© Ayasrah A.Ali Evaluation of cyber protection in information systems // Ukrainian Scientific Journal of Information Security, 2021, vol. 26, issue 3, pp. 132-136.

КІБЕРБЕЗПЕКА ТА ЗАХИСТ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ / CYBERSECURITY & CRITICAL INFORMATION INFRASTRUCTURE PROTECTION

DOI: 10.18372/2225-5036.27.16514

ОЦІНЮВАННЯ КІБЕРЗАХИСТУ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Аясрах Ахмад Расмі Алі

Аясрах Ахмад Расмі Алі
Рік та місце народження: 1992 рік, м. Джераш, Йорданія.
Освіта: Київський національний університет будівництва і архітектури, 2019 р.
Посада: аспірант, Національний авіаційний університет.
Наукові інтереси: інформаційна безпека, кібербезпека в інформаційних системах.
Публікації: 3 наукових публікації, серед яких наукові статті та тези.
E-mail: ahmadaesr@gmail.com.
ORCID ID: 0000-0003-4392-1806.

Анотація. *У статті розглянуто шляхи підвищення системності підходу до самої проблеми захисту інформації при комплексному використанні всіх наявних засобів захисту. При цьому всі засоби, методи та заходи, які використовуються для захисту інформації, об'єднуються в єдиний цілісний механізм – систему захисту, що повинна забезпечувати захист не тільки від зловмисників, але й від некомпетентних або недостатньо підготовлених користувачів та персоналу. Також розглянуто системне рішення проблеми оцінювання якості захисту(кіберзахисту) при проектуванні або модифікації інформаційної системи. У статті розглянуто шляхи підвищення системності підходу до самої проблеми захисту інформації при комплексному використанні всіх наявних засобів захисту. При цьому всі засоби, методи та заходи, які використовуються для захисту інформації, об'єднуються в єдиний цілісний механізм – систему захисту, що повинна забезпечувати захист не тільки від зловмисників, але й від некомпетентних або недостатньо підготовлених користувачів та персоналу. Також розглянуто системне рішення проблеми оцінювання якості захисту(кіберзахисту) при проектуванні або модифікації інформаційної системи. У статті розглянуто шляхи підвищення системності підходу до самої проблеми захисту інформації при комплексному використанні всіх наявних засобів захисту.*
Ключові слова: *інформаційні системи, захист інформаційних систем, кіберзахист, захист інформації, оцінювання кіберзахисту.*

Вступ

Процес впровадження нових інформаційних технологій в усі сфери життя сучасного суспільства, що вступає в інформаційний період, неможливий без рішення ниток інформаційної та кібербезпеки в різних сферах діяльності суспільства. Широкомасштабне використання обчислювальної техніки та телекомунікаційних систем, перехід до безпаперової технології, збільшення об'ємів оброблювальної інформації й розширення кола користувачів, приводить до якісно нових, можливостей несанкціонованого доступу до ресурсів і даних інформаційних систем (ІС), до її високої вразливості.

В сучасних умовах захист інформації в цілому й кіберзахист в інформаційних системах зокрема стає все більш складною проблемою. Масове створення впровадження і експлуатація ІС привели до виникнення нових проблем в сфері безпеки інформації. І це закономірно. Потреби в забезпеченні безпеки пов'язані з тим, що існує множина суб'єктів і структур, які зацікавлені в чужій інформації та готові платити за це високу ціну.

В таких умовах все більше розповсюджується аксіома, що захист інформації повинен по своїм характеристикам відповідати масштабам загроз. Відхилення від цього правила приведе до додаткових збитків. Для кожної ІС мається оптимальний рівень захищеності, який необхідно постійно підтримувати [1]. Немає сумнівів, що захист, критично важливих для ІС масивів повинен відповідати сучасним нормативним документам. Застосовуються високовартісні технічні засоби та впроваджуються суворо регламентовані заходи та методи.

Однак немає відповіді на найважливіше питання – наскільки рішення, які запропоновуються або реалізовуються, дійсно відповідають вимогам.

