МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

ITSec-2021

МАТЕРІАЛИ

XI міжнародної науково-технічної конференції

1-6 жовтня 2021

м. Анталія (Туреччина)

УДК [003.26+004+519.816]:004.056:65(063)

ITSec: Безпека інформаційних технологій: XI міжнародна науково-технічна конференція, 1-6 жовтня 2021 р. – К.: НАУ, 2021. – 78 с.

Збірник містить тексти наукових матеріалів доповідей та тез учасників XI міжнародної науково-технічної конференції «ITSec: Безпека інформаційних технологій». Основною метою конференції є ознайомлення з сучасними досягненнями та висвітлення результатів наукових досліджень з усіх аспектів захисту інформації, консолідації інформації та бізнес-аналітики.

Призначено вченим, інженерам, аспірантам наукових спеціальностей 05.13.21 – системи захисту інформації, 21.05.01 – інформаційна безпека держави, студентам вищих навчальних закладів, які отримують вищу освіту за спеціальностями: 125 – Кібербезпека (напрями: «Безпека інформаційних і комунікаційних систем», «Системи технічного захисту інформації», «Управління інформаційною безпекою» («Адміністративний менеджмент у сфері захисту інформації»), «Системи і технології кібербезпеки») та 124 – Системний аналіз (напрям «Консолідована інформація»), а також всім зацікавленим.

ОРГАНІЗАТОРИ КОНФЕРЕНЦІЇ

- Кафедра безпеки інформаційних технологій Національного авіаційного університету;
- Наукове товариство студентів, аспірантів, докторантів та молодих учених НАУ;
- Європейський університет;
- Інститут спеціального зв'язку та захисту інформації НТУУ «КПІ ім. І. Сікорського»;
- Університет у Бєльсько-Бялій (Польща);
- ТОВ «Акксон Софт»;
- ТОВ «Безпека інформаційних систем «Дельта»;
- Студентське науково-технічне товариство «CyberTag»;
- Редакція наукового журналу «Безпека інформації»;
- Редакція наукового журналу «Захист інформації»;
- ГО «Асоціація спеціалістів кібербезпеки».

ОРГКОМІТЕТ КОНФЕРЕНЦІЇ

Голова д.т.н., проф. **Олександр Корченко**
Національний авіаційний університет (м. Київ, УКРАЇНА)

Заступник голови к.т.н., проф. Євгенія Іванченко
Національний авіаційний університет (м. Київ, УКРАЇНА)

Відповідальний секретар Марина Коломієць
Національний авіаційний університет (м. Київ, УКРАЇНА)

Члени програмного комітету

д.т.н., проф. **Бахитжан АХМЄТОВ**, Казахський національний педагогічний університет ім. Абая (м. Алмати, КАЗАХСТАН)

д.т.н., проф. **Євген ВАСІЛІУ**, Державний університет інтелектуальних технологій і зв'язку (м. Одеса, УКРАЇНА)

д.т.н., проф. **Микола КАРПІНСЬКИЙ**, Університет у Бєльсько-Бялій (м. Бєльсько-Бяла, ПОЛЬЩА)

к.т.н., доц. **Геворг МАРҐАРОВ**, Державний інженерний університет Вірменії (м. Єреван, ВІРМЕНІЯ)

д.т.н., проф. чл.-кор. НАН України **Володимир МОХОР**, Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова, НАН України (м. Київ, УКРАЇНА)

д.т.н., проф. **Станіслав РАЙБА**, Університет у Бєльсько-Бялій (м. Бєльсько-Бяла, ПОЛЬЩА)

д.ф.н. доц. **Олена ТИМОШЕНКО,** Європейський Університет (м. Київ, Україна)

ктн. доц. **Василь ЦУРКАН,** Національний технічний університет України "Київський політехнічний інститут ім. Ігоря Сікорського" (м. Київ, Україна)

Зміст

Службова інформація: розмір істотної шкоди у разі розголошення

УДК 004.056.5

Юрій Дрейс[12]

[1]*Національний авіаційний університет,*
[2]*Національний університет біоресурсів і природокористування*
y.dreis@nau.edu.ua

Службовою інформацією є інформація, що міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень, а також інформація зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці (ДТ) [1].

Основною нормою, яка повинна застосовуватись в усіх без винятку випадках, коли обмежується доступ до публічної інформації, є частина друга статті 6 Закону України «Про доступ до публічної інформації», яка встановлює вимоги, при дотриманні яких здійснюється обмеження доступу до публічної інформації, так званий "трискладовий тест" [2]:

1. виключно в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя;

2. розголошення інформації може завдати істотної шкоди цим інтересам;

3. шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні.

"Трискладовий тест" обов'язково застосовується у таких випадках: при "первинному" віднесенні певних відомостей до таємної інформації; при "первинному" віднесенні певних відомостей до службової інформації; при вирішенні питання надання чи відмови в доступі стосовно конкретної інформації (документу) [2].

Метою даної роботи є розрахунок величини (розміру) "істотної шкоди" та "тяжких наслідків", необхідної (достатньої) для притягнення до кримінальної відповідальності у разі розголошення службової інформації відповідно до вимог діючого законодавства.

Щодо можливості урахування "інтересів" держави, наприклад, у сфері охорони ДТ під час проведення експертизи матеріальних носіїв інформації на

наявність чи відсутність у них відомостей, що становлять ДТ, висвітлено у працях [1, 3].

А тому спробуємо розібратися, що ж таке "істотна шкода" та "тяжкі наслідки" відповідно до розміру можливої шкоди, необхідної для притягнення до кримінальної відповідальності у разі розголошення службової інформації.

Так, відповідно до п. 3 примітки до ст. 364 КК під "*істотною шкодою*" в ч. 1 ст. 367 КК мається на увазі така шкода, яка в сто і більше разів перевищує неоподатковуваний мінімум доходів громадян (становить 17 грн., за винятком норм адміністративного та кримінального законодавства у частині кваліфікації злочинів або правопорушень, для яких сума неоподатковуваного мінімуму встановлюється на рівні податкової соціальної пільги, визначеної підпунктом 169.1.1 пункту 169.1 статті 169 розділу IV ПКУ для відповідного року [4]). З огляду на вищевказане для притягнення особи до кримінальної відповідальності за ч. 1 ст. 367 КК України потрібно, щоб її діями / бездіяльністю було завдано шкоди на суму, яка перевищує: у 2019 р. – 96 050 грн.; у 2020 р. – 105 050 грн.; у 2021 р.: з 1 січня – 113 500 грн., з 1 липня – 118 950 грн., з 1 грудня – 124 050 грн.

А згідно п. 4 примітки до ст. 364 КК під "*тяжкими наслідками*" в ч. 2 ст. 367 КК маються на увазі такі наслідки, які у двісті п'ятдесят і більше разів перевищують неоподатковуваний мінімум доходів громадян. А для притягнення особи до кримінальної відповідальності за ч. 2 ст. 367 КК України потрібно, щоб її діями / бездіяльністю було завдано шкоди на суму, яка перевищує: у 2019 р. – 240 125 грн.; у 2020 р. – 262 625 грн.; у 2021 р.: з 1 січня – 283 750 грн., з 1 липня – 297 375 грн., а з 1 грудня – 310 125 грн.

Література

1. О. Корченко, Ю. Дрейс "Проблема формування переліку відомостей, що становлять службову інформацію", Актуальні проблеми управління інформаційною безпекою держави: зб. мат. наук.-практ. конф., 20 березня 2014 р., м.Київ. – К: Наук. вид. центр НА СБ України, 2014. – Ч. 2. – С.168-169.

2. Службова інформація: порядок віднесення та доступу. Практичний посібник / За редакцією Д. М. Слизьконіс. Автори-укладачі: О.Л. Огданська, В.В. Таран, В.В. Щербаченко – К.: Центр політичних студій та аналітики, 2014. - 76 с.

3. Ю. Дрейс, "Враховування інтересів держави в методиці оцінювання шкоди у сфері охорони державної таємниці", Інтегровані інтелектуальні робототехнічні комплекси (ІІРТК-2012) = Integrated Intellectual Robotechnical Complexes (IIRTC2012) : П'ята міжнародна науково-практична конференція, 15-16 травня 2012р. – С.316-318.

4. "Є два розміри неоподатковуваного мінімуму. У чому різниця?", Головне управління ДПС у Львівській області, Новини від 23.12.2019, URL: https://lv.tax.gov.ua/media-ark/news-ark/402663.html

Науковий консультант – д.т.н., професор Корченко О.Г.

Оптимизация состава контуров кибербезопасности на основе генетического алгоритма

УДК 32.973.202 (004.8)

Лахно Валерий[1], Ахметов Бахытжан[2], Ягалиева Багдат[3]

Национальный университет биоресурсов и природопользования[1], Казахский национальный педагогический университет имени Абая[2], Каспийский университет технологий и инжиниринга имени Ш.Есенова[3],
[1]valss21@ukr.net, [2]bakhytzhan.akhmetov.54@mail.ru,
bagdat.yagaliyeva@yu.edu.kz

Увеличивающееся количество и сложность успешно реализованных кибератак на различные ОБИ [1, 2] порождает потребность в качественно новых процедурах формирования состава комплексов СЗИ и кибербезопасности (КрБ) для всех контуров защиты информационных массивов ОБИ. Не теряющая актуальности задача формирования эффективных контуров защиты информации (ЗИ) и КрБ ОБИ породила множество теоретических и прикладных исследований, посвященных вопросам оптимизации состава СЗИ и КрБ [3, 4].

В подобных задачах, необходимо находить допустимые парето-оптимальные решения для комплексов СЗИ. Решение подобной задачи является неотъемлемой частью процедуры построения многоконтурных СЗИ в условиях роста количества попыток деструктивных воздействий на ОБИ различного масштаба. А решение подобных задач выполняется на базе не только классических процедур многокритериальной оптимизации (МКО), но и более универсальных методов. В частности, к таким методам можно отнести различные вариации генетического алгоритма (ГА), доказавшего свою эффективность при решении большого круга сложных задач [5, 6].

Заметим, что эффективность ГА зависит от тщательной настройки и контроля их параметров. Целесообразность применения ГА диктуется ситуацией, при которой, помимо традиционной МКО задачи выбора состава СЗИ для ОБИ, рассматриваются и различные метрики оценивания эффективности применения отдельных составляющих средств защиты информации по контурам кибербезопасности ОБИ. А кроме того, еще необходимо учитывать величины рисков, стоимостные показатели отобранных средств защиты информации, исходя из специфики конкретных информационных активов - базы данных, базы знаний, почта, сайт и др.

Решение выполнено на основе общего эволюционного алгоритма и его составляющих многокритериальных ГА. Основным при этом стал метод VEGA – Vector Evaluted Genetic Algorithm [1,2].

Данный метод предусматривает расширение традиционного ГА, которое реализовано путем применения векторных оценок степени пригодности экземпляров (индивидуумов), а также возможностей параллельно оценивать популяции по каждому из критериев в отдельности, например, для каждого из

компонентов СЗИ это могут быть – эффективность, масштабируемость, стоимость, техническая поддержка.

Таким образом можно реализовать одновременную оптимизацию всех контуров защиты объекта информатизации в соответствии с заданными целевыми функциями.

На начальном этапе работы МГА имеются две родительские хромосомы. В двух случайным образом выбираемых местах выполняются разрывы между позициями генов. Далее происходит обмен частей между хромосомами. Как результат образуются два потомка. Из потомков выбирается случайным образом один потомок, который передается как результат оператора скрещивания.

Далее переходим к оператору мутации – случайному изменению всех потомков популяции. Цель мутации является сделать более разнообразным анализируемые в ходе решения задачи индивидуумы (экземпляры). Мутировавшие гены показаны на рисунке 2 в виде ячеек со светло-зеленой заливкой. То есть в ходе мутации значение бита в ячейке изменилось на противоположное. Так в первой ячейке с «0» на «1». Во второй с «1» на «0».

Далее формируем новое поколение из массива родителей и образованных потомков. В ходе формирования нового поколения применялись как родителей, так и потомков уже известные значения функции пригодности.

Порядок работы с модифицированным алгоритмом решения задачи многокритериальной оптимизации параметров многоконтурной СЗИ объекта информатизации такой:

Шаг 1.

Выбираем области определения для всех переменных (метрик кибербезопасности ОБИ), см. таблицу 1:

Таблица 1

Переменные для ГА

Номер бита в хромосоме	Метрики кибербезопасности для анализируемого объекта информатизации
0	Доля инцидентов с кибербезопасностью (КБ) на ОБИ (по типам)
1	Доля инцидентов с КБ на ОБИ с соблюдением сроков реагирования
2	Средняя продолжительность времени реагирования на инциденты с КБ (по уровням критичности)
3	Доля уязвимостей на ОБИ, которые устранены в установленные сроки

4	Среднее время, которое затрачено на устранение уязвимостей ОБИ
5	Доля рисков для информационных активов ОБИ (недопустимого уровня для каждого актива)
6	Доля рисков для КБ ОБИ, по которым были приняты соответствующие меры
7	Индекс соответствия стандарту (стандартам) ИБ
8	Эффективность обучения сотрудников мерам по соблюдению правил КБ
9	Показатели достаточности ресурсов (финансовых, технических, организационных и др.) для выполнения задач ИБ и КБ ОБИ

Шаг 2.

Ввод параметров ГА. Задаем: размер популяции; число поколений (от 100 до 2000); тип мутации: число прогонов.

В отличие от существующего классического алгоритма VEGA в модифицированном алгоритме дополнительно применены принцип Парето.

Описанный выше ГА был программно реализован в виде отдельных модулей системы поддержки принятия решений (СППР) для задачи многокритериальной оптимизации затрат на СЗИ ОБИ. Среда программирования – Visual Studio.

Выводы. Изложена методика многокритериальной оптимизации затрат на систему защиты информации объекта информатизации. Методика базируется на применении генетического алгоритма. В отличие от существующего классического генетического алгоритма VEGA, в модифицированном алгоритме дополнительно применены принцип Парето, а также новый механизм селекции. Принцип Парето применяется для лучшей точки. В этой точке решение, трактуемое как лучшее, если по одной из метрик кибербезопасности есть улучшение, а по другой метрике (или метрикам) будет строго не хуже.

Новый механизм селекции в отличие от традиционной, предполагает создание промежуточной популяции. Эта промежуточная популяция формируется в несколько этапов. На первом этапе первая половина популяции формируется на основе метрики - доля уязвимостей ОБИ, которые устранены в установленные сроки. На втором этапе вторая половина промежуточной популяции формируется на основе метрики - доля рисков, которые недопустимы для информационных активов ОБИ. Далее эти части промежуточной популяции смешиваются. После смешивания формируется массив номеров и производится смешивание. На заключительном этапе селекции для скрещивания будут браться экземпляры (индивиды) по номеру из этого массива. Номера выбираются случайно.

Список литературы

1. Okutan, A., Yang, S. J., McConky, K., & Werner, G. (2019). CAPTURE: Cyberattack Forecasting Using Non-Stationary Features with Time Lags. In 2019 IEEE Conference on Communications and Network Security (CNS) (pp. 205–213). IEEE.

2. Barreto, C., & Koutsoukos, X. (2019, October). Design of Load Forecast Systems Resilient Against Cyber-Attacks. In International Conference on Decision and Game Theory for Security (pp. 1–20). Springer, Cham.

3. Chandra, Y., & Mishra, P. K. (2019). Design of cyber warfare testbed. In Software Engineering (pp. 249–256). Springer, Singapore.

4. Sándor, H., Genge, B., Szántó, Z., Márton, L., & Haller, P. (2019). Cyber attack detection and mitigation: Software Defined Survivable Industrial Control Systems. International Journal of Critical Infrastructure Protection, 25, pp. 152–168.

5. Chiba, Z., Abghour, N., Moussaid, K., El Omri, A., & Rida, M. (2019). New Anomaly Network Intrusion Detection System in Cloud Environment Based on Optimized Back Propagation Neural Network Using Improved Genetic Algorithm. International Journal of Communication Networks and Information Security, 11(1), 61–84.

6. Nozaki, Y., & Yoshikawa, M. (2019). Security evaluation of ring oscillator puf against genetic algorithm based modeling attack. In International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (pp. 338–347). Springer, Cham.

З історії режимних обмежень на пересування радянських громадян.

1917 – 1922.

УДК 351.756.6:341.222
«1917/1922» (045)

Валерій Ворожко

Національний авіаційний університет, ГДА СБУ, wp06vv@gmail.com

Нині Україна протистоїть потужним зусиллям своїх зовнішніх і внутрішніх ворогів, мета яких – ліквідація української державності, знищення України як суб'єкта міжнародного права і геополітичної реальності. Сучасні суспільно-політичні виклики зумовлюють необхідність об'єктивного аналізу історичних аспектів функціонування «державного організму» України та його подальшої трансформації в сучасну вільну і демократичну країну.

Метою даної роботи є забезпечення прав українських громадян на вільне пересування світом і власною країною, недопущення рецидивів минулого.

Наприкінці листопада 1917 р. комуністична влада запровадила нечувані обмеження на в'їзд і виїзд з «країни рад», яких ще не знала багатовікова історія Європи та Російської імперії. Тут були одночасно і паспорти з фотографіями, і «належні печатки», і спеціальні дозволи зі спеціальними підписами, «виїзні» і «в'їзні»

візи. Були передбачені обшуки і особисті огляди для всіх під час перетину кордону, включаючи жінок, старих і дітей (лише для дипломатів, відповідно до міжнародних норм, робилися винятки, але й то не завжди). Все «недозволене до перевезення» конфісковували, звичайно ж, і заборонялось вивезення документів, що можуть «нашкодити» економічним або політичним інтересам, ще як слід не утвореної радянської влади, до того ж особи, у яких такі «документи» були знайдені, підлягали негайному арешту.

Так, наприкінці 1917 р. закінчився «безвіз» для українців – громадян Російської імперії, який повернувся рівно через сто років у 2017 р.

2 грудня 1917 р. голова Реввійськради РСФРР Л. Троцький видав указ про «візування паспортів при в'їзді до більшовицької Росії». Відтоді прибуття в «країну Рад» було дозволено лише тим, хто мав візу.

На створені у 1919 р. прикордонні особливі відділення серед їхніх завдань було й таке – «не дати можливість перевезти, переслати і переправити за кордон різні документи і відомості, які за своїм змістом можуть полегшити буржуазії боротьбу з радянською Росією».

24 квітня 1919 р. декретом РНК РСФРР право видачі іноземних паспортів було закріплено виключно за НКЗС. Водночас відомство мало право видавати паспорти, але тільки тим особам, проти виїзду яких не було заперечень з боку НКВС і військового відомства. Право на закордонні поїздки та відрядження належали до розряду виняткових привілеїв вищої номенклатури.

Від самого початку більшовицького панування можливість виїзду за кордон була дуже обмеженою, аж доки не перетворилась на винятковий політичний привілей. Від червня 1919 р. на НКЗС було покладено обов'язок отримувати від усіх радянських організацій, що направляли своїх співробітників у службових справах за кордон, документи, які б містили гарантії їхньої відданості та лояльності режиму.

Створений у 1919 р. уряд радянської України також розпочав свою законодавчу діяльність із спроби контролю в'їзду та виїзду. Він запровадив закордонні паспорти для осіб, які бажали виїхати з радянської України, причому прохання про видачу таких паспортів подавалися до відділів управління губвиконкомів.

До прохання мали додаватися дозволи (виїзні візи) на виїзд за кордон від цивільної влади і місцевих ЧК, а для чоловіків ще і від військового комісаріату. Вимагалась також довідка виконкому про те, чи є за прохачем недоїмки, а також три фотографії. Прохач повинен був заповнити в іноземному відділі «довідковий лист», причому показання повинні підтверджуватись завіреними нотаріально підписами двох поручителів.

ВЧК 17 вересня 1919 р. видала «Інструкцію особливим відділам і транспортним надзвичайним комісіями» зі здійснення контролю за пересуванням водним, ґрунтовим і залізничним транспортом на території РСФРР», метою якої визначали «протидію вільному пересуванню шпигунів, білогвардійців, спекулянтів та інших злочинних елементів».

Більшовицький режим також заходився регулювати порядок пересування радянською територією. Вже у 1918 р. ВЧК було надано виключне право визначати порядок пересування в окремих місцевостях, а у серпні 1920 р., згідно з постановою РПО, виняткове право щодо організації порядку в'їзду і виїзду в окремі місцевості та надання відповідних дозволів надавалося НКВС.

Одним важливим привілеєм новоствореної радянської номенклатури можна вважати її право на безкоштовний проїзд у поїздах. Особливі правила, що регулювали поїздки відповідальних працівників ВЦВК, РНК, наркоматів у військових справах, пошти і телеграфів, закордонних справ РСФРР були розроблені ще в вересні 1918 р. Їм надавалися у постійне користування вагони всіх класів, у тому числі й салони.

Закордонний паспорт с візою для радянського громадянина дорівнював тодішній місячній зарплаті спеціаліста вищої кваліфікації, а віза на повторну поїздку – 100 тис. крб. Радянські номенклатурні діячі, які відправлялися у ділову поїздку за кордон, паспорт і візу отримували безкоштовно.

Не забули радянці і про повітряний простір, так 17 січня 1921 р. РНК РСФРР ухвалила декрет «Про повітряні пересування». Реввійськраді надавалося право забороняти або обмежувати польоти над певними місцевостями. Заборонялося мати під час польотів на борту фотографічні, радіотелеграфні та радіотелефонні апарати, поштових голубів, зброю тощо.

Правовий режим 15-верстової прикордонної зони був законодавчо визначений РНК УСРР від 12 грудня 1922 р. Особи, які проживали на цій території, відповідно могли пересуватись тільки за особливими посвідченнями.

У 1922 р. дію закордонного паспорту обмежили до 6 місяців і ускладнили процедуру його отримання.

Таким чином можемо зазначити, що з перших днів свого існування радянська влада на сто років закрила право своїм громадянам можливість вільного пересування світом і власною країною, залишив це право виключно радянській номенклатурі. Разом із культом секретності почав створюватися і культ прикордонної служби.

Дослідження методів виявлення атак у кіберфізичних системах

УДК 004.092

Анастасія Нічепорук[1], Євгеній Колісник[2], Андрій Нічепорук[3]

Хмельницький національний університет, [1]eldess06@gmail.com, [2]koliesnik1998ua@gmail.com@gmail.com, [3]andrey.nicheporuk@khnu.km.ua

Протягом поточного десятиліття частина дослідників зрозуміли, що вбудовані системи еволюціонують до систем, де фізичні аспекти відіграють ключову роль. Взаємодія між інтелектом, що забезпечується розподіленими взаємопов'язаними процесорами, та їхнім фізичним світом набула великого

значення. Проте, разом з еволюцією технологій обміну даними між фізичним та кібернетичним середовищем, що лежить в основі кіберфізичних систем (КФС), з'являються нові «вузькі місця», які є джерелом до вторгнень за участю кібератак. Основними методами виявлення атак у кіберфізичних системах є методи віддаленої атестації, виявлення вторгнень у мережу, виявлення на основі відстеження аномальної поведінки та активне виявлення. Розглянемо детальніше наведені підходи.

