1. Методи і засоби автентифікації біометричних даних в інформаційних системах [Текст] / Я.П.Кісь, В.М.Теслюк. // ACTUAL PROBLEMS OF ECONOMICS #12(138), 2012. – С. 174-180.
2. Бурячок, В. Алгоритм оцінювання ступеня захищеності спеціальних інформаційно – телекомунікаційних систем [Текст] / В. Л. Бурячок // Захист інформації. НАУ. - К. – 2011. - №3. – С. 1-9.
3. Мороз А.О. Біометричні технології ідентифікації людини. Огляд систем. [Текст] // Математичні машини і системи / Інститут проблем математичних машин і систем НАН України. – 2011. - №1. – С. 39- 45. – ISSN 1028-9763.

КРИВЕНКО С. В., к.т.н., доцент
кафедри математичних методів та
системного аналізу,
Маріупольський державний
університет

УДОСКОНАЛЕННЯ СИСТЕМНОЇ БЕЗПЕКИ МЕРЕЖ ПРОМИСЛОВОЇ КОМУНІКАЦІЇ

Кількість кібератак на промислові мережі неухильно зростає. У промисловості об'єктами кіберзагроз можуть ставати розподілені системи управління (РСУ), програмовані логічні контролери (ПЛК), системи збору даних (SCADA-системи) і елементи людино-машинного інтерфейсу (HMI). На сьогодні один з ключових факторів вразливості - загальна низька культура процесів забезпечення кібербезпеки. На багатьох підприємствах не проводиться оцінка ключових ризиків, не забезпечується безпечне управління операціями, включаючи базове управління паролями. Відсутній комплексний аудит, не гарантується злагоджене та ефективне дотримання політик безпеки, недооцінюються доступні інструменти контролю і виявлення загроз. Навіть в сучасному світі досить поширеними проблемами залишаються недостатній контроль фізичного доступу на територію, недбале ставлення до процедур авторизації і аутентифікації при вході в корпоративні та промислові мережі (наприклад, занадто легкі, рідко змінювані паролі).

Програмно-апаратними лазівками для зловмисників можуть ставати незахищені канали віддаленого доступу, неадекватні міжмережеві екрани, неправильно вибудувана архітектура мережі, в тому числі відсутність сегментації. Іноді в системах зустрічаються незахищені віддалені термінали, комп'ютери, USB-порти, мобільні і периферійні пристрої і також специфічні види пристроїв людино-машинного інтерфейсу.

Поступовий перехід до використання комерційних IT-рішень, безсумнівно, несе

комерційну вигоду і спрощує експлуатацію та інтеграцію систем. Але при цьому системи управління виявляються більш уразливими перед шкідливим програмним забезпеченням і загрозами безпеці, націленими саме на комерційні системи.

Причиною виникнення вразливостей можуть служити різноманітні помилки «людського чинника», зокрема неправильні дії проектувальника або інсталятора при конфігурації і установки системи. Негативно позначаються на безпеці неадекватні плани супроводу і модернізації АСУ ТП, недостатній рівень кваліфікації персоналу, відповідального за їх впровадження та обслуговування. Виробничий сектор пишається висококваліфікованими фахівцями з систем автоматизації, однак така експертиза в конкретних продуктах і рішеннях далеко не завжди транслюється в адекватну експертизу в промислових IT-мережах. Цей пробіл послаблює здатність організації розробляти всебічні стратегії захисту і запобігання загроз.

Зокрема, компанія Schneider Electric рекомендує промисловим підприємствам використовувати підхід Defense-in-Depth.

Defense-in-Depth була розроблена для оборонних цілей Агентством національної безпеки США, однак згодом виявилася придатною і для цивільних галузей. На думку ряду експертів, у майбутньому ця концепція стане стандартом забезпечення безпеки в промисловому середовищі.

Підхід Defense-in-Depth передбачає шість ключових компонентів:

• Розробка плану забезпечення безпеки: опис процедур оцінки ризиків та їх мінімізації, а також методів аварійного відновлення.

• Відділення мереж промислової автоматизації від інших мереж шляхом створення буферних зон, здатних захистити промислову систему від запитів та повідомлень з корпоративної мережі.

• Захист периметра від несанкціонованого доступу, що включає міжмережеві екрани, засоби аутентифікації, авторизації, VPN (віртуальної приватної мережі) і антивірусне програмне забезпечення.

