмови окремих ІС або всієї ІС, помилок пов'язаних з флуктуацією напруги живлення тощо.

У системах з багатьма користувачами і поділом за часом довгі виконавчі повідомлення поділяються на пакети.

Повідомлення, подані довгими послідовностями біт, що розбиваються на більш короткі послідовності бітів, називаються пакетами. Пакети можна передати по мережі як незалежні об'єкти і збирати з них повідомлення на кінцевому пункті. Пакет, забезпечений ім'ям і керуючими бітами на початку і в кінці, називається кадром. Управління лінією передачі даних здійснюється за спеціальним алгоритмом, званому протоколом.

Наявність перешкод ставить додаткові вимоги до методів кодування. Для захисту інформації від перешкод необхідно вводити в тому чи іншому вигляді надмірність: підвищення потужності сигналу; повторення повідомлень; збільшення довжини кодової комбінації тощо.

Збільшення потужності сигналів призводить до ускладнення і подорожчання апаратури, крім того, в деяких системах передачі інформації є обмеження для передачі потужності, наприклад, супутниковий зв'язок.

Повторна передача повідомлень вимагає наявності буферів для зберігання інформації та наявності зворотного зв'язку для підтвердження достовірності переданої інформації. При цьому, значно падає швидкість передачі інформації, крім того цей метод не завжди м. б. використаний, наприклад, в система реального часу.

Одним з найбільш ефективних методів підвищення достовірності та надійності передачі даних є завадостійке кодування, що дозволяє за рахунок внесення додаткової надмірності (збільшення мінімального кодового відстані) у кодових комбінаціях переданих повідомлень забезпечити можливість виявлення та виправлення одиночних, кратних і групових помилок.

У залежності від величини мінімальної кодової відстані існують коди, які виявляють і виправляють помилки.

Кодова відстань визначається як кількість одиниць в результаті підсумовування за модулем два двох кодових комбінацій. Мінімальна кодова

відстань d_0 – мінімальне з кодових відстаней всіх можливих кодових комбінацій. Для виявлення r помилок мінімальна кодова відстань дорівнює:

$$d_0 \geq r + 1. \quad (1)$$

Для виявлення r помилок та виправлення s помилок мінімальна кодова відстань дорівнює:

$$d_0 \geq r + s + 1. \quad (2)$$

Тільки для виправлення помилок мінімальна кодова відстань дорівнює:

$$d_0 \geq 2s + 1. \quad (3)$$

Виявляючі коди – це коди, що дозволяють виявити помилку, але не виправити її. Найпростіший спосіб виявлення помилки – це додавання до послідовності бітів даних ще одного біта перевірки на парність (непарність), значення якого дорівнює сумі по модулю два вихідної послідовності біт.

У символьному коді ASCII до семи бітам коду додається восьмий біт перевірки на парність – k_1.

S_1	S_2	S_3	S_4	S_5	S_6	S_7	K_1

Однобітова перевірка дозволяє виявити будь-яку одиничну помилку, дві помилки знайти не можна, в загальному випадку виявляється будь непарна кількість помилок.

Внесення надмірності за рахунок збільшення довжини кодової комбінації призводить до зниження швидкості передачі інформації.

Найчастіше шуми (блискавки, розрив і т.д.) породжують довгі пакети помилок і ймовірність парного і непарного числа помилок однакова, а значить і однобітова перевірка не ефективна.

Перевірка на парність по вертикалі і горизонталі. При цьому послідовність біт даних перебудовується в двовимірний масив, і обчислюються біти на парність як для кожного рядка, так і для кожного стовпця.

При цьому можна виявити кілька помилок, якщо вони не розташовуються в однакових рядках і стовпцях.

При передачі даних коду кожен символ можна вважати рядком масиву. Така перевірка може не тільки встановити факт помилки, але і виявити її місце, а значить, є принципова можливість її виправлення.

Після виявлення помилок іноді можна повторити передачу повідомлень. Така ситуація актуальна в дуплексних каналах, де застосування кодів, що виявляють помилки, достатня як сигналізація про помилку, що викликає повторну передачу від джерела. Це основні методи, використовувані в інформаційних мережах.

Таблиця 1

Приклад кодування п’яти 7-розрядних слів

1	0	1	1	0	1	1	***1***
0	1	0	0	0	1	0	***0***
1	0	1	0	0	1	0	***1***
1	1	0	0	1	0	1	***0***
0	0	0	1	0	1	0	***0***
1	***0***	***0***	***0***	***1***	***0***	***0***	

Наприклад, при зчитуванні інформації з носія у разі, коли умова на парність не виконується – проводиться повторне зчитування, тобто якщо відбулася мала втрата намагніченості, то після другої спроби зчитування може відбутися правильно.

Приклад. Символи алфавіту джерела кодуються семіразрядним двійковим кодом з вагою кодових векторів (кількістю одиниць в кодової комбінації) $w = 3$. Визначити необхідну потужність коду і його надмірність.

Рішення. Потужність семирозрядного коду дорівнює $N = 2^7 = 128$.

Оскільки для кодування використовуються тільки кодові вектори з вагою три, то кількість таких векторів у семирозрядному коді – один.

Надмірність коду дорівнює $R = 1 – \log_2 K / \log_2 N = 0,265$.

Список використаних джерел:

1. Вернер М. Основи кодування. – М.: Техносфера, 2004 – 176 с.
2. Зюко А.Г., Кловський Д.Д., Назаров М.В., Фінк Л.М. Теорія передачі сигналів. М: Радіо і зв’язок, 2011 р . – 368 С.
3. Кнут Дональд, Грехем Роналд, Паташнік Орен Конкретна математика. Основи інформатики – М.: Світ; Біном. Лабораторія знань, 2006. – С. 703.
4. Лідовскій В.І. Теорія інформації. – М., «Вища школа», 2002 – 120 с.
5. Метрологія та радіовимірювання в телекомунікаційних системах. Підручник для ВНЗ. / В. І. Нефьодов, В.І. Халкин, Є.В. Федоров та ін – М.: Вища школа, 2001 р . – 383 с.
7. Стахов О.П. Коди золотої пропорції. – М.: Радіо та зв’язок, 2004 – 178 с.
8. Цапенко М.П. Вимірювальні інформаційні системи. – М.: Енергоатомиздат, 2015. – 440 с.

ПРОБЛЕМИ РОЗВИТКУ ТА СТРАТЕГІЯ ЗАКОНОДАВЧОГО РЕГУЛЮВАННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ

Одінцов В.С.,
магістрант факультету інформаційних систем і технологій,
ПВНЗ «Європейський університет»

Кіберпростір – це новий канал для створення і поширення різноманітної інформації, він став новим двигуном зростання економіки, новою платформою соціального управління, новим способом міжнародного співробітництва, до того ж, і зовсім новою сферою державного суверенітету. Однак, кіберпростір не тільки надає нам ресурси, можливості, але і містить загрози. Посилена цифровізація та зв'язок збільшують ризики кібербезпеки тим самим роблячи суспільство загалом більш вразливим до кіберзагроз, посилюючи небезпеку, з якою стикаються люди, включаючи вразливих осіб, таких як діти. Для зменшення цих ризиків необхідно вжити всіх необхідних заходів для поліпшення кібербезпеки у світі, щоб мережеві та інформаційні системи, комунікаційні мережі, цифрові продукти, послуги та пристрої, якими користуються громадяни, організації та підприємства були б краще захищені від кіберзагроз [1].

На сьогодні, законодавче регулювання кіберзахисту в нашій країні знаходиться на початковому етапі свого формування. Згідно зі ст. 2 Закону України «Про основи національної безпеки України» правову основу у сфері національної безпеки України становлять Конституція, цей та інші закони України, міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, а також видані на виконання законів інші нормативно-правові акти.

Серед таких актів слід окремо виділити Закони України: «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки», «Про Концепцію Національної програми інформатизації», «Про Національну програму інформатизації», «Про інформацію», «Про державну таємницю», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про доступ до публічної інформації»; Проект Закону України «Про Концепцію національної інформаційної політики»; Указ Президента України «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері кібербезпеки України».

Згідно ст. 2 Закону України «Про основи національної безпеки України», Стратегія національної безпеки України і Воєнна доктрина України є документами, обов'язковими для виконання, і основою для розробки конкретних програм за складовими державної політики національної безпеки [3].

Невирішеними є питання державно-приватної взаємодії, ще не сформовані переліки об'єктів критичної інфраструктури, триває розроблення

підходів до кібероборони, попереду ще великий пласт проблем та обсяг роботи, спрямованої на нормативно-правове врегулювання у сфері кібербезпеки.

Необхідно зауважити на те, що дія Закону України «Про основні засади здійснення кібербезпеки України» не поширюється на відносини та послуги, пов'язані зі змістом інформації, що обробляється (передається, зберігається) в комунікаційних та/ або в технологічних системах, соціальних мережах, приватних електронних інформаційних ресурсах у мережі Інтернет (включаючи блог-платформи, відеохостинги, інші веб-ресурси), а також не стосується інформаційно– телекомунікаційних систем, у яких циркулює інформація, яка складає державну таємницю. Проте, запровадження положень Закону у цій сфері може розглядатися, як істотне порушення прав людини відповідно до положень Європейської конвенції про захист прав людини і основних свобод, зокрема ст.10 Конвенції [2].

Необхідно звернути увагу на нормативно-правове регулювання кібербезпеки в банківському секторі України. Стрімкий розвиток нормативно-правового забезпечення у сфері кібербезпеки банківського сектору є можливим завдяки незалежному становищу Національного банку, яке визначається Законом України «Про Національний банк» [4]. Забезпечення безпеки в кіберпросторі не вичерпується заходами державного регулювання і контролю, а, в багатьох випадках, залежить від свідомої і відповідальної поведінки учасників правовідносин, зокрема, суб'єктів господарювання.

Як бачимо, існує ще великий пласт невирішених питань в законодавчій базі та нормативному регулюванні кіберзахисту. Строк дії чинної Стратегії кібербезпеки України завершується наступного року, тому варто розпочинати роботу над новою сучасною Стратегією кібербезпеки України, що має враховувати наявний досвід як професійного середовища, так і іноземних партнерів. Саме Стратегія повинна оцінити виклики і визначити перспективи підвищення захищеності в кіберпросторі. Проте, це завдання є спільним, як для держави, так і для суспільства в цілому, оскільки особливістю кіберпростору є відсутність кордонів і меж, а тому забезпечення безпеки є питанням кожного.

Список використаних джерел:

1. *Бакалінська О., Бакалінський О*. Правове забезпечення кібербезпеки в Україні. Підприємництво, господарство і право. №9. 2019. С. 100-107.
2. Про захист прав людини і основних свобод. Європейська конвенція. від 04.11.1950. Офіційний вісник України від 16.04.1998. № 13 / № 32 від 23.08.2006. С. 270
3. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про стратегію національної безпеки України» : Указ Президента України від 26 травня 2015 року, № 287/2015.
4. Офіційний вісник України від 09.06.2015. – 2015. – № 43. – С. 679-XIV. Відомості Верховної Ради України (ВВР). 1999. № 29. С. 238.

ІНДИВІДУАЛЬНІ РЕЗЕРВНІ ДЖЕРЕЛА ЖИВЛЕННЯ ЯК ВАРІАНТ ЗАБЕЗПЕЧЕННЯ ЕНЕРГЕТИЧНОЇ БЕЗПЕКИ КОМП'ЮТЕРНИХ ІНТЕРНЕТ-МЕРЕЖ

Опольський М.В.,
старший викладач кафедри математичних дисциплін
та інноваційного проектування,
аспірант,
ПВНЗ «Європейський університет», м. Київ

Ракетні атаки росії на Україну не оминули і енергосистему України, внаслідок цього майже не залишилось вцілілих ТЕС та ГЕС. [1] Ці атаки призвели до значного дефіциту електроенергії в енергосистемі [2], що як наслідок призвело до віялових відключень і можливого блекауту [3]. Тому і очевидно що важливим постає питання резервних систем живлення. Самі «популярні» рішення в Україні станом на 2022 рік були бензинові генератори [4], дизельні генератори [5], газові генератори [6], інверторні генератори [7] та джерела безперебійного живлення [8] та гібридні сонячні станції [9].

Що стосується рішення на основі генераторів то тут відбувається перетворення внутрішньої енергії палива (бензину, дизелю чи газу) в електричну за допомогою двигуна внутрішнього згоряння і електродвигуна, який може працювати в режимі генератора [10]. Одні з най типових рішень є бензинові і дизельні генератори, перші з них – дешевші, але в більшості випадків не призначені для роботи 24/7, другі є більш дорожчим рішенням зате більш економічним і можуть працювати без зупинок. Є ще цікавий варіант газових генераторів, які ближче до бензинового, що використовує більш дешевий енергоносій – газ, але тут треба зразу визначитись з типом палива: скраплений газ+бензин, який не потребує дозвільної документації чи природній газ, який вимагає підключення до газової магістралі і відповідної сертифікації та дозволів [11]. Проте ці рішення скоріше підходять для приватних будинків, а не для квартир, адже дані генератори мають значний рівень шуму та викиди вихлопних газів у атмосферу, що унеможливлює їх установку в квартирі. Цікавим вирішенням є інверторний генератор [12], який експлуатує двигун в оптимальних параметрах і має невеликий рівень шуму, та вже може бути встановлений на відкритих балконах і саме такий тип генераторів іноді називають навіть «квартирний» [13]. Але незважаючи на свої переваги від має недоліки: ціна, обмежений модельний ряд і здебільшого малу потужність [14].