Віддалена атестація ґрунтується на перевірці поточного внутрішнього стану (наприклад, оперативної пам'яті) ненадійного пристрою довіреним верифікатором. Існує три варіанти дистанційної атестації: програмна, апаратна та гібридна атестації. Програмна атестація не покладається на будь-яке спеціальне обладнання безпеки в пристрої, але даний метод має слабкі гарантії безпеки і зазвичай вимагає бездротового каналу передачі даних між верифікатором та пристроєм, що перевіряється. На відміну від програмної, апаратна атестація (наприклад, атестація з підтримкою TPM, TrustZone або SGX) забезпечує посилену безпеку, але вимагає спеціального захищеного обладнання у структурі КФС, що в значно збільшує їх вартість та може бути недоступним у деяких недорогих вбудованих системах.

Методи виявлення вторгнень у мережу засновані на тому, що КФС демонструють порівняно простішу поведінку мережі у порівнянні із класичними IT-системами: сервери змінюються рідше, є більш стабільна мережева топологія, менша популяція користувачів, усталена поведінка комунікації. Тому, системи виявлення вторгнень, алгоритми виявлення аномалій та елементи керування доступом до білого списку легше проектувати та впроваджувати, ніж у класичних IT-системах. Якщо проектувальник КФС може спрогнозувати специфікацію передбачуваної поведінки мережі, то будь-який підозрілий трафік може бути позначений як аномалія.

Методи виявлення атак на основі фізики. Основною відмінністю систем управління від інших IT-систем, є взаємодія системи управління з фізичним світом. На відміну від групи методів виявлення вторгнень у КФС, яка фокусується на моніторингу "кібер-шаблонів", інший напрямок вивчає, як значення датчика моніторингу, отримані за допомогою фізичних спостережень, та сигнали управління, що надсилаються виконавчим механізмам, можна використовувати для виявлення атак; такий підхід зазвичай називають виявленням атак на основі фізики. Моделі фізичних змінних у системі можуть бути суто керованими даними або базуватися на фізичних моделях системи. Існує два основних напрямки виявлення атак на основі фізики: історичні аномалії та виявлення аномалії на основі відстеження законів фізики.

Методи відстеження історичних аномалії. Дана група методів спрямована на визначення фізичної конфігурації, якої раніше не спостерігалось в рамках КФС. Типовим прикладом є обмеження спостережуваної поведінки змінної. Наприклад, якщо на етапі навчання рівень води в резервуарі завжди знаходиться між 1 м і 2 м, то якщо рівень води підніметься вище або нижче цих значень, система виявлення може подати попередження. Моделі машинного навчання історичної поведінки змінних також можуть фіксувати історичні кореляції цих змінних. Наприклад, вони можуть зафіксувати той факт, що коли резервуар з

рівнем води високий, рівень води другого резервуара в процесі експлуатації завжди низький.

Виявлення аномалії на основі відстеження законів фізики: Додатковий підхід до історичних спостережень, які можуть мати меншу кількість помилкових спрацювань, полягає у створенні моделей фізичної еволюції системи. Наприклад, у випадку із датчиком, який контролює висоту підстрибуючої кулі, можна стверджувати, що ця висота відповідає диференціальним рівнянням із законів механіки Ньютона. Таким чином, якщо датчик повідомляє про неправдоподібну траєкторію з огляду на закони фізики, система може відразу виявити, що датчки знаходиться в одному з двох станів: несправність або атака. Подібним чином, фізичні властивості водних систем (динаміка рідин) або електромережі (електромагнітні закони) можуть бути використані для створення моделей часових рядів, які ми потім можемо використовувати для підтвердження того, що команди управління, надіслані на поле, були виконані правильно та інформація надходження від датчиків відповідає очікуваній поведінці системи.

Активне виявлення. На додаток до пасивного моніторингу КФС, система виявлення вторгнень може активно надсилати запити пристроям для відстеження поведінки, що визначає, як пристрої реагують на ці запити. Однак активне виявлення може завдати шкоди шляхом утворення непотрібних збурень в системі через їх зміну фізичного світу з метою безпеки. Цей підхід також відомий як фізична атестація, де керуючий сигнал використовується для зміни фізичного світу, і у відповідь він очікує побачити зміни, зроблені у фізичному світі, відображеними у значеннях датчика.

Таким чином огляд методів виявлення атак у КФС показав, що основними підходами є віддалена атестація, виявлення вторгнень у мережу, виявлення на основі відстеження аномальної поведінки та активне виявлення. Проте, існуючі методи характеризуються високим рівнем хибних спрацювань, надмірністю інформації, яка передається по каналах зв'язку КФС, часовими затримками виявлення, що є особливо критичним у системах реального часу. Тому напрямками подальших досліджень є розробка нових методів, які ґрунтувались б на системах превентивного захисту, активному виявленні та усували недоліки відомих методів.

Науковий керівник – д.т.н., професор, Савенко О.С.

Можливості використання хімічно модифікованих плівок бактеріородопсину у системах захисту інформації.

УДК 539.23, 538.958, 004.056.53

Іван Трикур[1], Зіта Баторі-Тарці[2], Михайло Січка[3], Галина Різак[4], Василь Різак[5]

ДВНЗ «Ужгородський національний університет»
[1]ivan.trikur@uzhnu.edu.ua, [2]root@bathori.uzhgorod.ua,

[3]mykhaylo.sichka@uzhnu.edu.ua, [4]galyna.rizak@uzhnu.edu.ua,
[5]vrizak@uzhnu.edu.ua

Фотохромний трансмембранний білковий комплекс бактеріородопсин (БР), який синтезується галофільними мікроорганізмами, володіє унікальними властивостями, що привертає до нього увагу багатьох дослідницьких колективів у цілому світі. Бактеріородопсин на молекулярному рівні поєднує в собі кілька функцій, які можуть бути ефективно використані у системах безпеки, шифрування та захисту інформації. Матеріали на основі БР чутливі до поляризаційного запису інформації, демонструють значний фотохромний ефект у видимому діапазоні і володіють практично необмеженою реверсивністю, роздільна здатність носіїв даних на основі БР обмежується тільки оптичною системою, матеріал може бути забезпечений молекулярними мітками, які, в разі необхідності, дозволяють відстежувати матеріал до єдиної виробничої партії крім того для нього характерна екологічна чистота отримання і практична необмеженість ресурсів.

Поглинання кванту випромінювання переводить молекулу БР з основного у збуджений стан, після чого, за час близько 10 мс, вона проходить через ряд проміжних станів і повертається у вихідний стан, а поглинута енергія витрачається на трансмембранний перенос протону. Найбільшим часом життя та максимальним спектральним зсувом відносно основного стану (більше 150 нм) володіє інтермедіат M_{412}. Саме велика реверсивна фотоіндукована зміна спектру поглинання матеріалу і забезпечує механізм для його практичного використання. Однак для ефективного практичного використання необхідно збільшити час життя проміжного стану, а у деяких випадках покращити світлочутливість. Різними авторами був запропонований ряд методів, що дозволяють продовжити час життя стану M_{412}. Найбільш ефективними є методи генетичної модифікації амінокислотної послідовності БР або заміни фотохромної частини молекули на її синтетичні аналоги. Хоча процедури генетичної модифікації добре вивчені і відпрацьовані, вони все ж таки досить складні і передбачають отримання фіксованих змін фотохромності для конкретного виду мутації. В той же час відомо, що зміна хімічного складу плівок БР може в значній мірі впливати на їх оптичні властивості та динаміку фотоіндукованих змін. Хімічна модифікація має ряд переваг: внесення домішок набагато простіше з технологічної точки зору; різного типу домішки можуть у різній мірі впливати на певні властивості плівок; така методика модифікації передбачає можливість виготовлення плівок з різними властивостями на основі БР, отриманого за оптимізованими і добре відпрацьованими класичними методиками.

Метою даної роботи є дослідження можливостей хімічної модифікації оптичних властивостей плівок на основі бактеріородопсину для покращення ефективності їх використання у систем захисту інформації.

Речовини, які можна використати як сенсибілізатори для модифікації властивостей БР, повинні відповідати ряду вимог: розчинність речовини у воді, помірна хімічна агресивність, прозорість у області 350 – 750 нм. Ефективно впливати на час життя M_{412} будуть речовини, які за рахунок електровід'ємності

своїх функціональних груп або атомів, можуть зв'язувати вільні протони. Керуючись вищеперерахованим вимогам, в якості домішок були використані наступні речовини: триетаноламін (ТЕА), тетрабутиламіномід (ТБАБ), етилендіамінодигідрохлорид (ЕДА), додецилтриметиламінобромід (ДТМАБ), гексадецилтриметиламінобромід (ГТМАБ), L-аргінін гідрохлорид (АГХ), глутаральдегід (ГА), фенілтіосемикарбазид (ФТСК), тіосечовина (ТС). На основі кінетиики фотоіндукованих змін коефіцієнта поглинання на довжинах хвиль 412 та 570 нм проводили оцінку впливу хімічного складу на сенситометричну чутливість (S_{570}, S_{412}), фотоіндуковані зміни оптичної густини ΔD_{570}, ΔD_{412}, коефіцієнт участі молекул у фотоциклі (k_{412}) та час життя інтермедіату M_{412}.

Вводячи до складу плівки хімічні домішки у певних співвідношеннях можна у достатньо широкому діапазоні впливати на її характеристики. Найбільш помітний вклад у модифікацію параметрів фотоциклу, зокрема збільшення часу життя M_{412}, вносить триетаноламін що свідчить про високу чутливість БР до цієї речовини. Основна його дія проявляється в мікросекундному інтервалі часу і впливає на процес релаксації інтермедіату M_{412}, що приводить до росту амплітуди зміни поглинання та збільшення часу його життя до сотень секунд. Солі амінів АГХ, ЕАБГБ, ЕДАГХ та ГМДАГХ, приводять до зростання світлочутливості плівок, що означає зменшення енергетичних бар'єрів переходу $БР_{570} \leftrightarrow M_{412}$ у молекулі БР.

Як показали результати наших досліджень, варіюючи композиційний та кількісний склад плівок можна змінювати час збереження інформації у діапазоні від кількох до сотень секунд, змінювати сенситометричну чутливість S_{570} від $3.9 \cdot 10^{-3}$ до $54 \cdot 10^{-3}$ м^2/Дж неперервно. Дані властивості можуть ефективно використовуватися у системах захисту інформації та ідентифікації користувача, коли необхідний зворотній зв'язок між користувачем та терміналом. Абсолютна величина часу життя інтермедіату M_{412}, за умови можливості її неперервної зміни, може бути наперед задана, легко визначена терміналом і служити додатковим елементом захисту від підробок. Певні домішки, як наприклад ГА, можуть покращувати технологічність плівок (стійкість до вологи). Метод виготовлення хімічно модифікованих плівок технологічний, добре відпрацьований, не потребує складного обладнання. Перераховані вище факти дозволяють рекомендувати метод хімічної модифікації властивостей плівкових структур на основі БР для розширення можливостей прикладного використання останніх у сфері захисту інформації та контролю доступу.

Елементи технічного захисту інформації на аморфних напівпровідникових плівках.

УДК 53.03, 537.533.9

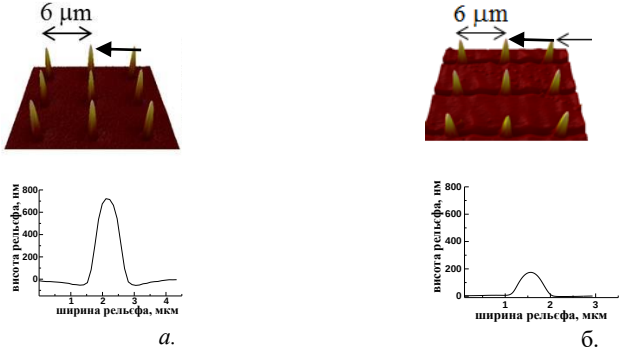
Василь Біланич[1], Oleg Shilenko[2], Vladimir Komanicky[2], Віталій Біланич[1], Alexander Feher[2], Іван Різак[1], Василь Різак[1]

Ужгородський національний університет[1]; vrizak@uzhnu.edu.ua
Pavol Jozef Šafárik University in Košice[2], alexander.feher@upjs.sk

Технічний захист інформації є важливим елементом національної безпеки держави. Концепція технічного захисту інформації в Україні є складовою забезпечення національної безпеки України. Окремими захисними елементами є рельєфні голограми. В останній час для виготовлення таких поверхневих структур використовують метод електронної літографії на полімерних резистах.

Метою даної роботи є розробка перспективних і екологічно чистих технологій виготовлення елементів технічного захисту на основі процесів акумуляції локальних і протяжних областей просторового заряду в тонких напівпровідникових плівках Ge(As)-Se при їх опроміненні променем електронного мікроскопа.

Для дослідження та реалізації процесу формування захисних елементів у вигляді поверхневих періодичних наноструктур були виготовлені аморфні плівки $Ge(As)_4Se_{96}$ товщиною 3 μm. В подальшому плівки опромінювали електронним пучком скануючого електронного мікроскопу Tescan, модель VEGA. Час експозиції t змінювали від 0,5 мс до 5 с. При цьому доза опромінення G становила $9.3*10^2$ - $9.3*10^7$ мкКл/см^2. Рельєф структури поверхні плівки був просканований з використанням атомно-силового мікроскопа (АСМ) Bruker, модель ICON з подальшою обробкою та визначенням параметрів з допомогою програми NanoScope Analysis.



а. б.

Рис.1. АСМ-зображення та профілі поверхневого рельєфу, індукованого електронним пучком на поверхні плівок Ge_4Se_{96} (*а.*) та As_4Se_{96} (*б.*) які формуються при опроміненні протягом 50 мкс.

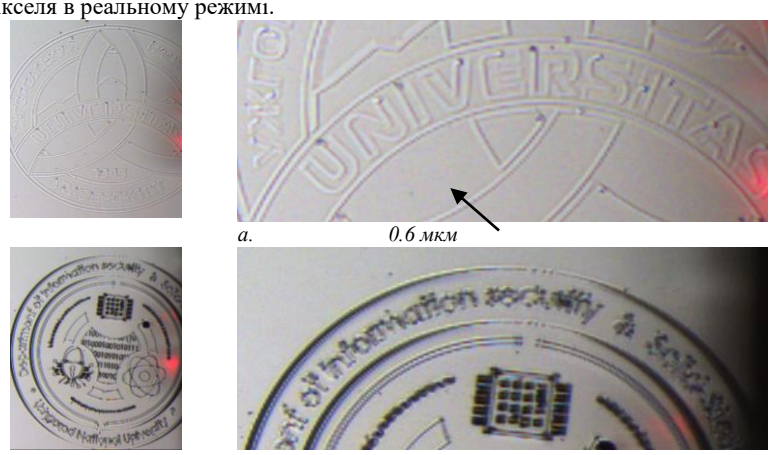
Плівки $Ge(As)_4Se_{96}$ були локально опромінені протягом різних часів експозиції, які визначали різні дози електронного опромінення. Для кожної окремої дози G на поверхні плівки формували матрицю (20x20) локально опромінених областей. Відстань між центрами таких областей уздовж ліній руху променя і між ними становила 6 μm.

На рис.1, показані скани опромінених областей плівок $Ge(As)_4Se_{96}$ і профілі індукованого електронним променем поверхневого рельєфу.

Величина області взаємодії (глибини проникнення електронного променя) для плівок $Ge(As)_4Se_{96}$ була обчислена за формулою Kanaya и Okayama:

$$R = 0.0276 \cdot \frac{A \cdot E_0^{\frac{5}{3}}}{\rho \cdot Z^{\frac{8}{9}}}$$

де A – середня атомна маса, Z - средній заряд ядра, ρ – густина плівок, E_o – енергія первинних електронів. Для досліджених плівок вона становила R ≈6.3 мкм. Оскільки при електронному опроміненні в об'ємі даних плівок утворювалися області просторового заряду, захисні елементи (мікро-зображення на поверхні плівок) формували при малих часах експозиції. Для такого літографічного процесу була використана технологія In-Flight Beam Tracing, яка дозволяє відстежувати параметри електронного променя в реальному часі. Вона дозволила змінювати час експонування від пікселя до пікселя в реальному режимі.



а. *0.6 мкм*

б.

Рис.2. Зображення логотипів, утворених на поверхні халькогенідних плівок з вмістом Ge (*а.*) і As (*б.*) з допомогою електронного променя без хімічного травлення.

На рис.2. показані зображення логотипів, утворених на поверхні плівок з вмістом Ge і As при опроміненні протягом 50 мкс на точку. Також з рис.1. видно, що висота електронно індукованого поверхневого рельєфу на плівці Ge_4Se_{96} у 4 рази більша ніж на плівці As_4Se_{96}. Це може бути пов'язано з більшою чутливістю даної плівки до електронного пучка.

Таким чином, на Ge і As вмісних халькогенідних плівках на основі селену реалізовано процес виготовлення якісного майстер-оригіналу захисного елемента методом одноступеневої (сухої) електронної літографії. Його репліка може бути використана для виготовлення відповідних захисних елементів методом штампування на полімерну основу

Задачи масштабирования облачных приложений для образовательной среды университетов

УДК
004.77:004.424

Береке Мадина

Казахский национальный педагогический университет им. Абая.
madina13.04@mail.ru

Как показал анализ зарубежных публикаций одной из наиболее востребованных технологий, применяемых в образовательных учреждениях в условиях не прекращающейся пандемии Covid 19, стало применение разнообразных облачных сервисов и технологий.

Пандемия Covid 19 привела к существенным изменениям в сфере образования Республики Казахстан (РК). Сегодня применение облачных технологий в университетах РК выступает эффективным инструментом в дистанционном учебном процессе. Облачные технологии изменили не только организационный процесс образования для студентов, но и научную и методическую работу преподавателей.

Переход на онлайн образование с использованием современных Интернет-технологий привел к определенным проблемам в системе высшего образования не только в РК, но и в других государствах.

Условно эти проблемы можно разбить на две группы.

К первой группе относятся проблемы, которые вызваны недостаточным опытом преподавателей, особенно ранее не связанных с применением информационных технологий в образовательном процессе. Тут сказался недостаток у преподавателей предыдущего опыта и навыков дистанционного обучения и организации самостоятельной работы учащихся. Изменилась и роль преподавателей университетов, которые по сути стали наставниками-консультантами, координирующими процесс обучения студентов.

Ко второй группе можно отнести более специфические вопросы, связанные с техническими аспектами применения различных облачных сервисов и приложений в образовательном процессе, начиная со школы и заканчивая университетами.

Сегодня технологии cloud computing стали одними из наиболее востребованных и интенсивно развиваемых в сфере образования не только РК, но и всего мира. В тоже время, возрастающая нагрузка на серверы как непосредственно учебных заведений, так и компаний провайдеров и центров обработки данных, порождает необходимость не только решать задачи методологического развития образовательного контента дистанционного обучения, но и уделять внимание техническим аспектам, в частности, вопросам масштабирования облачных приложений, используемых в образовательном процессе университетов.

Кроме того, говоря о технических аспектах и перспективах развития облачных приложений в учебном процессе университетов, следует обратить внимание и на критически важные характеристики облачных решений по показателям скорости и защищенности информационного обмена. Эти два показателя, как показал опыт применения облачных сервисов в университетах за последние два года, зачастую оказываются «противоположно направленными». Высокий уровень защиты зачастую существенно понижает скорости облачных взаимодействий и обмена данными. Напротив, комфортное взаимодействие в процессе обучения на высокой скорости обмена данными, порождает необходимость соблюдения весьма жестких требований к архитектуре и функциональности систем информационной безопасности (ИБ) облачной среды учебных заведений.

Переходя к масштабированию системы и большинства web-приложений, применяемых, при дистанционном образовании, прежде всего следует определить, какой из слоев является «узким местом» – то есть работает медленнее остальных в системе. Для начала можно применить утилиты *top* (*htop*). Это необходимо в ходе оценивания потребления мощностей процессора и памяти, а также *df, iostat* для оценивания расхода дискового пространства. Однако, предпочтительно выделять отдельный хост. Это дает возможность эмулировать нагрузку, например, с помощью программы JMeter.

Обычно «узкое место» зависит от архитектуры web-приложения. Самыми вероятными кандидатами на «узкие места» будут базы данных и коды приложений. Если приложения работают с большими объемами пользовательских данных, то «узкими местами», соответственно, скорее всего будут - хранение статики и контента пользователей (учащихся).

Типовое облачное приложение состоит из таких компонентов:

- управляющий модуль;
- программа, балансирующая нагрузку;
- горизонтально масштабируемые вычислительные модули.

Узлы, на которых функционируют вычислительные модули, можно как включить, так и выключить в режиме реального времени. Собственно, данный процесс и будет главной составляющей решения задачи масштабирования облачного приложения.

Для обеспечения комфортной и надежной работы облачных приложений, применяемых в образовательном процессе необходимо предусмотреть возможность автоматизированного управления ресурсами соответствующей облачной среды университета. Такую возможность может предоставить модуль автоматического масштабирования. Данный модуль должен войти в состав облачного приложения, которое предоставляет сервис приложения. Заметим, что модуль автоматического масштабирования будет использовать облачную инфраструктуру как на базе собственных серверов университета так ин базе

арендованных серверов, например, получая доступ к множеству серверов центров обработки данных крупных компаний, присутствующих на рынке облачных приложений.

По мере развития облачных технологий в образовательном процессе все большее количество систем становится доступным как педагогам, так и учащимся. Это в частности, такие системы как: Moodle, Blackboard, Canvas, Zoom, Webex meeting, Google Meet, GoogleClassroom и др., которые дают широкие возможности как непосредственно для создания дистанционных курсов, так и для проведения видео лекций и практических занятий с широкой интеграцией образовательного контента в структуру дистанционного курса, онлайн тестированием и т.п.

Заметим, что результаты исследований в данном направлении требуют отдельного изложения, которое выходит за рамки тезисов.

Таким образом, подводя итоги можно констатировать, что современные облачные технологии в образовании обеспечивают предоставление ресурсов учащимся и педагогам как online-сервисов. При этом отпадает необходимость в сменных носителях. При использовании облачной среды информация будет храниться в облаке. Кроме того, не нужно специально устанавливать дополнительное программное обеспечение на свой ПК. Главная функция облачных технологий – удовлетворение потребностей пользователей (учащихся), которым необходима полная обработка данных. При этом сохраняется концепция электронного обучения, основная суть которого заключается в возможности учиться на расстоянии. В таком случае облачные технологии выступают высокоэффективным инструментом, повышающим качество обучения и способствующим большей мобильности учащихся.

