6.Офіційний сайт Tor [Електронний ресурс] – Режим доступу до ресурсу: https://www.torproject.org/about/reports/.

7.Tor: Pluggable Transports [Електронний ресурс] – Режим доступу до ресурсу: https://2019.www.torproject.org/docs/pluggable-transports.

8. Бертсекас Д., Галлагер Р. Сети передачи данных: Пер. с англ.- М.: Мир, 1989.- 544 с.

9.Анонимный браузер TOR - что это такое? [Електронний ресурс] – Режим доступу до ресурсу: http://procomputer.su/program-obespechenie/118-anonimnyj-brauzer-tor-chto-eto-takoe.

10. Анонимность в сети с помощью Tor Browser [Електронний ресурс] – Режим доступу до ресурсу: https://safe.roskomsvobodaorg/tor/.

УДК: 004.056.53

ДО ПИТАННЯ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Марченко В. С., студ. гр. КБ-161, **Ткач Ю. М.,** д.пед.н., доц.
Національний університет «Чернігівська політехніка»

Кожен день збільшується кількість організацій і підприємствах котрі використовують для своєї роботи інформацію котру потрібно захищати. Дуже велику роль грає технічний захист даної інформації від зловмисників, але ще впливає на захист людський фактор, а саме знання працівників у сфері захисту інформації.

Від витоку інформації колами електроживлення я порекомендую використати фільтри ЕМСБІ типу ФЗП103-2 котрі надійно захищають в широкому у межах частот – починаючи зі звукових (10 кГц) до надвисоких (1000 МГц) або Засіб активної оборони автоматизованих систем «DELTA-7» котрий створює захисні перешкоди у межах частот від 9 кГц до 3,3ГГц, підлаштованні до частотного розподілу приладів.

Пристрій «KVS-3000» призначений для створення електромагнітних завад в смузі частот від 9 кГц до 2 ГГц з метою захисту інформації від витоку каналами побічних електромагнітних випромінювань і наведень в інформаційно-телекомунікаційних системах та на об'єктах електронно-обчислювальної техніки. За своїх технічних характеристик він дозволяє створювати захист інформації від її витоку по лініях електроживлення і заземлення.

Трансформатор розділовий з екранованої обмоткою потужністю 10 кВт "PIAC-4TP / 10" його призначення для гальванічної розв'язки і технічного захисту інформації в однофазних і двофазних ланках мережі електроживлення напругою яка становить до 250 В, частотою 50 Гц від її витоку через канал, який створюється за рахунок акустично-електричних перетворень і паразитних модуляцій мовних сигналів високочастотного сигналу "накачування", створюваного засобами технічної розвідки.

Для захисту від витоку інформації акустичним і віброакустичним каналом я порекомендую використати генератор "Топаз ГША-4" спільно з вібро-акустичним випромінювачем "Топаз ВІ-1" котрий забезпечує захист за допомогою маскування можливої інформації, при реалізації методу енергетичного приховування акустичного і вібро-акустичного небезпечного сигналу, що виникає під впливом мови на повітря і навколишні конструкції приміщення. Або БАЗАЛЬТ-4ДА, котрий активно захищає мовну інформацію від витоку акустичним і віброакустичним каналом.

Для захисту мережевих даних я використав би Фаєрвол Fortinet FG-300D- це пристрій мережевої безпеки котрий пропонує комплексну мережевий захист на одній платформі, з однієї операційної системи мережевої безпеки і з єдиною системою управління в одному вікні на основі заданих правил, що забезпечує максимальний захист підприємств від цільових атак і безперервно удосконалюються загроз для безпеки. Він дуже потужний і за це він може забезпечувати комплексний мережевий захист для середніх компаній, філій і відділень. В

обладнанні встановлений швидкий і продуктивний процесор, що забезпечує обробку даних до швидкості 8 Гбіт / с, незалежно від пропускної здатності внутрішніх каналів зв'язку

Для захисту даних котрі передаються телефонними лініями від витоку інформації я пораджу «Базальт-31» котрий забезпечує захист важливої мовної інформації яка циркулює в телефонній лінії на підприємстві і організації. Даний прилад встановлюється в середину лінії він проводить захист при покладеної трубки телефонах,

Маршрутизатор AR2200 під управлінням операційної системи V300R019 він може масштабуються та надавати безпечні і уніфіковані послуги передачі голосу і даних для головних офісів і філій середніх підприємств. Функції маршрутизації і комутації рівня 8 Гбіт / с це все улаштовано в один пристрій и за це ми тратимо менше грошей

Підтримка Native WLAN в поєднанні з неблокувальною архітектурою комутаційної матриці забезпечує стійку мультимедійний зв'язок з комплексними функціями безпеки, якій включає в себе вбудований міжмережевий екран і постійно оновлювані механізми захисту від шкідливих атак.

Модульна конструкція AR2200 дозволяє налаштовувати і оновлювати порти в міру необхідності - від модулів цифрової обробки сигналів (DSP) до «розумних інтерфейсних плат» (SIC) для індивідуальної настройки швидкостей і інтерфейсів.

Комутатор Cisco® Catalyst® серії 3850 належить до наступного покоління стекових комутаторів рівня доступу корпоративного класу, забезпечують повну конвергенцію між дротяними і бездротовими мережами на одній платформі. Даний комутатор підтримує програмне забезпечення для маршрутизації по IPv4 і IPv6, багатоадресну маршрутизацію, модульні функції якості обслуговування (QoS), FlexibleNetFlow (FNF) версії 9 і розширених функцій безпеки,

Маршрутизатор Cisco ISR 4400 це модульний маршрутизатор з доступом до локальної та глобальної мережі. Він підтримує різні інтерфейсні модулі, в яких вмонтовано сервісні модулі Cisco (SM-X) і модуль мережевого інтерфейсу (Network Interface Modules, далі - NIM) Cisco.