Тому для запобігання втрати або пошкодження інформації використовуються системи захисту інформації, що являють собою комплекс засобів і методів які перешкоджають несанкціонованому доступу до інформації.

Основним напрямком пошуку ефективних шляхів захисту є підвищення системності підходу до самої

проблеми захисту інформації. Поняття системності інтерпретується перш за все в тому сенсі, що захист інформації полягає не просто у створені відповідних механізмів, а являє собою регулярний процес, який здійснюється на всіх етапах життєвого циклу обробки даних при комплексному використанні всіх наявних засобів захисту.

При цьому всі засоби, методи та заходи, які використовуються для захисту інформації, об'єднуються в єдиний цілісний механізм – систему захисту, що повинна забезпечувати захист не тільки від зловмисників, але й від некомпетентних або недостатньо підготовлених користувачів та персоналу.

Тому при проектуванні або модифікації ІС однією з найважливіших проблем є проблема оцінювання якості захисту(кіберзахисту).

Ця проблема повинна вирішуватися системно, тому що довільне переважання одного з аспектів захисту приводить до недооцінки інших, що врешті може суттєво зменшити рівень захисту(кіберахисту) системи загалом [1,2].

Це пояснюється тим, що для проникнення в систему в більшості випадків достатньо зламати одну з систем захисту, тобто фактично рівень захисту (кіберзахисту) визначається рівнем захищеної системи. Як не дивно, але в багатьох випадках зловмисники діють більш системно ніж користувачі ІС, особливо коли усілякі доробки системи реалізуються власними силами, а не первісними проектами.

Основна частина

Виходячи з цього розглянемо основні компоненти, які найчастіше зазнають активних втручань в роботу ІС оскільки системний аналіз можливих втручань у роботу цих компонент і дає можливість оцінити дійсний рівень захисту тієї чи іншої системи. Основними компонентами, які найчастіше зазнають активних втручань в роботу ІС є наступні (рис.1):

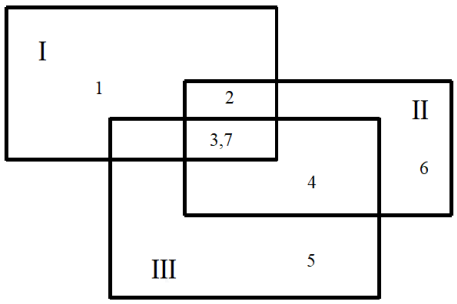
-користувачі системи (1);
-моделі довірчих відношень (2);
-проектні рішення та їх реалізації (3);
-архітектура системи (4);
-обладнання (5);
-програмні засоби відновлення після збоїв (6);
-засоби захисту (7);

Одним з найбільш розповсюджених видів атаки на ІС з боку зловмисника, який зазвичай прекрасно знає психологію користувача, є атака з врахуванням «людського» чинника.

Тобто, якщо аналіз алгоритмів потребує багато місяців кропітної щоденної праці, то атака з врахуванням фактору реального користувача може виявитися значно більш швидкою та ефективною. Це особливо відчутно, якщо ще й ІС спроектовано недостатньо добре, та «кодекс поведінки» користувача або не існує, або дотримання його положень не контролюється з боку адміністратора системи [2].

Часто користувачі не приділяють необхідної уваги перевірці електронного підпису. Секретні паролі часто повторно використовуються в ІС. Звичайно, навіть системи, які мають потужну систему захисту, не в змозі ліквідувати наслідки «людського» фактору, але вони можуть зводити їх до мінімуму. Необхідно забезпечити чітко регламентовану з паролями та іншими засобами ідентифікації користувачів, виконувати мінімальні вимоги до надійності паролів.

Моделі довірчих відношень в системі повинні бути чітко прописані.Тобто, якщо модель довірчих відношень не визанчена, то в процесі розгортання в інформаційної бази випадково внести деякі непродумані зміни, після чого нормальне функціонування систем безпеки буде порушено.



I , II , III – обладнання
Рис.1 Основні компоненти та ланки можливого втручання в роботу ІС

Крім цього, слід враховувати, що процес захисту, пов'язаний з конфліктом між стороною, що забезпечує безпеку (кібербезпеку) інформації та стороною яка бажає незаконним шляхом отримати її.