Попередні рішення на основі генераторів підходять у випадку довгочасних блекаутів, коли світло пропадає на дні. В цьому випадку питання ціни однієї години електроенергії відходять на другий план, адже дане рішення є одним із найдорожчих в перерахунок кВт*год/грн [15]. У випадку віялових відключень по декілька разів на день більш дешевшим рішенням стає

використання безперебійного джерела живлення [8]. Основна функція джерел безперебійного живлення – це короткочасне живлення електрообладнань під час зникнення електроживлення. Проте оскільки до багатьох ДБЖ можна приєднати зовнішні акумулятори то цей час автономного живлення можна дуже суттєво розширити. При такому вирішенні проблеми необхідно враховувати деякі основні нюанси: потужність ДБЖ на виході, форма вихідного сигналу, ємність акумуляторів та їх тип. Найпростіше питання – вихідна потужність ДБЖ, яка розраховується як сума потужностей всіх приладів + 3-кратний запас для тих приладів в складі яких є електродвигуни, адже вони в момент запуску споживають втричі більшу потужність. Подібним чином розраховується і ємність акумуляторів: для цього нам необхідно знати сумарну потужність всіх приладів які ми будемо використовувати і час який ми плануємо, щоб вони працювали, але тут є один нюанс пов'язаний з глибиною розрядки акумуляторів. Для різних видів акумуляторів є різні максимальні глибини розрядів, які впливають на ресурс акумулятора, причому чим більша глибина розряду тим менший ресурс і навпаки [16]. Проте ще одним важливим питанням є форма вихідного сигналу джерела безперебійного живлення [17], адже деяка техніка в складі якої є електродвигуни дуже чутлива до форми струму і для їх живлення необхідно використовувати БЖД з чистою синусоїдою на виході [18]. Тому серед різних типів БЖД: резервних, інтерактивних, on-line або подвійного перетворення варто вибирати БЖД під конкретну задачу або діапазон задач[19].

На основі вищевикладеного, ми можемо сказати, що у випадку коли нам необхідно джерело з оптимальним співвідношенням ціни/якості і з низькими експлуатаційними витратами при тимчасових відключеннях світла найкращим варіантом є безперебійне джерело живлення. Проте, незважаючи на свої переваги, дане рішення має свій основний недолік – для даного приладу необхідно хоч на деякий час джерело електрики, щоб підзарядити свої акумулятори. В якості вирішення цієї проблеми в якості такого джерела на ринку рекомендують використовувати сонячні панелі. Для даного технічного рішення крім самих сонячних панелей необхідний ще й контролер заряду, що в кінцевому рахунку перетворює дану систему на гібридну сонячну станцію[20]. Тут ми будемо розглядати сонячну станцію саме як джерело енергії, а не електростанцію для отримання прибутку за рахунок продажу електроенергії по зеленому тарифу [21], економічна доцільність якого залишається під великим питанням [22]. Звичайно, в цьому випадку спочатку буде підніматись питання економічної доцільності і окупності приватної сонячної станції при різних «сценаріях» зеленого тарифу [23]. Проте, у індивідуальних сонячних станціях є ще одна проблема, про яку згадують але не часто – це вироблення електроенергії сонячними панелями взимку [24]. Через зниження світлового потоку і низького кута падіння сонячних променів вироблення електроенергії сонячними панелями в грудні в 20 разів менше ніж влітку [25]. На практиці ми отримуємо: що в зимові місяці 1 кВт встановленої потужності за день виробляє всього 0,5 кВт*год електрики на противагу 4,5-

5,5 кВт*год влітку [25]. Тому щоб накопичити за день 4 кВт*год електрики для нормального функціонування будинку нам необхідно мінімум 8 кВт сонячних панелей. Але це вже сонячна станція середньої потужності із своїм ціновим діапазоном, яка не всім фінансово доступна через те, що це є самим дорожчим рішенням на ринку.

Список використаних джерел:

1. https://www.bbc.com/ukrainian/news-63718624
2.https://suspilne.media/334170-v-ener-gosistemi-ukraini-zberigaetsa-znacnij-deficit-elektroenergii-ukrenergo/
3. https://www.epravda.com.ua/publications/2022/11/10/693656/
4. https://uk.wikipedia.org/wiki/%D0%91%D0%B5%D0%BD%D0%B7%D0%B8%D0%BD%D0%BE%D0%B2%D0%B0_%D0%B5%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D1%81%D1%82%D0%B0%D0%BD%D1%86%D1%96%D1%8F
5. https://uk.wikipedia.org/wiki/%D0%94%D0%B8%D0%B7%D0%B5%D0%BB%D1%8C%D0%BD%D0%B8%D0%B9_%D0%B3%D0%B5%D0%BD%D0%B5%D1%80%D0%B0%D1%82%D0%BE%D1%80
6. https://220volt.com.ua/news/useful/generatori/gazovie-generatori-osnovnie-preimushchestva-montazh-i-podklyuchenie.html
7. https://sea-tools.com.ua/ua/blog/chto-takoe-invertornyy-generator-i-stoit-li-ego-pokupat
8. https://uk.wikipedia.org/wiki/%D0%94%D0%B6%D0%B5%D1%80%D0%B5%D0%BB%D0%BE_%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D1%80%D0%B5%D0%B1%D1%96%D0%B9%D0%BD%D0%BE%D0%B3%D0%BE_%D0%B6%D0%B8%D0%B2%D0%BB%D0%B5%D0%BD%D0%BD%D1%8F
9. https://uk.wikipedia.org/wiki/%D0%93%D1%96%D0%B1%D1%80%D0%B8%D0%B4%D0%BD%D0%B0_%D1%81%D0%BE%D0%BD%D1%8F%D1%87%D0%BD%D0%B0_%D0%B5%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D1%81%D1%82%D0%B0%D0%BD%D1%86%D1%96%D1%8F
10. https://www.bezpeka-shop.com/ua/blog/poleznye-sovety/kak-v-brat-generator-dlya-doma-kakoy-luchshe/?gclid=CjwKCAiAnZCdBhBmEiwA8nDQxaTPtp3RaqXKP8GAgzSB_M2zs9guEbp2QW6QTxLEgtJvaCk-tKCyZRoCcvEQAvD_BwE
11. https://shponka-plus.com.ua/ua/a381168-generatory-gazovye-kakoj.html
12. https://optoweek.com.ua/blog/chto-takoe-invertornyj-generator-preimuschestva-i-otlichiya
13. https://matari.ua/invertorni-heneratory-osoblyvosti-perevahy-i-nedoliky-oblast-zastosuvannya.html
14. https://storgom.ua/ua/novosti/chto-takoe-invertornyi-generator-i-stoit-li-ego-pokupat.html
15. https://lviv.vgorode.ua/news/sobytyia/a1227842-je-vidpovid-skilki-koshtuje-hodina-roboti-heneratora-
16. https://best-energy.com.ua/support/battery/411-features-battery
17. https://lantorg.com/article/ibp-s-pravilnoj-chistoj-sinusoidoj-dlya-kotlov-i-ne-tolko
18. https://klimat-market.com.ua/ua/a287337-forma-vyhodnogo-signala.html
19. https://www.sven.fi/ua/support/techsupport/service-article.php?id=16806
20. https://uk.wikipedia.org/wiki/%D0%93%D1%96%D0%B1%D1%80%D0%B8%D0%B4%D0%BD%D0%B0_%D1%81%D0%BE%D0%BD%D1%8F%D1%87%D0%BD%D

0%B0_%D0%B5%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D1%81%D1%82%D0%B0%D0%BD%D1%86%D1%96%D1%8F
21. https://uk.wikipedia.org/wiki/%D0%97%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D0%B9_%D1%82%D0%B0%D1%80%D0%B8%D1%84
22. https://expertcentr.com.ua/zeleni-tarifi-privablivi-ilyuzii-abo-groshova-realnist/
23. З. Щур, Т.В. Галайко, Т.Я. Дзьоба. Економічна ефективність сонячної електростанції в індивідуальному домогосподарстві за різних сценаріїв динаміки «зеленого» тарифу. SEPES. 2021; Випуск 3, Номер 2 : сс. 87 – 102
24. https://texty.org.ua/articles/102890/moya-malenka-enerhonezalezhnist-yak-zhyvetsya-u-budynku-z-avtonomnym-enerhopostachannyam-na-okolyci-obuhova/
25. https://inteleng.com.ua/blog-uk/shho-mozhut-sonyachni-paneli-vzimku-zhivle/

ВИКОРИСТАННЯ МАТРИЧНИХ ПОЛІНОМІВ ДЛЯ ГОМОМОРФНОГО ШИФРУВАННЯ

Покидько Д.Ю.,
магістрант факультету інформаційних систем та технологій,
ПВНЗ «Європейський університет»

В найближчій перспективі методи гомоморфного шифрування істотно впливатимуть на ринок хмарних послуг і в тій чи іншій мірі на вигляд сучасних інформаційних технологій. Однак поки не створені ефективні алгоритми повністю гомоморфного шифрування, що забезпечують рівень продуктивності, придатний для практичного застосування, а тим більше для застосування в системах реального часу.

Слід враховувати, що деякі гомоморфні криптосистеми можуть піддаватися навмисним зовнішнім впливам (наприклад, принципово уразливі до атаки з адаптивно-підібраним шифрованим текстом) і тому не завжди підходять для безпечної передачі даних. Оцінка крипто стійкості гомоморфних систем вимагає окремого дослідження.

На відміну від полегшеної криптографії для гомоморфного шифрування поки не розроблені відповідні міжнародні стандарти, проте активно тривають роботи по створенню прийнятних рішень, що дозволяють безпечно обробляти конфіденційні дані в хмарах і інших додатках.

Для повністю гомоморфної криптосистеми доцільне використання матричних поліномів, оскільки така схема задовольняється доволі малими обчислювальними витратами та підтримує можливість розпаралелювання. Шифро-текст в такій криптосистемі представлений поліномом, коефіцієнтами якого є матрицею. Основна ідея побудови повністю гомоморфної криптосистеми з використанням матричних поліномів полягає в наступному.

Вважатимемо, що секретним ключем є матричний поліном K(X) та вектор $\bar{k}$, а m_1 та m_2 є відкритими текстами. Тоді відповідні шифро-тексти будуть матричні поліноми такого вигляду

$$C_1(X) = R_1(x)K(X) + M_1 \text{ та } C_2(X) = R_2(x)K(X) + M_2,$$

де $M_1\bar{k} = m_1\bar{k}$ та $M_2\bar{k} = m_2\bar{k}$.

Для того, щоб отримати розшифрований текст, потрібно взяти остачу від ділення шифро-тексту на К(Х), потім виділити з отриманої матриці відкритий текст за допомогою вектора $\bar{k}$.

Нехай $Z_p^{N\times N}$ кільце $N \times N$ матриць з елементами кільця цілих чисел Z_p. Тоді множину послідовних матриць із $Z_p^{N\times N}$ елементів можна представити у вигляді

$$F = \{A_0, A_1, A_2, ...\}, A_i \in Z_p^{N\times N}$$

Всі матриці A_i, окрім кінцевого їх числа, дорівнюють нульовій матриці.

Позначимо множину послідовностей матриць $Z_p^{N\times N}[X]$. Для випадку, коли

$$F, G \in Z_p^{N\times N}[X], G = \{B_0, B_1, B_2, ...\}, B_i \in Z_p^{N\times N},$$

визначені такі операції:

$$F + G = \{A_0 + B_0, A_1 + B_1, A_2 + B_2, ...\},$$

$$F \cdot G = \{A_0 \cdot B_0, A_0 \cdot B_1 + A_1 \cdot B_0, A_0 \cdot B_2 + A_1 \cdot B_1 + A_2 \cdot B_0, ...\} = \{C_k\}$$

$$C_k = \sum_{i+j=k} A_i B_j, k = 0,1,2,...$$

Введені операції додавання та множення дозволяють множині $Z_p^{N\times N}$ утворювати кільце, елементами якого є матричні поліноми.

Розглянемо приклад гомоморфних обчислень. Для зіставлення поліному $f^{\perp}(X_1,...,X_t)$ над шифро-текстами $C_1,...,C_t$ з поліномом $f(x_1,...,x_t)$ над шифро-текстами $m_1,...,m_t \in Z_p$ потрібно замінити операції над Z_p на операції додавання та множення поліномів в $Z_p^{N\times N}$.

Для шифро-текстів $c \leftarrow R(X)K(X) + M$ результатом операції розшифрування є

$$m = k_i^{-1}((C(X) \bmod K(X))\bar{k}).$$

Тоді

$$c_1 + c_2 = (R_1(X) + R_2(X))K(X) + M_1 + M_2,$$

що є вірним шифро-текстом для $(m_1 + m_2) \bmod 2$, оскільки є справедливою умова

$$(M_1 + M_2)\bar{k} = (m_1 + m_2)\bar{k}.$$

Для випадку множення маємо:

$$c_1 c_2 = R_1(X)K(X)R_2(X)K(X) + R_1(X)K(X)M_2 + R_2(X)K(X)M_1 + M_1M_2 =$$
$$= (R_1(X)K(X)R_2(X) + R_1(X)M_2 + R_2(X)M_1)K(X) + M_1M_2$$

Після розшифрування маємо $(m_1 \cdot m_2) \bmod 2$, оскільки

$$(M_1M_2)\vec{k} = M_1(M_2\vec{k}) = M_1(m_2\vec{k}) = m_2(M_1\vec{k}) = m_1m_2\vec{k}$$

Розглянута вище криптосистема є коректною та компактною, та, як наслідок, реалізує повністю гомоморфне шифрування.

Список використаних джерел:

1. Antoine Guellier. Can Homomorphic Cryptography ensure Privacy? [Research Report] RR-8568, 2020, pp.111. https://hal.inria.fr/hal-01052509v1

2. D. Boneh, C. Gentry, S. Halevi, F. Wang, D. J. Wu. Private database queries using somewhat homomorphic encryption. Applied Cryptography and Network Security. – Springer Berlin Heidelberg, 2013. – pp. 102-118. doi: 10.1007/978-3-642-38980-1_7

ОСОБЛИВОСТІ ОРГАНІЗАЦІЇ ЗАХИСТУ КІБЕРПРОСТОРУ УКРАЇНИ В УМОВАХ ВІЙНИ: ВИКЛИКИ ТА СТРАТЕГІЇ ПРОТИДІЇ

Попенко Е.С.,
магістрант факультету інформаційних систем і технологій,
Ніколаєвський О.Ю.,
к.т.н., доцент кафедри інформаційних систем,
програмування та кібербезпеки,
ПВНЗ «Європейський університет»

Питання кібербезпеки в Україні в останні роки постають дуже гостро, що пов’язано спочатку з війною на сході країни, а потім з повномасштабним вторгненням росії в Україну, внаслідок чого з’явилася необхідність захисту інформаційної та критичної інфраструктури від кібератак. Організація кібербезпеки в таких умовах стає особливо важливою та викликає специфічні проблеми та загрози.