Дослідження методів виявлення зловмисного програмного забезпечення в мобільних операційних системах Android

УДК 004.056:004.49

Віталій Дильовий[1], Кіра Бобровнікова[2]

Хмельницький національний університет, [1]dylovyy.vitaliy@gmail.com, [2]bobrovnikova.kira@gmail.com

Стрімкий розвиток ринку мобільних пристроїв та використання цих пристроїв для зберігання конфіденційних даних призводять до підвищення кількості атак, спрямованих на порушення цілісності, конфіденційності та доступності інформації, що зберігається на цих пристроях. На сьогоднішній день зловмисне програмне забезпечення (ЗПЗ), орієнтоване на мобільні

пристрої, таке як криптомайнери, шпигунське програмне забезпечення, бекдори, банківські трояни та дроппери стають все більш актуальною загрозою для пристроїв, що працюють під управлінням операційної системи (ОС) Android [1]. Сучасне зловмисне програмне забезпечення володіє широким спектром можливостей, спрямованих на компрометацію мобільних пристроїв: від крадіжки грошових коштів з рахунків абонентів за допомогою відправки SMS на платні номери та номери з підвищеною вартістю, крадіжки контактів, історії телефонних переговорів та вмісту SMS до віддаленого керування мобільним пристроєм, контролю за переміщеннями власника мобільного пристрою, прослуховування телефонних розмов, переведення мобільного пристрою в режим мікрофону. Крім того, інфіковані мобільні пристрої використовуються для нанесення шкоди третім особам шляхом організації DDoS-атак і спам-розсилок з використанням мобільного пристрою. Оскільки ОС Android є найбільш поширеною операційною системою для користувачів мобільних пристроїв, то проблема виявлення ЗПЗ в мобільних ОС Android набуває важливого значення [1].

В сучасних наукових джерелах широко представлені різноманітні підходи до виявлення ЗПЗ в ОС Android. В [2] розроблено метод виявлення зловмисних програм, який класифікує програми на основі зворотного зв'язку з користувачами мобільних додатків. Однак у випадку мобільних ресурсів, що потребують значної частини дозволів, запропонований підхід може призвести до значної кількості хибних спрацювань. В [3] представлено підхід, заснований на комбінації дозволів та намірів, що залучає для виявлення ЗПЗ декілька етапів класифікації: багатошаровий персептрон, таблиці рішень та дерева рішень. Виявлення ЗПЗ здійснюється на основі визначення середнього значення ймовірностей, добутку ймовірностей та більшості голосів.

В [4] розроблено систему виявлення ЗПЗ, що базується на використанні глибокої згорткової нейронної мережі (CNN). Класифікація зловмисних програм здійснюється на основі статичного аналізу необроблених послідовностей кодів з дизасембльованих програм. В [5] розроблено систему глибокого навчання для виявлення зловмисних додатків Android за допомогою динамічного аналізу з використанням генерації вхідних даних з відстеженням стану. В [6] представлено систему, що використовує статичний аналіз та функціонує в чотири етапи. Система будує граф викликів для кожного додатку, з якого отримує послідовності API-викликів, після чого відносить кожен виклик до певного класу. Третій етап передбачає моделювання поведінки додатку шляхом побудови з послідовностей API-викликів ланцюгів Маркова. Ймовірності переходу, з яких формується вектор ознак, використовуються для класифікації додатків на доброякісне або зловмисне програмне забезпечення. Запропонований в [7] підхід використовує дискримінаційну змагальну мережу (DAN) з глибоким навчанням для класифікації додатків на зловмисні або доброякісні за трьома наборами ознак: необроблені коди операцій, дозволи та API-виклики. Запропонований підхід надає можливість виявлення зловмисних програм, які для ухилення від виявлення використовують методи обфускації.

Огляд літературних джерел показав, що проблема виявлення ЗПЗ в ОС Android є надзвичайно актуальною. Відомі методи виявлення ЗПЗ в мобільних

пристроях демонструють високий рівень ефективності, тим не менше, їх спільним недоліком є високий рівень хибних спрацювань. Також суттєвим недоліком вищезазначених підходів є потреба у значних обсягах обчислювальних ресурсів, ігнорування упакованого програмного забезпечення та нездатність адаптивно реагувати на атаки нульового дня. З огляду на вищезазначене, актуальною задачею є розроблення нових методів виявлення зловмисного програмного забезпечення у мобільних ОС Android.

Список літератури

1. McAfee Mobile Threat Report Q1, 2021. [Електронний ресурс] – Режим доступу: https://www.mcafee.com/content/dam/consumer/en-us/docs/2021-Mobile-Threat-Report.pdf.

2. Amro, B. Personal Mobile Malware Guard PMMG: a mobile malware detection technique based on user's preferences / B. Amro. – International Journal of Computer Science and Network Security, 2018. – Vol. 18, No. 1. – pp. 18–24.

3. Idrees, F. Pindroid: a novel android malware detection system using ensemble learning methods / F. Idrees, M. Rajarajan, M. Conti, T. Chen, Y. Rahulamathavan. – Computers & Security, 2017. – Vol. 68. – pp. 36–46.

4. McLaughlin, N. Deep android malware detection / N. McLaughlin, J. Martinez del Rincon, B. Kang. – Proc. of the Seventh ACM on Conference on Data and Application Security and Privacy, 2017. – pp. 301–308.

5. Alzaylaee, M. K. DL-Droid: Deep learning based android malware detection using real devices / M. K. Alzaylaee, S. Y. Yerima, S. Sezer. – Computers & Security, 89, 2020. – 101663.

6. Mariconti, E. MaMaDroid: Detecting Android Malware by Building Markov Chains of Behavioral Model / E. Mariconti, L. Onwuzurike, P. Andriotis, E. De Cristofaro. – ACM Trans. Priv. Sec., 2019. – Vol. 1, No. 1. – pp. 1–33.

8. Millar, S. DANdroid: A multi-view discriminative adversarial network for obfuscated Android malware detection / S. Millar, N. McLaughlin, J. Martinez del Rincon, P. Miller, Z. Zhao. – Proceedings of the tenth ACM conference on data and application security and privacy, 2020. – pp. 353-364.

Науковий керівник – к.т.н.,доцент Бобровнікова К.Ю.

Методи виявлення кіберзагроз мережного типу

УДК 004.492.2

Дмитро Сокальський[1], Яна Михасько[2]

Хмельницький національний університет, [1]sokalskij7@gmail.com, [2]yashamyy@gmail.com

Метою даної роботи є аналіз методів та класифікація виявлення кіберзагроз мережного типу.

Сьогодні однією з найпоширенішою кіберзагрозою мережного типу є атака на відмову в обслуговуванні або розподілену відмову в обслуговуванні (DOS або DDoS), яка може пошкодити або заблокувати доступ до ресурсів (рис. 1).

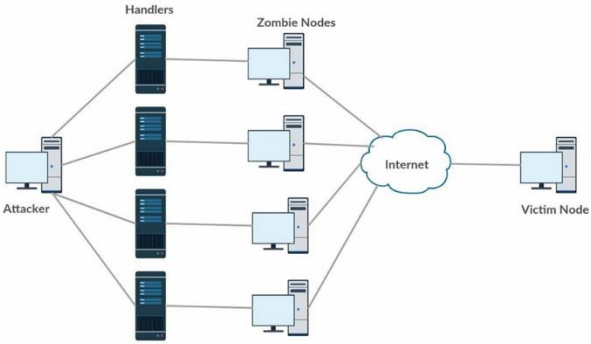


Рис. 1. Розподілена атака типу "відмова в обслуговуванні" (DDoS)

Методи виявлення та механізми захисту від DoS-атак можна умовно класифікувати за двома ознаками. Перша ознака - розташування механізму захисту в комп'ютерній мережі. Методи, які об'єднують різні схеми захисту і забезпечують їх взаємодію, зазвичай називають гібридними. Гібридні методи забезпечують кращий захист від кібератак, ніж окремі методи захисту, що працюють самостійно на різних сегментах мережі. Друга ознака - час застосування методу. Методи, які застосовуються до настання атаки, відносяться до методів запобігання, а ті методи, які використовуються під час атаки, відносяться до групи виявлення атаки і ідентифікації джерела. Після виявлення атаки застосовуються методи реакції на атаку. Найкращим варіантом є запобігання атаки. Воно може бути досягнуто на всіх етапах шляху мережевого трафіку, починаючи від джерела атаки і закінчуючи обробкою даних на стороні сервера, на який здійснюється атака. Найчастіше використовуються комбіновані засоби запобігання (IPS) і виявлення атак (IDS) - IPDS. Класифікація методів захисту від DoS-атак зображена на рисунку 2. Зазвичай у механізмах захисту на стороні сервера використовується клієнт-серверна модель для протоколів прикладного рівня. В такому випадку, сервер отримує запити, які створюються клієнтом (DNS-сервер, веб-сервер). Такий механізм мережевої взаємодії використовується в багатьох DoS-атаках.

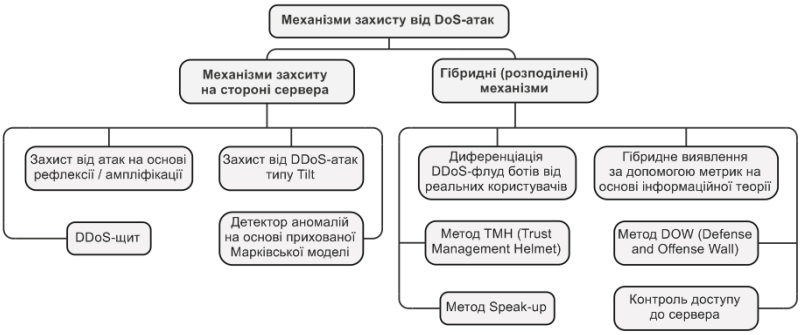


Рис. 2. Класифікація методів захисту від DoS-атак

Основними механізмами захисту проти подібних DoS-атак є:

- захист від DoS-атак на основі рефлексії/ампліфікації. Такі методи захисту спрямовані на виявлення шкідливого трафіку, який був створений при використанні таких протоколів як DNS та SIP та за допомогою різних прикладних методів, таких як, наприклад, технології машинного навчання;
- DDoS-щит - характеристики отриманих HTTP-запитів обчислюються за допомогою статистичних методів та детектор аномалій;
- захист від DDoS-атак типу Tilt призначений для моніторингу мережевого трафіку, і для різних користувачів забезпечує різні можливості.

Гібридні або розподілені механізми забезпечують захист мережі за допомогою взаємодії механізмів захисту як на стороні клієнта, так і на стороні сервера. Прикладами гібридних механізмів захисту є:

- метод Speak-Up. Принцип дії даного методу полягає у диференціації справжніх користувачів від зловмисників. Даний метод використовується для захисту від сесійних флуд-атак;
- метод DOW (Defense and Offense Wall). Даний механізм захисту використовує метод кластеризації K-Means, який призначений для виявлення та фільтрації сесійних атак, флуд-атак на основі запитів та асиметричних атак;
- диференціація DDoS-флуд-ботів від реальних користувачів. Цей механізм призначений для розрізнення звичайних користувачів та мережевих ботів;
- контроль доступу до сервера. Даний метод використовується для обмеження кількості одночасно підключених до сервера клієнтів. Контроль доступу до сервера здійснюється за допомогою приховування портів;
- метод TMH (Trust Management Helmet). В даному методі захисту використовується так зване “управління довірою”, яке призначене для розрізнення звичайних користувачів від зловмисників. Метою методу є забезпечення попереднього захисту зв’язку користувачів під час кібератаки;
- гібридне виявлення. Даний механізм захисту призначений для фільтрування підозрілих потоків та визначення параметрів поведінки користувача у мережі (швидкість HTTP-запиту, час перегляду сторінки).

Науковий керівник – науковий ступінь, д.т.н, доцент, Лисенко С.М.

Безпечна ідентифікація клієнта в протоколах передачі інформації без збереження стану

УДК 004.056.53 (043.2)

Василь Буковецький[1], Василь Різак[2]

Ужгородський Національний Університет, [1]bukovetsky@outlook.com, [2]vrizak@uzhnu.edu.ua

Стрімкий розвиток мережі Інтернет та технологій відкрив шлях до створення динамічних веб-ресурсів та клієнт-серверних додатків, які можуть надавати користувачеві персоналізовані сервіси. Такий функціонал досягається постійним обміном даними клієнтського додатку із сервером. Найпоширенішим

протоколом передачі даних в мережі Інтернет є HTTP, який є протоколом без збереження стану. Використання протоколу без збереження стану потребує постійної передачі ідентифікуючих користувача даних в кожному запиті. Одним з найрозповсюдженіших методів ідентифікації при такій комунікації є прикріплення певного маркера (токена) доступу до кожного нового запиту. Прикладами таких маркерів є ідентифікатор сесії та JSON Web Token.

Передача таких даних через мережу відкриває чимало можливостей для атак, головною ціллю яких буде саме маркер доступу. Отримання цієї інформації дозволить зловмиснику представлятися користувачем, навіть не знаючи його основних даних для входу у веб-сервіс (зазвичай це ім'я користувача та пароль). Такими веб-сервісами можуть бути онлайн-банкінг, керування системою розумного будинку, тощо.

Найрозповсюдженішим методом захисту є використання шифрування протоколів SSL/TLS. SSL/TLS — криптографічні протоколи, які забезпечують встановлення безпечного з'єднання між клієнтом та сервером.

Саме на ці криптографічні протоколи покладається функція захисту конфіденційності даних в більшості сучасних веб-додатків, відповідно саме ці протоколи захищають такі важливі дані як маркери доступу.

Нажаль, протоколи HTTPS та SSL/TLS мають свої недоліки та по тим чи іншим причинам можуть не вберегти конфіденційні маркери доступу від рук зловмисника

Метою даної роботи є покращення захисту маркерів доступу за допомогою методу ідентифікації клієнта, в якому ідентифікатор сесії не буде передаватись в доступному для використання зловмисником виді.

Розглянемо найрозповсюдженішу методику обміну даними між клієнтом та сервером. Клієнт ініціює нову сесію відправляючи в тілі першого запиту своє ім'я користувача та пароль. На такий запит сервер може відповісти негативно (якщо дані для входу неправильні) або позитивно. У випадку позитивної відповіді сервер надсилає маркери доступу. При кожному наступному запиті клієнт відправляє отримані маркери доступу в тілі запиту, в окремому заголовку чи в Cookie. По отриманому маркеру доступу, сервер шукатиме в БД відповідного йому користувача, та відносно цього вже буде формувати свій запит.

Розглянемо найрозповсюдженішу методику обміну даними між клієнтом та сервером. Клієнт ініціює нову сесію відправляючи в тілі першого запиту своє ім'я користувача та пароль. На такий запит сервер може відповісти негативно (якщо дані для входу неправильні) або позитивно. У випадку позитивної відповіді сервер надсилає маркери доступу. При кожному наступному запиті клієнт відправляє отримані маркери доступу в тілі запиту, в окремому заголовку чи в Cookie. По отриманому маркеру доступу, сервер шукатиме в БД відповідного йому користувача, та відносно цього вже буде формувати свій запит.

Розглянемо найрозповсюдженішу методику обміну даними між клієнтом та сервером. Клієнт ініціює нову сесію відправляючи в тілі першого запиту своє ім'я користувача та пароль. На такий запит сервер може відповісти негативно (якщо дані для входу неправильні) або позитивно. У випадку позитивної

відповіді сервер надсилає маркери доступу. При кожному наступному запиті клієнт відправляє отримані маркери доступу в тілі запиту, в окремому заголовку чи в Cookie. По отриманому маркеру доступу, сервер шукатиме в БД відповідного йому користувача, та відносно цього вже буде формувати свій запит.

При використанні запропонованого методу, даних які відправляються з кожним запитом не буде достатньо для формування зловмисником нового запиту від імені справжнього користувача. Звичайно, такий метод передачі не захистить дані які відправляються від розкриття, але значно зменшить шанси зловмисника на отримання повного контролю над обліковим записом користувача.

Слід зауважити, що маркери доступу можуть бути перехоплені при початковому обміну секретом, тому на цьому етапі рекомендується використовувати протокол Діффі-Гелмана (або аналогічний асиметричний протокол) для обміну ключами та подальшій зашифрованій передачі секрету.

ТЕХНОЛОГІЇ УПРАВЛІННЯ ІНФОРМАЦІЄЮ СУЧАСНОЇ КОМПАНІЇ

УДК: 330.47

Людмила Кургузенкова

Приватний вищий навчальний заклад «Європейський університет»

kurguzenkova@ukr.net

У умовах сьогодення, коли четверта промислова революція (4IR) має яскраві прояви майже у всіх сферах життєдіяльності, цінність інформації як фактора конкурентоспроможності сучасних компаній набуває дедалі вагомішого значення. Сучасним компаніям доводиться вести діяльність в умовах стрімких змін, жорсткої конкурентної боротьби, необхідності забезпечення індивідуального підходу до кожного клієнта і підвищених вимог урядів і регуляторів до термінів підготовки звітності і достовірності наданої інформації. Коли доступ до традиційних ресурсів стає відкритим, коли майже зникають границі між економічними регіонами та системами внаслідок активного застосування інформаційно-комунікаційних технологій, коли класичні підходи до забезпечення конкурентоспроможності не спрацьовують, об'єктивно виникають передумови для пошуку нових джерел конкурентних переваг, перш за все — «всередині» організації, що знаходить своє відображення в концепції інформаційного менеджменту.

Управління інформацією (Enterprise Information Management, EIM) є окремою галуззю знань, метою якого є координація діяльності по роботі з інформацією, включаючи інформаційні технології, інформаційну безпеку, маркетинг, рекламу; спеціалізується на рішеннях щодо раціонального використання інформації в межах організацій, наприклад, для підтримки управлінських рішень або операційної діяльності, що вимагає наявності знань.

Управління інформацією організацій (виявлення, отримання, нарощування і управління) можна здійснювати за допомогою різних програмних продуктів, зокрема з використанням Microsoft SQL Server 2016. Розглянемо більш детально окремі із його компонентів.

Компонент «Project Barcelona» служить для автоматичного збору інформації про наявні сервіси, портали, інтеграційні проекти, джерела фінансування даних, служби звітності, а потім простежити зв'язок між цими об'єктами.

Компонент «Integration Services» дозволяє завантажувати і перетворювати дані між різними системами (в тому числі, для завантаження даних в сховище даних).

Компонент «Master Data Services» надає можливість управляти нормативно-довідковою інформацією як на рівні Excel- і Web-інтерфейсів, так і на рівні програмних інтерфейсів.

Компонент «Data Quality Services» надає стандартні засоби очищення і зіставлення даних, на підставі наявних баз знань.

В результаті застосування перерахованих вище технологій процес управління інформацією організації може здійснюватися в наступній послідовності:

За допомогою проекту Barcelona здійснюється аналіз наявних баз даних та систематизація інформації. На підставі цієї інформації можна розробляти інтеграційні проекти. В інтеграційному проекті Integration Services по завантаженню даних в сховищі даних першим кроком виконується вилучення даних в проміжну область. Наступним кроком, для автоматичної очистки наявних некоректних даних застосовується Quality Services, після чого потік даних зіставляється з сутностями в Master Data Services. У випадку, якщо відповідність з нормативно-довідковою інформацією не знайдено, ці записи можна зберегти в окремому місці зберігання і потім зіставити з застосуванням Data Quality Services в ручному режимі, наприклад, з використанням Excel і надбудови MDS з функціями DQS. Відкориговані дані за допомогою SSIS публікуються в системі-споживачі (наприклад, в сховище даних). Подальшу автоматичну інвентаризацію наявних даних, інтеграційних проектів та звітних систем можна здійснити за допомогою проекту Barcelona. Це дозволить в майбутньому врахувати всі залежні системи при внесенні змін до структури даних.

Метод вилучення формантних частот на основі побудови огинаючої спектральної декомпозиції для мовного сигналу

УДК 004.056.5:004.93

Сергій Зибін[1], Яна Бєлозьорова[2]

Національний авіаційний університет, [1]serhii.zybin@nau.edu.ua, [2] yana.bielozorova@npp.nau.edu.ua

У системах ідентифікації мовного сигналу отримання характерних ознак мови особи, є одним з основних запорук успіху роботи системи ідентифікації

мовної інформації. У завданнях аналізу мовного сигналу з метою визначення найважливіших характеристик, як правило, використовують методи його частотно-часового або спектрального уявлення, одними з найбільш ефективних є методи вейвлет перетворення мовного сигналу. Найважливішим параметром, що характеризує спектр (розподіл енергії або амплітуди по частотах) мовного сигналу є форманти, які визначають як концентрацію енергії в обмеженій частотній області. Форманта характеризується частотою, шириною частотної смуги і амплітудою.

Форманти є одними з основних елементів ідентифікації особи в мовному сигналі тому, що природа їх походження пов'язана з порожнинами людського мовного тракту. Зважаючи на індивідуальність подібних компонентів для кожної людини можна зробити висновок, що визначення формантих частот є важливим компонентом побудови системи ідентифікації мовної інформації.

Виділення формант супроводжує цілий ряд проблем, пов'язаних з їх динамічної зміною в процесі мови. Навіть однакові голосні змінюють формантий набір в залежності від свого розташування у складі слів, складів та ін. Складність також визивають цілий ряд проблем, пов'язаних з близьким розташуванням піків при аналізі спектрограм та проблемами правильного визначення піків максимумів формант на спектрограмі. Визначення розташування формант на спектрограмах мовного сигналу достатньо легко виконується людиною, але автоматизація цього процесу визиває деякі складнощі.

Типове представлення спектрограми з розміченими людиною розташування формант представлено на рис. 1. Проведення подібного розмічення є досить складною задачею, зважаючи на велику кількість конкуруючих частотних піків.

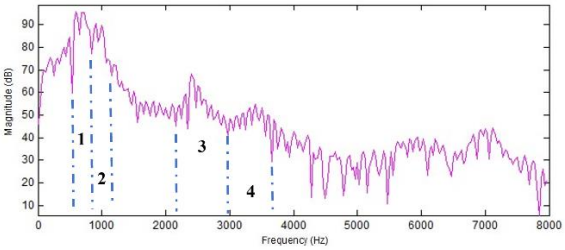


Рис 1. Визначення формант людиною

Крім того, під час проголошення окремих видів звуків на положення формант можуть впливати безліч факторів, що може приводити до коливань фрактальних частот, а на окремих елементах навіть відсутності деяких з них.

Існує декілька підходів для визначення положень формант на частотній шкалі, але всі вони базуються на аналізі та перетвореннях спектрограми мовного сигналу. При виділенні формантих частот першим етапом дослідження завжди є побудова спектрограми за визначеними дослідником критеріями. Серед них є ширина фрейму, тип вейвлет-базису, частотний діапазон та ін.

Проведені дослідження вказують на відповідність розподілу частот відносно голосних звуків, які вносять найбільшу вагу в формування формант в мовному сигналі. Встановлено, що українські голосні звуки "і" та "и", розташовані в частотному діапазоні 200 – 500 Гц, більшість інших голосних звуків лежать в діапазоні від 500 до 1500 Гц. Зважаючи на це, раціональним є окремий розгляд цих частотних діапазонів, при формуванні характерних ознак мовного сигналу, що дозволяє підвищити кількість параметрів, та набирати більшу статистику при визначенні максимумів формантих частот.