Для аналізу такого конфлікту краще за все підходить теорія ігор, так нам вона дозволяє моделювати дії обох сторін.

Теорія ігор – це теорія математичних моделей прийняття оптимальних рішень в умовах конфліктів. Вона дозволяє отримати стратегію раціональної поведінки для отримання максимального виграшу чи максимальної ймовірності виграшу [3].

В залежності від цінності інформації до системи захисту (кіберзахисту) можуть ставитись різні вимоги. При цьому можливі дві принципово різні ситуації, що обумовлюють необхідність вирішення відповідно першої чи другої проблем.

Перша ситуація передбачає, що інформація є комерційною або некомерційною таємницею. В даному випадку наслідком втрати інформації для власника будуть економічні втрати, що можна оцінити кількісно. Тобто, задача оптимізації полягає в тому, щоб при мінімальному розмірі затрат на систему захисту забезпечити максимальний рівень захисту.

Друга ситуація виникає, коли інформація складає державну таємницю, і неможливо оцінити вартість затрат від її втрати. При цьому система захисту (кіберзахисту) має забезпечити необхідний рівень безпеки (кібербезпеки) інформації, а оптимізація полягає в мінімізації затрат ресурсів для забезпечення максимального та необхідного рівня захисту.

Не потрібно цілком і повністю покладатись на захищеність апаратних та програмних засобів. Багато користувачів занадто довіряються захищеності програмних засобів замість апаратних засобів. Передбачається, що ПЕОМ абсолютно безпечний.

Рано або пізно в апаратне забезпечення функціонування комп'ютера, проникає програма яка підбирає паролі, зчитує незашифрований текст або якимось іншим чином втручається в роботу ІС та систем захисту.

Розробникам ІС, що функціонують у інформаційних мережах, варто потурбуватися про безпеку мережевих протоколів. Уразливість ПЕОМ, залучених до Internet, багаторазово зростає. В особливо складних випадках можлива побудова двох не пов'язаних між собою мереж.

Дуже часто система проектується в розрахунку на одну модель довірливих відносин, а в реалізації функціонує зовсім інша. Прийняті в процесі проектуванні рішення ігноруються користувачем після передачі йому системи.

Існує багато способів подолання захисних механізмів, які пов'язані з моделями довірчих відношень усередині системи. Насамперед, варто виявити зв'язок між окремими компонентами систем, усвідомити обмеження та механізми реалізації схем довірчих відношень. Тому необхідно визначити критерії оцінювання захищеності ІС. В результаті аналізу характеристик (спроектованих та реальних) ІС та систем захисту визначаємо наступі характеристики:

l – кількість компонентів ІС;

m – кількість захисник механізмів, що використовуються тестовій ІС;

n – кількість загроз несанкціонованих дій до компонентів ІС;

$\mu_{ik} \in [0,1]$, i=1,2,…, n – коефіцієнт небезпеки загроз несанкціонованих дій(НСД) для кожного компонента ІС, k=1, l,…,l;

$\gamma_{ijk} \in [0,1]$ j=1,2,…, m – коефіцієнт ефективності використання механізму захисту j від і загрози НСД до компонентів ІС;

a_{ik} – затрати на реалізацію загроз на компонентах ІС;

b_{jk} – вартість засобів захисту на компонентах ІС;

C_k – інформаційна вартість компонента ІС.

Використовуючи [4] можна побудувати матрицю, що описує можливі інформаційні впливи на ІС при використанні різних варіантів, що використовуються в тестованих автоматизованих системах засобів та заходів захисту інформації:

$$\varphi_{i\theta}^{k},\ \text{i=1,2,…, } n.\ \theta\text{=1,2,…, } w.\ w=2^m\text{-1},$$

де $\varphi_{i\theta}^{k}$- елемент для компонента k;

$h_{i\theta}$ – коефіцієнт використання механізмів захисту **j** в варіанті системи захисту θ.

$$b_{\theta k=\sum_{j=1}^{m} b},$$

де B – сумарна вартість системи захисту тестованої ІС.