Специфіка та виклики

1. Безпека критичної інфраструктури. Україна має значну кількість об’єктів критичної інфраструктури, таких як енергетичні, транспортні, комунікаційні та фінансові системи, які є метою кібератак. Захист цих систем потребує значних зусиль та інвестицій.

2. Відповідальність державних структур. Україна потребує ефективної та координованої дії від державних структур для захисту від кібератак. Необхідно забезпечити взаємодію між різними відомствами та органами влади для швидкого реагування на кіберзагрози [1].

3. Ефективність законодавства. Україна потребує ефективного законодавства щодо кібербезпеки, яке відповідало би сучасним викликам та міжнародним стандартам.

Загрози та методи протидії

1. Кібершпигунство: росія займає лідируючу позицію у кібершпигунстві. Для протидії цій загрозі Україна повинна забезпечити відповідний захист своїх інформаційних систем та зменшити свою залежність від іноземних технологій.

2. Кібертероризм: Україна також стикається з загрозою кібертероризму, тобто кібератак, що спрямовані на вчинення насильницьких дій проти людей та інфраструктури. Для захисту від цієї загрози необхідно забезпечити високий рівень безпеки критичної інфраструктури, ретельно контролювати доступ до інформації та вчасно реагувати на кібератаки.

3. Фейкові новини та дезінформація: російська дезінформаційна кампанія є однією з найбільших загроз кібербезпеці України. Для боротьби з цією загрозою необхідно розробити ефективну стратегію протидії дезінформації та забезпечити широкий доступ до достовірної інформації.

4. Можливість кібератак на керівництво країни: Україна може бути об’єктом кібератак на керівництво країни, що може призвести до різких наслідків для національної безпеки. Для протидії цій загрозі необхідно забезпечити високий рівень безпеки інформаційних систем керівництва країни та розробити плани невідкладних заходів в разі кібератаки [2].

Отже, організація кібербезпеки в умовах війни вимагає від України високого рівня підготовки та координації зацікавлених сторін, таких як уряд, військові, правоохоронні органи, приватні компанії та громадянське суспільство [6].

Необхідно розробити ефективну стратегію кібербезпеки, яка буде включати в себе наступні елементи [4].

1. Забезпечення безпеки критичних інфраструктур. Для цього необхідно створити відповідну інфраструктуру та механізми захисту, які будуть спроможні виявляти кібератаки та оперативно реагувати на них. Критичні інфраструктури, такі як енергетичні системи, транспорт, банки та інші, повинні бути захищені від можливих кібератак.

2. Підвищення кваліфікації кадрів. Необхідно забезпечити високий рівень кваліфікації кадрів, які будуть займатися кібербезпекою. Для цього потрібна відповідна підготовка фахівців, організовувати навчальні заходи та тренування, а також використовувати новітні технології та методики.

3. Розвиток співпраці з міжнародними партнерами. Україна повинна активно співпрацювати з міжнародними партнерами у сфері кібербезпеки, зокрема з НАТО, Європейським Союзом, США та іншими країнами. Це

дозволить отримати доступ до новітніх технологій та знань, а також забезпечити спільний захист від кібератак.

4. Використання сучасних технологій. Україна повинна використовувати сучасні технології для захисту від кібератак, такі як штучний інтелект, машинне навчання, блокчейн та ін.

5. Забезпечення правової підтримки. Україна повинна розробити та прийняти відповідні законодавчі акти, які забезпечать правову підтримку в сфері кібербезпеки. Також необхідно забезпечити ефективне виконання цих законів та проводити відповідні заходи проти порушників.

6. Підвищення культури кібербезпеки. Необхідно проводити інформаційну роботу серед населення щодо заходів забезпечення кібербезпеки та вчасно повідомляти про можливі кіберзагрози. Громадяни повинні бути обізнані в питаннях кібербезпеки та знати, як діяти в разі кібератаки [3].

Отже, організація кібербезпеки України в умовах війни стає дедалі більш важливою та складною задачею. Це вимагає від українських владних структур прийняття цілеспрямованих заходів забезпечення кібербезпеки, розвитку відповідних технологій та кваліфікації фахівців, а також від громадян – підвищення культури кібербезпеки та обізнаності з питань захисту від кіберзагроз. Також важливим елементом організації кібербезпеки в умовах війни є усвідомлення кожним громадянином своєї відповідальності за власну та загальну безпеку. Кожен користувач Інтернету повинен дотримуватися базових правил кібербезпеки, таких як використання складних паролів, оновлення програмного забезпечення, обережність при відкриванні пошти та натисканні посилань і т.ін. [5].

Загалом, організація кібербезпеки в умовах війни є важливим елементом національної безпеки України. Зростаюча кількість кібератак на державні та комерційні інформаційні системи потребує розвитку відповідних законодавчих та нормативних актів, підвищення кваліфікації фахівців, забезпечення необхідних матеріальних та технічних ресурсів, співпрацю з міжнародними партнерами і постійну оцінку та вдосконалення заходів захисту.

Крім того, важливим елементом є усвідомлення кожним громадянином своєї відповідальності за власну та загальну безпеку, виконання базових правил кібербезпеки та бережливе використання інтернет-ресурсів.

Невідкладність та важливість питань кібербезпеки в умовах війни вимагає від держави та громадян належної уваги та зусиль. Забезпечення надійного захисту від кібератак є ключовим для забезпечення стійкості країни в умовах війни та змінного світового порядку. Кібербезпека є складним та динамічним процесом, що потребує постійної уваги та зусиль для забезпечення ефективного захисту від кіберзагроз.

Список використаних джерел:

1. *Будько, Є.І.* (2019). Кібербезпека в Україні: сучасний стан, проблеми та перспективи. //Науковий вісник Національного університету цивільного захисту України, №3(79), – С.60-68.

2. *Даниленко, В.* (2020). Інформаційна війна на сході України: історія та сучасність. //Наукові записки Національного університету "Острозька академія". Серія "Історичні науки", №34, – С.94-98.
3. Національний інститут стратегічних досліджень. (2021). Кібербезпека в Україні: загрози, виклики та тенденції. Доступно: https://nisd.org.ua/publication/cyberbezpeka-v-ukrayini-zagrozi-vikliki-ta-tendenciyi/
4. *Потапенко, С.В.* (2019). Кібербезпека як фактор забезпечення національної безпеки. Вісник Придніпровської державної академії будівництва та архітектури, №35(1), – С.129-134.
5. Про затвердження Стратегії національної кібербезпеки на період до 2025 року: Указ Президента України від 18 вересня 2020 року № 392/2020. Доступно: https://www.president.gov.ua/documents/3922020-34494
6. *Шиманська, І.В.* (2020). Кібербезпека України в умовах гібридної війни. //Економічний вісник Запорізької державної інженерної академії, №3, – С. 56-61.

ОСОБЛИВОСТІ КРИМІНАЛЬНОЇ ВІДПОВІДАЛЬНОСТІ ЗА ПОРУШЕННЯ ПРАВИЛ ЗАХИСТУ ІНФОРМАЦІЇ

Рибалко В.,
магістрант факультету інформаційних систем та технологій,
ПВНЗ «Європейський університет»

Перед початком та в ході повномасштабної війни на українські інформаційні системи – сайти органів влади, оборонний, фінансовий, енергетичний та комерційний сектори було здійснено понад 4500 кібератак. Протягом 2022 року Державним центром кіберзахисту було зареєстровано у 2,8 раза більше кіберінцидентів, ніж у 2021 році. Але нанести суттєву шкоду інформаційним ресурсам атакуючі не змогли. Українські фахівці з кіберзахисту гідно витримали удар, і навіть перейшли у наступ. Виводяться з ладу сайти державних установ агресора, замість ворожої пропаганди по цифровим телевізійним каналам транслюється інформація про військові злочини солдатів рф та ставлення світової спільноти до цієї війни. Війна із загарбником йде в тепер на чотирьох фронтах: на землі, в повітрі, у воді та в кіберпросторі.

Метою цього виступу є оцінити дії фахівців з кіберзахисту, що працюють в державній установі, і стикаються з спробами атак на державні інформаційні ресурси. Спробуємо з’ясувати, які наслідки для фахівця з кіберзахисту може мати успішна кібератака на інформаційні ресурси, що він захищає.

Ми знаємо що понад 90% успішних кібератак відбуваються завдяки людським факторам. Тож спробуємо також оцінити наслідки успішної кібератаки для працівника, який неумисно або умисно вчинив дії, що порушують інформаційну безпеку, і, внаслідок яких, успішна кібератака стала можливою, а також для керівника установи, що зазнала успішної кібератаки.

Кримінальний кодекс України містить низку статей (ст.ст. 361 – 363 КК України), які передбачають кримінальну відповідальність за кіберзлочини. Розглядаючи ситуацію, яка цілком може статись в державній установі, ми побачимо зв'язок між кібербезпекою, правилами захисту інформації та кримінальним злочином.

Пропоную оцінити дії фахівця з кіберзахисту, працівника та керівника установи з точки зору ст. 363 КК України, яка має назву: Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється.

Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється, якщо це заподіяло значну шкоду, вчинені особою, яка відповідає за їх експлуатацію, караються штрафом від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років з позбавленням права обіймати певні посади чи займатися певною діяльністю на той самий строк.

Бажаючі можуть переглянути на загальнодоступних ресурсах науково-практичний коментар до цієї статті, а ми спробуємо для початку розглянути дії фахівця з кібербезпеки, що припустився порушення правил захисту інформації.

Уявимо, наприклад, що фахівець з кібербезпеки відкрив за проханням керівника одного з підрозділів доступ його підлеглим до російського сайту, або встановив (дозволив встановити) програмне забезпечення, що має російське походження.

Маємо явне порушення, чи буде кримінальне покарання (адміністративне в рамках цього матеріалу не розглядаємо). Поки ні, оскільки подія, що відбулась, відповідає не всім вимогам ст. 363 КК України.

Розвиваємо ситуацію далі: скачаний файл або програмне забезпечення містять в собі шкідливе програмне забезпечення, з його використанням проексплуатовано одну з вразливостей Active Directory та викрадено аутентифікаційні дані користувача та адміністратора одного з фізичних серверів.

Нагадаю, ми не оцінюємо тут дії зловмисника, який здійснив ці дії, ми оцінюємо дії фахівця з кібербезпеки з точки зору кримінального законодавства.

І на даному етапі кіберзлочину кримінального покарання для фахівця з кіберзахисту не буде.

Використовуючи скомпрометовані облікові дані адміністратора, зловмисник знищив інформацію (зокрема, спеціально розроблене програмне забезпечення) на жорстких дисках сервера разом з резервними копіями. Вартість послуг з відновлення програмного забезпечення, а відповідно і шкоди, нанесеній державній установі, склала 450 тис. грн. (понад 402 600 грн.).

Багатьом може здатись, що це не дуже реальний сценарій, тому додам ще один. Фахівець з кіберзахисту виявив кібератаку, але не заблокував

зловмисника (хоч і мав таку можливість), а за власною ініціативою відслідковував його дії з метою встановлення особи атакуючого, вивчення методів та способів атаки. Навіть перебуваючи під контролем, зловмисник встиг скачати або знищити файли з важливою інформацією, що врешті призвело до завдання шкоди, яка склала 450 тис. грн.

У обох випадках в дії фахівця з кіберзахисту можуть бути кваліфіковані за ст. 363 КК України, оскільки законодавець встановив, що значною шкодою у статтях 361-363 вважається така шкода, яка в триста і більше разів перевищує неоподатковуваний мінімум доходів громадян (на 2023 рік -1342 грн.).

Після детального розгляду дій фахівця з кібербезпеки стає зрозуміло, в яких випадках буде мати місце кримінальна відповідальність працівника, якщо його навмисні чи ненавмисні дії призведуть до успішної кібератаки. Так, у випадку, якщо працівник самостійно встановив на свій робочий комп'ютер програмне забезпечення, користуючись яким зловмисник знищив або пошкодив інформаційні ресурси, або припинив на який час роботу інформаційної системи, кримінальна відповідальність може наступити лише за умови, якщо розмір шкоди перевищить 402 600 грн. При цьому наявність умислу в діях працівника необов'язкова, достатньо довести факт порушення правил захисту інформації.

Пропоную розглянути ще одне питання: а якою є відповідальність керівника установи у таких випадках?

Низка законів (Закони України «Про інформацію» , «Про захист інформації в інформаційно-комунікаційних системах», «Про державну таємницю», «Про захист персональних даних», "Про основні засади забезпечення кібербезпеки України") в тій чи іншій мірі регламентують дії керівника установи щодо забезпечення інформаційної безпеки.

Але особливої уваги заслуговує підзаконний акт, а саме Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджених Постановою Кабінету міністрів України від 29.03.2006 № 373 (далі – Постанова № 373).

Саме слову "правила" слід приділити головну увагу. Бо в тексті ст. 363 КК є слова "порядку та правил захисту інформації". Таким чином, саме на цей документ, на його вимоги буде дивитись слідчий або суд, визначаючи наявність порушень і діях (чи бездіяльності) керівника.

Якщо стисло, то Постанова № 373 вимагає забезпечити захист державних інформаційних ресурсів, навіть таких, у яких обробляється відкрита інформація, за допомогою комплексної системи захисту інформації, атестованої у відповідному порядку. А відповідальність за захист інформації, згідно з тією ж Постановою № 373, покладається на керівника організації, що є власником системи.

Таким чином, через відсутність комплексної системи захисту інформації в інформаційній системі, до кримінальної відповідальності може бути притягнутий керівник установи, яка є власником відповідної інформаційної

системи. Але, знов таки, лише за наявності завданої шкоди більше ніж 402 600 грн.

Узагальнюючи викладене, можна зазначити наступне.

✔ Фахівець з кібербезпеки повинен знати основи законодавства, що регламентує інформаційну безпеку та відповідальність за його порушення. Цю інформацію він має донести до керівника установи, щоб разом з ним сформувати відповідне ставлення до кіберзахисту в установі, а також до працівників, які безпосередньо експлуатують комп'ютери та інформаційні системи.

✔ Як правило, в момент порушення правил захисту інформації, людина не тільки не може передбачити розмір шкоди, яка буде завдана її діями, а й навіть передбачити сам факт її заподіяння не має можливості, тому до кожного порушення слід ставитись як до такого, що може заподіяти значну шкоду.