Результатом проведеного огляду підходів до визначення формантних частот став алгоритм, що складається з наступних складових:

1. Розділення МС на часові фрагменти.
2. Для кожного фрагменту отримання спектру.
3. Побудова огинаючої лінії.
4. Находження всіх максимумів.
5. Визначення положень формант.
6. Побудова графіків траєкторії положення формант.
7. Розрахунок залежності щільності імовірності розподілу кожної з чотирьох формантих частот (максимумів формантих частот).

Згідно розглянутого підходу до визначення формантних частот необхідно побудувати огинаючу спектру для кожного з фрагментів мовного сигналу. Фактично побудова функції огинаючої представляє собою задачу інтерполяції.

Результатом розрахунку огинальної буде сумісний графік спектру мовного сигналу, в заданому фрагменті, та огинальної спектру для цього ж інтервалу.

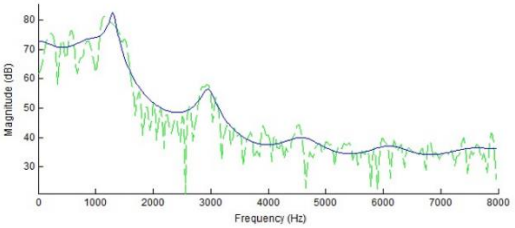


Рис. 2. Огинальна спектру мовного сигналу

Проведений порівняльний аналіз показує достатньо високу точність визначення формантих частот в порівнянні з кепстральним та LPC методами. Поряд з цим, необхідно відзначити простоту реалізації, низьку обчислювальну складність, швидкість та відповідність методу існуючим фізичним процесам.

Information security methods in the enterprise

УДК 316.774:351.75

Svetlana Ermishova, Kurhuzenkova Lyudmila, Husey Qiyasov
European University, qgusein@gmail.com

In order to start listing the methods of protecting information in an enterprise, you need to decide what types of information security threats are often encountered by the enterprises themselves.

- Natural.

These are threats caused by reasons beyond human control. These include hurricanes, fires, lightning strikes, floods, and other natural disasters.

- Artificial.

This is a complex of human-created information security threats. Man-made threats, in turn, are divided into intentional and unintentional. Intentional threats include the actions of competitors, hacker attacks, sabotage of offended employees, etc. Unintentional threats arise as a result of actions committed due to lack of competence or through negligence.

- Internal.

These are threats that arise within the information infrastructure of an enterprise. These include:

1. aging and wear and tear of hardware parts, as a result of which data is damaged;
2. computer resources are used incorrectly;
3. the software is used incorrectly or incorrectly;
4. over time, a large number of various errors accumulate in the data structure, which can lead to their damage.

- External.

These are threats that originate outside the information infrastructure of the enterprise. There are also passive threats and active threats. Passive threats are influencing factors that cannot change the content and structure of information.

Active threats are influencing factors that can change the content and structure of information. These include malicious software. Malware means the following:

1. viruses;
2. macro viruses for Word and Excel;
3. boot viruses;
4. script viruses, including batch viruses that infect the Windows shell, Java applications, etc.
5. keyloggers;
6. programs for stealing passwords.

In order to build competent and professional protection for the enterprise, information security concepts are created. Due to the fact that each enterprise has different areas and volumes of data, different structures, there are individual approaches to the creation of concepts, which take into account all the specifics and characteristics of a particular enterprise. An example of one of the concepts is as follows:

- develop internal documentation that establishes the rules for working with computer equipment and confidential information;
- conduct briefings and periodic checks of personnel; initiate the signing of additional agreements to labor contracts, which indicates responsibility for the disclosure or misuse of information that has become known from work;
- delimit areas of responsibility in order to exclude situations when the most important data sets are at the disposal of one of the employees; organize work in common workflow programs and make sure that critical files are not stored outside network drives;
- implement software products that protect data from copying or destruction by any user, including the top management of the organization;
- make plans for system recovery in case of failure for any reason.

Let's move on to the means of protecting information. What do means of information protection mean? Information security means are devices, devices, gadgets, software, organizational measures that prevent information leakage and ensure its preservation under the influence of the entire spectrum of current threats.

A wide range of specialized software is used to protect data in modern networks. The following types of software protection can be distinguished:

- Antivirus software. Specialized software for detecting, neutralizing and removing computer viruses. Discovery can be performed during scheduled or administrator-run scans. Programs detect and block suspicious program activity in "hot" mode.
- Cloud antiviruses (CloudAV). Combining the capabilities of modern antivirus programs with cloud technologies. Such solutions include Crowdstrike services, Panda Cloud Antivirus, Immunet and many others. All the basic functionality of the software is located in the cloud, and a client is installed on the protected computer - a program with minimal technical requirements. The client uploads the bulk of the data analysis to the cloud server. This ensures effective anti-virus protection with minimal resource requirements for equipment. CloudAV solutions are ideal for protecting PCs that do not have enough free computing power to run standard antivirus.
- DLP (Data Leak Prevention) solutions. Special software solutions to prevent data leakage. This is a set of technologies that effectively protect enterprises from the loss of confidential information for a variety of reasons. Implementation and support of DLP - requires a fairly large investment and effort on the part of the enterprise. However, this measure can significantly reduce the level of information risks for the company's IT infrastructure.
- Cryptography systems. They transform the data, after which their decryption can only be performed using the appropriate ciphers. In addition, cryptography can use other useful applications to protect information, including message digests, authentication methods, encrypted network communications, and digital signatures. Today, new applications that use encrypted communications, such as Secure Shell (SSH), are gradually replacing outdated solutions that do not provide the required level of security in today's environment, such as Telnet and the FTP file transfer protocol. Modern WPA /

WPA2 protocols are widely used for wireless encryption. The rather old WEP protocol is also used, which is inferior in terms of security.

- Firewalls (ITU). Solutions that filter and block unwanted traffic control network access. There are such types of firewalls as network and host servers. Network firewalls are located on LAN gateway PCs, WANs and intranets. The firewall can be executed in the format of a program installed on a regular computer or have a software and hardware implementation.
- Virtual private networks VPN (Virtual Private Network). A solution that uses a private network to send and receive data over a public network, effectively protecting network-connected applications. VPN provides the ability to remotely connect to a local network, creating a common network for the head office with branches. Directly for users, VPN provides location hiding and protection of online activities.
- Proxy server. Serves as a gateway between a computer and an external server. A request sent by a user to the server first goes to the proxy and on its behalf goes to the server. The response is also returned with the passage of an intermediate link - proxy. The advantage is that the proxy server cache is available to all users. This improves usability because the most frequently requested resources are in the cache.
- SIEM solutions - information security monitoring and management systems. Specialized software that takes over the data security management function. SIEM collects information about events from all sources that support security, including antivirus software, IPS, firewalls, as well as operating systems, etc. SIEM also analyzes the collected data and provides its centralized storage in the event log. Based on data analysis, the system identifies possible failures, hacker attacks, other deviations and possible information threats.

Cryptanalysis of Markov ciphers and Markov-type ciphers

УДК 621.395.7 (043.2)

Ruslan Skuratovskii[1], Lisa Kostina[2]
National Aviation University
[1] r.skuratovskii@kpi.ua, ruslan@imath.kiev.ua,
[2] 6324462@stud.nau.edu.ua

The object of the research is block ciphers with a round function of the form $G_k(x) = L_m(S(x \oplus k_i))$ These ciphers are considered from the point of view of their belonging to the class of Markov or generalized Markov cipher.

The main results described in this article are as follows (note that by complexity we mean the number of encryptions required to create all the necessary pairs, and during the attack, the algorithm itself uses, generally speaking, less material). DES with 6 rounds was cracked in less than 0.3 seconds on a personal computer using 240 ciphertext. 8-round DES was cracked in less than two minutes on a computer by analyzing 15,000 ciphertext, selected from a set of 50,000 ciphertext candidates. 15-round DES breaks faster than brute-force, but 16-round DES still requires 2^{58} steps (this is slightly more than brute force complexity).

It is well known, for the DES algorithm, after finding 48 bits of the key of the last round, the remaining 8 bits are complete search [7].

The following condition is necessary for successful application of attack by the DC (differential cryptoanalysis) method:

$$\exists \Delta x, \Delta y \in V_m \forall K \in (V_n)^2 \forall x \in V_m : P(E_K^{(r-1)}(x \oplus \Delta x) \oplus E_K^{(r-1)}(x) = \Delta y) = p, \text{ where } p >> 2^{-m},$$

and probability is taken by all $x \in V_m$.

In work [5,9,10], definitions of the Markov cipher (hereinafter - MS) are given for the first time.

Definition 1 An iterated cipher with round function $Y = f(X, Z)$ is Markov [9,10,5] if there is a group operation $\otimes$ for defining differences such that, for all choices of α ($\alpha \neq e$) and $\beta : \beta \neq e$:

$$P(\Delta Y = \beta \mid \Delta X = \alpha, X = \gamma) \qquad (1)$$

is independent of γ, when the subkey Z is uniformly random (distributed).

Let's denote the reflection $f_k : V_m \to V_m$ which $\forall k \in V_m$: is a bijection. Therefore, $\exists f_k^{-1} : V_m \to V_m$. Here and further, as in all works devoted to the DC, we will assume that the round keys are random and independent. Let's denote $x_0 \in V_m$ — vector, fed to the input of the first round of the cipher; for $i = \overline{1, n}$ denote a vector which is the output of the i-th round (or the input of the i + 1 round) by $x_i = f_{k_i}(x_{i-1})$.

- We present the following algorithm of finding the key of the last round by the DC method.

1. Let's choose about $N \approx \frac{1}{p}$ pairs of type $x_0^{(i)}, x_0^{(i)} \oplus \Delta x, \partial e\, x_0^{(i)} \in V_m, \ i = \overline{1, N}.$
2. Using the 'black box', we calculate the corresponding pairs $E_K(x_0^{(i)}), E_K(x_0^{(i)} \oplus \Delta x), \ i = \overline{1, N}.$
3. We fix some $k_r \in V_n$, that will be a "candidate" for the key of the last round.
4. Calculate : $\Delta z_i = f_{k_r}^{-1}(E_K(x_0^{(i)})) \oplus f_{k_r}^{-1}(E_K(x_0^{(i)} \oplus \Delta x)), i = \overline{1, N}.$

That is, in point 4, for each pair $x_0^{(i)}, x_0^{(i)} \oplus \Delta x$ from point 1, we calculate the results of encryption of its components after the r-th round and find their difference

Δz_i, $i = \overline{1,N}$. We calculate $N(k_r)$ that is the number of pairs for the Δ, namely $N(k_r) = \#\{i = \overline{1,N} : \Delta z_i = \Delta y\}$.

The procedure described in items 3 and 4 is repeated for each ‘candidate in the key of the last round, that is, for each element from V_n.

5. The correct key k_r for the last round (most likely, such a key will be the only one) is the one for which the number $N(k_r)$ will be the largest.

This algorithm of finding the key of the last round are extended by us on generalized Markov ciphers [4].

References

1. Eli Biham and Adi Shamir. «Diferential Fault Analysis of Secret Key Cryptosystems». Proceedings of Eurocrypt, Lecture Notes in Computer Science, 1233:37-51, 1997.
2. Debdeep Mukhopadhyay. An improved fault based attack of the advanced encryption standard. In Bart Preneel, editor, AFRICACRYPT, volume 5580 of Lecture Notes in Computer Science, pages 421–434. Springer, 2009.
3. Michael Tunstall and Debdeep Mukhopadhyay. Differential fault analysis of the advanced encryption standard using a single fault. Cryptology ePrint Archive, Report 2009/575, 2009, http://eprint.iacr.org/.
4. R. C.-W. Phan and S.-M. Yen. Amplifying side-channel attacks with techniques from block cipher cryptanalysis. In Smart Card Research and Advanced Applications, 7th IFIP WG 8.8/11.2 International Conference, CARDIS 2006, volume 3928 of Lecture Notes in Computer Science, pages 135–150. Springer, 2006.
5. FIPS PUB 197: Advanced Encryption Standard, http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf
6. C. Giraud, “DFA on AES,” Cryptology ePrint Archive, Report 2003/008, 2003.
7. Ruslan~Viacheslavovich Skuratovskii. Employment of minimal generating sets and structure of sylow 2-subgroups alternating groups in block ciphers. Advances in Computer Communication and Computational Sciences, pages 351--364. Springer, 2019.
8. Skuratovskii, R. An Application of Metacyclic and Miller-Moreno p-Groups to Generalization of Diffie-Hellman Protocol. Advances in Intelligent Systems and Computing, 2021, 1290, pp. 869–876.
9. Xuejia Lai, James L. Massey, Markov Ciphers and Differential Cryptanalysis, Advances in Cryptology, proceedings if EUROCRYPT '91, Lecture Notes in Computer Science 547. pp. 17-38, 1992..

10. X.Lai and J.L.Massey, “A Proposal for a New Block Encryption Standard”, Advances in Cryptology-EUROCRYPT’90 Springer-Verlag, Berlin 1991, pp. 389-404.

Modeling Strong Keys Generating in Blockchain and key distribution problem

УДК 621.395.7 (043.2)

Ruslan Skuratovskii[1], Alexandr Kalenyk[2]

National Aviation University, ORCID: 0000-0002-5692-6123.

[1]ruslcomp@gmail.com, [2]oleksandr.kalenyk.bit@stud.nau.edu.ua

Keywords— non-commutative cryptography, CSP and CDH problems; Miller-Moreno p-group, generalization of CDH problem, conjugacy problem, blockchain.

Since the idea of public key cryptography (PKC) was introduced by Diffie and Hellman [2, 4] in 1976, many PKC schemes have been proposed and broken. For instance Diffie Hellman key exchange protocol is vulnerable to man in the middle attack during key exchange steps. To prevent these attacks we propose to use block chain and divide on domains blockchain. The automatic generation of unique one-time keys prevents the connectivity of transactions and is possibly due to the optimization of the key exchange using the Diffie-Hellman method.

Any subset of nodes had to have a unique multisignature key. Multisignature is a technology for signing transactions with multiple private keys to increase the level of security and privacy during the approval process for sending transactions. A multisignature is a kind of threshold signature, implemented as a check of conditions specified in the basic scripting language of the cryptocurrency.

Multisignature technology has become widespread in the world of cryptocurrencies. A token is a digital certificate that guarantees the company's obligations to its owner, an analogue of shares on the stock exchange in the world of cryptocurrencies Threshold signature - a variant of an electronic signature, for the imposition of which the cooperation of at least t members of a group of n participants is required, denoted as S_n. In essence, it is a special case of the threshold division of a secret according to the (*t, n*) scheme, when the private key is divided into n parts, and any t parts are sufficient to restore it. The public key is used in the usual way. Generation, sharing of a key and distribution of its fragments requires a group manager (dealer).

Note that such a group can be in particular a manning pool consisting of n participants. Let us denote by $m_{ij}(n)$ the number of tokens in the wallet of the *i*-th account belonging to the subset S_n of *n* accounts from the blockchain. Note that one participant can have several accounts, so we consider double indexing $m_{ij}(n)$ where a number of wallet in the blockchain network denoted by *i* and j is the owner of the

wallet. More generally, cryptocurrency can be used instead of tokens. It is convenient to express the value of a token in cryptocurrency as in monetary terms. We introduce a double threshold signature condition according to the scheme (t, n), where any t participants from S_n satisfying the inequality

$$\sum_{i=1}^{t} m_{ij}(n) \geq S(n)$$

where $j \in S_n$ that is, the participant j really belongs to a group S_n of n persons. And S_n is the boundary number of tokens (or their value in the specified crypto currency) that persons must have in order to be eligible for multisignature. Thus, our multisignature is a double threshold signature with a boundary condition tied to a certain cryptocurrency or a certain type of tokens.

It should be noted that the right to sign on behalf of the group also had some of the nodes that collectively satisfy certain conditions. We propose the condition of financial solvency in relation to this group of users. In the simplest case, a certain percentage of the number of nodes. For example, there are 10 users in a group. But any 3 can sign if their accounts have the required number of tokens in total.

We will divide the entire blockchain into domains, each of which has its own digital signature. Only those domain entities whose wallets have the number of tokens in excess of a percentage of the critical number of tokens of the entire blockchain domain have the right to sign. The persons who has the authority to sign in the i-th domain will be denoted by S_i. If a domain member does not have a number of tokens that exceed the percentage of critical tokens of the entire domain i, it can apply for the right to sign to the authorized person of his domain S. It should be noted that S can be located at the intersection of domains, then the process of transferring the key is simplified due to the fact that an authorized person acts as a surety of two parties at once.

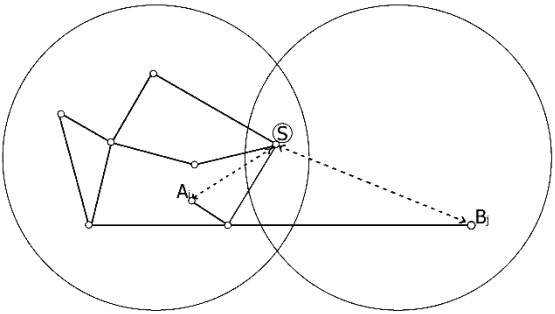


Fig. 1 Location of information exchange participants, with S at the intersection

We consider this case that is specified at Fig. 1. Suppose that *S*, as shown in the figure, is at an intersection, A located in *i*-th domain intends to transfer the secret key a, to person *B* in domain j, then A encrypts the component of new secret key k wich *A* and *B* going to construct, with using the conjugating by secret key x and sends it for signature to authorized persons *S*, in turn, returns the message with signature. Then the process of transferring the key to side *B* takes place. Side *B* receives the message and sends it for verification to S, and only then encrypts the received message with its key.

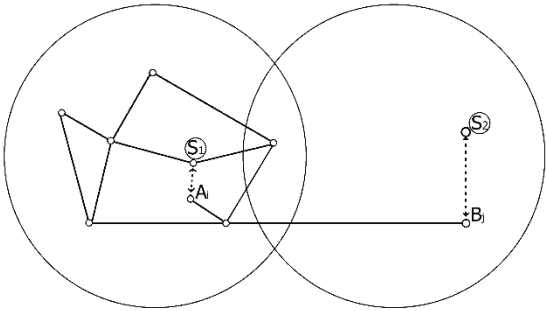


Fig. 2 Location of information exchange participants, without S at the intersection

In the second case that is specified at Fig. 2, at the intersection of domains there is no person with the authority to sign S, then we denote the person with the authority to sign in the domain in which A is located as S_1, in the case of side B, as S_2, respectively. It is worth noting that the parties S_1 and S_2 must have a part of the digital signature of the neighboring domain, or the ability to exchange with a secure transmission channel. Then A, as in the first case, encrypts the message and transmits it to S_1, then, S_1 returns the tuple [$x^{-1}ax$, $Sign(x^{-1}ax)$]. After the transfer now side B sends the not signed message to S_2 for identification.

We consider non-commutative generalization of CDH problem [6] on base of metacyclic group *G* of Miller-Moreno type (minimal non-abelian group). We show that conjugacy problem in this group is intractable.

For preventing attacks of decomposition or man in the middle attack [3] both key exchange protocol participants send to network arbitrator (*O*) hash $h(\beta)$ and a hash of conjugated element $h(\beta^g)$ [1] by an private key element β.

Thus, our protocol it not vulnerable for the attack of the man in the middle by solving the decomposition problem [8] of key exchange.

[1] Skuratovskii, R. V. Employment of Minimal Generating Sets and Structure of Sylow 2-Subgroups Alternating Groups in Block Ciphers. Advances in Computer Communication and Computational Sciences, Springer, pp. 351–364, 2019.

[2] Skuratovskii, R. V. A Multi Agent-Based System for Securing University Campus: Design and Architecture - IEEE Conference Publication. 2019-12-17. doi:10.1109/ISMS.2010.25.

[3] Skuratovskii, R. V. The timer compression of data and information.Proceedings of the 2020 IEEE 3rd International Conference on Data Stream Mining and Processing, DSMP 2020, pp. 455–459.

[4] Skuratovskii, R. An Application of Metacyclic and Miller-Moreno p-Groups to Generalization of Diffie-Hellman Protocol. Advances in Intelligent Systems and Computing, 2021, 1290, pp. 869–876.

[5] Gu, L., Zheng, S.: Conjugacy systems based on nonabelian factorization problems and their applications cryptography, J. Appl. Math. 6 pp. 1–10, 2014.

[6] Gu, L. Wang, L., Ota, K., Dong, M., Cao Z. and Yang, Y.: New public key cryptosystems based on non-abelian factorization problems, Secur. Commun. Netw. 6 (7), pp. 912–922, 2013.

[7] Bohli, J.-M., Glas B., and Steinwandt, R.: Towards provable secure group key agreement building on group theory, Cryptology ePrint Archive: Report 2006/079, 2006.

Functional security profile settings model

UDC 004.056.5 (043.2)

Maxim Shaban[1], Olena Vysotska[2], Natalia Vyshnevska[3], Volodymyr Shcherbyna[4]

[1]Pukhov Institute for modeling in energy engineering of NAS of Ukraine, [1]maximsaban@gmail.com
[2]National Aviation University, [2]lek_vys@ukr.net
[31]National Aviation University, [3]viserj@ukr.net
[4]National Aviation University, [4]smya@nau.edu.ua

To solve the problem of identification of the functional profile of protection (FPP), it is necessary to carry out: determination of levels of functional security services (FPS), implemented in complex systems of information security (CSIS) of the object of expertise; determining the completeness and inconsistency of the profile; identification of the FPs description in the source documents. With this in mind, a model of parameters for the identification of FPP in computer systems (CS) is proposed.

Defining a set of criteria. We will form a set of all criteria for information security

$$\mathrm{MK} = \left\{ \bigcup_{q=1}^{w} \mathrm{MK}_q \right\} = \left\{ \mathrm{MK}_1, \mathrm{MK}_2, ..., \mathrm{MK}_w \right\}. \quad (1)$$

Defining criteria sets elements. Further, on the basis of (1) determine the elements of the $МК_q$ set of criteria.

$$МК_q = \left\{ \bigcup_{e=1}^{w_q} МК_{q,e} \right\} = \left\{ МК_{q,1},\ МК_{q,2},\ ...,\ МК_{q,w_q} \right\}, \qquad (2)$$

where $МК_{q,e} \subseteq МК_q$ ($e = \overline{1,w_q}$) – e element $МК_q$ criteria sets, and w_q they quantity.

Specify the levels of elements of criteria sets. Next, on the basis of (3) determine the level of each $МК_{q,e}$ element $МК_q$ set of criteria

$$МК_{q,e} = \left\{ \bigcup_{y=1}^{w_{q,e}} МК_{q,e,y} \right\} = \left\{ МК_{q,e,1},\ МК_{q,e,2},\ ...,\ МК_{q,e,w_{q,e}} \right\}, \qquad (4)$$

where $МК_{q,e,y} \subseteq МК_{q,e}$ ($y = \overline{1,w_{q,e}}$) – y level $МК_{q,e}$ -го element $МК_q$ - set of criteria, and $w_{q,e}$ they max level.

