УДК 659.441.8:004.056 **DOI:** 10.31673/2412-9070.2021.041416

Т. М. МУЖАНОВА, канд. наук з держ. управління, доцент;
С. В. ЛЕГОМІНОВА, доктор екон. наук, професор;
Ю. М. ЯКИМЕНКО, канд. військ. наук, доцент;
В. О. ВЛАСЕНКО, канд. техн. наук, доцент,
Державний університет телекомунікацій, Київ

ЗАСОБИ ІНФОРМУВАННЯ Й НАВЧАННЯ ПЕРСОНАЛУ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ЦИФРОВІЗАЦІЇ

Досліджено сучасні програмні засоби інформування й навчання персоналу у сфері інформаційної безпеки і встановлено основні тенденції їх розвитку. На основі вивчення ринку ПЗ для формування обізнаності й навчання з питань інформаційної безпеки визначено такі тенденції розвитку цієї сфери: спрямування зазначених програм на формування поведінки та культури безпеки персоналу; індивідуальний підхід до навчання для кожної компанії; якісний контент та різноманіття методів, зокрема гейміфікація, мікронавчання та віртуальна реальність; вимірювання якості навчання завдяки відстеженню змін поведінки персоналу на практиці; використання засобів навчання й інформування персоналу як невід'ємної складової ефективної реалізації програми корпоративної інформаційної безпеки.

Ключові слова: інформаційна безпека підприємства; інформування й навчання персоналу у сфері інформаційної безпеки; програмні засоби інформування й навчання персоналу у сфері інформаційної безпеки.

Вступ

Постановка проблеми. В умовах масштабної цифровізації всіх сфер підприємницької діяльності забезпечення інформаційної безпеки набуває особливого значення: постійного захисту потребують корпоративні ІТКС, конфіденційна е-інформація, яка належить або обробляється компанією, усі бізнес-процеси, які в переважній більшості базуються на використанні інформаційно-телекомунікаційних технологій. Через постійне зростання кількості та різноманіття загроз інформаційним активам підприємства прагнуть проводити превентивну політику інформаційної безпеки, яка має на меті мінімізувати реалізацію відповідних ризиків.

Як свідчить статистика, левова частка порушень інформаційної безпеки відбувається внаслідок помилок працівників, причому переважно не фахівців відділу ІТ чи захисту інформації, а найкращими засобами запобігти інцидентам є розуміння персоналом основних проблем інформаційної безпеки та методів їх подолання, а також формування належної поведінки кожного працівника у сфері інформаційної безпеки [1].

Крім того, дослідження компанії Webroot щодо ефективності інформаційних та навчальних заходів [4] підтверджують, що регулярне проведення інформаційних кампаній та тренінгів із питань захисту інформації для персоналу компанії сприяє зниженню кількості інцидентів інформаційної безпеки, зокрема пов'язаних із використанням методів соціальної інженерії.

Аналіз останніх досліджень і публікацій. Основою дослідження стали публікації дослідницької компанії Forrester: праця, присвячена аналізу програмних вирішень найбільших постачальників ПЗ для інформування (формування обізнаності) та навчання з інформаційної безпеки (*Security Awareness And Training*, SA&T) [3], стаття експерта компанії Дж. Бадж про зміну цілей інформування й навчання в зазначеній сфері [2], а також статистичні дані щодо порушень інформаційної безпеки та засобів їх запобігання [1; 4].

Мета статті — дослідити сучасні програмні засоби інформування й навчання персоналу у сфері інформаційної безпеки і встановити основні тенденції їх розвитку.

Основна частина

Для задоволення потреб підприємства в забезпеченні високого рівня обізнаності та професійної підготовки персоналу з питань інформаційної безпеки сьогодні широко використовують велику кількість різноманітних програмних інструментів. Ринок ПЗ із формування обізнаності й навчання є надзвичайно динамічним, конкурентним і затребуваним, а розробники спеціалізованого ПЗ у цій сфері шукають вирішення, які б максимально відповідали очікуванням компаній — потенційних клієнтів.

Провідна компанія з досліджень глобального ринку Forrester у 2020 році провела дослідження найбільш значущих постачальників ПЗ для обізнаності та навчання у сфері інформаційної безпеки (SA&T) [3].

За результатами дослідження визначено 12 найкращих компаній — розробників ПЗ у сфері SA&T, які поділено на чотири групи: лідери, стійкі гравці, конкуренти і претенденти (рис. 1).