✔ Наявність умислу в діях фахівця з кібербезпеки, працівника або навіть керівника установи, якими він порушив порядок або правила захисту інформації, не впливає на його відповідальність за ст. 363 КК України.

Список використаних джерел:

1. Карчевський М.В. Злочини в сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (тези лекцій) / М.В. Карчевський // Злочини в сфері використання ІТ [Електронний ресурс]. – Режим доступу: http://it-crime.at.ua/index/tezi_lekcij/0-31
2. Конвенція про кіберзлочинність від 23.11.2001 р. [Електронний документ] / Верховна Рада України : Законодавство. – Режим доступу: http://zakon1.rada.gov.ua/laws/show/994_575.
3. Кримінально-правова характеристика злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку у схемах: посібник для підрозділів Національної поліції / Т. І. Созанський, С. Я. Бурда, А. Я. Скиба. Львів: Львівський державний університет внутрішніх справ, 2019. 20 с.
4. Науково-практичний коментар Кримінального кодексу України / За ред. М. І. Мельника, М. І. Хавронюка. – 7-ме вид., переробл. та допов. – К. : Юридична думка, 2010. – 1288 с.
5. Необхідність створення комплексної системи захисту інформації (КСЗІ) / Технічний захист інформації [Електронний ресурс]. – Режим доступу: https://tzi.com.ua/neobxdnst-stvorennya-kompleksno-sistemi-zaxistu-nformacz-ksz.html
6. Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється. / Legal IT group [Електронний ресурс]. – Режим доступу: https://legalitgroup.com/porushennya-pravil-ekspluatatsii-elektronno-obchislyuvalnih-mashin-*komp-yuteriv-*

avtomatizovanih-sistem-komp-yuternih-merezh-chi-merezh-elektrozv-yazku-abo-poryadku-chi-pravil-zahistu-informatsii-ya
7. Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах. Постанова від 29 березня 2006 р. N 373 [Електронний документ] / Верховна Рада України : Законодавство. – Режим доступу: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text
8. Про захист інформації в інформаційно-комунікаційних системах. Закон України від 5 липня 1994 року № 80/94-ВР [Електронний документ] / Верховна Рада України: Законодавство. – Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text
9. Роль керівника у забезпеченні кіберзахисту своєї установи. Інтерв'ю з головою Держспецзв'язку Юрієм Щоголем / Реформа державного управління [Електронний *ресурс]. – Режим доступу: https://par.in.ua/en/information/publications/90*

КРИПТОГРАФІЧНІ ТА СТЕГАНОГРАФІЧНІ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ

Савченко Я.О., Чмиренко О.В.,
магістранти факультету інформаційних систем та технологій,
ПВНЗ «Європейський університет»

У сучасному цифровому світі, захист інформації є вкрай важливим завданням. Інформація може бути вкрадена або підроблена, що може призвести до серйозних наслідків, які можуть бути фінансовими, соціальними або політичними. Тому криптографічні та стеганографічні засоби захисту інформації є надзвичайно важливими для забезпечення конфіденційності, цілісності та доступності даних як для бізнесу, так і для держави та приватних осіб. Використання цих методів може забезпечити захист від зловмисного доступу, вірусів, хакерських атак та інших загроз.

Криптографія – це наука про захист інформації шляхом перетворення її у нечитану форму. Криптографічні засоби захисту інформації забезпечують конфіденційність, цілісність та аутентичність даних. Криптографічні протоколи забезпечують захист даних у транзиті та стаціонарному зберіганні.

Стеганографія – це наука про приховування інформації. Стеганографічні засоби захисту інформації дозволяють вставляти приховані повідомлення у різний контент, наприклад, у зображення, аудіо або відео файл.

Одним з найбільш поширених методів криптографічного захисту інформації є шифрування. Цей процес включає застосування математичних алгоритмів для перетворення повідомлення в незрозумілий для читача формат, відомий як шифртекст. Шифрування може бути симетричним, коли той самий ключ використовується для шифрування та розшифрування, або

асиметричним, коли два ключі використовуються для цих процесів – приватний та публічний.

Іншим методом криптографічного захисту інформації є хешування, що полягає у створенні унікального значення, відомого як хеш, для вихідних даних. Це значення може бути використано для перевірки цілісності даних та для забезпечення безпеки паролів та інших конфіденційних даних.

Одним з найбільш важливих криптографічних алгоритмів є RSA (Rivest-Shamir-Adleman), який використовується для захисту даних у транзиті. RSA використовує публічний та приватний ключі, щоб зашифрувати та розшифрувати дані. При цьому публічний ключ доступний всім користувачам, що дає можливість безпечно обмінюватися даними.

Інший важливий криптографічний алгоритм – AES (Advanced Encryption Standard), який використовується для захисту даних у стаціонарному зберіганні. AES забезпечує конфіденційність даних шляхом шифрування даних у блоках і забезпечує дуже високий рівень захисту.

Стеганографія, з іншого боку, є методом приховування інформації в межах іншого повідомлення або файлу, щоб ця інформація залишалася непомітною для сторонніх користувачів. Це може бути корисним для забезпечення конфіденційності даних в разі їх пересилання через незахищені канали зв’язку.

Одним з найпоширеніших стеганографічних методів є метод Least Significant Bit (LSB), який використовується для вставки бітів інформації у менш важливі біти зображення або іншого контенту. Цей метод може бути використаний для приховування повідомлень різної довжини та складності.

Ще один метод стеганографії – це використання шуму. Шум може бути використаний як вектор для вставки інформації у зображення або інші типи контенту. Цей метод може бути більш безпечним, оскільки його важче виявити, ніж метод LSB. Однак, він потребує більше обчислювальних ресурсів та може бути менш ефективним для великих обсягів інформації.

У підсумку, криптографічні та стеганографічні засоби захисту інформації важливі для забезпечення безпеки та конфіденційності даних в цифровому світі. Кожен метод має свої переваги та недоліки, і їх використання залежить від потреб користувача. Однак, комбінація криптографічних та стеганографічних методів може забезпечити більший рівень захисту інформації. Криптографічні методи дозволяють зашифрувати повідомлення таким чином, що навіть якщо зловмисник зможе отримати доступ до нього, він не зможе розшифрувати його без правильного ключа. Стеганографічні методи дозволяють приховати інформацію таким чином, що зловмисник навіть не підозрює про її наявність.

Хоча криптографічні та стеганографічні методи захисту інформації можуть забезпечити високий рівень безпеки, вони не є панацеєю. Наприклад, використання слабких ключів або алгоритмів шифрування може призвести до зламу захисту. Крім того, зловмисники можуть використовувати методи

соціальної інженерії, щоб отримати доступ до конфіденційної інформації, наприклад, отримуючи доступ до паролів від користувачів.

Тому для забезпечення максимального рівня захисту інформації, необхідно використовувати комплексний підхід, який включає в себе як криптографічні та стеганографічні методи, так і заходи забезпечення фізичної безпеки та резервне копіювання даних.

Крім того, дуже важливо дотримуватися базових принципів кібербезпеки, таких як використання складних та унікальних паролів, регулярне оновлення програмного забезпечення та операційних систем, обмеження доступу до конфіденційної інформації лише необхідним користувачам, використання сучасних технологій захисту, таких як двофакторна автентифікація та біометричні методи.

Також важливо мати на увазі, що зловмисники постійно вдосконалюють свої методи атак та шифрування, тому для забезпечення безпеки даних необхідно постійно вдосконалювати та оновлювати захист, щоб забезпечити максимальну безпеку даних так як кіберзлочини та кібератаки стають все поширенішими та складнішими.

Тому у сучасному світі, де обсяги цифрової інформації зростають з кожним днем, захист конфіденційної інформації є дуже важливим завданням. Криптографічні та стеганографічні методи забезпечення інформаційної безпеки є потужними засобами захисту від різноманітних загроз, проте їх використання повинно бути доповнене іншими технічними та організаційними заходами, щоб забезпечити максимальний рівень безпеки та захисту інформації.

Список використаних джерел:

1. Методи сучасної криптографії. URL: https://tarasenkoag14.wordpress.com/2014/09/14/
2. Стеганографічний алгоритм захисту даних з використанням файлів зображень.URL: http://www.economy.nayka.com.ua/?op=1&z=5584
3. Information security. URL: https://en.wikipedia.org/wiki/Information_security

АНАЛІЗ СУЧАСНОГО СТАНУ КІБЕРПРОСТОРУ В АСПЕКТІ УКРАЇНСЬКО-РОСІЙСЬКОЇ ВІЙНИ

Савчук В.С.,
PhD, старший викладач кафедри інформаційної боротьби
Лобода В.В.,
науковий співробітник науково-дослідного відділу
Латко І.І.,
молодший науковий співробітник науково дослідного відділу,
Житомирський військовий інститут імені С. П. Корольова

У сучасному світі забезпечення кібернетичної безпеки стає все більш актуальним і важливим завданням для держав у всьому світі. Після масштабного вторгнення та кібератак на Україну російська федерація (рф) зіткнулася з широким спектром кіберзагроз, а її система кібербезпеки стала предметом значних атак з боку багатьох країн світу, які виявили вразливості у ній.

Своє загальне бачення зовнішніх інформаційних загроз і стратегічних пріоритетів рф виклала в документі від 2013 р. "Основи державної політики рф у сфері міжнародної інформаційної безпеки на період до 2020 року". Ще тоді Україна була визначена як "… довгострокове вогнище нестабільності в Європі й безпосередньо біля кордонів росії...", а рф при цьому "… надає перевагу використанню насамперед політичних і правових інструментів, механізмів дипломатії і миротворчості. Застосування військової сили для захисту національних інтересів можливе тільки в тому разі, якщо всі вжиті заходи ненасильницького характеру виявилися неефективними…"

Визначені напрямки засвідчують завчасну підготовку інформаційно-психологічних, інформаційних та кібернетичних операцій проти України з боку рф. У лютому 2014 року в інтерв'ю, присвяченому кібербезпеці, президент Барак Обама заявив, що розглядає Китай і росію як одну із загроз кібербезпеці США. Зазначається, що Китай підтримує ініціативи росії щодо встановлення більшого державного контролю над кіберпростором. Хоча росії ще потрібен час для побудови аналогічних відносин між державою та її народом, що є запорукою успіху власної політики Китаю в інформаційному та кіберпросторі. Також певними гальмами для росії слугують фіктивні заходи з "імпортозаміщення" в IT-секторі, що мали місце в рф ще у 2014 році. Наприклад, за даними журналістів, у міністерстві оборони рф за розпорядженням міністра Шойгу логотипи іноземних брендів на службових мобільних телефонах заклеїли наклейками "Воентелеком". У своїй політиці щодо майбутнього кіберпростору рф, як і Китай, робить великий акцент на контентній складовій. Створюючи закриту інформаційну систему в країні, російське керівництво намагається встановити пріоритетний контроль над внутрішніми інформаційними потоками. На роскомнагляд покладено такі

завдання (РКН), як: відповідальність за публікації в Інтернеті, глобальний моніторинг національної частини мережі, можливість відключення сайтів, розташованих у російській частині Інтернету (відключення усього, що суперечить побудованій ідеологічній платформі "руського міру").

Політика у сфері кібербезпеки заздалегідь передбачала підготовку до широкомаштабної війни з Україною та пов'язаних із нею реакцій міжнародної спільноти. Уже у 2019 році в російських ЗМІ почали з'являтися такі заяви: "Відповідно до закону, російські інтернет-провайдери повинні будуть забезпечити незалежність інтернет-простору Рунету, якщо іноземні держави спробують ізолювати націю в Інтернеті…". Хоча заява про створення "національного інтернету" озвучена ще у 2015 році в офіційній заяві російського військово-історичного товариства [1]. На засіданні робочої групи "Інформаційна безпека", що реалізує національний проєкт "Цифрова економіка" було прийнято рішення про проведення навчань, до яких залучено таких операторів зв'язку росії, як: "мегафон", "вимпелком", "МТС", "ростелеком", під час яких перевірялась на практиці можливість застосування закону "про суверенний інтернет". Увесь трафік усередині росії має проходити через точки обміну, схвалені роскомнагляд. Для цього мобільні оператори та інтернет-провайдери повинні встановити на своїх мережах обладнання, за допомогою якого РКН зможе втручатися у потоки трафіку, а також блокувати заборонені до росії ресурси. Зрозуміло, що підготовка такого "контрольованого державою інтернету" дає можливість не лише контролювати кіберзлочинність, а й особисту інформацію, поширювану в мережі, та блокувати той контент, що суперечить поглядам влади. Сюди ж можна додати діяльність з обмеження розповсюдження в мережі певного контенту (передусім – опозиційного характеру) державною структурою "роскомнадзор", впровадження обмежень на анонімний доступ до публічних точок вайфай, випадки переслідування людей за розповсюдження в Інтернеті ідей, які дисонують із панівною ідеологічною концепцією рф (щодо війни в Україні) [2].

Оскільки рф завчасно готувалася до повномасштабного вторгнення й у сфері кібербезпеки, то постійно проводилися кібернавчання, наприклад, у межах комплексних навчань колективних сил оперативного реагування одкб "взаємодія–2014". Сюди ж можна віднести приклади ефективних кібератак з боку рф. Американська компанія "FireEye", що спеціалізується на дослідженні проблем забезпечення міжнародної кібербезпеки, відкрито заявила, що група хакерів під кодовою назвою "APT28" тривалий час проводила інформаційні операції на замовлення російського уряду.

Незважаючи на це, сучасний стан забезпечення інформаційної та кібернетичної безпеки можна описати такими словами: високий рівень загроз. Call-центр прямої лінії з президентом рф зазнав масованої кібератаки з-за кордону, що була нібито "проведена з території України". Це зумовило підвищення рівня захисту інформаційної та кібернетичної безпеки країни. Тому у 2014 році було заявлено про створення у структурі міністерства оборони рф військ інформаційних операцій [3]. Слід зазначити, що ще

всередині 2013 року. Були створені так звані наукові роти у складі зс рф. Їх формальне завдання – виконання конкретних науково-прикладних завдань відповідно до наказів та в інтересах органів військового управління [4].