Thus, (1) taking into account (2) we present in the following form:

$$МК = \left\{ \bigcup_{q=1}^{w} МК_q \right\} = \left\{ \bigcup_{q=1}^{w} \left\{ \bigcup_{e=1}^{w_q} МК_{q,e} \right\} \right\} = \left\{ \left\{ МК_{1,1},\ МК_{1,2},\ ...,\ МК_{1,w_1} \right\}, \right.$$

$$\left. \left\{ МК_{2,1},\ МК_{2,2},\ ...,\ МК_{2,w_2} \right\},\ ...,\ \left\{ МК_{w,1},\ МК_{w,2},\ ...,\ МК_{w,w_w} \right\} \right\}. \qquad (3)$$

Thus, (3) taking into account (4) has the form:

$$МК = \left\{ \bigcup_{q=1}^{w} МК_q \right\} = \left\{ \bigcup_{q=1}^{w} \left\{ \bigcup_{e=1}^{w_q} МК_{q,e} \right\} \right\} = \left\{ \bigcup_{q=1}^{w} \left\{ \bigcup_{e=1}^{w_q} \left\{ \bigcup_{y=1}^{w_{q,e}} МК_{q,e,y} \right\} \right\} \right\} =$$

$$= \left\{ \bigcup_{q=1}^{w} \left\{ \bigcup_{e=1}^{w_q} \left\{ МК_{q,e,1}, МК_{q,e,2}, ..., МК_{q,e,w_{q,e}} \right\} \right\} \right\} =$$

$$= \left\{ \bigcup_{q=1}^{w} \left\{ \left\{ МК_{q,1,1}, МК_{q,1,2}, ..., МК_{q,1,w_{q,1}} \right\}, \left\{ МК_{q,2,1}, МК_{q,2,2}, ..., МК_{q,2,w_{q,2}} \right\}, \right. \right.$$

$$\left. \left. ..., \left\{ МК_{q,w_q,1}, МК_{q,w_q,2}, ..., МК_{q,w_q,w_{q,w_q}} \right\} \right\} \right\} =$$

$$= \left\{\left\{\left\{MK_{1,1,1}, MK_{1,1,2}, ..., MK_{1,1,w_{1,1}}\right\}, \left\{MK_{1,2,1}, MK_{1,2,2}, ..., MK_{1,2,w_{1,2}}\right\}, \right.\right.$$
$$..., \left.\left\{MK_{1,w_1,1}, MK_{1,w_1,2}, ..., MK_{1,w_1,w_{1,w_1}}\right\}\right\},$$
$$\left\{\left\{MK_{2,1,1}, MK_{2,1,2}, ..., MK_{2,1,w_{2,1}}\right\}, \left\{MK_{2,2,1}, MK_{2,2,2}, ..., MK_{2,2,w_{2,2}}\right\}, \right.$$
$$..., \left.\left\{MK_{2,w_2,1}, MK_{2,w_2,2}, ..., MK_{2,w_2,w_{2,w_2}}\right\}\right\},$$
$$..., \left\{\left\{MK_{w,1,1}, MK_{w,1,2}, ..., MK_{w,1,w_{w,1}}\right\}, \left\{MK_{w,2,1}, MK_{w,2,2}, ..., MK_{w,2,w_{w,2}}\right\}, \right.$$
$$..., \left.\left.\left\{MK_{w,w_w,1}, MK_{w,w_w,2}, ..., MK_{w,w_w,w_{w,w_w}}\right\}\right\}\right\}.$$

An integral part of the application of any comprehensive information security system is its expertise. Accordingly, a software application for the method of identification of the functional profile of protection of the decision support system during the examinations of the CSIS was developed.

The functionality of the decision support system meets the requirements of the Law of Ukraine "On Information" and the Law of Ukraine "On Information Protection in Information and Telecommunication Systems".

The software application has functionality (or the ability to improve the program to achieve functionality in the future) for the possibility of software implementation of all modules of the decision support program during state expertise CSIS.

Conclusion. That's it, the proposed model of parameters, which due to the theorist-multiple representation of certain sets of criteria for the security of information, their elements and corresponding levels, allowed in formal form to form the necessary set of values for the implementation of the process of identification of FPP in the CS. Next, it is necessary to develop a method of identification of FPP, which will automate the process of determining the requirements for security functions (security services) and guarantees.

Definition energy function in self-organization processes by hebb's neurons networks in the case of multidimensional data

UDC 004.056.5 (043.2)

Anatolii Davydenko[1,]
Maryna Kolomiiets[2],
Volodymyr Pogorelov[3]

[1]National Aviation University, Pukhov Institute for modeling in energy engineering of NAS of Ukraine, [1]davidenkoan@gmail.com
[21]National Aviation University, [2]mv.kolomiiets@gmail.com
[3]National Aviation University, [3]volodymyr.pogorelov@gmail.com

The ramped-up development of high-performance computing capabilities of rocks is many variants of computational architectures and technologies, the example of which are supercomputers such as Tianhe-2, Titan – Cray XK7, Sequoia – Blue Gene/Q, K Computer, Mira – Blue Gene/Q and others. Most of these computers are combined by a massively parallel architecture that is built from a set of processors connected to a single computing network. Starting and exploring such networks requires new structures to manage and protect the processing of information. Artificial neural networks are used for these purposes. The main advantage of high-performance computing systems is the ability to combine resources to solve resource-rich computational tasks that should be performed irregularly. At the same time, there is a contradiction between the desire to get maximum productivity and the need to ensure information security. The architecture of information security in grid services ensures the implementation of a wide range of security tasks – from cases in which the protection requirements are minimal or not at all, to tasks with high levels of requirements for privacy, integrity and accessibility.

Grid services combine different administrative domains, each of which has a personal autonomous security mechanism.

If we are talking about the processing of multidimensional data, then it is necessary to organize neurons in a certain way. This arrangement is that data from multidimensional space is projected into two or at least three dimensional spaces, while maintaining the basic properties of the distribution in a multidimensional space.

Let's accept that we have n vectors in N - dimensional space X_i. According to them, n vectors in the M measured space are defined, which are denoted as $(M = 2,3)$. Let the distances between them in N -dimensional space are described as $d_{ij}^* = d(X_i, X_j)$, in M space - measured $d_{ij} = d(y_i, y_j)$.

A nonlinear transformation is to match vectors to minimize the error function described by the ratio:

$$E = (1/C)\sum_{i<j}^{n}([d_{ij}^* - d_{ij}]^2)/d_{ij}^*,$$

where $C = \sum_{i<j}^{n} d_{ij}^*$, $d_{ij} = \sqrt{\sum_{K=1}^{M}[y_{iK} - y_{jK}]^2}$, where y_{ij} means j component of the vector y_i.

When interdependence between signals is used to implement self-organization processes, such self-organization processes are called correlation or Heb's. This type of network includes two types of networks:

– a network that decomposes the data of the main components, or a network of the RSA type;

– a network that decomposes an adaptation system to independent components, or an ICA network.

These two networks are by nature linear networks. The basic Hebb rule is related to the linear model of the neuron described by the ratio:

$$y_j = \sum_{i=0}^{N} w_{ji} x_i.$$

According to Hebb's postulates, a change in the weight of a neuron, after presenting a vector X , is described in the following expression:

$$\Delta w_{jK} = \eta\,(y_i - y_i^{(0)})(x_K - x_K^{(0)}),$$

where $y_i^{(0)}$ and $x_K^{(0)}$ - certain constant, η - training coefficient.

Taking into account, the change in the weight of the network in time can be presented as the following ratio:

$$\frac{dw_{jk}}{dt} = \sum_{i=1}^{N} w_{ji} C_{ik} + \frac{K_2}{N} \sum_{i=1}^{N} w_{ji} + K_1,$$

where K_1 and K_2 - certain constant, related to $x_K^{(0)}, y_j^{(0)}$ and η, C_{iK} - average activity covariation i and k neurons, which is described by the following ratio:

$$C_{iK} = (1/P)\sum_{j=1}^{P}(x_i^{(j)} - x_i)(x_k^{(j)} - x_k),$$

where constant x_i means the average value of the input references, which corresponds to the i component of the average vector $\bar{X}$, where $\bar{X} = (1/P)\sum_{K=1}^{P} x^{(K)}$.

If the change in weight is carried out in accordance with the rule of the largest descent of the energy function E, we get:

$$\frac{dE}{dw_{jk}} = -\frac{dw_{jk}}{dt} = -\sum_{i=1}^{N} w_{ji} C_{ik} - K_1 - (K_2 / N)\sum_{i=1}^{N} w_{ji}.$$

When solving this differential equation, we obtain an energy function in the form of:

$$E = E_v + E_K,$$

where

$$E_v = (-1/2)\sum_{i=1}^{N}\sum_{K=1}^{N} w_{ji} C_{ik} w_{kj},$$

$$E_K = -K_1 \sum_{i=1}^{N} w_{ji} - (K_2 / 2N)\left(\sum_{i=1}^{N} w_{ji}\right)^2.$$

The first component of the energy component E_v determines a variation σ_j^2 in the activity of j neuron. The second component can be identified from the component of the fine energy function.

Conclusion. Thus, energy function in self-organization processes by hebb's neurons networks in the case of multidimensional data are defined.

Analysis of self-taught model of dependence of safety factors using model of semantic transformations .

UDC 004.056.5 (043.2)

Oleksandr Korchenko[1], Igor Sinitsyn[2] Yevheniy Rodin[3]

[1]National Aviation University, agkorchenko@gmail.com
[2]Institute of Software Systems of National Academy of Sciences of Ukraine, igo@isofts.kiev.ua

[3]*Institute of Software Systems of National Academy of Sciences of Ukraine, yevheniy.s.rodin@gmail.com*

Experimental study of construction of model of semantic transformations of distributed security system was carried out on the basis of the company LLC "NewGround" (https://newground.ua/). The company is engaged in the development of special software, fulfills orders of large international corporations, participates in distributed teams of developers, which causes the presence of a distributed information system in the company.

Participation in international projects, availability of access to information environments of other companies, availability of employees working remotely - all these factors increase the company's responsibility to organize information security. At the beginning of the experiment, the company was provided with a process model of protection. Models of infrastructure, information resource, user, administrator, violator, vulnerabilities, threats were built.

The policy was supplemented by the requirements of partners and customers, according to which the company carried out joint projects. Instrumental information security was supported by built-in IDS operation systems, brandmausers of demilitarized zones. No models for calculating the information security budget, the mechanics of case logging describing further measures and consequences were introduced. The defense specialist faced the task: to build a model for assessing the security of the company's infrastructure, to establish incident logging mechanisms, to build a model for calculating the defense budget, to build a model for expanding the company's information security framework in order to reduce the effectiveness of infrastructure protection, reduce the number of incidents, rationally calculate the annual budget for protection.

The security team analyzed the following dates and analytical data from LCG Risk Analysis resources, GridPP Risk Register https://www.gridpp.ac.uk/collaboration/docs/gridpp-risk-register/, https://nvd.nist.gov/ - 94,000 vulnerabilities, BITS Calculator - 600 threats, Microsoft Threat Model - 36 threats, NIST SP800-30 - 32 threats, ISO 27005 - 43 threats, BSI Base IT Security Manual - 370 threats. Most of the existing threats and vulnerabilities relate to software and hardware. Protection against these threats and vulnerabilities is provided by IDS systems, archaetic network solutions, brandmauer systems. But the greatest risk among the analyzed vulnerabilities and threats at this time are those associated with the human factor. Therefore, it was decided to build an integrated information security system.

According to the selected factors and the kind of taxiconomy, a scheme of influence of factors on the integrity, confedence and availability of the selected resource - the database of the company's customers was built.

Based on the taxonomy of vulnerabilities, threats, consequences, schemes of influence of factors on threats and vulnerabilities, the date of sets of open vulnerability databases was built a semantic dictionary of information security of the company and built vague rules for the dependencies of vulnerabilities-threat-incidents. Semantic transformations of basic factors of influence, consequences were formalized thanks to the tool of fuzzy logic into linguistic variables.

Fuzzy rules of selected safety factors are presented in the following on-screen form.

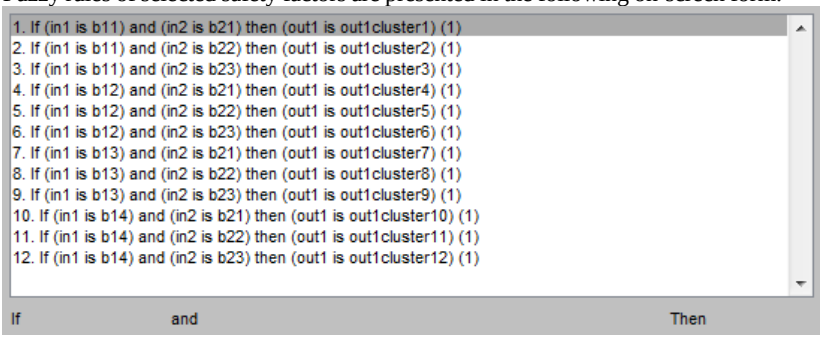
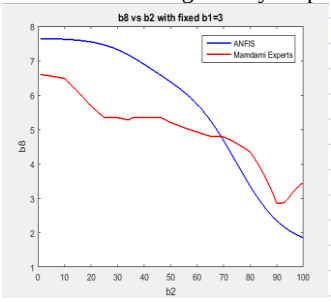


Fig. 1. Fuzzy rules of selected safety factors

Let's calculate the reliability of the expert model and built on the basis of a wide-cut database of notes using the MatLab software package and confirm the effectiveness of the application of the offered model. Let's compare the constructed models by constructing graphs of fuzzy b8 outputs when fixing one variable for all values of another. We get fuzzy outputs of two models according to test data.



b1	b2	b8	ANFIS	Expert
1	41	6	7.775485	5.715039
8	58	2	2.37743	3.808011
4	75	0	2.208782	4.590151
0	100	2	1.637644	3.45
0	0	10	7.435831	6.769272
4	25	6	6.783816	5.33882
9	25	6	6.591982	5.419527
8	37	7	4.972211	4.636002
4	65	3	3.287226	4.593285
1	32	6	7.717872	5.870802

Fig. 2. Fuzzy outputs of two models

Conclusion: The self-taught model of dependence of safety factors using the model of semantic transformations shows better results than the expert-statistical model.

Диференціальні інваріанти відносно локальних обертань

Пилип Приставка[1], Чолишкіна Ольга[2]

[1]*Національний авіаційний університет, chindakor37@gmail.com*

[2]*Міжрегіональна Академія управління персоналом,*

greenhelga5@gmail.com

Визначення локальних особливостей цифрових зображень (ЦЗ) є невід'ємною складовою обчислювальних процедур пошуку та розпізнавання об'єктів, фотограмметрії, орторектифікації даних повітряної розвідки, детектінгу цілей на цифровому відео, тощо. Говорячи про особливості ЦЗ маємо на увазі локальні, низького рівня особливості, що не пов'язані з просторовими співвідношеннями – краї об'єктів, кривизна, що подається швидкістю зміни інтенсивності освітлення у напрямку краю, – тобто, такі, котрі є інваріантними відносно маштабування, обертання та, частково, відносно змін точки спостереження та інтенсивності зображення. Вони добре локалізуються як в просторовій, так і в частотній областях, стійкі до зашумлення, а індивідуальна особливість дозволяє пошук співвідношень особливостей об'єктів, представлених на різних зображеннях сцени.

Альтернативою до моделі згладженого зображення на основі гауссіана може бути модель на основі лінійних комбінацій *B*–сплайнів, близьких до інтерполяційних у середньому, наприклад

$$S_{r,0}\left(p,t,q\right)=\sum_{i\in Z}\sum_{j\in Z}p_{i,j}B_{r,h_t}\left(t-ih_t\right)B_{r,h_q}\left(q-jh_q\right),$$

$$r=2,3,\ldots. \qquad (1)$$

Маючи фактично аналогічні властивості в частотній області, що й функція Гаусса, *B*–сплайни більш прості в обчисленні та дозволяють побудову моделі зображення, яка за рахунок аналітичного вигляду надає можливість отримання часткових похідних, на основі яких можна будувати швидкодіючі інваріантні відносно обертань та зміни масштабу оператори пошуку особливостей ЦЗ.

Нехай в неперервній моделі двовимірного зображення $p(t,q)$ в якості функції імпульсного виклику використовується модель (1), тоді, для дискретного аналогу виразу

$$D(t,q,\sigma)=\left(G\left(t,q,k\sigma\right)-G\left(t,q,\sigma\right)\right)*p\left(t,q\right)=L\left(t,q,k\sigma\right)-L\left(t,q,\sigma\right)$$

, (2)

що є придатним для пошуку положень ключових точок в просторі маштабу-положення, можна використовувати лінійні оператори

$$p_{i,j,\kappa} = \sum_{ii=2i-1}^{2i+1} \sum_{jj=2j-1}^{2j+1} \delta L_{3,2}\, p_{ii,jj,\kappa-1}, \tag{3}$$

$$p_{i,j,\kappa} = \sum_{ii=2i-2}^{2i+2} \sum_{jj=2j-2}^{2j+2} \delta L_{rr}\, p_{ii,jj,\kappa-1},$$

$$rr = \{"4,3","5,4"\} \tag{4}$$

$$p_{i,j,\kappa} = \sum_{ii=2i-3}^{2i+3} \sum_{jj=2j-3}^{2j+3} \delta L_{6,5}\, p_{ii,jj,\kappa-1}\,. \tag{5}$$

Набір похідних для сімейства (2) та їх аналогів в просторі масштаб–положення аж до порядку k в даній точці зображення і при заданому масштабі називається k –джетом і відповідає обрізаному розкладу Тейлора для локально згладженого фрагменту зображення. Ці похідні разом описують базові види особливостей в просторі масштаб–положення та компактно представляють локальну структуру зображення. Для $k = 2$, при вибраному масштабі 2–джет містить похідні

$$\left(S'_{r,0}(p,t,q)_t, S'_{r,0}(p,t,q)_q, S''_{r,0}(p,t,q)_{tt}, S''_{r,0}(p,t,q)_{qq}, S''_{r,0}(p,t,q)_{tq}\right), \tag{6}$$

З п'яти компонент 2–джета для кожної з моделей (1) порядку $r = 2,3,\ldots$ можуть бути сконструйовані чотири диференціальних інваріанти відносно локальних обертань – магнітуда градієнта $\left|\nabla S_{r,0}\right|$, лапласіан $\nabla^2 S_{r,0}$, детермінант Гессіана $\det \mathrm{H}_{r,0}$ і кривизна кривої масштабування $\tilde{k}_{r,0}$ (з точністю до позначень операторів різного порядку):

$$\left|\nabla S\right| = S_t'^2 + S_q'^2, \tag{7}$$

$$\nabla^2 S = S_{tt}'' + S_{qq}'', \tag{8}$$

$$\det \mathrm{H} = S_{tt}'' S_{qq}'' - S_{tq}''^2, \tag{9}$$

$$\tilde{k} = S_t'^2 S_{qq}'' + S_q'^2 S_{tt}'' - 2S_t' S_q' S_{tq}'', \tag{10}$$

Детектор єдиного масштабу для знаходження структур типу крапель, який реагує на яскраві і темні структури, схожі на краплі, може базуватися на мінімумі і максимумі лапласіанів $\nabla^2 S$. Афінно–коваріантний детектор структур типу крапель, який також реагує на сідла, може бути представлений як максимум і мінімум детермінанта Гессіана (9). Прямолінійний і афінно–коваріантний детектор кутів може бути представлений як максимум і мінімум кривих рівня масштабування (10) для різних порядків сплайн-операторів, залежно від $r = 2,3,\ldots$ в моделі (1).

Запропоновані інваріанти, сукупно з операторами, на кшталт (3)-(5), або низькочастотних фільтрів на основі сплайн-моделі (1.8), можуть бути рекомендовані для визначення особливостей на даних аерозйомки в якості альтернативи операторів на основі двовимірних функцій Гаусса.

Удосконалення методології HTRA за допомогою системи профілювання персоналу

УДК 004.056.53

Тарас Паращук[1], Анна Корченко [2]

Національний авіаційний університет,[1]taras1039@gmail.com, [2]annakor@ukr.net

Визначення та оцінка людського фактору є важливої для будь-якої інформаційної системи в поточних реаліях. Оскільки останні кібератаки показали, що захист поточних систем базується не тільки на впроваджених системах захисту та моніторингу атак, а й на загальній обізнаності персоналу та інформаційній кваліфікації співробітників. Оскільки захист будь-якої системи починається не тільки

з впровадження політики інформаційної безпеки, визначенням відповідальних осіб, документуванні всіх процесів і т.д., але й слід розглядати кожного працівника компанії, як потенційну точку доступу до інформаційної системи в цілому, а також складову системи, яку важко оцінити та задати конкретні границі впливу на частину системи або всю систему в цілому.

Тому однією із задач при розробці алгоритму для покращення системи оцінки ризиків на базі методології гармонізованої оцінки загроз і ризиків (HTRA), є збір статистики та формування профіля співробітника організації, підвищення інформаційної обізнаності працівників для можливості протидії інформаційним загрозам.

Метою роботи є удосконалення системи на базі HTRA, для розширення можливостей системи по визначенню і оцінці ризиків та загроз, що орієнтовані на співробітника, як найбільш вразливу ланку інформаційної безпеки в цілому.

Опорною складовою, що дозволить розширити оцінку ризиків та загроз, існуючих в оцінюваній системі, пов'язаних зі персоналом є профіль конкретного співробітника. Будь-який профіль співробітника складається з таких блоків:

1. Інформаційний блок:
   - загальна частина (включає в себе загальну інформацію про особу, про посаду, спеціальність, кількість підлеглих, професійні вміння та знання і т.д.);
   - специфічна частина профіля залежно від відділу/професійної спеціалізації/посади.
2. Блок кількісних оцінок (включає в себе оцінки за пройдені тести, так детальну інформацію про формування коефіцієнтів та залежностей між вхідними параметрами).

Інформаційний блок складається з описаних положень, з визначеними ступенями (коефіцієнтами), які можуть бути визначенні алгоритмом або експертом. Ступень важливості певного критерію при подальшій оцінці профілю є певним коефіцієнтом, який може впливати на кінчену оцінку профілю та при побудові ланцюгів ймовірності проведення атаки, з використанням даного співробітника чи групи співробітників.

Блок кількісних оцінок не тільки дозволяє описати кількісно кожен із критеріїв визначених в інформаційному блоці, але і відповідає за відображення всіх розрахованих параметрів (отриманих на основі оцінок інформаційного блоку та системою тестування), що будуть використовуватись в визначенні ймовірності реалізації атаки.