Ethernet Комутатор Edge-Core ECS4120-28F-це Gigabit Ethernet комутатор рівня доступу з 4 роз'ємами 10G uplink. Комутатор ECS4120-28F дуже добре підходить для мереж які розвертаються на підприємствах, мереж малого і середнього бізнесу, а також Підприємств які надають услуги інтернета (ISP) і операторів різноманітних систем (MSO) для надання послуг Triple-Play з пропускною спроможністю до 1G.

Маршрутизатор HPE серії MSR93x призначені для невеликих філій. Ці компактні пристрої оснащені інтегрованими функціями маршрутизації, забезпечення безпеки, SIP, підключення через WLAN 802.11n і 4G LTE або 3G. Конвергентна інфраструктура, єдиний інтерфейс управління і автоматизоване розгортання прискорюють обслуговування і підвищують продуктивність, а також знижують складність мережі. Пристрої HPE MSR93x підвищують гнучкість і адаптивність інфраструктури завдяки підтримці розширених можливостей підключення і компактному фіксованому форм-фактору.

Мережний крипто модуль «Гряда-301» призначений для апаратної реалізації криптографічних перетворень у складі центральних серверів центру сертифікації ключів (ЦСК)

Електронний ключ «Кристал-1»- це апаратний засіб криптографічного захисту інформації, що виконаний у вигляді малогабаритного USB-пристрою та використовується в якості носія ключової інформації

Висновок: На даний час дуже мала кількість організацій або підприємств задумуються про технічний захист інформації яка циркулює між різними вузлами передачі інформації, Один вагомий мінус полягає в тому що прилади технічного захисту на даний час коштують не маленькі гроші, але якщо порахувати збитки які можуть завдати дані витоки інформації то ціна не велика . Отже потрібно розрахувати всі ризики і зрозуміти чи необхідно тратити такі гроші на прилади чи ні на вашому підприємстві або організації.

Список використаних джерел

1. http://emsbi.ua/fzp-103-2
2. https://tzi.com.ua/bazalt-31.html
3. https://romsat.ua/products/telecommunication-equipment/ethernet-kommutator-switch/edge-core-ecs4120-28f/
4. https://e.huawei.com/kz/products/enterprise-networking/routers/ar-g3/ar2200

УДК 004.056.5

ДОСЛІДЖЕННЯ СИСТЕМ ЗАХИСТУ БАЗ ДАНИХ

Махняєва К. С., студ. гр КБ-161
Науковий керівник: **Гур'єв В. І.,** к.т.н., доцент
Національний університет «Чернігівська політехніка»

В результаті зростання кількості інформації значними темпами поширюється використання баз даних, а з цим і зростає кількість кіберзлочинців. Кожен день зламується велика кількість баз даних, і часто трапляється, що власник бази даних може не дізнатись, що його база зламана, і з неї іде витік інформації. Ця теза стосується питання про те, як закон про захист даних повинен реагувати на проблеми, що виникають у зв'язку з постійно зростаючою поширеністю великих даних.

Розслідування проводиться на прикладі вивчення поведінкової реклами в Інтернеті (ОВА) і в рамках нормативно-правової бази ЄС про захист даних, особливо Загального регламенту захисту даних (GDPR). Стверджується, що закон про захист даних повинен відповідати на проблеми з великими даними, використовуючи можливості регулювання, які вже існують в поточному правовий режим або потенційно доступні для політиків. З дуже складною, потужною і непрозорою мережею ОВА, як в технічному, так і в економічному плані, використання великих даних може представляти фундаментальну загрозу певним індивідуалістичної, колективним або суспільним цінностям. Незважаючи на обмежене число економічних вигод, таких як безкоштовний доступ до онлайн-сервісів і зростання цифрового ринку, приховані ризики ОВА вимагають ефективного режиму регулювання великих даних. Росс Андерсон часто казав, що по своїй природі більша кількість баз даних ніколи не буде свободна від зловживань в результаті порушень безпеки. Якщо велика система предназначена для полегшення доступу, вона стає небезпечною. Якщо зроблена водонепроникна, стає неможливо використовувати.

Хоча GDPR ЄС являє собою новітню і найбільш всеосяжну правову базу, яка регулює використання персональних даних, він все ще не досяг певних важливих аспектів. Нормативна модель, яка характеризується індивідуальним згодою і перевіркою необхідності, залишається недостатньою для повного захисту суб'єктів даних як автономних осіб, споживачів і громадян в контексті ОВА.

Таким чином, існує нагальна необхідність для політиків переглянути свої інструменти регулювання в світлі потенційних загроз. З одного боку, необхідно переглянути можливості внесення в чорний список або внесення в білий список певних видів використання даних за допомогою механізмів, які або існують в правовій базі, або можуть бути введені додатково. З іншого боку, також необхідно реалізувати весь спектр варіантів політики, які можуть бути прийняті, щоб допомогти людям в прийнятті обґрунтованих рішень в епоху великих даних.

Список використаних джерел

1. Wikipedia Database security [Електронний ресурс]. Режим доступу: URL: https://ru.wikipedia.org/wiki/Database_security – Назва з екрану.
2. Data protection in the age of Big Data [Електронний ресурс]. Режим доступу: URL: https://era.ed

---