На сьогоднішній день рф веде активну політику щодо розвитку технологій та інформаційних систем, зокрема в галузі кібербезпеки. Уряд росії приділяє значну увагу розробці та впровадженню нових технологій та заходів, спрямованих на захист інформації та кіберпростору країни. Окрім створення самостійного Інтернету (“рунету”), основні напрямки діяльності рф у сфері кібербезпеки такі:

– ведення реєстру організаторів розповсюдження інформації, до якого входять багато популярних у росії сайтів та інтернет-сервісів: “яндекс”, “мамба”, “вконтакте”, “mail.ru” і “tinder” [5].

– обмеження користування закордонними інформаційними ресурсами, мінкомзв’язку має намір запровадити адміністративні штрафи для операторів зв’язку за використання іноземних супутникових мереж [6].

Незважаючи на зусилля уряду росії, рівень кіберзагроз та кібератак зросли протягом останніх років. Це пов’язано зі збільшенням використання Інтернету та інших інформаційних технологій, наявністю санкцій і розв’язаною війною. Більшість країн світу активно модернізують свої сектори безпеки, щоб відповідати викликам сучасності, особливо з огляду на використання Інтернету у військових цілях, як у випадку українсько-російської війни. Активна фаза протистояння в міжнародному кіберпросторі триває, що стимулює Україну та країни–члени НАТО розробляти нові стратегічні підходи до запобігання інформаційним та психологічним впливам з боку рф.

P.S. Ми використовуємо джерела з російськими доменами, оскільки для нас важливо отримати повну картину інформації щодо системи кібербезпеки рф, включаючи погляди нашого “ворога”. Для цього ми відвідуємо фахові онлайн форуми рф та аналізуємо відповідні дослідження.

Список використаних джерел:

1. Михалков и Пореченков создадут в России «патриотический интернет» URL: http://timeua.com/news/2/31214.html (дата звернення: 12.01.2023)
2. Россиянку, которая распространяла украинские новости в соцсетях, следственный комитет РФ записал в «Правый сектор» URL : http://surl.li/fvexh (дата звернення: 07.01.2023)
3. Источник в Минобороны: в Вооруженных силах РФ созданы войска информационных операций URL: http://tass.ru/politika/1179830(дата звернення: 22.02.2023)
4. Об утверждении Положения о научных ротах Вооруженных Сил Российской Федерации URL: http://surl.li/fvewy(дата звернення: 15.03.2023)
5. Мария Коломыченко, ФСБ потребовала ключи шифрования переписки пользователей у «Яндекса»//РБК URL : https://www.rbc.ru/t_echnology_and_media/ 04/06/2019/5cf50e139a79474f8ab5494b. (дата звернення: 12.01.2023)
6. Мінкомзв’язку запропонувало штрафувати операторів за підключення до іноземних супутників // URL: https://mbknews.appspot.com/news/minkomebo/(дата звернення: 17.01.2023)

ЗАСТОСУВАННЯ МЕТОДІВ КІБЕРАНАЛІТИКИ ДЛЯ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ КІБЕРАТАК НА ПІДПРИЄМСТВО

Скляренко П.А.,
аспірант,
Гаврилюк Д.М.,
магістрант факультету інформаційних систем і технологій,
ПВНЗ «Європейський університет»

В останні роки в Україні спостерігається значне зростання кількості кібератак на бізнес. Ці атаки становлять серйозну загрозу економічній безпеці підприємств і можуть призвести до значних фінансових втрат, шкоди репутації. Щоб вирішити цю проблему, впровадження методів кібераналітики стає все більш важливим для виявлення та запобігання кібератакам на підприємства. Зростання кількості кібератак на бізнес можна пояснити різними факторами, зокрема дедалі більшим використанням технологій у бізнес-операціях, зростаючою залежністю від Інтернету та відсутністю ефективних заходів кібербезпеки. Кіберзлочинці стали більш досвідченими та постійно розробляють нові методи зламу систем безпеки та отримання доступу до конфіденційної інформації. Відсутність заходів кібербезпеки та обізнаності в багатьох компаніях робить їх уразливими до цих атак. Крім того, зусилля українського уряду щодо боротьби з кіберзагрозами були недостатніми, а правова база кібербезпеки потребує вдосконалення [1,2].

Кібераналітика – це методологія збору, обробки та аналізу великих обсягів даних з метою виявлення кібератак та інших кіберзагроз. Цей підхід дозволяє підприємствам оперативно виявляти вразливості своїх систем і реагувати на них, перш ніж злочинці зможуть скористатися ними.

Методи кібераналітики включають використання алгоритмів машинного навчання та аналізу даних для виявлення та запобігання кібератакам. Ці методи можна застосовувати до різних типів даних, таких як мережевий трафік, системні журнали та поведінка користувачів. Кібераналітика може допомогти виявити аномальні моделі та поведінку, які вказують на кібератаку. Застосування методів кібераналітики також може допомогти підприємствам покращити реагування на інциденти та скоротити час і витрати, пов’язані з відновленням після кібератак [3,4] .

Впровадження кібераналітики в Україні потребує комплексного підходу, який передбачає поєднання технологій, політики та людей. Організації повинні інвестувати в передові рішення кібербезпеки, які інтегрують кібераналітику для виявлення та запобігання кібератакам. Вони також повинні розробити політику, яка сприятиме дотриманню кібергігієни та навчатиме співробітників найкращим практикам кібербезпеки. Крім того, організації можуть використовувати досвід фахівців з кібербезпеки для впровадження та

керування рішеннями кібераналітики. Щоб сприяти впровадженню методів кібераналітики в Україні, уряд має вдосконалити законодавчу базу кібербезпеки та підвищити обізнаність щодо важливості заходів кібербезпеки для бізнесу.

Підсумовуючи, загроза кібератак на підприємства в Україні є значною, а впровадження методів кібераналітики може бути ефективним інструментом у виявленні та запобіганні таким атакам. Однак, важливо усвідомлювати проблеми, пов'язані з впровадженням цих методів і інвестувати в необхідні ресурси для забезпечення їх ефективності. Завдяки цьому українські підприємства зможуть посилити заходи кібербезпеки та зменшити ризики, пов'язані з кібератаками.

Список використаних джерел:

1. В. Дейнека, «Загрози кібербезпеці та їхній вплив на економіку України», Journal of Security and Sustainability Issues, vol. 9, № 1, стор. 51-62, 2019.
2. Харченко А., Коваленко І. «Кібербезпека в Україні: поточна ситуація та шляхи її покращення», Journal of Cybersecurity and Information Management, vol. 3, № 1, С. 23-36, 2020.
3. Райт, А. (2018). Аналітика кібербезпеки: що повинен знати кожен спеціаліст із безпеки. Бока-Ратон: CRC Press.
4. Абад К., Лопес Р. та Сантос Н. (2019). Систематичний огляд машинного навчання для кібербезпеки: виявлення, класифікація та пом'якшення кіберзагроз. Журнал інформаційної безпеки та програм, 50, 102360.

БЕЗПЕЧНЕ ВИКОРИСТАННЯ БІБЛІОТЕК PYTHON З ВІДКРИТИМ ВИХІДНИМ КОДОМ

Слюсаренко Н.А.,
студент,
ПВНЗ «Європейський університет»

Мова Python стала однією із найпопулярніших за останні роки, і одна з головних причин полягає в тому, що вона має величезну кількість різних бібліотек з відкритим вихідним кодом, які є не лише безкоштовними, а й досить простими у використанні. Бібліотека – це набір кодів, які часто використовуються, і які розробники можуть включати в свої програми Python, щоб не писати код з нуля.

PyPI – репозиторій, що дозволяє будь-кому публікувати бібліотеки для Python. Плюси використання PyPI не обмежуються можливістю повторного використання коду, але й легкістю доступу.

Розробники можуть завантажити бібліотеку з будь-якого місця за допомогою pip. Проте проблема залишається: ненадійні учасники, які розміщують пакети на PyPI, і бібліотеки не завжди отримують належну

перевірку. І хоча більшість бібліотек PyPI є безпечними, шкідливе програмне забезпечення також може поширюватися в сховищі, якщо його не перевіряти.

Ця проблема стала очевидною в 2019 році, коли дві бібліотеки, що містять шкідливий код, було видалено з PyPI після їх публікації за допомогою техніки, відомої як тайпсквотинг. Бібліотеки jellyfish і dateutil були розділені на дві нові шкідливі бібліотеки під назвою jeLlyfish (з великою літерою L) і python-dateutil відповідно. Після встановлення вони поводились точно так само, як оригінали, за винятком спроби викрадення особистих даних у розробника.

Розглянемо найпоширеніші проблеми безпеки бібліотек з відкритим вихідним кодом:

- викрадення особистих даних: зловмисники можуть заволодіти бібліотеками, якими вже не займаються розробники через брак часу, і оновити код шкідливими файлами;
- тайпсквотинг: бібліотеки з іменами, з виду ідентичними оригіналу, тому розробники випадково встановлюють шкідливу бібліотеку, а не оригінал;
- вразливості залежностей: деякі бібліотеки залежать від інших бібліотек для реалізації своїх функцій. Коли одна залежна бібліотека має вразливість, це зрештою впливає на бібліотеку parent.

Щоб запобігти вищезгаданим проблемам при створенні програмного забезпечення, необхідно проаналізувати дії на кожному з етапів розробки:

Збір та аналіз вимог. Необхідно визначити які компоненти з відкритим кодом будуть включені в програмний продукт.

Дизайн. Необхідно дослідити інформацію Common Vulnerabilities and Exposures (CVE) (укр. поширені вразливості та ризики), щоб зробити залежності більш безпечними. Також слід провести оцінку, щоб обрати бібліотеки, які не містять великої кількості власних непрямих залежностей. Рекомендується перевірити та оцінити потенційну залежність перед тим, як її прийняти.

Оскільки перевірка залежності вручну може вимагати багато часу, можна використати відповідні інструменти – The Security Metrics Tool, Open Source Insights tool, Socket.dev та інші. Зменшивши кількість залежностей можна більш ефективно керувати вразливостями.

Розробка. Слід використовувати Sandbox (укр. пісочниця) при розробці – це копія робочої області комп’ютера без доступу до іншої частини мережі. Вона імітує систему та працює ізольовано, що захистить компанію у разі виникнення проблем із безпекою.

Не слід запускати будь-які команди менеджера пакетів як суперкористувач (sudo), оскільки код отримує необмежений доступ і можливості файлової системи.

Окрім того, слід ретельно перевіряти ім'я пакету під час введення його вручну в команді встановлення. Під час встановлення пакетів npm до команди встановлення слід додати позначку «-ignore-scripts», щоб вимкнути виконання будь-яких сценаріїв сторонніми пакетами.

Також слід віддавати перевагу пакетам PyPi, що розповсюджуються у форматі wheels, оскільки вони не виконують код у файлі setup.py автоматично під час встановлення.

Тестування. Використання статичного аналізу на етапі перевірки та тестування може допомогти виявити помилки як у програмному забезпеченні, написаному розробником, так і в коді, знайденому в залежностях.

Підтримка. Слід звернути увагу на підтримку залежностей в актуальному стані. Рекомендується видалення будь-яких невикористаних залежностей, функцій, компонентів, файлів або документації на етапі обслуговування, щоб зменшити вразливість програми до застарілих компонентів.

Отже, використовувати бібліотеки з відкритим вихідним кодом зручно, адже це економить час. З іншого боку, слід бути пильними, адже вони можуть надсилати персональні дані зловмиснику або записувати діяльність. Слід дотримуватись правил безпеки на всіх етапах розробки програмного забезпечення, щоб убезпечити себе і компанію від втрат.

Список використаних джерел:

1. What is Python? – Python Language Explained – Amazon AWS [Електронний ресурс] – Режим доступу до ресурсу: https://aws.amazon.com/.
2. *Aurore I.* Reasons why Python libraries are not secure [Електронний ресурс] / Inara Aurore – Режим доступу до ресурсу: https://spectralops.io.
3. National Security Agency Releases Guide on Mitigating Cloud Vulnerabilities [Електронний ресурс] – Режим доступу до ресурсу: https://www.securitymagazine.com/.

СУЧАСНІ РЕАЛІЇ КІБЕРБЕЗПЕКИ В АВТОМОБІЛЕБУДУВАННІ: ОСНОВНІ ЗАХОДИ ТА ВПЛИВ НА ЕКОНОМІКУ

Тарнавський А.С.,
аспірант,
ПВНЗ «Європейський університет»

Автомобільна кібербезпека набуває дедалі більшого значення для світових економічних процесів через зростання кількості транспортних засобів, робота яких залежить від комп'ютерних систем [1]. Якщо ці комп'ютерні системи не захищені належним чином, це може призвести до низки негативних наслідків.

По-перше, масштабна кібератака може спричинити значне порушення роботи транспортної мережі, що призведе до аварій, переривання ланцюжків

постачання, каскадного обвалу промислових процесів та навіть людських жертв. По-друге, потенційна мережева вразливість приватних транспортних засобів може призвести до втрати довіри споживачів до безпеки цих транспортних засобів. Це призведе до зниження попиту на автомобілі і завдасть шкоди автомобільній галузі в цілому. Також очікувано може значно зменшитися обсяг інвестицій в галузь, оскільки інвестори будуть вагатися, чи вкладати гроші в сектор, який є вразливим до кібератак [2].

Оскільки автомобілі стають все більш зв'язаними та автоматизованими, дуже важливо впровадити потужні заходи кібербезпеки, щоб гарантувати, що вони залишатимуться безпечними як для споживачів, так і для економіки в цілому. Існує ряд заходів безпеки, які виробники автомобілів впроваджують, щоб захистити свої транспортні засоби від кібератак. Ці заходи можна умовно поділити на дві категорії: превентивні та регулятивні.

Превентивні заходи безпеки спрямовані на запобігання потенційним кібератакам. Серед них виділяють наступні.

Брандмауери – це програмне забезпечення, яке моніторить вхідний та вихідний трафік комп'ютерної системи транспортного засобу. В разі виявлення спроби несанкціонованого доступу, програма блокує доступ системи до мережі.

Шифрування – процес кодування даних для запобігання несанкціонованому доступу. Більшість автовиробників використовують шифрування для захисту конфіденційних даних, таких як GPS-телеметрія, контрольні параметри силових агрегатів, система екстреного виклику, бази шифрів антиугінної системи та інші важливі дані.