Тоді загальний показник захищеності компонента ІС від НСД Q_{θ}^{k} визначається виразом:

$$Q_{\theta}^{k}=\frac{V_{em}^{k}}{V_{\theta}^{k}},$$

де V_{em}^{k}- значення ціни гри що задається виразом(1), в змішаних стратегіях;

V_{θ}^{k} – значення ціни гри для використання в ІС варіанта системи захисту θ.

Значення показників μ_{ik}, γ_{ijk}, a_{ik}, b_{jk}, c_k, пропонується визначати експертно на основі методу прямого встановлення переваг шляхом попарних порівнянь [4].

Рішення про відповідність ІС вимогам захищеності від НСД приймаються на основі порівняння результатів розрахованого шляху захищеності з вимогам, що визначені в програмі випробовування. Дана модель розрахунку інформаційної захищеності може бути використана для розрахунку узагальненого (пізнання) захищеності ІС, використовуючи поля загроз, характерних для інформаційної моделі ІС. Часто у програмі електронної пошти може використовуватися супернадійний алгоритм шифрування повідомлень, але якщо ключі не сертифіковані джерелом, що заслуговує довіри, і сертифікація не може бути підтверджена в реальному часі, безпека системи залишається під сумнівом. Якісні моделі довірчих відношень продовжують працювати навіть у тому випадку, якщо окремі компоненти ІС або систем захисту відмовляють.

Проектні рішення та реалізації слід перевіряти на наявність типових «дір» в захисті та усунути їх. При чому багато систем підводять помилки в реалізації рішень. Деякі реалізації проектних рішень не гарантують, що зашифрувавши текст, вони знищать оригінал. У інших системах для попередження втрати інформації у випадку системного збою використовують тимчасові файли, у цьому випадку на них можуть залишатися окремі фрагменти незашифрованого тексту. Усе це приклади дір у системах НСД, котрі часто використовуються зловмисниками.

У сучасних крипто системах термін життя ключів обмежується максимально коротким проміжком часу. Процедура відновлення дозволяє продовжити життя ключа вже після того, як від нього відмовилися. Використовувані для відновлення ключів бази даних, само по собі є джерелом небезпеки, і їхня архітектура повинна бути вивірена з особливою старанністю.

Тому, проектні рішення повинні орієнтуватися на чітку регламентацію роботи з метою забезпечення необхідного рівня захисту системи загалом. У випадку використання різних стандартів в одному середовищі, необхідно забезпечити чітку взаємодію між ними. Тому в системі слід звернути увагу на точки взаємодії між протоколами обміну даних та методами шифрування, які окремо один від одного є надійними [5].

Деякі системи шифрування, що використовують пов'язані ключі, можуть бути зламані, навіть якщо кожен ключ окремо надійний.

Іноді в зловмисників з'являється можливість скористатися оберненою сумісністю різноманітних версій програмного забезпечення. Як правило, у кожному новому варіанті програмного забезпечення розробники намагаються усунути «діри», що були в старому.

Надійність – це важлива складова комплексної системи безпеки, але не варто сподіватися, що захищають лише від зловмисних дій і НСД. Деякі системи мають так зване «кільце безпеки», що складається з апаратних засобів підвищеної стійкості до несанкціонованого проникнення [6].

Розробники виходять із припущення, що архітектура системи усередині цього кільця надійно захищена від НСД. Більшість подібних технологій не працюють, а інструменти для захисту безупинно удосконалюються. Слід уникати використання алгоритмів шифрування власної розробки або випадкових та коротких ключів.

Це пов'язано з тим, що, як правило, розкрити відомі алгоритми шифрування вдається лише у виняткових випадках. Якщо розробник робить ставку на власні методи, шанси ламання підвищуються багаторазово і незнання секрету алгоритму не є особливою перешкодою.

Тому у ІС повинні використовуватись якісні генератори випадкових чисел щодо роботи по створенню ключів. В багатьох випадках генератор випадкових чисел залежить від особливостей апаратного а програмного забезпечення [7].