До числа кращих виробників увійшли такі, переважно західні, компанії:

♦ лідери — KnowBe4, CybSafe, Infosec та Elevate Security (три з чотирьох створено у США);

♦ стійкі гравці — Proofpoint, Mimecast і Webroot;

♦ конкуренти — Cofense, MediaPRO та Kaspersky (єдина компанія з пострадянського простору);

♦ претенденти — до категорії претендентів на зайняття місця на ринку програмних вирішень SA&T експерти віднесли американську компанію PhishLabs.

Для внесення постачальника до списку експерти Forrester послуговувалися такими критеріями: глобальною присутністю та базою клієнтів (не менш ніж на двох континентах); сегментацією даних користувачів для збору показників програми; просуванням ідеї поширення культури безпеки та кращих практик на всю робочу силу; значним інтересом до виробника з боку клієнтів компанії Forrester.

Рис. 1. Ринкові позиції компаній – розробників ПЗ у сфері SA&T

Аналіз програмних продуктів з інформування та навчання персоналу у сфері інформаційної безпеки показав, що акценти в здійсненні інформаційно-освітньої діяльності продовжують зміщуватися з понять короткої часової дії: «обізнаність» і «покарання» на поняття довготривалої перспективи: «поведінка» і «культура», що точно відображає зміну розуміння і ставлення до проблем недостатньої фахової підготовки персоналу в галузі інформаційної безпеки. Тобто сучасні вирішення SA&T насамперед виховують у персоналу культуру інформаційної безпеки, а не проводять бездоганну підготовку та тестування. Проєктування культури безпеки часто здійснюється на підставі вимірювання настроїв та емоцій, пов'язаних із захищеністю в інформаційній сфері.

Розробники пропонують вирішення, яким притаманний високоякісний, позитивний, надійний і легкий для сприйняття контент з інклюзивними, чіткими і переконливими зображеннями, який формується, ґрунтуючись на практичному досвіді та вивченні змістовного наповнення попередніх програм. У процесі навчання працівників залучають до різних видів практичної діяльності з використанням альтернативних методів навчання, зокрема гейміфікації, мікронавчання та віртуальної реальності.

Сьогодні кожна компанія для реалізації завдань із SA&T може вибрати не тільки загальнодоступні варіанти вирішень, а й індивідуальні розроблення, які створюються відповідно до наявних проблем і потреб конкретного замовника (здійснення впливу за окремим напрямом інформаційного захисту або формування культури безпеки тощо). Розробники надають всебічну і неперервну підтримку компанії-замовнику незалежно від місця розташування та мови спілкування через використання різних стилів комунікації та навчання (вербальний, текстовий, аудіо- та візуальний), беручи до уваги специфіку кожного регіону та підприємства.

Наявні програмні продукти передбачають вимірювання якості засвоєння навчальних матеріалів не традиційними методами оцінювання знань та навичок після завершення навчальних програм, а використовують кількісне вимірювання рівня ризиків із боку персоналу відстеженням змін поведінки на основі зазначених даних (наприклад, даних щодо дотримання політики керування паролями або використання VPN до і після тренінгу).

Загалом програмні вирішення SA&T розглядаються не як засоби інформування й навчання персоналу з окремих аспектів інформаційної безпеки, а як внесок у реалізацію корпоративної програми інформаційної безпеки, про ефективність якої свідчить зменшення кількості порушень та інцидентів безпеки внаслідок нефахових дій або недбалості з боку персоналу.

На основі вивчення програмних продуктів із питань формування обізнаності й навчання у сфері інформаційної безпеки від найкращих світових виробників можна виокремити основні тенденції розвитку зазначеної сфери, наведені на рис. 2.