Регулятивні заходи безпеки – це реагування на втручання, яке вже сталося. Наведемо далі основні з них.

Оновлення «по повітрю» – дистанційна доставка нових версій програмного забезпечення до комп'ютерного модуля транспортного засобу.

Це може допомогти швидко виправити виявлені слабкі місця та запобігти подальшим атакам або нівелювати наслідки атаки, що відбулася.

Плани реагування – чітко регламентована система заходів, розрахованих на те, щоб допомогти виробникам автомобілів швидко й ефективно реагувати на кібератаки, інформувати й захищати клієнтів.

Резервування даних – передбачає дублювання критичних систем і процесів, щоб гарантувати, що кібератака не призведе до повної відмови системи. Це може допомогти мінімізувати вплив атаки та запобігти простою.

Загалом, виробники автомобілів впроваджують багато різних заходів безпеки, щоб захистити свої транспортні засоби від кібератак. Оскільки автомобільна промисловість продовжує розвиватися та стає все більш уніфікованою, ми побачимо ще більш складні та прогресивні заходи безпеки, які будуть впроваджені для убезпечення, як транспортної, так і автомобілебудівної галузей [3]. Оскільки транспорт – це «кров» у жилах світової економіки.

Список використаних джерел:

1. Eden G. (July 2018) Transforming Cars into Computers: Interdisciplinary Opportunities for HCI (*Conference session*) Belfast, Northern Ireland. https://www.researchgate.net/publication/326232756_Transforming_Cars_into_Computers_Interdisciplinary_Opportunities_for_HCI
2. Why Automotive Cybersecurity Is Important. URL: https://www.eetimes.eu/why-automotive-cybersecurity-is-important/#:~:text=Cybersecurity%20is%20becoming%20a%20fundamental,put%20human%20lives%20at%20risk.
3. Soja R. (2014) Automotive Security: From Standards to Implementation. URL: https://www.nxp.com/docs/en/white-paper/AUTOSECURITYWP.pdf

КІБЕРБЕЗПЕКА В ДЕРЖАВНИХ УСТАНОВАХ США

Терешкін П.,
студент,
Українсько-американський університет Конкордія

Кібербезпека є однією з найбільш актуальних та нагальних проблем у сфері інформаційної безпеки. У сучасних умовах вона має велике значення для державних установ США, оскільки багато даних та інформації, що містяться в їхніх системах, є критичними та надзвичайно важливими для національної безпеки країни. У зв'язку з цим, відбувається постійне вдосконалення заходів забезпечення кібербезпеки державних установ США.

Зараз державні установи США використовують велику кількість технічних засобів та програмного забезпечення, що забезпечують безпеку їхніх інформаційних систем. Серед них можна виділити використання сучасних антивірусів, систем виявлення вторгнень та інших засобів захисту. Однак, на жаль, навіть найбільш сучасні заходи забезпечення кібербезпеки не є гарантією на 100% захисту від кібератак.

З метою підвищення рівня кібербезпеки, у державних установах США використовуються різні стратегії та підходи. Одним з таких підходів є використання принципу "найменшого доступу", що передбачає, що користувачі мають доступ лише до необхідних для їхньої роботи ресурсів та даних. Також, використовуються заходи, що передбачають регулярну зміну паролів та інших облікових даних, а також перевірку користувачів на предмет відповідності політиці безпеки.

У зв'язку зі зростанням кількості кібератак на державні установи США, останніми роками було прийнято низку заходів з підвищення рівня кібербезпеки. Одним з таких заходів є запровадження мережевого сегмента, що відокремлює критичні системи від інших частин мережі. Це дозволяє

підвищити рівень безпеки та забезпечити швидке виявлення та реагування на можливі кібератаки.

Також, державні установи США активно взаємодіють з іншими країнами та міжнародними організаціями з метою вдосконалення заходів забезпечення кібербезпеки та виявлення та протидії кіберзагрозам. Важливу роль у цьому відіграють міжнародні конвенції та угоди, такі як Конвенція про кіберзлочинність, яка була прийнята в Раді Європи у 2001 році та забезпечує міжнародне співробітництво у боротьбі з кіберзлочинністю.

Незважаючи на всі заходи та зусилля забезпечення кібербезпеки в державних установах США, проблема кібератак не зникає. Недавнім прикладом таких атак є кібератака на систему управління транспортом міста Атланти, яка сталася у 2018 році та призвела до відключення транспортних світлофорів та інших систем управління транспортом.

Отже, кібербезпека є надзвичайно важливою проблемою для державних установ США. У зв’язку з цим, вони приділяють велику увагу питанням забезпечення кібербезпеки та використовують різні заходи для підвищення безпеки своїх мереж та інформаційних систем. Проте, кібератаки продовжують ставатися, тому необхідно продовжувати вдосконалювати заходи забезпечення кібербезпеки та виявлення та протидії кіберзагрозам.

Список використаних джерел:

1. "Federal Cybersecurity Risk Determination Report and Action Plan", Office of Management and Budget, May 2018.
2. "Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure", The White House, May 2017.
3. "Protecting the Nation’s Critical Infrastructure from Cyber Threats", Department of Homeland Security, accessed March 2023.
4. "The Cybersecurity Information Sharing Act of 2015", U.S. Congress, accessed March 2023.
5. "The National Cyber Strategy", The White House, September 2018.

БЕЗПЕКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ В ХМАРНОМУ СЕРЕДОВИЩІ

Троян К.М.,
аспірант,
Скляренко О.В.,
к.ф.-м.н., доцент,
завідувач кафедри математичних дисциплін
та інноваційного проектування,
ПВНЗ «Європейський університет»

В останні роки хмарні обчислення (англ. *cloud computing*) стали головною парадигмою для надання послуг і управління даними в мережі Інтернет. Хмарні платформи надають підприємствам доступ до обчислювальних ресурсів, сховищ і додатків, дозволяючи їм швидко масштабуватися та зменшувати витрати. Однак, цей перехід до хмарних обчислень також приніс нові виклики кібербезпеці. Використання інфраструктури хмарних платформ вимагає комплексної стратегії безпеки, яка враховує унікальні загрози та вразливості, пов'язані з використанням хмарних платформ.

Наразі основні провайдери хмарних платформ, таких як Amazon Web Services, Azure й Google Cloud Platform, регулярно проходять аудити безпеки, такі як SOC 1/ISAE 3402, SOC 2, SOC 3, ISO 27001 й PCI DSS, результати яких доступні у відкритому доступі [1, 2, 3] і демонструють один з найвищих рівнів безпеки в галузі інформаційних технологій [4]. Проте, цей рівень безпеки стосується саме платформ, а не розгорнутого на них програмного забезпечення, що може містити вразливості, які можуть бути використані зловмисниками для отримання несанкціонованого доступу до конфіденційних даних або систем. Такі ризики особливо високі при використанні компонентів програмного забезпечення з відкритим кодом.

Іншим критичним аспектом для забезпечення безпеки є безпечна інфраструктура, яка використовується для розгортання програмного забезпечення, особливо це стосується використання системи контейнеризації програмного забезпечення Docker, що є фактичним стандартом у галузі через їх легкість і портативність. Однак, контейнери спільно використовують хостову операційну систему з іншими контейнерами, що може становити загрозу, якщо один контейнер було скомпроментовано. Зловмисники можуть використовувати вразливості в контейнерах, щоб отримати доступ до конфіденційних даних або розповсюдити шкідливе програмне забезпечення по всій інфраструктурі.

Згідно з недавнім дослідженням, більшість контейнерів Docker, які використовуються для наукових обчислень, містять велику кількість виявлених вразливостей [5]. Ці вразливості варіюються від проблем з високим ризиком, таких, як можливість віддаленого виконання коду, до менш

серйозних проблем, які можуть мати наслідком розкриття конфіденційної інформації [6]. Результати дослідження узгоджуються з результатами іншого опитування проведеного у 2019 році, яке проливає додаткове світло на стан кібербезпеки контейнерів у сучасній IT-галузі. Згідно з опитуванням, яке включало 269 IT-фахівців, відповідальних за роботу з хмарною інфраструктурою, значний відсоток організацій не впевнені в безпеці своїх контейнерів. Зокрема, 46% респондентів повідомили, що вони не впевнені у безпеці своїх контейнерів, а 47% зізналися, що мають у виробництві контейнери з відомими вразливостями [7]. За результатами звіту, опублікованому в 2023 році компанії Sysdig, що спеціалізується на безпеці хмарної інфраструктури, 87% образів контейнерів у виробництві мають критичні вразливості, що на 75% більше ніж у 2022 році [8]. Ці статистичні дані вказують на те, що переважна більшість організацій не вживають належних заходів і потенційно наражаються на серйозну небезпеку. Таким чином, існує очевидна потреба в тому, щоб організації приділяли пріоритет безпеці хмарної інфраструктури і гарантували, що їхні контейнери захищені від кіберзагроз.

Неможливо переоцінити важливість безпеки контейнерів, розгорнутих на хмарних платформах. У той час, як хмарні провайдери несуть відповідальність за безпеку своїх платформ, саме організації відіграють вирішальну роль у забезпеченні захисту своєї інфраструктури. Організаціям важливо прийняти комплексну стратегію кібербезпеки, що включатиме в себе передові практики, такі як регулярне сканування вразливостей, їх усунення та контроль доступу до даних, що може суттєво зменшити ризик успішних кібератак, запобігти витоку даних і фінансовим збиткам. Крім того, організаціям слід надати пріоритет навчанню та підвищенню обізнаності співробітників, щоб переконатися, що весь персонал знайомий зі стандартами кібербезпеки і може визначити потенційні загрози для інфраструктури. Впроваджуючи ці заходи, організації можуть значно підвищити рівень безпеки, захистити конфіденційні дані та зберегти довіру своїх клієнтів.

Список використаних джерел:

1. Earthpledge Foundation. (n.d.). Security and Compliance. Amazon. Retrieved March 20, 2023, from https://docs.aws.amazon.com/whitepapers/latest/aws-overview/security-and-compliance.html
2. Google. (n.d.). Google Cloud Security Whitepaper. Google security overview | documentation | google cloud. Retrieved March 20, 2023, from https://cloud.google.com/docs/security/overview/whitepaper
3. Stevevi. (n.d.). ISO/IEC 27001 – azure compliance. ISO/IEC 27001 – Azure Compliance | Microsoft Learn. Retrieved March 20, 2023, from https://learn.microsoft.com/en-us/azure/compliance/offerings/offering-iso-27001
4. Majhi, S. K., & Dhal, S. K. (2016). A study on security vulnerability on cloud platforms. Procedia Computer Science, 78, 55–60. https://doi.org/10.1016/j.procs.2016.02.010
5. Kaur, B., Dugré, M., Hanna, A., & Glatard, T. (2021). An analysis of security vulnerabilities in container images for scientific data analysis. GigaScience, 10(6). https://doi.org/10.1093/gigascience/giab025

6. Alyas, T., Ali, S., Khan, H. U., Samad, A., Alissa, K., & Saleem, M. A. (2022). Container performance and vulnerability management for Container Security using Docker engine. Security and Communication Networks, 2022, 1–11. https://doi.org/10.1155/2022/6819002
7. Saran, C. (2019, January 7). Almost half of containers in production have vulnerabilities, study finds: Computer Weekly. ComputerWeekly.com. Retrieved March 20, 2023, from https://www.computerweekly.com/news/252455307/Almost-half-of-containers-in-production-have-vulnerabilities-study-finds
8. Sysdig. (2023, February 1). Sysdig 2023 Cloud-Native Security and Usage Report. sysdig.com. Retrieved March 20, 2023, from https://sysdig.com/blog/2023-cloud-native-security-usage-report/

ОРГАНІЗАЦІЯ КІБЕРБЕЗПЕКИ УКРАЇНИ В УМОВАХ ВІЙНИ: СПЕЦИФІКА ТА ВИКЛИКИ, ЗАГРОЗИ ТА МЕТОДИ ПРОТИДІЇ

Частоколенко І.П.,
канд.фіз.-мат. наук., доц.,
доцент кафедри вищої математики та інформаційних технологій
Башук І.О.,
студентка 2 курсу,
Черкаський інститут пожежної безпеки імені Героїв Чорнобиля Національного університету цивільного захисту

У сучасному світі кібербезпека є одним із ключових елементів національної безпеки кожної держави. В Україні в умовах війни, коли військові та державні органи відчувають підвищену потребу в надійних і безпечних інформаційних системах, кіберфронт набуває особливої важливості.

Під час російського вторгнення в Україну було здійснено величезну кількість кібератак на сайти банків та державних установ Україну. Зокрема, 15 лютого 2022 року було вчинено найбільшу в історії країни DDoS атаку, яка була спрямована на банківський сектор, офіційні сайти органів влади, енергетичний блок та портал Дія.

Метою цієї доповіді є опис особливостей кібербезпеки у рамках військового конфлікту, розгляд проблем, з якими зіштовхується Україна у сфері кібербезпеки, та опис шляхів вирішення цих проблем з метою посилення кіберстійкості держави за будь-яких сценаріїв.

Специфіка та виклики кібербезпеки в умовах війни

Кібервійна полягає у здійсненні кібератак на інформаційні системи супротивника з метою внесення хаосу, руйнування, або злому критичної інфраструктури.

Такі атаки включають:

- Злом мережі. Наприклад, DDoS атаки, що навантажують мережеві ресурси великою кількістю трафіка та призводять до збоїв в їх роботі.

- Атаки на навігаційні системи. Наприклад, втручання у роботу глобальних систем, таких як GPS.
- Атаки на критичну інфраструктуру (енергоблок, водопостачання, транспорт, та інше).
- Атаки на фінансові системи.
- Атаки на хмарні сервіси. Кібератаки можуть також спрямовуватись на веб-сервери, бази даних, системи архівування та інші з метою отримання доступу до конфіденційних даних або зламу хмарної інфраструктури.

В умовах війни, коли військові та державні структури залежать від роботи критичної інфраструктури, пріоритетами кібербезпеки стають забезпечення її безперебійного функціонування та відновлення після можливих атак.

Відмінність кібератак від традиційних військових дій полягає: у їх швидкості та масштабах. Кібератаки можуть проводитись миттєво та одночасно впливати на велику кількість об'єктів, що робить їх ефективним засобом ведення війни. Такі атаки можуть призвести до значних руйнувань та втрат, особливо якщо супротивник недостатньо підготовлений до протистояння кіберзагрозам.