Система тестування може бути визначена за допомогою блоку питань сформованих експертом або специфічних тестів, які мають за собою інформаційну складову (наприклад, лист з вкладенням з програмною закладкою для подальшого отримання до робочої станції). При проведенні будь-якого тестування, для оцінки профілю, необхідно використовувати такий ряд правил:

- тест має мати сформовану задачу, цільову групу співробітників, перелік застосованого обладнання чи програмного забезпечення, кінцеву мету та строго визначений результат;
- оцінки отримані в результаті тестування повинні впливати на профіль співробітника та на відділ;

– вибір суб'єктів тестування має відповідати задачі тесту і має бути пов’язаний на пряму з діяльністю відділу чи конкретного суб’єкта.

На основі профілів, теорії графів та ряду правил та алгоритмів теорії ймовірності, можна побудувати граф залежностей між відділами, де вершинами будуть відділи або співробітники, а ребрам буде виставлена вага залежності від значень отриманих в ході обчислень на основі можливих оцінок виникнення загроз та критичності ресурсів. Даний вид інтерпретації дозволить візуально оцінити взаємозв’язки між відділами чи співробітниками та визначити пріоритетні маршрути в інформаційній системі в цілому.

Підводячи підсумок, істотну роль в мінімізації ризиків та загроз грає розробка і застосування профілів співробітників, що допоможуть кількісно оцінити можливі загрози і розширити можливості існуючої методології HTRA. Таким чином, для інформаційних систем профілі, дозволять не тільки ефективно оцінити загрози і ризики, но і дозволять вигідніше проводити моніторинг діяльності персоналу, отримувати останню і повну інформацію про конкретного співробітника та визначати залежності між співробітниками в кількісній площині.

Формування параметрів функціональних обов’язків для оцінки загроз в соціотехнічних системах

УДК 004.056.53

Тарас Паращук[1], Анна Корченко [2]
Національний авіаційний університет,[1]taras1039@gmail.com,
[2]annakor@ukr.net

В даний час для вирішення проблеми виявлення атак та загроз пов’язаних з людською складовою приділяється багато уваги. Доказом цього можуть бути дослідження та звіти по всім можливим атакам за 2018-2021р. Тому на основі проаналізованих джерел можна зробити висновок про неухильне зростання атак такого виду, та наявність невеликої кількості систем оцінки загроз та ризиків пов’язаних з людським фактором, дозволяє стверджувати, що дана тема є актуальною, обгрунтованою та потребує подальшого дослідження.

Метою даної роботи є створення методу формування параметрів функціональних обов’язків для оцінки загроз в соціотехнічних системах.

Для початкурозглянемо персонал компанії CE працюючих в певний часовий проміжок t в компанії, тобто:

$$CE^t = \{\bigcup_{i=1}^{n} CE_i^t\} = \{CE_1^t, CE_2^t, \dots, CE_n^t\}, \quad (i = \overline{1,n}) \tag{1}$$

де n визначає кількість всіх співробітників, в певний період часу t.

Далі після сформованої множини CE^t, визначмо множину всі функціональних обов’язків WR, які можуть виникати в процесі функціонування бізнес процесів в певний часовий проміжок t в компанії та можуть бути спільними для декількох співробітників одного відділу або різних, тобто:

$$WR^t = \left\{\bigcup_{i=1}^{n} WR_i^t\right\} = \{WR_1^t, WR_2^t, \dots, WR_n^t\}, \quad (i = \overline{1,n}) \tag{2}$$

де n визначає кількість функціональних обов'язків, що можуть бути у співробітників компанії в певний період часу t.

Визначивши множини для персоналу CE^t та функціональних обов'язків WR^t компанії, визначмо залежність між даними множинами математично, тобто встановимо відповідність. Відповідність між множиною CE^t та WR^t визначимо як кортеж (CE^t, WR^t, ER^t), де CE^t та WR^t — дані множини, між якими встановлюється відповідність, а ER^t— підмножина відповідності.

Підмножину ER^t можна описати графом відповідності (див. рис. 1).

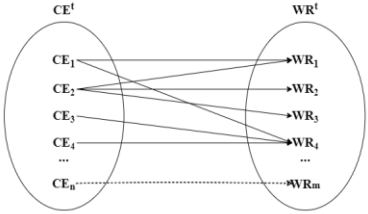


Рис. 1. Граф відповідності між множинами CE^t та WR^t

На основі проілюстрованого графа, маємо що дане відображення є несюр'єктивним та неін'єктивним, тобто кожний елемент WR^t множини асоціюється щонайменше з одним або більше елементів CE^t множини або дані асоціації можуть бути відсутні. Також дану підмножину ER^t можна подати в вигляді:

$$ER^t = \left\{\bigcup_{i=1}^{n}\bigcup_{j=1}^{m}\left(CE_i^t, WR_j^t\right)\right\} = \begin{Bmatrix} (CE_1^t, WR_1^t), (CE_1^t, WR_4^t), \\ (CE_2^t, WR_1^t), (CE_2^t, WR_2^t), \\ (CE_2^t, WR_3^t), (CE_3^t, WR_4^t), \\ (CE_4^t, WR_4^t), \\ \dots \\ (CE_n^t, WR_m^t) \end{Bmatrix}, \quad (3)$$
$$\left(i = \overline{1,n}\right), \left(j = \overline{1,m}\right)$$

де n визначає кількість всіх співробітників та m визначає кількість всіх функціональних обов'язків в компанії.

Проаналізувавши вище описанні відношення та математичні залежності, можна стверджувати що кожному співробітнику може відповідати декілька функціональних обов'язків. Також один функціональний обов'язок може мати відношення до декількох співробітників одночасно.

Описавши залежності вище, перейдемо до визначення та описання загальних параметрів функціональних обов'язків. Для цього опишемо в загальному виді обов'язок WR_i^t з формули (7), за допомогою кортежу з параметрами:

$$WR_i^t = \langle WR_i, PR_i, FPR_i, LC_i, DDR_i \rangle \quad (4)$$

в якому:

- PR_i – пріоритет показує ступень важливості обов'язку в структурі бізнес процесів компанії (шкала оцінки від 1 до 10);

- FPR_i – частота виконання певного обов'язку відносно всіх обов'язків конкретного профілю (шкала оцінки від «рідко» до «дуже часто»);
- LC_i – рівень компетентності конкретного співробітника (профілю) для виконання певного обов'язку (шкала оцінки від «дуже низький» до «високий»);
- DDR_i – ступінь залежності обов'язку від критичних активів та конфіденційної інформації в компанії (шкала від 1 до 10).

Отже, виявлення атак, оцінка загроз та ризиків в соціотехнічних системах є важливим питанням, особливо з точки зору людської складової. Тому розглянутий метод формування параметрів для функціональних обов'язків є важливим етапом при формуванні методології профілювання співробітників певної компанії. Даний метод дозволяє оцінити функціональні обов'язки конкретного співробітника та встановити залежності між співробітником та обов'язками за допомогою параметрів.

Актуальні питання створення систем кібербезпеки в Україні

УДК 355.405.1

Владимир Хорошко[1], Юлия Хохлачева[2], Сергій Скворцов[3], Ахмад Аясрах[4], Аблуллах Аль-Далваш[5]

Национальный авиационный университет,

[1]professor va@ukr.net, [2]hohlachova@gmail.com, [3]ssamailer@gmail.com

Кількість деструктивних інцидентів у сфері комп'ютерних та Internet-технологій за період 2015-2021 років збільшилась приблизно у 2,7 рази. На сьогодні триває кібер-війна України з Росією, під час якої Україна перетворилась на тіньовий полігон для російських хакерів. Щомісяця наша держава піддається кібератакам 3000-3500 разів. Саме тому найбільш пріоритетним напрямом керівництво України вважає реформування систем забезпечення кібербезпеки. Це є одним з головних напрямів забезпечення конфіденційності, цілісності та доступності інформації в національних інформаційних ресурсах від кібератак шляхом створення в інформаційно-телекомунікаційних системах (ІТС) комплексних системах захисту інформації з підтвердженою відповідністю.

Враховуючи таке вже зараз у Адміністративному та Кримінальному кодексах України до переліку протиправних дій у кіберпросторі віднесено :

- несанкціоноване втручання в роботу комп'ютерів та ІТС;
- несанкціонований збут або розповсюдження інформації з обмеженим доступом;
- створення та використання шкідливих програмних та технічних засобів ;

- несанкціоновані дії з інформацією, яка обробляється в комп'ютерах та комп'ютерних мережах;
- здійснення незаконного доступу до інформації в ІТС ;
- незаконне використання чи розповсюдження копій баз даних тощо.

Протидіяти таким діям на теренах України спроможні:

- Центральні органи виконавчої влади у сфері інформації та телекомунікації (зокрема приватні) та установи, які експлуатують об'єкти критично важливої інфраструктури або здійснюють господарську діяльність і сфері захисту інформації а ІТС.
- Національний банк України, який формує та реалізує державну політику із забезпечення інформаційної та кібернетичної безпеки банківських установ.
- Підрозділи спеціального призначення, що виконують завдання із забезпечення кібернетичної безпеки.
- Оператори (провайдери) телекомунікації тощо.

Все, що з огляду на тенденції розвитку національного кібернетичного простору, потребує від України координації зусиль державного та приватного секторів у протидії новим викликам в інформаційній сфері та вказує на необхідність подальшого секторального вироблення принципів і механізмів реагування на можливі комп'ютерні інциденти.

Серед підрозділів та формувань спеціального призначення найбільше навантаження в ході вирішення завдань кіберзахисту лягає на :

- Державну службу спеціального зв'язку та захисту інформації України, що реалізує державну політику в сфері захисту інформації в інформаційно-телекомунікаційних мережах;
- Службу безпеки України, що реалізує державну політику в сфері охорони інформації з обмеженим доступом, яка є власністю держави.
- Міністерство внутрішніх справ України, що здійснює досудову слідство у справах про злочини у сфері інформаційних технологіях (ІТ).
- Міністерство оборони України, що планує та реалізує заходи протидії та нейтралізації кіберзагроз національним інтересам України у воєнній сфері, впровадження новітніх інформаційних технологій у сфері оборони.
- Службу зовнішньої розвідки України.

З моменту здобуття незалежності Україна прагне створити комплексну систему протидії внутрішнім і зовнішнім загрозам власному кібернетичному простору, однак існує низка проблем, що заважають нашій державі це зробити:

- Деградація науково-технічного потенціалу, нерозвиненість інноваційної системи в інфосфері та низький рівень конкурентоздатності в ній.

- Значна уразливість інфосфери через надмірно широке впровадження до неї іноземних програмних та матеріальних технічних засобів.
- Непрозорість розподілу обов'язків між відомствами, правоохоронними органами та силовими структурами, які спеціалізуються на проблемах кіберзахисту та їх незадовільне кадрове забезпечення.
- Відсутність загальнонаціонального координаційного центру, який був би сформований узгоджувати та координувати діяльність правоохоронних органів, силових стуктур і відомств щодо протидії реальним загрозам інформаційному та кіберпростору України.
- Відсутність єдиного політико-термінологічного поля кібербезпеки України, як головної складової інформаційної безпеки та системних нормативно-правових документів, які б регламентували діяльність відомств, правоохоронних і силових структур у сфері кіберзахисту.

Такий стан фактично є каталізатором для реалізації втручань і загроз в інфосферу України, результатом чого може стати порушення управління державою, її інституціями та окремими об'єктами критично важливої інформаційної інфраструктури. Це вимагає від керівництво держави формування надійної системи кібернетичної безпеки шляхом започаткування низки міжвідомчих, а можливо й міждержавних ініціатив на кшталт:

- визначення політико-категорійного апарату та потенціальних загроз власній інформаційній та кібернетичній безпеці;

- формування критеріїв унесення об'єктів кіберпростору до критично важливої інформаційної та кіберінфраструктури;

- удосконалення механізмів надання взаємодопомоги у технічних і методологічних аспектах випереджувального виявлення джерел, фіксації та оперативного обміну інформацією про факти здійснення кібератак;

- вироблення та реалізація єдиної науково-технічної політики щодо захисту державних інформаційних ресурсів та IT інфраструктури від деструктивного кібервпливу;

- створення нової сучасної навчально-наукової бази для аідготовки фахівців;

- розробка єдиних механізмів аудита та сертифікації програмно-апаратних комплексів, використовуваних у державних та військових системах управління;

- модернізації існуючих та розробка нових захисних інформаційних технологій;

- організація міжвідомчої взаємодії та координації державних органів при оцінюванні реальних і потенційних загроз в інформаційній сфері, а також вироблення та реалізація заходів щодо їх посилення;

- удосконалення міждержавних консультативних механізмів з питань законодавчого забезпечення та регулювання діяльності у сфері боротьби з кіберзлочинністю та кіберзагрозам і внесення змін до низки існуючих нормативно-правових станів України;

- створення міжнародного експертного центру з питань регулювання взаємовідносин у галузі телекомунікацій та зв'язку тощо.

Було б раціональним удосконалити організаційно-правові норми міжнародної взаємодії з питань боротьби з кіберзлочинністю та кібертероризмом і світовій спільності внести зміни та оновлення до низки існуючих міжнародних нормативно-правових документів.

У результаті це дасть можливість:

- провести огляд кібербезпекової сфери держави, що дозволило б чітко визначити сучасний обсяг її нормативного забезпечення та основних проблем які мають бути вирішені вже найближчим часом;

- розробити на підгрунтті моделей розвитку світового кібернетичного простору власну модель та реалізувати її;

- впорядкувати політику України у сфері інформаційної та кібернетичної безпеки та виробити так звані загальні правила поведінки у кіберпросторі;

- визначитись з розбіжностями між військовими та цивільними об'єктами в інформаційному та кіберпросторах і сформулювати вимоги щодо безпеки для ключових доменів;

- визнати міжнародним злочином проведення кібератак і кібероперацій на об'єкти інформаційної та кіберінфраструктури України, які здійснює Росія та які спроможні призвести до виникнення техногенних катастроф або надзвичайних ситуацій.

Аналіз основних стандартів захисту персональних даних

УДК 004.056.5

Євгенія Іванченко[1], Ірина Лозова[2],
Ігор Іванченко[3], Євгеній Педченко[4]

Національний авіаційний університет, [1]evivancenko@gmail.com,
[2]illozovaya@gmail.com, [3]ivanchenko.igor33@gmail.com,
[4]ypedchenko@intrasystems.ua

Для організацій, які працюють із персональними даними (ПД) своїх клієнтів та співробітників важливо пам’ятати, що будь-який витік даних за межі компанії може коштувати занадто дорого та тягне за собою втрату репутації на конкуруючому ринку. Тому постає проблема захисту ПД клієнтів та працівників компанії, вибору єдиного набору рекомендацій для попередження непередбачуваних витрат по сплаті штрафів та втрати репутації компанії.

Метою даної роботи є проведення комплексного аналізу стандартів, що описують принципи опрацювання ПД клієнтів в інформаційному просторі для запобігання втрати коштів та репутації компаній.

ISO/IEC 29100 – міжнародний стандарт, який забезпечує високий рівень захисту ПД в межах систем інформатизації та комунікаційних технологій. Даний стандарт охоплює організаційні та технічні аспекти у всій приватній мережі.

Asian-Pacific Economic Cooperation Privacy Framework (APEC PF) – це встановлені та впроваджені управлінські принципи для ефективного захисту конфіденційності, задля уникнення перешкод в передачі інформаційних потоків для забезпечення торгівлі та економічного розвитку в APEC із 27 країнами. APEC PF встановлює початок створення системи APEC Cross-Border Privacy Rules.

Generally Accepted Privacy Principles (GAPP). Американський інститут дипломованих бухгалтерів (AICPA) та Канадський інститут дипломованих бухгалтерів (CICA) організовували «Цільову групу з питань конфіденційності (ЦГПК)» для створення відповідних засобів, які організації можуть ефективно впроваджувати для попередження втрати конфіденційності даних. ЦГПК розглядає міжнародні засоби управління конфіденційністю та виробничі практики для розробки інструкцій з конфіденційності. Засіб, який був розроблений ЦГПК отримав назву Generally Accepted Privacy Principles (GAPP). Він містить 10 принципів конфіденційності: Управління; Сповіщення; Вибір та узгодження; Збір даних; Використання, зберігання та знищення; Доступ; Розкриття третім особам; Забезпечення конфіденційності; Якість; Моніторинг та застосування.

General Data Privacy Regular. Регламент General Data Privacy Regular (GDPR) – регламент, що бере свій початок із 2018 року. Це набір рекомендацій для попередження витоку ПД громадян ЄС за межі компанії.

Під час здійснення обробки ПД компанії необхідно додержуватись семи основних принципів захисту:

1) Законність, справедливість та прозорість – обробка ПД повинна бути законною, справедливою та прозорою для суб'єкта ПД.

2) Обмеження цілей обробки – компанія повинна обробляти ПД лише для законних цілей, оговорених із суб'єктом ПД під час отримання.

3) Мінімізація даних – компанія повинна збирати та обробляти лише стільки даних, скільки їй потрібно для описаних цілей.

4) Точність – компанія повинна забезпечувати точність та актуальність ПД.

5) Обмеження часу зберігання – компанія може зберігати ПД лише такий термін, що є необхідний для досягнення мети збору інформації.

6) Цілісність та конфіденційність – обробка ПД повинна здійснюватися таким чином, щоб забезпечити належний захист, цілісність та конфіденційність, наприклад, шляхом шифрування чи маркування ПД.

7) Підзвітність – контролер ПД є відповідальним за відповідність обробки ПД усім вище перерахованих принципам Регламенту GDPR.

California Consumer Privacy Act. В Каліфорнії розроблено національний закон по забезпеченню конфіденційних даних – California Consumer Privacy Act

(CCPA), що набрав чинності 1 січня 2020 року. Закон CCPA орієнтований лише на комерційні підприємства, які розташовуються в Каліфорнії чи обробляють ПД жителів Каліфорнії, та відповідає одному із наступних критеріїв – річний дохід компанії перевищує 25 мільйони $; компанія отримує персональних даних не менше ніж 50 000 жителів Каліфорнії, домогосподарств щорічно; компанія отримує щонайменше 50% свого щорічного доходу від продажу персональних даних жителів Каліфорнії.

Information Systems Audit and Control Association (ISACA) Privacy Principles. В 2013 році міжнародна цільова група з керівництва конфіденційністю ISACA була зібрана для: 1) Ідентифікації сучасних проблем конфіденційності у світі. 2) Ідентифікації використовуваних принципів, стандартів та засобів конфіденційності. 3) Визначення найкращих дій, які необхідно застосувати організаціям, щоб допомогти членам ISACA при створенні та управлінні програмою керування конфіденційністю. 4) Розробка практичних рекомендацій, засобів мінімізації ризиків та вимог конфіденційності.

Результатом роботи ISACA є 14 принципів конфіденційності (ПрК), які гармонізують прийняті стандарти, принципи та засоби конфіденційності.

– Принцип 1: Вибір та узгодження.
– Принцип 2: Специфікація законної мети та обмеження використання.
– Принцип 3: Особиста та Чутлива інформація
– Принцип 4: Точність та якість
– Принцип 5: Відкритість, передача та впровадження
– Принцип 6: Особиста участь.
– Принцип 7: Відповідальність.
– Принцип 8: Гарантії безпеки.
– Принцип 9: Моніторинг, оцінка та звітність.
– Принцип 10: Попередження шкоди.
– Принцип 11: Треті особи.
– Принцип 12: Управління порушеннями.
– Принцип 13: Безпека та конфіденційність.
– Принцип 14: Вільний потік інформації та законні обмеження.

Таблиця 1.Співставлення ПрК ISACA з основними принципами інших методик

ПрК ISACA	**ISO 29100:2011**	**APEC**	**GAPP**	**GDPR**	**CCPA**
1. Вибір та узгодження	+	+	+	+	+
2. Специфікація законної мети та обмеження використання	+	+	+	+	+
3. Особиста та Чутлива інформація	+	+	+	+	+

4. Точність та якість	+	+	+ / -	+	+
5. Відкритість, передача та впровадження	+	-	-	+	+
6. Особиста участь	+	+	+	+	+
7. Відповідальність	+	+	+	+	+
8. Гарантії безпеки	+	+	+	+	+
9. Моніторинг, оцінка та звітність	+ / -	-	+	+	+
10. Попередження шкоди	-	+	-	+	-
11. Треті особи	-	-	+	+	+
12. Управління порушеннями	-	-	-	+	+
13. Безпека та конфіденційність	-	-	-	+	+
14. Вільний потік інформації та законні обмеження	-	-	-	+	+
15. Застосування до країн ЄС	+	+	+	+	-

Виходячи із проведеного дослідження та порівняння міжнародних стандартів, що описують правильність та законність опрацювання ПД в інформаційному просторі, визначено, що не всі стандарти відповідають вимогам ISACA, але всі вони можуть допомогти компаніям точно і якісно визначити, які саме ПД дані компанії потрібно захищати та визначити найкритичніші точки в інформаційному просторі.

Регламент GDPR повністю відповідає принципам конфіденційності ISACA, що відповідає повноцінній захищеності ПД громадян. Тому компаніям, що працюють на ринку України необхідно перевірити власну відповідність нормам Регламенту, де, під час аудиту буде отримано висновок, що допоможе чітко та якісно оцінити захищеність ПД, та допомогти побудувати захищену інфраструктуру для опрацювання ПД громадян України.

Multisignature with double threshold condition in the blockchain

УДК621.395.7
(043.2)

Ruslan Skuratovskii[1], Anastasia Arnautova[2]

National Aviation University, ORCID: 0000-0002-5692-6123.

[1]ruslan.skuratovskii@nau.edu.ua, [2]anastasia.arnautova.bit@stud.nau.edu.ua

Abstract

Improving the reliability of account protection in the blockchain is one of the most important goals of the entire cryptographic arsenal used in the blockchain and cryptocurrency exchange.

We propose a new threshold multisignature scheme with a double boundary condition.

Access to funds stored on a multisig wallet is possible only when two or more signatures are provided at the same time.

A simple analogy is a safe deposit box or safe with two locks and two keys. Maria holds one key, Juan holds the other. They can open the cell only if they present both keys at the same time. Individually, they cannot open a cell without the approval of the other [1].

Thus, multisig wallets provide an additional layer of security. With this technology, users can avoid the problems often encountered with single-key wallets, single point of failure, and vulnerable to attacks from cybercriminals who are constantly developing new phishing techniques.

Since multisig wallets require more than one signature to move funds, they are also suitable for businesses and corporations looking to store funds in shared wallets.

Definition. Multisignature is a technology for signing transactions with multiple private keys to increase security and privacy during the approval process for sending transactions.

A multisignature is a kind of threshold signature, implemented as a check of conditions specified in the basic scripting language of the cryptocurrency. Multisignature technology has become widespread in the world of cryptocurrencies [2].

Definition. A token is a digital certificate that guarantees the company's obligations to its owner, an analogue of shares on the stock exchange in the world of cryptocurrencies [3].

Definition. Threshold signature is a variant of an electronic signature, for the imposition of which the cooperation of at least t members of a group of n participants is required, denoted as. . In essence, it is a special case of the threshold division of a secret according to the scheme (t, n), when the private key is split into n parts, and any t parts are enough to recover it. The public key is used in the usual way. Generation, sharing of a key and distribution of its fragments requires a group manager (dealer).