Сама система шифрування може бути виконана на високому рівні, але якщо генератор випадкових чисел видає ключі, що можна вгадати, захист руйнується.

Логічно навести багато прикладів помилок у системах шифрування: програми повторно генерують особливі випадкові значення, алгоритми шифрованого підпису не в змозі забезпечити контроль за переданими параметрами, хеш-функції відкривають те, що повинні захищати. У протокол шифрування вносяться не передбачені розробниками зміни.

Користувачі люблять «оптимізувати» наявні засоби, зводячи нанівець захист(кіберзахист) інформаційної системи.

Висновки

Надійна система захисту (кіберзахисту), повинна самостійно виявляти несанкціоновані операції. При чому, один з основних принципів проектування подібних систем полягання в знанні того, що рано або пізно атаки зловмисника увінчаються успіхом, а тому дуже важливо своєчасно розпізнати такий напад та прийняти всі необхідні заходи для того щоб мінімізувати збитки. Важливою є наявність засобів та організаційних процедур для якнайшвидшого відновлення працездатності ушкодженої в наслідок атаки системи.

Тобто, необхідно генерувати нові пари ключів, замінити протокол, припинити використання розкритих зловмисником засобів, виключити із системи вузли, до яких зловмиснику вдалося одержати доступ і т.д. Нажаль, багато програмних засобів не займаються збором потрібної інформації, не контролюють ситуацію і не в змозі надійно захистити дані від змін. Всі події, що дозволяють встановити факт нападу або несанкціонованих дій, повинні реєструватися. Тобто, система безпеки (кібербезпеки) повинна бути комплексною та не обмежуватися рамками засобів шифрування та спеціальним обладнанням.

Якщо зловмисникам вдасться перебороти перші оборонні рубежі, повинні спрацьовувати додаткові механізми захисту.

Потрібно постаратися максимально ускладнити задачу супротивника та зробити її рішення не вигідним з економічної точки зору.

Література

[1] Кобозєва А.А. Аналіз захищеності інформаційних систем / А.А. Кобозєва, І.О. Мочалін, В.О. Хорошко. – ІС: Вид. ДУІКТ, 2010. – 316 с.

[2] Козюра В.Д. Комплексні системи захисту інформації в інформаційно-телекомунікаційних системах / В.Д. Козюра, Ю.М. Ткач, М.Є. Шелест та ін. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2019. – 144 с.

[3] Мулен Е. Теорія ігор / Е. Мулен. – М:Мир, 1985. – 199 с.

[4] Петросян Л.А. Теорія ігор / Л.А. Петросян, Н.А. Зінкевич, Е.А. Семеня. – Высшая школа менеджмента, 1998. – 301 с.

[5] Скотт Бармен Розробка правил інформаційної безпеки / Бармен Скотт. – М: ІД «Вільямс», 2002. – 208 с.

[6] Brailovskyi N., Khoroshko V., Khokhlacheva Y., Ayasrah Ahmad. Evolution of the Level of Cyber Security of Information // Scientific and Practical Cyber Security Journal, vol.3, №3, 2019. – pp. 18-24.

[7] Сушко С.О. Математичні основи криптоаналізу / С.О. Сушко, І.В. Кузнецов, Л.Я. Фомічова, А.В. Корольов. – Нац. гірничий ун-т, 2010. – 465 с.

УДК 004.081.3:681

Ayasrah A.

Ali EVALUATION OF CYBER PROTECTION IN INFORMATION SYSTEMS

Abstract*. The article considers ways to increase the systematic approach to the problem of information protection with the integrated use of all available means of protection. At the same time, all means, methods and measures used to protect information are combined into a single integrated mechanism - a system of protection that should provide protection not only from attackers, but also from incompetent or untrained users and staff. The system solution of the problem of assessing the quality of protection (cybersecurity) in the design or modification of the information system is also considered. The article considers ways to increase the systematic approach to the problem of information protection with the integrated use of all available means of protection. At the same time, all means, methods and measures used to protect information are combined into a single integrated mechanism - a system of protection that should provide protection not only from attackers, but also from incompetent or untrained users and staff. The system solution of the problem of assessing the quality of protection (cybersecurity) in the design or modification of the information system is also considered.*

Keywords: *information systems, information systems protection, cybersecurity, information protection, cyber security assessment.*

Аясрах А.