Кібербезпека в умовах війни стає крос-доменним питанням, що потребує координації дій та співпраці між різними сферами: військовою, державною, промисловою та громадською. Це вимагає розробки комплексних підходів до забезпечення кібербезпеки, а також взаємодії на міжнародному рівні для обміну інформацією про кіберзагрози та координації дій проти спільних ворогів.

Загрози кібербезпеки України та методи протидії кіберзагрозам

Україна зіштовхується із значним обсягом інформаційних та дезінформаційних операцій, спрямованих на дестабілізацію ситуації у країні та підрив довіри населення до державних інститутів. Ці операції можуть бути проведені через кібератаки на ЗМІ, соціальні мережі та інші комунікаційні канали.

В умовах війни, економічна стабільність та фінансова безпека держави відіграють важливу роль. Кібератаки на фінансові установи, економічні структури та системи можуть призвести до серйозних втрат та негативного впливу на економіку країни. Забезпечення кібербезпеки цих секторів є важливим пріоритетом для України в умовах війни.

Превентивні заходи:

- Регулярний аудит інформаційної інфраструктури: цей процес включає систематичну оцінку інформаційних систем та мереж з метою виявлення потенційних слабких місць та загроз, які можуть бути використані зловмисниками. Аудити допомагають організаціям виявляти неправильні конфігурації, вразливості та інші проблеми, що можуть підтримувати безпечність інформації та систем. Крім того, аудити

слугують контрольним засобом для перевірки дотримання політик та стандартів кібербезпеки.

- Підтримання оновлення інформаційної інфраструктури: оновлення програмного забезпечення, включаючи операційні системи, застосунки та мережеве обладнання, є важливим аспектом кібербезпеки. Відомо, що багато кібератак здійснюється шляхом використання відомих вразливостей в застарілому програмному забезпеченні. Регулярне оновлення програмного забезпечення допомагає закрити вразливості та захистити системи від потенційних атак.
- Резервне копіювання даних та створення резервних систем: регулярне резервне копіювання даних є – важливою складовою стратегії кібербезпеки. Воно допомагає забезпечити, що важлива інформація буде захищена від втрати або пошкодження внаслідок кібератак або системних збоїв. Резервні копії повинні зберігатися окремо від основних систем, якщо можливо, у інших місцях, щоб уникнути спільного впливу на обидва набори даних.
- Освіта та підготовка: кібернавчання, що включає тренінги та навчання співробітників військової, державної, промислової та громадської сфер. Також важливо створювати спеціалізовані навчальні програми та курси для підготовки фахівців у галузі кібербезпеки.
- Розробка планів відновлення після кіберінцидентів: план відновлення після кіберінцидентів включає ряд процедур та дій, які мають бути вжиті для відновлення систем, даних та мереж після кібератаки або іншого безпекового інциденту.

Отже, кібербезпека є ключовим аспектом сучасної війни, який вимагає уваги на рівні держави та військових структур.

Для протистояння кіберзагрозам необхідно зосередитись на розвитку кадрового потенціалу, зміцненні кібербезпеки інфраструктури, підвищенні обізнаності населення та підтримці міжнародної співпраці.

Забезпечення кібербезпеки України в умовах війни включає відповідні законодавчі та фінансові інструменти, а також злагоджену роботу всіх зацікавлених сторін.

Список використаних джерел:

1. Стратегія кібербезпеки України, (опублікована на сайті Міністерства цифрової трансформації України)
2. Національний план дій з кібербезпеки, (опублікована на сайті Міністерства цифрової трансформації України)
3. Кібербезпека та кібервійна: що всі повинні знати, П. В. Сінгер та Аллан Фрід
4. Кібербезпека для початківців, Рауль Чіс
5. Архів Міністерства цифрової трансформації України
6. Звіти Європейського агентства кібербезпеки (ENISA)
7. Звіти та аналітика НАТО з питань кібербезпеки
8. Звіти та аналітичні матеріали ООН з кібербезпеки

МОДЕЛЬ ЕШЕЛОНОВАНОГО КІБЕРЗАХИСТУ ІНФОРМАЦІЙНИХ СИСТЕМ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ

Шиповський В.В.,
Національний університет оборони України
імені Івана Черняховського

В сучасному світі кіберзахист інформаційних систем є надзвичайно важливим завданням, особливо для об'єктів критичної інфраструктури. Ешелонована архітектура кіберзахисту є ефективним інструментом для запобігання кібератак і зменшення їх впливу. Використання штучного інтелекту (ШІ) у математичних моделях кіберзахисту може значно покращити ефективність захисту від нових та невідомих загроз. У цих тезах буде представлена математична модель ешелонованої архітектури кіберзахисту інформаційних систем об'єктів критичної інфраструктури з використанням ШІ. Модель дозволяє врахувати взаємодію різних ешелонів захисту та адаптувати їх під поточні загрози, що дозволяє забезпечити ефективний захист від кібератак. Штучний інтелект (ШІ) може бути використаний для захисту інформаційних систем від кібератак. Розглянемо відомі методики кіберзахисту з застосуванням ШІ:

Методика захисту на основі машинного навчання.

Машинне навчання – це метод використання ШІ для навчання системи розпізнавати певні характеристики кібератак та приймати рішення про відповідні дії. В даній методиці ШІ навчається розпізнавати потенційно небезпечні дії, які можуть бути пов'язані з кібератаками, та приймати рішення про відповідні дії для захисту системи. Цей підхід дозволяє розпізнавати нові типи кібератак, які не були відомі раніше, та адаптувати систему захисту до нових загроз.

Методика захисту на основі аналізу поведінки.

Цей підхід базується на тому, що кіберзлочинці мають свій унікальний стиль атаки, тому ШІ може вивчити цей стиль та розпізнавати атаки на основі їх поведінки. В даній методиці ШІ аналізує поведінку користувачів та системи, щоб виявити незвичайні дії, які можуть бути пов'язані з кібератаками. Цей підхід також дозволяє виявляти нові типи кібератак та захищати систему від них.

В обох методиках, ШІ може навчатися на основі даних, які зібрані з попередніх кібератак або з інших джерел. Використання ШІ дозволяє покращити ефективність кіберзахисту та зменшити ризик виявлення небезпечних дій. У таблиці 1 таблиці порівнюються методики кіберзахисту з застосуванням штучного інтелекту на основі машинного навчання та аналізу поведінки за допомогою переваг та недоліків.

Таблиця 1

Методика	Переваги	Недоліки
Машинне навчання	– Може розпізнавати нові типи кібератак, які раніше були невідомі. – Дозволяє розвиватися та адаптуватися до нових загроз.	– Потребує багато даних для навчання. – Може бути складним у розумінні та конфігурації.
Аналіз поведінки	– Може виявляти кібератаки на основі їх унікального стилю. – Дозволяє виявляти нові типи кібератак та захищати систему від них.	– Може викликати більші кількості помилкових спрацювань, оскільки під час нормальної роботи системи може бути зареєстрована незвичайна поведінка. – Потребує збору великої кількості даних для навчання.

Архітектурна модель для методики "аналіз поведінки" може включати наступні елементи:

1. Вектор ознак – множина характеристик, які використовуються для опису поведінки об’єкта (наприклад, кількість запитів до бази даних, кількість невдалих авторизаційних спроб, кількість відправлених електронних листів тощо).

2. Алгоритм навчання – процес навчання моделі на основі векторів ознак. У процесі навчання можуть використовуватися різні алгоритми, такі як класифікація, кластеризація, асоціативне навчання тощо.

3. Модель класифікації – алгоритм, який використовується для виявлення аномальної поведінки в об’єкті. Модель може бути заснована на різних методах, таких як нейронні мережі, дерева рішень, метод опорних векторів тощо.

4. Метрики віддаленості – міра відстані між векторами ознак. Можуть використовуватися різні метрики, такі як Евклідова відстань, косинусна відстань, Манхеттенська відстань тощо.

5. Критерій порогового значення – критерій, який визначає, коли поведінка об’єкта вважається аномальною. Зазвичай, порогове значення встановлюється на основі статистичних даних та експертної оцінки.

6. Алгоритм виявлення аномальної поведінки – алгоритм, який використовує модель класифікації та критерій порогового значення для виявлення аномальної поведінки в об’єктах.

Зазвичай, модель аналізу поведінки використовується як частина системи кіберзахисту інформаційних систем, де вона працює в режимі реального часу. У процесі роботи система навчається на основі поведінки користувачів та невідомих атак, що дозволяє забезпечити більш ефективний кіберзахист.

Однак, математична модель аналізу поведінки також має свої недоліки, серед яких можна виділити наступні:

- Потребує багато часу на навчання моделі на великій кількості даних.
- Вимагає великої кількості ресурсів для обробки великих обсягів даних.

- Може спричинити помилкові срабатування, коли нормальна поведінка об’єкта вважається аномальною.
- Не здатна виявляти нові типи атак, які не були враховані при навчанні моделі.

Отже, при використанні математичної моделі аналізу поведінки необхідно враховувати переваги та недоліки цієї методики та забезпечувати постійне оновлення моделі для ефективного кіберзахисту.

Список використаних джерел:

1. Як працює machine learning та його застосування на практиці. URL: https://nachasi.com/tech/2019/01/31/yak-pratsyuye-machine-learning/
2. Як ШІ бореться з ключовими кіберзагрозами. URL: https://10guards.com/ua/articles/how-ai-handles-top-cybersecurity-threats/

АКТУАЛЬНІ ПОРАДИ ЩОДО БЕЗПЕКИ WI-FI МЕРЕЖІ

Яровий Р.О.,
к.т.н.,доцент кафедри економіки, фінансів,
обліку, математичних та інформаційних дисциплін
Польова А.В.,
старший викладач кафедри менеджменту
та соціально-гуманітарних дисциплін
Лєбєдєв Є.М.,
магістрант
Черкаська філія ПВНЗ «Європейський університет»

Wi-Fi – це технологія бездротової локальної мережі з пристроями на основі стандартів IEEE 802.11. На даний час, за простоти створення, Wi-Fi мережі набули широкого розповсюдження, в порівнянні з дротовими мережами. Але при використанні Wi-Fi мережі виникає низка проблеми які пов’язані з перехопленням вашого трафіку по Wi-Fi мережі і оволодінням вашими конфіденційними, фінансовими та особистими даними.

Щоб уникнути цього, краще вжити належні заходи, а саме:

1. Змініть ідентифікатор SSID вашої мережі.

Ідентифікатор SSID (Service Set Identifier – ідентифікатор набору служб) – це, по суті, ім’я точки доступу Wi-Fi. За замовчуванням, ідентифікатор SSID вашого роутера буде одним із таких:

– Фірмова назва та/або модель роутера, якщо ви придбали роутер безпосередньо у виробника.

– Ім’я вашого інтернет-провайдера, якщо ви придбали роутер у нього.

Якщо ім’я мережі збігається з моделлю роутера, це може становити загрозу безпеці. Тому що хакер може побачити ідентифікатор SSID і просто переглянути посібник з експлуатації роутера в Інтернеті. Якщо ви не змінили

дані авторизації, зловмисник може знайти цю інформацію та використовувати її для злому вашого роутера.

Якщо ідентифікатор SSID мережі – це ім’я вашого інтернет-провайдера, це не так погано, але все ж таки небезпечно. Хакер може використовувати цю інформацію для відправки атак фішингу вашому провайдеру з метою заволодіти вашою конфіденційною інформацією. Звичайно, це трапляється не так часто, але ризик завжди є.

Тому найкраще просто перейменувати свою мережу Wi-Fi. Не треба вигадувати щось надто химерне – жодних справжніх імен та адрес. Просто абстрактна, непомітна назва.

2. Не використовуйте пароль та ім’я користувача за замовчуванням.

Практично кожен роутер має пароль і логін, присвоєні за замовчуванням. Це дозволяє власникам роутерів легко отримати доступ до управління роутером. Саме тому вам потрібно змінити ім’я користувача та пароль. При цому треба враховувати:

– Використовуйте пробіли, якщо це можливо.

– Не використовуйте словникові слова. Якщо ви використовуєте ці слова, просто напишіть літери в них у зворотному порядку.

– Чергуйте великі та малі літери, цифри та символи.

– Придумайте пароль та ім’я користувача, що складаються щонайменше з 15 символів.

– Уникайте очевидних замін (наприклад, "$" замість "s").

І обов’язково регулярно змінюйте пароль та ім’я користувача. Крім того, якщо у вас є кілька роутерів, краще використовувати диспетчер паролів, щоб вам було простіше запам’ятати їх.

3. Не давайте нікому свій пароль від Wi-Fi.

Можна ділитися своїм паролем від Wi-Fi зі своїми дітьми або близькими друзями, але не потрібно давати його кожному, хто приходить до вашої оселі.

Для цього є можливість налаштування гостьової мережі. Таким чином, ви можете запропонувати своїм гостям доступ до Wi-fi, і вам не доведеться турбуватися про конфіденційність вашої основної мережі.

4. Використовуйте на своєму роутері шифрування WPA2

Шифрування Wi-Fi гарантує, що небажані користувачі матимуть обмежений доступ до вашого Wi-Fi та всіх пов’язаних з ним даних. У роутера може бути шифрування WEP, WPA та WPA2. В ідеалі краще не використовувати шифрування WEP та WPA, тому що вони значно застаріли і можуть бути легко зламані кіберзлочинцями. Тому, перевіряйте, чи працює на вашому роутері WPA2.

Також рекомендується регулярно оновлювати прошивку, але це не гарантує повного захисту від кібератаки KRACK.

5. Налаштуйте підключення до VPN на своєму роутері.

VPN – це онлайн-сервіс, який ви можете використовувати для приховання вашої реальної IP-адреси за допомогою шифрування Інтернет-з’єднання. Це відмінний сервіс при використанні загальнодоступного Wi-Fi,

тому що він гарантує, що ніхто не може контролювати те, що ви робите в Інтернеті.

Також ви можете використовувати VPN на своєму роутері просто у себе вдома. У цьому випадку вам навіть не потрібно турбуватися про те, що кіберзлочинець може зламати ваше шифрування, тому що шифрування VPN забезпечить додатковий захист. Більше того, VPN на роутері захистить вас від злому WiFi-мережі.