Note that such a group can be, in particular, a manning pool consisting of n members.

Let's denote – the number of tokens in the wallet of the -th account belonging to a subset of the accounts from the blockchain. Note that one participant can have several accounts, therefore, we consider double indexing where – denotes a wallet in the blockchain network and – this is the owner of the wallet. More generally, cryptocurrency can be used instead of tokens. It is convenient to express the value of a token in cryptocurrency as in monetary terms.

We introduce a double threshold signature condition according to the scheme (t, n), where different t participants from satisfying the inequality where that is, participant really belongs to the group from persons. The this is the boundary number of tokens (or their value in the specified crypto currency) that persons must have in order to be eligible for multisignature.

Access to funds stored on a multisig wallet is possible only when two or more signatures are provided at the same time. At its core, a user's account can be identified with his wallet. But one person can have several accounts (for example, this happens during a CB-attack). Therefore, if person j proves that she has in the aggregate at least the threshold amount necessary to satisfy the inequality of the threshold amount for multisignature, then the sums of tokens or currency equivalents on all her wallets are summed up and included in the total amount of the group. To install accounts on a node, each of the participants can use the BIP 39 algorithm. Even on one node, one person can have several accounts. Therefore, we will summarize each wallet -th the participant indexing it by its index and then we summarize the amounts available to different participants in the external amount by . Then we construct multisignature with sheme, where number of wallets of participant denoted by and is sum of taken in -th wallet of -th participant of blochain

The method of proving that -th a person has a certain amount in the wallet can be a simple contract, where the money is transferred back to the same -th user. Thus,the -th participant shows in the contract that he has this amount explicitly, but then transfers it back to himself (possibly by paying for the transaction). In most cases, for example, in the Effirium currency, the amount in the wallet is visible inside the blockchain. In addition, such an amount can be counted as the sum of incoming money from records inside blockchain transactions and the amount of outgoing spending from this wallet visible in blockchain transactions. Thus, in any case, the total amount of tokens or currency of the -th participant can be calculated without cost.

We will divide the entire blockchain into domains, each of which has its own digital signature. Only those domain entities whose wallets have the number of tokens in excess of a percentage of the critical number of tokens of the entire blockchain domain have the right to sign. The persons who has the authority to sign in the -th domain will be denoted by. If a domain member does not have a number of tokens that exceed the percentage of critical tokens of the entire domain i, it can apply for the right to sign to the authorized person of his domain S. It should be noted that S can be located at the intersection of domains, then the process of transferring the key is simplified due to the fact that an authorized person acts as a surety of two parties at once.

References:

1. Funds stored on a multisig wallet is possible only when two or more signatures are provided at the same time. [Electronic resource] / According to the general edition «Multisignature»

Access mode: https://www.okex.com/academy/ru/%D0%BC%D1%83%D0%BB%D1%8C%D1%82%D0%B8%D0%BF%D0%BE%D0%B4%D0%BF%D0%B8%D1%81%D1%8C

2. Multisignature is a technology for signing transactions with multiple private keys to increase security and privacy during the approval process for sending transactions. [Electronic resource] / According to the general edition «What is multisignature? What is a ring signature?»

Access mode: https://forklog.com/chto-takoe-multipodpis/

3. A token is a digital certificate that guarantees the company's obligations to its owner, an analogue of shares on the stock exchange in the world of cryptocurrencies. [Electronic resource] / According to the general edition Karpova K.

Access mode: https://secretmag.ru/enciklopediya/chto-takoe-token-obyasnyaem-prostymi-slovami.htm

Напрямки підвищення ефективності та якості підготовки кадрів для сфери захисту інформаційної безпеки

УДК 331.5.024.

Мельник Сергій

Кандидат економічних наук, доцент, заслужений економіст України, завідувач сектору професійної освіти відділу освітньої статистики і аналітики ДНУ «Інститут освітньої аналітики», член Національного агентства кваліфікацій, к.е.н., доц., Заслужений економіст України, Київ, Україна

s.melnik@iea.gov.ua

Ключовим питанням якісної та ефективної підготовки кадрів для будь-якої країни виступає система їх оцінювання. Багато країн це питання уже давно та успішно вирішили. Напрямків реалізації оцінювальної діяльності безліч, це й Інформаційна мережа занять США (Occupational Information Network (O'net)[1] та американська мережа центрів з видання ліцензій на професійну діяльність [2], національні бази інформаційних матеріалів з оцінювання, мережі центрів з незалежного оцінювання та присвоєння професійних кваліфікацій у більшості країн ЄС, у Великій Британії та Канаді, в основу яких покладено ключові положення Міжнародної стандартної класифікації занять 2008 року (ISCO-08)

[1] Інформаційна мережа занять США.- URL: https://www.onetonline.org/

[2] Національна база даних з професійного ліцензування.- URL: https://www.ncsl.org/research/labor-and-employment/occupational-licensing-statute-database.aspx

[3] та Європейської класифікації занять, кваліфікацій та навичок (ESCO) [4] тощо. Слід зазначити, що питанням валідації, незалежного оцінювання, присвоєння та присудження здобувачам кваліфікацій різних типів (освітніх (академічних), професійних, повних, часткових, змішаних, мікрокваліфікацій тощо) приділяється постійна та дуже велика увага, що призводить до досить динамічних, хоча й дуже витратних, змін, перш за все, у методологічній площині.

У цьому контексті Україна тільки починає створювати сучасну систему незалежного оцінювання та присвоєння професійних кваліфікацій. Так, за останні 5 років в країні: був прийнятий базовий для цього спрямування Закон України "Про освіту", де в статті 34 законодавчо закріплено процедуру присвоєння професійних кваліфікацій, порядок створення кваліфікаційних центрів, а в статті 38 закріплено, окрім іншого, функцію акредитації цих центрів Національним агентством кваліфікацій тощо [5]; у грудні 2018 року було засноване Національне агентство кваліфікацій [6], яке на сьогодні розробило цілу низку проєктів нормативного спрямування, які знаходяться на різних стадіях проходження погоджувальних процедур, навчено десятки майбутніх експертів з акредитації кваліфікаційних центрів тощо; у вересні 2020 року урядовою постановою був затверджений перелік спеціальностей, за якими здійснюється підготовка фахівців у сфері фахової передвищої освіти з професій, для яких запроваджено додаткове регулювання [7], а наказом МОН України перелік спеціальностей, здобуття ступеня освіти з яких необхідне для доступу до професій, для яких запроваджено додаткове регулювання [8] тощо.

Поряд з цим, відповідно до чинного законодавства про вищу освіту випускникам закладів вищої освіти (крім тих, що навчалися за "регульованими спеціальностями) у дипломах зазначається тільки освітня кваліфікація. За

[3] Міжнародна стандартна класифікація занять 2008 року (ISCO-08). - URL: https://www.ilo.org/public/english/bureau/stat/isco/isco08/

[4] Європейська класифікація занять, кваліфікацій та навичок (ESCO). - URL: https://ec.europa.eu/esco/portal/home

[5] Закон України «Про освіту». - URL: https://zakon.rada.gov.ua/laws/show/2145-19#Text

[6] Деякі питання Національного агентства кваліфікацій. Постанова КМУ від 5 грудня 2018 року за № 1029 .- URL: https://www.kmu.gov.ua/npas/deyaki-pitannya-nacionalnogo-agentstva-kvalifikacij

[7] Про затвердження переліку спеціальностей, за якими здійснюється підготовка фахівців у сфері фахової передвищої освіти з професій, для яких запроваджено додаткове регулювання. Постанова КМУ від 2 вересня 2020 року за № 765. - URL:https://zakon.rada.gov.ua/laws/show/765-2020-%D0%BF

[8] Про затвердження переліку спеціальностей, здобуття ступеня освіти з яких необхідне длядоступу до професій, для яких запроваджено додаткове регулювання. Наказ МОН України від 22.05.2020 року за №673. - URL: https://mon.gov.ua/ua/npa/pro-zatverdzhennya-pereliku-specialnostej-zdobuttya-stupenya-osviti-z-yakih-neobhidne-dlya-dostupu-do-profesij-dlya-yakih-zaprovadzheno-dodatkove-regulyuvannya

теперішньої ситуації відсутності в країні мережі кваліфікаційних центрів, як у більшості випускників закладів вищої освіти, так і роботодавців, виникають суттєві проблеми з працевлаштуванням та професійною ідентифікацією і розподілом за вакансіями майбутніх працівників. Додатковою проблемою виступає й те, що в Україні системою освіти жоден освітній стандарт не приведений у відповідність до більш як 180 затверджених та запроваджених на практиці професійних стандартів[9].

Виходячи із ситуації, що склалася, вперше у вітчизняній практиці автором підготовлені методичні підходи щодо визначення професійної придатності випускників закладів освіти в умовах відсутності мережі центрів з незалежного присвоєння професійних кваліфікацій (далі – МП). В їх основу, окрім матеріалів з Інформаційної мережі занять США (Occupational Information Network (O'net) були покладені авторські напрацювання та доробки [10] [11] [12] [13].

МП направлені на:

оцінювання заінтересованими сторонами як основних, так і додаткових професійних компетентностей, та/чи їх складників (методом самооцінки під наглядом експертів чи зовнішнього спостереження незалежними експертами у процесі роботи за індикаторами, зведеними до певних груп вимог);

співставлення результатів оцінювання із еталонними значеннями індикаторів вимог до певної професії, посади чи професійної назви роботи;

розроблення персоніфікованих рекомендацій щодо подальшого працевлаштування чи роботи за професією (суміжними професіями), посадою чи професійною назви роботи, додаткового професійного навчання за окремими навчальними програмами, професійною підготовкою чи навчанні на робочому місці;

їх внутрішньо фірмове застосування під час атестації, добору, розстановки кадрів, їхнього кар'єрного зростання, визначення потреби в підвищенні кваліфікації, додаткову підготовку (перепідготовку) кадрів та використання під

[9] Реєстр професійних стандартів. - URL: https://www.me.gov.ua/Documents/Detail?lang=uk-UA&isSpecial=True&id=22469103-4e36-4d41-b1bf-288338b3c7fa&title=RestrProfesiinikhStandartiv

[10] Європейський фонд освіти: інформаційні матеріали для України. - URL: https://openspace.etf.europa.eu/blog-posts/etf-bridging-support-ukraines-vocational-education-and-training-system-and

[11] Мельник С.В. та інші. Опис найбільш вживаних професій. В-во "Медіа про"- Київ, 2007. 302с.

[12] Мельник С.В. Освітньо – професійні стандарти у контексті реформування системи підготовки кадрів. Монографія. Видавництво ТОВ "Віртуальна реальність", Луганськ, 2008р., 278с.

[1313] Мельник С.В. Методичні підходи щодо визначення мотивації вивільнюваних працівників вугільних підприємств до працевлаштування та визначення їхньої професійної придатності для цього. - URL: https://smelnikukr.com/all_materials/ (Рубрика "Загальні матеріали").

час розроблення професійних стандартів, а також при переході від професійних стандартів до стандартів освіти та освітніх програм.

Оцінювання професійної придатності випускників закладів освіти, співставлення його результатів з еталонними значеннями та розроблення відповідних рекомендацій та/чи рішень полягають у наступному:

один із методів оцінювання, який застосовується у цих МП, зорієнтований на самооцінку випускником закладу освіти під наглядом експертів. Зростання суб'єктивності за цим методом полягає в тому, що випускники закладів освіти, як правило, є професійно недосвідченим сегментом робочої сили, та не можуть самостійно, навіть під наглядом експертів, об'єктивно оцінювати свої здатності та здібності. Більш об'єктивним та рекомендованим методом оцінювання професійної придатності випускників закладів освіти є зовнішнє спостереження за їх професійною діяльністю (у визначений період) незалежними експертами, до складу яких входять представники кадрової служби підприємства, керівники його профільних структурних підрозділів та найдосвідченіші працівники підприємства за професією чи їх групою, представники інших заінтересованих сторін;

у результатах оцінювання важливі не абсолютні показники (кількість балів), а їх відношення до рівнів шкали оцінювання;

оцінювання проводиться у 3 етапи:1 етап – безпосереднє оцінювання за прийнятими підходами; 2 етап – співставлення результатів оцінювання з еталонними значеннями індикаторів (середні показники, визначені шляхом опитування профільних роботодавців, фахівців та експертів) вимог до певних професій (посад, професійних назв робіт); 3 етап – прийняття рішення про професійну придатність оцінюваного чи надання йому рекомендацій в іншому випадку щодо подальшої професійної траєкторії (професійне навчання, професійне навчання за окремими навчальними програмами тощо);

за своєю структурою вимоги до професії (професійної назви роботи, посади) поділяються на 11 груп індикаторів вимог, а саме:1) необхідні знання; 2) необхідні уміння та навички; 3) інші необхідні елементи компетентностей; 4) виробнича діяльність; 5) умови праці; 6) професійні інтереси; 7) очікування від роботи; 8) вимоги до працівника та/чи вимоги працівника; суміжні та подібні заняття; 10) необхідна кваліфікація; 11) освітній рівень. Окремі підходи, структуру та змістовну частину груп індикаторів вимог частково взято із Інформаційної мережі занять (Occupational Information Network, O'Net), яка застосовується Управлінням зайнятості та освіти США, та доповнено додатковими параметрами. Слід зазначити, що в процесі оцінювання експерти можуть застосовувати, виходячи з потреби, будь-які з цих 11 груп індикаторів вимог, але в обов'язковому порядку ті, що виписані у 1-5, 8 та 10 групі. Крім того, експертній групі надається можливість розширювати за необхідності перелік та зміст індикаторів до вимог 1-8 групи;

кількісну оцінку (еталонні значення) для кожного індикатора в межах його групи визначає експертна група, до складу якої входять представники зацікавлених сторін національного та/чи регіонального рівня (кадрові служби підприємств, роботодавці, центри зайнятості, професійні асоціації тощо), що формують державну, галузеву та регіональні потреби в кадрах у професійному

розрізі. Бажано залучати при розробленні еталонних індикаторів якомога більше число експертів (за межами формальної освіти), що дозволить зменшувати суб'єктивність при формуванні усереднених еталонних індикаторів та їх значень. Абсолютні значення індикатора за 100-бальною шкалою, де 0 – відсутність здатностей, а 100 – максимальна їх наявність. При формуванні змістовної частини індикаторів використовуються також наявні нормативні документи щодо професії чи їх групи (професійні стандарти, кваліфікаційні характеристики, посадові (робочі) інструкції, норми та нормативи часу, виробітку, вимоги до умов та охорони праці тощо). Крім того, ураховується думка найбільш досвідчених працівників за певною професією. Таким чином, еталонні значення індикаторів (показників) вимог до певної професії розроблюються окремими групами експертів, які за нею (професією) найбільш професійно можуть визначити рівень вимог до компетентностей;

співставлення результатів оцінювання зі шкалою оцінки необхідних (еталонних) компетентностей. Шкала оцінювання представлена у Таблиці1.

Таблиця 1.

Шкала оцінювання компетентностей для професії (посади, професійної назви роботи)

Рівні шкали	Кількість балів (від 0 до 100)	Оцінка
Основні	80 – 100	Висока
	60 – 79	Достатня
	50 – 59	Прийнятна
Допоміжні	40 – 49	Перехідна
	20 – 39	низька
Несуттєві	до 20	наднизька

Ця шкала сформована за результатами авторських досліджень за 6 професійними групами, та носить рекомендаційний характер для експертної групи з розробки еталонних значень індикаторів. За допомогою шкали експертна група відсіює з еталонного набору індикаторів допоміжні (за необхідності) та несуттєві. Співставлення результатів оцінювання випускників закладів освіти з еталонними індикаторами вимог за певною професією, посадою чи професійною назвою роботи проводиться експертами за кожною із 11 груп вимог чи їх обов'язковою частиною (1-5, 8 та 10 група).

Інформація, виписана у 6, 7, 9 та 11 групах індикаторів носить допоміжний характер для розробників еталонних значень індикаторів та при співставленні з ними результатів оцінювання;

прийняття рішення експертами щодо наявності відносної відповідності компетентностей оцінюваного еталонним значенням індикаторів за певною професією можливе за умови:

якщо більше половини індикаторів за 1–8 групою співпадає (або вище) еталонних їх значень за кожною з них;

якщо оцінюваний відповідає мінімальному рівню вимог за кожною з 1–4 групою індикаторів та не менш як двома групами із 5–8 груп;

якщо оцінюваний відповідає мінімальному рівню вимог за кожною з 1–4 групи індикаторів та має не менше третини "відповідностей" еталонним значенням за кожною із 5–8 груп індикаторів;

стосовно оцінюваних, які не пройшли професійний відбір за описаними вище підходами, експертна група відбирає для кожного з них набір індикаторів, які слід досягти у майбутньому через визначений період шляхом підвищення кваліфікації, навчання на робочому місці, через наставництво, навчання на корпоративних короткотермінових курсах, стажування тощо. За умови, коли оцінюваний отримав низькі результати, то за ними йому будуть підібрані робочі місця чи посади за нижчими за кваліфікаціями, або буде відмовлено у працевлаштуванні, зокрема з пропозицією пройти відповідне оцінювання через визначений комісією період часу.

Вибірковий перелік показників (з їх описами) за їх окремими групами має такий вигляд:

Необхідні знання: економіка та бухгалтерський облік (теоретичні та практичні знання у сфері економіки та бухгалтерського обліку, фінансових ринків, банківської справи, аналізу та звітності фінансових показників); адміністрування й управління (знання ділових та управлінських принципів стратегічного планування, розподілу ресурсів, моделювання людських ресурсів, техніки управління, виробничих методів і координації людей та ресурсів); математичні (знання арифметики, алгебри, геометрії, статистичних розрахунків та їх форм); право (знання права, юридичних законів, судових процедур, прецедентів, урядових інструкцій та розпоряджень, правил політичного процесу); державна мова (знання структури та змісту української мови, включаючи значення, вимову та правила складання слів, граматику); комунікації та засоби інформації (знання виробництва засобів інформації, комунікацій, технік і методів її розповсюдження. Сюди входить пошук альтернативних шляхів для інформування й ознайомлення через письмові, усні та візуальні засоби інформації); психологія (знання людської поведінки та її характеристик, індивідуальних особливостей та відмінності у здібностях та інтересах, визначення здібностей до навчання і мотивації, наукових методів психології, оцінка та аналіз поведінкових та емоційних розладів); навчання та підготовка (знання принципів і методів проектування навчального плану і тренінгів, групового та індивідуального навчання, інструктування та вимірювання ефекту від навчання); продажі та маркетинг (знання принципів і методів представлення, просування та продажу продуктів чи послуг. Сюди відноситься знання маркетингової стратегії та тактики, демонстрації продукції, техніки продажу та систем контролю за продажами); комп’ютери й електроніка (знання схем управління, процесорів, чипів, електронного оснащення, комп’ютерного устаткування та програмного забезпечення, включаючи власне програмування); персональні ресурси (знання принципів і процедур персонального рекрутингу, відбору, навчання, компенсації за користь, трудових взаємовідносин і переговорів (співбесід), персональних систем інформації);

діловодство (знання адміністративних і канцелярських процедур і систем, таких як обробка текстів, управління реєстрацією та записами, стенографія та запис, правил оформлення, та інших офісних процедур і технологій); клієнтські та індивідуальні послуги (знання принципів і процесів надання (забезпечення) клієнтських і індивідуальних послуг. Сюди відноситься оцінка потреб клієнтів, застосування стандартів якості послуг та оцінка задоволення клієнта); суспільна безпека й охорона (знання необхідного оснащення, процедур і дій, що сприяють ефективному захисту людей та підприємств, установ, організацій); телекомунікації (знання трансляції, радіомовлення, перемикання, контролю й управління телекомунікаційними системами); історія (знання історичних явищ та їх наслідків, впливу на цивілізацію та культуру); філософія (знання різних систем філософії та релігії. Сюди відноситься знання їх основних принципів, значення, етики, способів мислення, звичаїв, методів їх впливу на культуру людини); виробництво та оброблення (знання вартості сировини, процесів виробництва, контролю якості та іншої техніки для максимізації ефективності виготовлення та розповсюдження виробів); соціологія й антропологія (знання колективної поведінки та соціальних тенденцій впливів, людських переміщень, етнічної приналежності, їх культури та історії); обстеження та рекомендації (знання принципів, методів і процедур діагностики, обстеження та відновлення фізичних і розумових дисфункцій); фізична географія (знання принципів і методів опису особливостей Землі, зокрема акваторій та повітря, включаючи їх фізичні характеристики, розташування, взаємозв'язки та розподіл рослин, тварин та людського життя); транспортування (знання принципів і методів переміщення людей чи виробів повітряними, залізничними, морськими чи автомобільними шляхами, включаючи відносні витрати та зиски); біологія (знання рослинних і тваринних організмів, їх тканин, клітин, функцій, взаємозв'язку та взаємодії один з одним та навколишнім середовищем); будівництво та конструювання (знання матеріалів, методів і інструментів, необхідних для конструювання та/чи ремонту будинків, будівель чи інших структур, таких як шосе й дороги); хімія (знання хімічної будови, структури та властивостей матерії і хімічних процесів перетворення, яким вони піддаються. Сюди відносяться знання про використання хімічних продуктів та їх взаємодію, виробничі технології небезпечних речовин та інші); проектування (знання технік проектування, інструментів і принципів, необхідних у виконанні точних технічних планів, світлокопіювальних паперів, малюнків і моделей); розроблення та технології (знання практичного застосування наукових розробок і технологій. Сюди відноситься застосування принципів, техніки, процедур і устаткування для виробництва різних виробів і послуг); мистецтво (знання теорії та техніки, необхідних для складання, представлення й виконання музики, танцю, візуального мистецтва, драми, скульптури та інше); харчове виробництво (знання технології й устаткування для садіння, вирощування та збору врожаю харчових продуктів (рослин і тварин), включаючи техніку їх складування, пересування та переробки); іноземна мова (знання структури та змісту іноземної мови, включаючи розуміння значень, принципів вимови слів, правил граматики); механіка (знання машин та інструментів, включаючи їх проектування, використання, ремонт та обслуговування); медицина та

стоматологія (знання інформації та техніки, які необхідні для діагностування та оброблення ушкоджень, хвороб та уражень людини. Сюди відноситься знання ознак, методів оброблення, властивостей препаратів, їх взаємодій та профілактичних засобів охорони здоров'я); фізика (знання та прогнозування фізичних принципів, законів, їх взаємозв'язку та використання для розуміння динаміки рідини, матеріалів і атмосфери та знання механічних, електричних, атомних та субатомних структур і процесів) тощо.