ОЦЕНКА КИБЕРЗАЩИТЫ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Аннотация*. В статье рассмотрены пути повышения системности подхода к самой проблеме защиты информации при комплексном использовании всех имеющихся средств защиты. При этом все средства, методы и меры, которые используются для защиты информации, объединяются в единый целостный механизм – систему защиты, которая должна обеспечивать защиту не только злоумышленников, но и некомпетентных или недостаточно подготовленных пользователей и персонала. Также рассмотрено системное решение про-*

блемы оценки качества защиты (киберзащиты) при проектировании или модификации информационной системы. В статье рассмотрены пути повышения системности подхода к самой проблеме защиты информации при комплексном использовании всех имеющихся средств защиты. При этом все средства, методы и меры, которые используются для защиты информации, объединяются в единый целостный механизм – систему защиты, которая должна обеспечивать защиту не только злоумышленников, но и некомпетентных или недостаточно подготовленных пользователей и персонала. Также рассмотрено системное решение проблемы оценки качества защиты (киберзащиты) при проектировании или модификации информационной системы.
***Ключевые слова**: информационные системы, защита информационных систем, киберзащита, защита информации, оценка киберзащиты.*

Аясрах Ахмад Расмі Алі, аспірант, Національний авіаційний університет.
Аясрах Ахмад Расми Али, аспирант, Национальный авиационный университет.
Ayasrah Ahmad Rasmi Ali, graduate student, National Aviation University.

Отримано *08 жовтня 2021 року*, затверджено редколегією *17 грудня 2021 року*

DOI: 10.18372/2225-5036.27.16001

БАГАТОАЛЬТЕРНАТИВНЕ ВИЯВЛЕННЯ КІБЕРАТАК В ІНФОРМАЦІЙНИХ МЕРЕЖАХ

Хорошко[1] В.О., Ткач[2] Ю.М., Шелест[2] М.Є.

[1]Національний авіаційний університет
[2] Чернігівський національний технологічний університет

ХОРОШКО Володимир Олексійович, д.т.н., професор.
Рік та місце народження: 1945 рік, м. Харків, Україна.
Освіта: Київський інститут інженерів цивільної авіації, 1968 рік.
Посада: професор кафедри безпеки інформаційних технологій.
Наукові інтереси: інформаційна безпека, технічні системи захисту інформації, аналіз функціонування складних систем.
Публікації: більше 500 наукових публікацій, серед яких наукові статті, монографії, підручники, патенти навчально-методичні посібники.
E-mail: professor_va@ukr.net.
ORCID: 0000-0001-6213-7086.

ШЕЛЕСТ Михайло Євгенович, д.т.н., професор.
Рік та місце народження: 1954 р., м. Ромни, Україна.
Освіта:. Національний університет "Львівська Політехніка"
Посада: професор кафедри кібербезпеки та математичного моделювання.
Наукові інтереси: інформаційна безпека, оцінювання вразливостей, оптимізація інформаційних систем.
Публікації: більше 100 наукових публікацій, серед яких наукові статті, монографії, підручники, навчально-методичні посібники та деклараативні патенти.
E-mail: mishel3141@gmail.com.
ORCID: 0000-0001-7110-4876.

ТКАЧ Юлія Миколаївна, д.пед.н., професор
Рік та місце народження: 1979 рік, м. Чернігів, Україна.
Освіта: Чернігівський національний технологічний університет, 2012 рік; Чернігівський державний педагогічний університет ім. Т.Г. Шевченка, 2001.
Посада: завідувач кафедри кібербезпеки та математичного моделювання з 2010 р.
Наукові інтереси: інформаційна та кібербезпека.
Публікації: більше 80 наукових публікацій, серед яких, підручники, навчальні посібники, монографії, наукові статті та тези.
E-mail: tkachym79@gmail.com.
ORCID: 0000-0002-8565-0525.