• Сегментація мережі, що дозволяє обмежити поширення потенційної загрози одним сегментом. Для розділення мережі на підмережі та обмеження передачі трафіку між сегментами використовуються комутатори і VLAN (група хостів із загальним набором вимог, які взаємодіють незалежно від їх фізичного місцезнаходження).

• Посилення захисту пристроїв: управління паролями, визначення профілів користувачів і деактивація невикористовуваних сервісів.

• Регулярний моніторинг та оновлення: постійне спостереження за активністю операторів і мережевими комунікаціями, а також своєчасне оновлення програмного і

мікропрограмного забезпечення.

Хоча підхід Defense-in-Depth вітає створення і реалізацію вичерпного плану захисту, буде невірним вважати, що перехід до цієї концепції здійснюється за принципом «все або нічого».

Ймовірно, що найближчим часом на міжнародному рівні будуть розроблені нормативні вимоги щодо забезпечення кібернетичної безпеки для автоматизованих систем управління технологічними процесами. Необхідно виробити єдину термінологію, правила сертифікації продуктів і стандарти (можливо, таким стандартом міг би стати IEC 62443 8). В першу чергу вони повинні торкнутися підприємств з критично значущою інфраструктурою.

БАРЕГАМЯН С. Х., старший викладач кафедри права та публічного адміністрування Маріупольського державного університету

СИСТЕМА ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КІБЕРПРОСТОРУ В УКРАЇНІ

На сьогоднішній день провідні держави світу та суспільство в цілому все більшою мірою покладаються і, відповідно, залежать від безперешкодного функціонування кіберпростору, під яким пропонується розглядати середовище, що виникає в результаті функціонування на основі єдиних принципів і за загальними правилами інформаційних (автоматизованих), телекомунікаційних та інформаційно-телекомунікаційних систем. Більшість держав світу активно модернізує власні сектори безпеки відповідно до викликів сучасності, особливо, зважаючи на потенціал використання мережі Інтернет у воєнних цілях. Цей процес відбувається паралельно з активним реформуванням управлінських структур, впорядкуванням нормативного поля, що має забезпечити цілісність державної політики в даній сфері, активною роз'яснювальною роботою серед населення щодо небезпек кіберзагроз, збільшенням чисельності підрозділів, зайнятих у системі кіберзахисту, розробленням кіберзброї та проведенням пробних військово-розвідувальних акцій у кіберпросторі, посиленням контролю за національним інформаційним простором (способами доступу, контентом тощо).

Україна інтегрована у світовий кіберпростір і, відповідно, зазнає різних загроз і негативних впливів, пов'язаних з його розвитком (зокрема від наслідків суперництва США і ЄС з РФ та КНР), що гостро актуалізує проблеми кібербезпеки на загальнодержавному рівні. Це призводить до необхідності концептуального розуміння нової кібербезпекової реальності, впорядкування внутрішнього нормативно-правового поля, визначення повноважень відомств

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДОНЕЦЬКА ОБЛАСНА ДЕРЖАВНА АДМІНІСТРАЦІЯ
МАРІУПОЛЬСЬКА МІСЬКА РАДА
ГОЛОВНЕ УПРАВЛІННЯ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ В ДОНЕЦЬКІЙ ОБЛАСТІ
ДОНЕЦЬКЕ УПРАВЛІННЯ КІБЕРПОЛІЦІЇ ДЕПАРТАМЕНТУ КІБЕРПОЛІЦІЇ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ
МАРІУПОЛЬСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

Збірник матеріалів наукового круглого столу

«КІБЕРБЕЗПЕКА ТА СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ: ВИКЛИКИ СЬОГОДЕННЯ»

26 ЖОВТНЯ 2017 РОКУ

Маріуполь – 2017 р.

УДК 004.49(08)
ББК 32.97

Кібербезпека та системи захисту інформації: виклики сьогодення: збірник матеріалів круглого столу, м. Маріуполь, 26 жовтня2017 р. / Маріупольський державний університет; Кафедра математичних методів та системного аналізу; уклад. Тимофєєва І. Б. – Маріуполь.: МДУ, 2017. – 104 с.

Рекомендовано до друку засіданням Вченої ради економіко-правового факультету Маріупольського державного університету (протокол № 2 від 18 жовтня 2017 р.)

ЗМІСТ