6. Не залишайте Wi-Fi мережу увімкненою, коли не користуєтеся нею.

Один із способів знизити ризик злому вашої мережі Wi-Fi – просто відключати її, коли вона вам не потрібна. Крім того, крім додаткового захисту, вимикання роутера на період, поки ви знаходитесь поза домом, захистить його від випадкових перепадів електроенергії, допоможе вам трохи заощадити на електриці, а також захистити навколишнє середовище.

7. Розмістіть роутер у центрі будинку.

Якщо ви розмістите роутер близько до вікна, частина сигналу піде назовні, і перехожі зможуть зловити його на своїх мобільних пристроях. У той же час, якщо роутер стоїть надто близько до стіни, то висока ймовірність, що ваш сусід може зловити сигнал вашого Wi-Fi.

8. Вимкніть віддалений доступ.

Віддалений доступ іноді дуже зручний, тому що він дозволяє керувати роутером через Інтернет без використання пристрою, підключеного до домашньої мережі Wi-Fi. Це чудовий спосіб вирішити проблеми або змінити налаштування, якщо ви не вдома. Однак віддалений доступ також має недоліки. Якщо ви можете використовувати Інтернет для віддаленого доступу до роутера, то досвідчений хакер теж зможе. Вам точно не захочеться, щоб хакер зламав ваш обліковий запис і використовував вашу мережу, щоб оволодіти конфіденційними даними. Тому вимкніть цю функцію, якщо вона увімкнена.

9. Встановіть захист від вірусів та шкідливих програм.

Так, сервіси для захисту від шкідливих програм та вірусів для роутерів насправді існують. Можливість їхнього налаштування повністю залежить від марки роутера. Це додатковий захід для захисту домашнього Wi-Fi.

Захист від шкідливих програм та вірусів для Wi-Fi мережі може бути як у програмному, так і апаратному форматах.

10. Переконайтеся, що фаєрвол роутера включено.

Більшість роутерів мають вбудований фаєрвол. Фаєрвол – гарний спосіб додаткового захисту для домашнього Wi-Fi, оскільки він може бути налаштований для запобігання використанню вашої мережі для шкідливого трафіку. Якщо ваш роутер не має вбудованого фаєрволу, ви можете придбати апаратний. Більшість сервісів, про які ми згадували вище, добре працюють.

11. Вимкніть UPnP (Universal Plug n Play).

UPnP насправді дуже корисний для роутера, оскільки він дозволяє йому взаємодіяти з веб-сайтом виробника для завантаження оновлення та інших файлів. UPnP – це протокол, який дозволяє інтелектуальним пристроям

підключатися до Інтернету для отримання інтелектуальних функцій. На жаль,UPnP також можуть легко використовувати хакериу своїх цілях. Саме тому краще відключити можливості та сумісність UPnP на роутері та смарт-пристроях.

12. Не використовуйте WPS (WiFi Protected Setup – стандарт безпеки бездротової мережі). WPS є досить зручним, оскільки пропонує альтернативні способи підключення до домашньої мережі Wi-Fi, ніж просто введення довгого пароля. Такі способи включають:

– Введення восьмизначного PIN-коду.

– Натисніть кнопку WPS на роутері.

Набагато простіше, так? Це правда, але є одна велика проблема – використання WPS є досить ризикованим, і ставить безпеку вашого Wi-Fi під загрозу.

13. Тримайте прошивку роутера в актуальному стані.

Якщо ви не оновлюєте прошивку вашого роутера регулярно, то ви наражаєтеся на всілякі потенційні кіберзагрози. Завдяки оновленню прошивки можна виправити критичні помилки, які дозволяють хакерам отримати доступ до вашого роутера.

14. Використовуйте фільтрацію MAC-адресу.

Багато роутерів мають опцію «Фільтрація MAC-адрес» або «Фільтрація MAC».

Фільтрація MAC в основному ефективна, коли ви хочете зберегти Wi-Fi від сусідів, які дізналися ваш пароль від вас, ваших друзів або ваших дітей.

15. Слідкуйте за портами.

Мати відкритий порт – вже саме собою достатній ризик безпеки, але якщо це ще й відкритий порт, який можна легко зламати – це ще небезпечніше.

Процес сканування портів може бути активований лише всередині мережі, Якщо порт відкритий, то вам потрібно якнайшвидше зв’язатися з постачальником роутера і попросити його про допомогу. Зазвичай постачальники можуть вирішити цю проблему (наприклад, патч). На жаль, якщо ви просто закрили порт, це не вирішить проблему. Він уже був відкритий один раз, тому його можна відкрити знову.

16. Приховайте SSID вашої мережі.

Якщо у вас є домашня мережа Wi-Fi, не потрібно роздавати її будь-кому. Найкраще відключити SSID, щоб воно не привертало уваги кіберзлочинців. Це також допоможе вам уникнути необхідності відмовляти вашим гостям у підключенні до вашого Wi-Fi, оскільки вони просто побачать «Приховану мережу» або взагалі нічого не побачать у своєму списку доступних мереж Wi-Fi.

17. Захистіть пристрої, які завжди підключені до вашого Wi-Fi.

Немає сенсу захищати домашній Wi-Fi, якщо не захищати пристрої, які постійно підключені до вашої мережі. Наприклад, ноутбук чи мобільний телефон. Якщо їх зламають, а ви підключаєте їх до своєї мережі Wi-Fi, її теж можуть зламати.

Список використаних джерел:

1. S.J., Hussain, M., Irfan, N.Z., Jhanjhi, et al. (2020). Performance Enhancement in Wireless Body Area Networks with Secure Communication. Wireless Pers Commun (2020). https://doi.org/10.1007/s11277-020-07702-7 [2].
2. K. Ramesh Rao, "Wireless Communication Security and Privacy issues and Challenges", Academia.edu, 2017. [Online]. Available: https://www.academia.edu/34148630/Wireless_Communication_Security_and_Privacy_issues_and_Challenges. [Accessed: 04– Jul– 2020].
3. Alferidah, D.K. and Jhanjhi, N.Z. (2020). A Review on Security and Privacy Issues and Challenges in Internet of Things. IJCSNS International Journal of Computer Science and Network Security, VOL.20 No.4, April 2020.
4. M. Almulhim and N. Zaman, "Proposing secure and lightweight authentication scheme for IoT based E-health applications," 2018 20th International Conference on Advanced Communication Technology (ICACT), Chuncheon-si Gangwon-do, Korea (South), 2018, pp. 481-487, doi: 10.23919/ICACT.2018.8323802.

ВРАЗЛИВОСТІ СИСТЕМИ «РОЗУМНИЙ БУДИНОК»

Яровий Р.О.,
к.т.н., доцент кафедри економіки, фінансів,
обліку, математичних та інформаційних дисциплін,
Савченко Р.О.,
Притула В.О.,
Слободяник С.С.,
студенти факультету інформаційних технологій,
Черкаська філія ПВНЗ «Європейський університет»

Концепція "Розумний будинок" базується на повсюдному впровадженні наступних технологій: бездротові мережі, хмарні обчислення, міжмашинна взаємодія. Ця концепція набирає популярності, і все більше проникає у повсякденне життя людей, тому зростають і ризики інформаційної безпеки.

В першу чергу ризики пов’язані, з особистими даними людини. Наприклад відстеження руху людини по дому, контроль стану людини, банківські реквізити, інформацію про сторінки, які відвідувала людина і т.д. Вся ця інформація накопичується у базі розумного будинку і надається різним сервісам, що полегшує життя людини.

При аналізі вразливості системи "Розумний будинок" було виявлено наступне:

1. Вразливість механізму автентифікації користувача.

Управління компонентами системи "Розумний будинок" має вестись тільки після автентифікації користувача та його дальньої авторизації. Зважаючи на те, що управління найчастіше відбувається за допомогою смартфона або з іншого портативного пристрою, що з’єднується за допомогою бездротової зв’язку, виникає загроза перехоплення ідентифікації.

Перехоплення може бути реалізований через впровадження шкідливого програмного забезпечення у пристрої системи "Розумний дім", використання вразливостей програмного забезпечення пристроїв, прослуховування каналу зв’язку керуючого пристрою (наприклад, смартфона користувача системи "Розумний будинок") з пристроями системи "Розумний дім" і т.д.

2. Відсутність повноцінних антивірусних систем, що забезпечують комплексний захист від шкідливого програмного забезпечення, розроблених спеціально для систем розумного будинку, немає. Більш того, програмний код, властивий вірусам для систем "Розумного будинку", не знаходиться більшістю сканерів сигнатур .

Розглянемо основні вразливості в програмне забезпечення систем "Розумного будинку", якими користуються зловмисники для впровадження шкідливих програм:

– відсутність можливості блокування підключень неавторизованих пристроїв;

– відсутність контролю над широкомовним розсиланням датаграм у мережі "Розумного будинку";

– відсутність автентифікації керуючої програми, що передає пакети в мережу "Розумного будинку".

3. Необхідність наявності захищених каналів зв’язку.

Переважне використання бездротового зв’язку для комунікації пристроїв один з одним – все це вимагає наявності захищених каналів зв’язку в системі "Розумний будинок". Несумлінна реалізація протоколів захисту інформації на одному з пристроїв може призвести до компрометації всіх даних, що циркулюють у системі.

– канал Bluetooth є вкрай ненадійним і легко може прийняти файл з вірусом від зловмисника, не запитавши аутентифікаційних даних;

– по каналу Wi-Fi зловмисник може авторизуватися у внутрішній мережі Wi-Fi "Розумного дому" та впровадити шкідливе програмне забезпечення;

– вразливості HTTP-каналу, за яким пристрої із системи "Розумний будинок" зв’язуються із зовнішньою мережею Інтернет, добре вивчені та можуть дозволити зловмиснику отримати контроль над "Розумним будинком", навіть не перебуваючи у його локальній мережі;

– через канал GSM зловмисник може відправити керуючі команди "Розумному дому", підмінивши свій номер номером санкціонованого користувача;

– якщо мережа "Розумного будинку" також знаходиться і в іншій локальній мережі, то шкідливе ПЗ також можна впровадити з останньої.

4. Потенційні уразливості системи "Розумний будинок" через функціонування в ній пристроїв від різних виробників.

Різні компанії розробляють аналогічні пристрої із можливим використанням своїх власних внутрішніх (нестандартизованих) протоколів обміну даними.

З огляду на це, впровадження пристроїв від різних виробників у систему "Розумний дім" тягне за собою потенційну наявність вразливості інформаційної безпеки (наприклад, некоректна реалізація захищеного з'єднання між двома пристроями).

Така проблема може бути вирішена придбанням готової системи одного виробника. Однак, по-перше, компаній, що виробляють повноцінну систему "Розумний дім", на даний момент на ринку представлено мало; по-друге, як показали недавні дослідження незалежної організації AV-TEST в галузі інформаційної безпеки IoT, у багатьох виробників рівень захищеності систем "Розумний будинок" знаходиться на низькому рівні.

5. Наявність вразливості у певних пристроях.

Пристрої системи "Розумний будинок" володіють різним функціоналом і набором завдань. Відповідно, пристрої мають різні вразливості:

– Smart TV. Більшість сучасних Smart-Телевізорів оснащені камерами. При недостатній захищеності системи "Розумний дім" зловмисники можуть використовувати дані камери для стеження за користувачами даної системи та приміщенням в цілому;

– Smart fridges. Холодильники в "Розумному будинку" перевіряють термін придатності продукції, аналізують їжу, що зберігається в ньому, і складають список продуктів, які потрібно буде купити господареві будинку. Отримавши контроль над цими даними, порушник може дізнатися, коли в будинку перебувають люди, а коли їх немає, тим самим сприяючи своєму подальшому проникненню в дім;

– Smart Cars. Згідно з останніми дослідженнями, зловмисники можуть отримати контроль над операційними системами "розумних" пристроїв. Таким чином, вони можуть здійснювати керування всіма компонентами системи;

– система автоматизованого управління будинком. Вона є головною системою "Розумного будинку", забезпечуючи контроль, у тому числі, за дверима, вікнами, зовнішніми та внутрішніми камерами, а також сигналізаціями. Отримавши контроль над нею, порушник може безслідно зробити фізичне проникнення на територію будинку.

6. Методи підвищення захищеності системи "Розумний будинок"

На основі проведеного аналізу вразливості системи "Розумний будинок" рекомендується наступне:

– встановлювати пароль високої складності на профіль адміністратора системи;

– своєчасно оновлювати ПЗ пристроїв системи "Розумний будинок" до останньої версії;

– встановити системи стеження за несанкціонованим доступом до системи "Розумний дім";

– налаштування мережі VPN для системи "Розумний будинок";

– встановлювати міжмережні екрани (файрволи) на межі локальної мережі системи "Розумний будинок", а також налаштовувати антивірусне програмне забезпечення під свої потреби;

– використовувати рішення для системи "Розумний будинок" від одного виробника для уникнення потенційних вразливості.

Список використаних джерел:

1. IoT Privacyand Security Challenges for Smart Home Environments. Базель, Швейцарія, 2016. URL: https://www.mdpi.com/2078-2489/7/3/44/htm
2. Alferidah, D.K. and Jhanjhi, N.Z. (2020). A Review on Security and Privacy Issues and Challenges in Internet of Things. IJCSNS International Journal of Computer Science and Network Security, VOL.20 No.4, April 2020.
3. M. Almulhim and N. Zaman, "Proposing secure and lightweight authentication scheme for IoT based E-health applications," 2018 20th International Conference on Advanced Communication Technology (ICACT), Chuncheon-si Gangwon-do, Korea (South), 2018, pp. 481-487, doi: 10.23919/ICACT.2018.8323802.

АКТУАЛЬНІ ПИТАННЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

Матеріали

IX Міжнародної науково-практичної конференції

30 березня 2023 р.

Підписано до друку 19.05.2023. Формат 60x841/16.
Папір офсетний. Гарнітура Times New Roman.
Ум. друк. арк. 7,09.
Зам. № 23.

Друк: поліграфкомбінат Європейського університету.
03115, Україна, Київ-115, вул. Депутатська, 15/17.

Реєстраційне свідоцтво ДК №3833 від 14.07.2010 р.