Необхідні уміння та навички: управління фінансовими ресурсами (визначення того, як будуть використані кошти для виконання роботи з розрахунку витрат); математичні (використання математичних методів для вирішення проблем); критичного мислення (використання логіки та міркування для визначення сильних та слабких сторін альтернативних рішень, наслідків та проблем); судження та прийняття рішення (розрахунок відносної вартості та прибутків від потенційної діяльності для вибору найбільш прийнятного варіанта); розуміння прочитаного (розуміння письмових речень та розділів документів, пов'язаних з роботою); розмовні (співбесіди для більш ефективного передавання інформації); оцінювання систем (визначення критеріїв чи індексів характеристик систем і необхідних дій для поліпшення чи корегування характеристики стосовно цілей системи); написання (ефективне володіння письмом); системного аналізу (визначення того, як має функціонувати система та який буде вплив на результати в певних умовах діяльності та середовища); комплексного вирішення завдань (визначення комплексу завдань і розгляд інформації, що з ними пов'язана, для прийняття рішення та його оцінки); активного навчання (розуміння значення нової інформації як для сучасного, так і для майбутнього розв'язання проблем та прийняття рішень); контрольні (наглядові) (контроль/оцінювання себе особисто, інших працівників чи організацій для прийняття заходів щодо удосконалення чи корегування); координаційні (регулювання діяльності інших); активного слухання (повна увага, коли говорять інші, надання часу підлеглим на обмірковування для розуміння певної роботи, постановка відповідних запитань, тобто вміння слухати); операційного аналізу (аналіз потреб та вимог до виробу (послуги) для створення його (її) проекту (макета); методологічні (використання наукових правил і методів для розв'язання проблем); управління персоналом (мотивація, розвиток та спрямованість людей до роботи, визначення найкращих кандидатів для певної роботи); переконання (переконання інших змінити позицію чи поведінку); соціальної проникливості (знання поведінки людей та розуміння їхніх дій); вивчення стратегічного планування (відбір та використання навчальних інструкційних методів і відповідних процедур у разі вивчення нових матеріалів); управління матеріальними ресурсами (дотримання відповідного використання устаткування, засобів та матеріалів, необхідних для виконання певної роботи); переговорні (уміння викликати в інших прихильність до себе та шукати компроміси); управління часом (відповідальне використання свого робочого часу та управління часом інших); інструктування (навчання інших певному виду діяльності (роботи); діяльності та управління (операційний контроль устаткування чи систем); аналізу контролю якості (проведення випробувань і перевірок виробів, послуг чи процесів для оцінки якості або

характеристики (відповідності); орієнтації обслуговування (активне спостереження за напрямками надання допомоги працівникам; відбору устаткування (визначення типів інструментів та устаткування, які необхідні для виконання роботи); програмування (написання комп'ютерних програм); пошуку несправностей (визначення випадків операційних помилок та прийняття рішення щодо їх усунення); встановлення устаткування (установлення устаткування, машин, електропроводки чи програм згідно з технічними умовами); операційного контролю (спостереження за датчиками, іншими показниками для контролю справності роботи машини (іншого обладнання); обслуговування устаткування (виконання технічного обслуговування устаткування та визначення необхідності ремонту); ремонту (ремонт машин та систем з використанням необхідних інструментів); проєктування технології – генерування чи пристосування устаткування й технології для задоволення потреб користувача).

Інші необхідні елементи компетентностей: дедуктивне міркування (здатність застосовувати загальні правила до специфічних проблем для їх розумного розв'язання); математичне міркування (здатність вибирати правильні математичні методи чи формули для вирішення проблем); усне розуміння (здатність слухати та розуміти інформацію й ідеї, висловлені під час розмови); письмове розуміння (здатність читати та розуміти інформацію та ідеї, що висловлені в письмовій формі); оперування цифрами (здатність швидко та правильно складати, віднімати, помножувати чи ділити); усне вираження (здатність викладати інформацію та ідеї в розмові таким чином, щоб розуміли інші); письмове вираження (здатність письмово викладати інформацію та ідеї таким чином, щоб розуміли інші); ясність мовлення (здатність чітко та дохідливо говорити, щоб змогли зрозуміти інші); індуктивне міркування (здатність комбінувати частку інформації для формування загальних правил чи висновків (включаючи визначення взаємозв'язку між очевидно не пов'язаними одна з іншою подіями); упорядкування інформації (здатність упорядковувати речі чи дії відповідно певних правил (упорядкування даних, листів, слів, малюнків, математичних операцій тощо) швидкість мислення (здатність генерувати велику кількість ідей стосовно певної теми (важлива кількість ідей, а не їх якість, правильність чи креативність); бачення ситуації (здатність бачити деталі); чутливість (здатність висловлюватися, коли щось є неправильним чи може бути неправильним. Сюди не входить вирішення проблем, а тільки їх фіксація); оригінальність (здатність подавати незвичайні та розумні ідеї щодо певної теми чи ситуації або передбачати розвиток креативних шляхів розв'язання відповідних проблем); гнучкість (здатність використовувати різні правила для комбінування чи групування предметів (ідей, процесів, категорій тощо) різними шляхами); запам'ятовування (здатність пам'ятати інформацію, зокрема таку, як слова, числа, картини та процедури); швидкість розуміння значення (здатність швидко сприймати значення, поєднувати та організовувати інформацію в значущі моделі); розуміння мовлення (здатність визначати та розуміти мовлення іншої людини); тямущість мови (здатність швидко та точно знаходити подібність та різницю в листах, числах, речах, картинах чи моделях. Елементи для порівняння можуть бути представлені разом чи один за одним);

аудиторна увага (здатність зосереджуватися на єдиному джерелі звуку в присутності інших відволікаючих звуків); селективна увага (здатність концентруватися на завданні впродовж часу без відволікання); стійкість рук та долонь (здатність тримати руки та долоні в одному положенні (не жестикулювати); гнучкість сприйняття (здатність визначати чи виявляти відомі моделі (фігури, об'єкти, слова чи звуки), які приховані (знаходяться) в іншому матеріалі; розподіл часу (здатність переключатися з однієї на іншу діяльність чи джерело інформації (такі, як мовлення, звуки, дотик чи інші джерела); швидкість рук (здатність робити швидкі, легкі, повторювані рухи пальців, рук і зап'ясть); сила (здатність використовувати свої мускули для утримання частини тіла в одному положенні тривалий час та без утоми); фізична маневреність (здатність швидко пересувати руку, руку з ліктем чи обидві руки для захвату, переміщення чи збирання предметів); маневреність пальців (здатність робити точно скоординовані рухи пальцями однієї чи обох рук для захвату, переміщення чи складання дуже малих предметів); просторове орієнтування (здатність знати своє місцезнаходження в певний момент чи місцезнаходження об'єкта); статична сила (здатність проявляти достатньо сил для підняття, натискання, відштовхування чи перенесення предметів); візуалізація (здатність уявляти, як щось буде виглядати після його обертання чи обертання й пересування його частин); далекозорість (здатність бачити предмети на великій відстані); координація всього тіла (здатність координувати рухи рук, колін і торса, коли тіло рухається); чуттєвий слух (здатність визначати різницю між звуками, що дуже змінюються за кількістю та силою голосу); нічне бачення (здатність бачити в слабко освітлених умовах); час реакції (здатність швидко реагувати (з руками, пальцями чи ногами) для подання сигналу (звуку, світла, картинки), коли це необхідно); швидкість рухів (здатність швидко пересувати лікті чи коліна); динамічна гнучкість (здатність швидко та багаторазово згинати, тягнути, крутити чи протягати все тіло, лікті чи коліна); тривала гнучкість (здатність тривалий період гнути, тягнути, крутити чи протягати все тіло, лікті чи коліна); координація кінцівок (здатність координувати дві чи більше кінцівки (наприклад, два лікті, два коліна, один лікоть та два коліна) упродовж сидіння, стояння чи лежання); боковий зір (здатність бачити об'єкти чи пересування об'єктів з якогось боку, коли очі дивляться вперед); звукова локалізація (здатність визначати джерело шуму); Точність керування (здатність швидко та безперервно контролювати керування машиною чи транспортним засобом для визначення необхідного положення); Сприйняття висоти (здатність оцінювати, який предмет знаходиться ближче, який далі, та відстань об'єктів від себе); Динамічна сила (здатність постійно чи послідовно застосовувати силу (напружувати мускули). Сюди входить витривалість мускул та опір утомі мускул); Вибухова сила (здатність використовувати мускули ривками (в стрибанні чи кидках); чуттєвість до блиску (здатність бачити предмети в умовах сліпучого блиску чи яскравого освітлення); рівновага тіла (здатність тримати чи балансувати тіло в стані хитання); регулювання швидкості (здатність регулювати, координувати свою швидкість зі швидкістю об'єктів); швидкість реакції (здатність швидко вибирати між двома чи більше рухами, реагуючи на різні сигнали (світло, звуки, картинки). Сюди відноситься швидкість, з якою

необхідно правильно зреагувати руками, ногами чи іншими частинами тіла); стійкість (здатність тримати фізичну активність упродовж тривалого часу без утоми); візуальне розрізнення кольорів (здатність погоджувати та виявляти різницю між кольорами, включаючи відтінки та яскравість).

Виробнича діяльність: аналіз даних чи інформації (визначення принципів, причин чи фактів аналізу та отримання інформації, шляхом її розкладання на окремі частки); співробітництво з керівниками, колегами чи підлеглими (надання інформації керівникам, співробітникам і підлеглим телефоном, у письмовій чи електронній формі. Проведення чи відвідування штатних зустрічей); отримання інформації (надання та отримання інформації з усіх джерел); прийняття рішень та розв'язання завдань (аналіз інформації та оцінка результатів для вибору найкращого рішення та розв'язання завдань); документування/реєстрація інформації (отримання, розшифрування, реєстрація, збереження чи підтримка інформації в письмовій чи електронній формі); оцінювання вимірюваних характеристик продуктів, подій чи інформації (оцінювання розміру, відстані та кількості; визначення часу, вартості, ресурсів чи матеріалів, необхідних для виконання роботи); визначення предметів, дій чи подій (пошук інформації шляхом класифікації, оцінки, визначення різниці чи подібності та визнання змін обставин чи подій); надання консультацій і порад іншим (надання консультацій чи компетентних порад з управління чи іншого кола питань щодо технічних проблем чи питань, пов'язаних із системою або операцією); координація роботи працівників (наставляння членів групи працювати разом для виконання поставлених завдань. Управління та координація діяльності працівників. Управління виконанням нових процедур чи програм. Нагляд за виконанням організаційних чи програмних завдань); розвиток цілей та стратегій (установлення довгострокових цілей та специфічних стратегій та діяльності для їх досягнення. Розвиток процедур, методів чи стандартів); пояснення значення інформації іншим – переклад чи пояснення значення інформації та шляхів її використання); контроль та управління ресурсами – контроль та управління ресурсами, нагляд за витратами коштів); організація, планування та класифікація роботи (розвиток специфічних цілей і планів для класифікації, організації та виконання роботи. Підготовка довгострокових та короткострокових планів); оброблення інформації (складання, кодування, класифікація, калькуляція, зведення, перевірка чи підтвердження інформації або даних); судження про якості речей, послуг чи людей (оцінювання вартості, значення чи якості (характеристик) предметів чи людей); контроль процесів, матеріалів чи оточуючого середовища (контроль і розгляд інформації про матеріали, події чи навколишнє середовище, обстановку для визначення чи оцінювання проблем); поповнення та використання відповідних знань (підтримка знань на високому рівні та їх постійне оновлення для виконання роботи, зокрема стосовно контракту, властивостей чи законів, економічних змін тощо); установлення та підтримка взаємозв'язку між персоналом (розвиток конструктивних і спільних трудових відносин з іншими працівниками та постійна їх підтримка); керівництво та мотивація (здійснення керівництва підлеглими, включаючи встановлення норм та стандартів роботи, контроль за їх виконанням); адміністративна діяльності (постійне виконання

адміністративних завдань, зберігання інформації та оброблення документів); оцінювання інформації для визначення відповідності стандартам (використання відповідної інформації й особисте міркування щодо визначення подій чи операцій відповідно до законів, інструкцій, настанов, регламентів чи стандартів); складання розкладу роботи чи діяльності (розклад подій, програм та іншої діяльності); розвиток та створення груп (заохочення та створення взаємної довіри, поваги та співробітництва серед членів групи); робота з комп'ютерами (використання комп'ютерів та комп'ютерних систем (включаючи обладнання та програмне забезпечення) для програмування, написання програмного забезпечення, встановлення функцій, вводу даних чи оброблення інформації); креативне мислення (розвиток, проєктування чи створення нових пропозицій, ідей, взаємозв'язків, систем чи продуктів, включаючи творчі внески); співробітництво з персоналом зовнішніх організацій (співробітництво з представниками інших організацій, клієнтів, громадських, урядових організацій та іншими зовнішніми джерелами. Обмін інформацією відбувається особисто, в письмовій формі, телефоном чи електронною поштою); підбір персоналу (залучення, інтерв'ювання, відбір, наймання та кар'єрне зростання працівників); розв'язання конфліктів та проведення переговорів (аналізування скарг, урегулювання суперечок під час вирішення конфліктів чи ведення переговорів із персоналом); стажування та розвиток персоналу (визначення необхідного розвитку інших, зокрема стосовно їх стажування, наставляння чи будь-яка інша допомога для підвищення знань і навичок персоналу); продаж і вплив (переконання клієнтів купувати товари, вироби та вплив на зміну свідомості та дій споживачів); перекладання та пересування предметів (використання рук та долонь під час перекладання, установки, розташування й пересування матеріалів та регулювання порядку (предметів); тренінг та навчання персоналу (визначення необхідної кваліфікації для працівника, розвиток навчальних програм на виробництві, навчання й інструктаж працівників); робота з людьми, безпосередній зв'язок із громадськістю (робота з людьми чи безпосередній зв'язок із громадськістю. зокрема щодо обслуговування клієнтів); допомога й турбота про інших (забезпечення медичної допомоги, медичного обслуговування, емоційної підтримки чи іншої допомоги підлеглим, клієнтам чи пацієнтам); виконання загальної фізичної діяльності (виконання фізичної діяльності, яка потребує значного використання рук і колін і пересування всього тіла: повзання, підйом, балансування, ходіння, нахили); управління машинами та операціями (використання механізмів керування чи прямої фізичної діяльності для роботи з машинами чи окремими операціями (за винятком комп'ютерів чи транспортних засобів); огляд обладнання, споруд чи матеріалів (огляд споруд чи матеріалів для визначення причин помилок чи інших проблем і дефектів); проєктування, розміщення та визначення технічних пристроїв, частин і устаткування (документальне забезпечення, детальні інструкції, креслення чи специфікації, які показують, як пристрої, деталі, обладнання чи структури складено, сконструйовано, зібрано, модифіковано, встановлено чи використано); керування транспортними засобами, механізованими пристроями чи обладнанням (пробіг, маневрування, навігація чи водіння транспортних засобів чи механізованих пристроїв, таких

як: автокари, пасажирські транспортні засоби, літаки чи водні судна тощо); ремонт і підтримка електронного обладнання (обслуговування, ремонт, калібрування, регулювання, точне настроювання чи випробування машин, пристроїв і обладнання, яке працює переважно за електричним чи електронним (не механічним) принципами); ремонт та підтримка механічного обладнання (обслуговування, ремонт, налагодження та випробування машин, пристроїв, частин, що рухаються, та обладнання, яке працює переважно за механічними (не електричними) принципами).

Умови праці: у приміщенні із контрольованим середовищем(Наскільки часто робота виконується в приміщенні з контрольованим станом навколишнього середовища?); координування та управління (Наскільки важливо координувати чи керувати службовою діяльністю?); відповідальність за результати (Наскільки керівник є відповідальним за результати своєї роботи чи роботи інших?); відповідальність за здоров'я та безпеку інших (Якою є відповідальність за здоров'я та безпеку інших?); наслідки помилок (Наскільки серйозними можуть бути наслідки, якщо керівник допустив помилку, яку не можна буде виправити?); робота із зовнішніми клієнтами (Наскільки важливою в роботі є співпраця із зовнішніми клієнтами чи громадськістю?); контакти (Скільки контактів із працівниками (віч-на-віч, за телефоном тощо) потребує робота для її виконання?); важливість точності та акуратності (Наскільки важливо дуже точно та акуратно виконувати роботу?); час роботи в положенні сидячи (Скільки часу займає робота в положенні сидячи?); значення повторення завдань (Наскільки важливо, виконуючи роботу, постійно та безперервно повторювати одну й ту ж фізичну (наприклад, натискання клавіатури) чи розумову діяльність (наприклад, перевірка записів)?); частота конфліктних ситуацій (Як часто виникають конфлікти із керівником?); робота із неприємними та неврівноваженими людьми (Наскільки часто частиною роботи керівника є спілкування з неприємними, сердитими чи невихованими особами?); час роботи стоячи (Скільки часу займає робота в положенні стоячи?); час на ходіння (Скільки часу під час роботи витрачається на ходіння та стрибання?); дуже яскраве освітлення (Наскільки часто виникає потреба працювати при дуже яскравому освітленні чи в неадекватних умовах опалення?); схильність до хвороб та інфекцій (Наскільки часто в роботі виникає схильність до хвороб/інфекцій?); ступінь автоматизації (Наскільки роботу автоматизовано?).

Професійні інтереси: підприємливість (найчастіше використовується у професії для початку та виконання проектів. Ці професії можуть бути пов'язаними з управлінням людьми та ухваленням багатьох рішень. Іноді вони мають справу з ризиками та часто – з бізнесом); традиційність (традиційність занять, що часто містять відпрацьований набір процедур та правил. До їх функцій можуть включатися роботи з даними та детальною інформацією, які переважають у діяльності з ідеями); соціальність (соціальність занять включає в себе роботу та зв'язок із людьми, які займаються навчанням. Ці професії часто необхідні для здійснення допомоги та забезпечення обслуговування інших); дослідництво (дослідні функції включають роботу над ідеями та потребують глибокого міркування. Заняття такого характеру можуть включати пошук

фактів, обчислення та обміркування проблем); художність (художність дій, як правило, включає в себе виконання робіт, пов'язаних із зовнішніми формами, проєктами та моделями. Вони часто потребують самовираження, до того ж робота може виконуватися без чіткого дотримання набору правил); реалістичність (реалістична складова професійної діяльності, яка включає дії, що охоплюють практичні завдання та рішення. Особи з такими професіями часто мають справу з рослинами, тваринами тощо. Багато професій потребують виконання робіт ззовні (не у приміщенні) та не передбачають значної паперової роботи в порівнянні з іншими).

7. Очікування від роботи: Досягнення (професії, що відповідають цій роботі, орієнтовано на отримання результату та дозволяють працівникам використовувати їх сильні здібності, що дає їм відчуття виконаної справи); умови праці (професії, що відповідають цій роботі, передбачають безпеку та прийнятні умови роботи); визнання (професії, що відповідають цій роботі, передбачають просування, схильність до лідерства та часто є престижними); незалежність (професії, що відповідають цій роботі, дозволяють працівникам працювати на себе або особисто приймати рішення); підтримка (професії, що відповідають цій роботі, передбачають відповідний підтримуючий менеджмент, що знаходиться на боці працівників); взаємовідносини (професії, що відповідають цій роботі, дозволяють працівникам надавати послуги та працювати із колегами в дружньому, неконкурентному середовищі).

8. Вимоги до працівника та/чи вимоги працівника: авторитет (працівники цієї професії керують іншими людьми та інструктують їх); умови праці (працівники цієї професії мають добрі умови праці); активність (працівники цієї професії зайняті весь час (повна зайнятість); використання здібностей (працівники цієї професії використовують свої індивідуальні здібності); політика та діяльність компанії (працівники цієї професії справедливо оцінюються компанією); досягнення (працівники цієї професії дістають відчуття досягнення); просування (працівники цієї професії мають можливості для кар'єрного зростання); автономність (працівники цієї професії планують свою роботу із незначним наглядом); компенсації (працівники цієї професії мають більшу заробітну плату ніж інші); гарантії зайнятості (працівники цієї професії мають великі шанси зберегти свою зайнятість у подальшому); відповідальність (працівники цієї професії самостійно приймають рішення); універсалізм (працівники цієї професії зайняті в різноманітних видах діяльності); творче мислення (працівники цієї професії подають власні ідеї); моральні цінності (працівники цієї професії ніколи не наполягають на виконанні того, що суперечить їх моральним цінностям); нагляд, людські відносини (працівники цієї професії мають керівників, які контролюють їх роботу); визнання (працівники цієї професії дістають схвалення роботи, яку вони виконують); соціальний статус (працівники цієї професії шановані іншими в їх компанії та середовищі); технічний нагляд (працівники цієї професії мають наставників, які навчають їх добре працювати); незалежність (працівники цієї професії самостійно виконують свою роботу); соціальне забезпечення (працівники цієї професії працюють для задоволення потреб інших людей); відданість роботі (працівники цієї професії цілком впевнені у важливості й

незамінності своєї діяльності та діють відповідним чином); співпраця (працівники цієї професії активно взаємодіють з колегами, клієнтами, партнерами); здатність до надання соціальних послуг (працівники цієї професії налаштовані на надання індивідуальних послуг найбільш незахищеним категоріям населення).

9. Суміжні та подібні заняття. Експертна група з розроблення еталонних значень індикаторів груп вимог до певної професії формує перелік суміжних та подібних професій, посад та професійних назв робіт, які застосовуються на національному та регіональних ринках праці.

10-11. Необхідні кваліфікація та рівень освіти. Експертна група з розроблення еталонних значень індикаторів груп вимог до певної професії формує перелік професійних кваліфікацій за визначеною професією з доступних джерел (реєстр кваліфікацій, професійні стандарти, переліки спеціальностей, державні стандарти професійної (професійно-технічної) освіти, ЄДЕБО тощо) та направляє його та питання щодо необхідного профільного трудового стажу, навчання на виробництві, рівня освіти найбільш досвідченим працівникам відповідного спрямування для опрацювання та визначення особистих думок, оцінок та значень.

Таким чином, можна зробити узагальнюючий висновок про те, що запропоновані МП можуть стати дієвим інструментом для роботодавців та провайдерів освітніх послуг для оцінювання випускників закладів освіти, перш за все, за тими спеціальностями, за якими не визначається отримання професійної кваліфікації після навчання. Принаймні до моменту формування в країні мережі кваліфікаційних центрів. Крім того, набір індикаторів з їх описами може застосовуватися як інструментарій під час розроблення професійних стандартів та стандартів освіти, професійно орієнтованих освітніх програм.

НАУКОВЕ ВИДАННЯ

МАТЕРІАЛИ
XI міжнародної науково-технічної конференції «ITSec»

1-6 жовтня 2021 року

м. Анталія (Туреччина)
НАУ

Організаційний комітет конференції та редакція можуть не поділяти думки авторів і не несуть відповідальність за достовірність викладеної інформації.

За науковий зміст і викладення матеріалу, достовірність та коректність фактичних даних (у тому числі класифікаційного індексу УДК) уся відповідальність покладається на авторів та їх наукових керівників.

Неінформативний текст матеріалів доповіді міг бути скорочений або вилучений на розсуд Оргкомітету конференції.

Оригінал-макет підготовлено на кафедрі
безпеки інформаційних технологій
Національного авіаційного університету