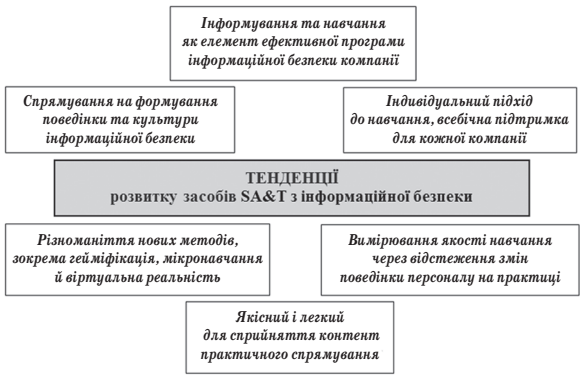

Рис. 2. Тенденції розвитку засобів інформування та навчання з інформаційної безпеки

Висновки

Таким чином, встановлено, що в умовах цифровізації бізнес-діяльності динамічний ринок програмних продуктів із формування обізнаності та навчання персоналу постійно репрезентує нові вирішення, які забезпечують досягнення цілей інформаційної безпеки кожного підприємства. Новітні програмні розроблення фокусуються на формуванні безпечної поведінки та корпоративної культури безпеки, залучають користувачів до альтернативних методів (гейміфікації, мікронавчання та віртуальної реальності), пропонують позитивний, надійний і легкий для сприйняття зміст, надають замовнику всебічну і неперервну підтримку незалежно від його локалізації.

Подальшими напрямами дослідження є вивчення програмних розроблень щодо контролю й оцінювання діяльності персоналу у сфері інформаційної безпеки.

Список використаної літератури

*1. **15 Alarming** Cyber Security Facts and Stats. 2020 [Електронний ресурс]. URL:*

https://www.cybintsolutions.com/cyber-security-facts-stats/ (дата звернення: 13.12.2021).

*2. **Budge Jinan.** The Days When SA&T Operated Solely To Train People About Security Are Vanishing [Електронний ресурс]. URL:*

https://www.forrester.com/blogs/the-days-when-sat-operated-solely-to-train-people-about-security-are-vanishing/ (дата звернення: 13.12.2020).

*3. **The Forrester Wave™:** Security Awareness And Training Solutions, Q1 2020 [Електронний ресурс]. URL:*

http://i.crn.com/ (дата звернення: 13.12.2021).

*4. **Webroot®** Security Awareness Training [Електронний ресурс]. URL:*

https://manufacturerstores.techdata.com/docs/default-source/carbonite/webroot_security_awareness_training_smb.pdf?sfvrsn=2 (дата звернення: 13.12.2021).

Т. М. Мужанова, С. В. Легоминова, Ю. М. Якименко, В. А. Власенко

СРЕДСТВА ИНФОРМИРОВАНИЯ И ОБУЧЕНИЯ ПЕРСОНАЛА В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

Исследованы современные программные средства обучения и информирования персонала в сфере информационной безопасности и установлены основные тенденции их развития. На основе изучения рынка ПО для обучения и формирования осведомленности по вопросам информационной безопасности определены следующие тенденции развития этой сферы: направление указанных программ на формирование поведения и культуры безопасности; индивидуальный подход к обучению для каждой компании; качественный контент и многообразие методов, включая геймификацию, микрообучение и виртуальную реальность; измерение качества обучения путем отслеживания изменения поведения персонала на практике; использование средств обучения и информирования как элемента эффективной реализации программы корпоративной информационной безопасности.

Ключевые слова: информационная безопасность предприятия; информирование и обучение персонала в сфере информационной безопасности; программные средства информирования и обучения персонала в сфере информационной безопасности.

T. M. Muzhanova, S. V. Lehominova, Y. M. Yakymenko, V. O. Vlasenko

TOOLS OF AWARENESS AND TRAINING ON INFORMATION SECURITY IN THE CONTEXT OF DIGITALIZATION

The article examines modern software tools for awareness and training personnel in the field of information security and identifies the main trends in their development. It is noted that the best ways to prevent information security incidents are to form personnel understanding the basic problems of information security and skills to overcome them, as well as the formation of safe behavior of each employee in the workplace.

The study was based on the publication of the Forrester research company on the market of software solutions for Security Awareness and Training (SA&T). Forrester experts identified the best world-class SA&T software vendors in the following categories: leaders, strong performers, contenders and challengers, and analyzed their software products in detail. It was found that the vast majority of companies mentioned in the study are Western.

Based on the SA&T software market research, the article identifies the following trends in this area: the focus of these programs on the formation of safety behavior and culture of personnel, not just knowledge and skills; individual approach to training for each company; quality content and a variety of methods, including gamification, microlearning and virtual reality; practical direction of training, which is carried out in conditions as close as possible to real; measuring the quality of training by further tracking changes in personnel behavior in the workplace; use of training and awareness tools for personnel as an integral part of the effective implementation of the corporate information security program.

Keywords: information security of the enterprise; information security awareness and training; software tools for information security awareness and training.