



**ОТНОСНО ПОДОБРЯВАНЕ НА КОМПЕТЕНЦИИТЕ ЗА КИБЕР ХИГИЕНА НА ПОТРЕБИТЕЛИТЕ ОТ
ДЪРЖАВНАТА И МЕСТНА АДМИНИСТРАЦИЯ ВЪВ ВРЪЗКА С РАЗРАБОТВАНЕ НА
КОНЦЕПТУАЛЕН МОДЕЛ ЗА ЕТИЧНО ПОВЕДЕНИЕ В СЪВРЕМЕННА КИБЕРСРЕДА**

Стоян Денчев, професор д.ик.н.*, Веселина Александрова, доц. д-р**, Виолета Василева, д-р***
*Университет по библиотекознание и информационни технологии (УниБИТ),
s.denchev@unibit.bg, **Военна академия “Г. С. Раковски”, v.gagamova@rndc.bg, ***Future
Innovation Labs, violetta.ziv@gmail.com

**ON IMPROVING CYBER HYGIENE COMPETENCIES OF STATE AND LOCAL GOVERNMENT USERS IN
CONNECTION WITH DEVELOPING A CONCEPTUAL ETHICAL MODEL FOR BEHAVIOR IN THE
MODERN CYBER ENVIRONMENT**

Prof. ScD Stoyan Denchev*, Veselina Aleksandrova, Assoc. Prof., PhD**, Violeta Vasileva, PhD***
*The University of Library Studies and Information Technologies (ULSIT), s.denchev@unibit.bg,
Rakovski National Defence College, v.gagamova@rndc.bg, *Future Innovation Labs,
violetta.ziv@gmail.com

ABSTRACT

The report analyzes the possibilities for increasing cyber awareness, which is an aspect of the manifestation of cyber ethics in the virtual world in the conditions of the information society. Possibilities have been synthesized both for researching cyber awareness of employees and for offering information services related to improving their ethical behavior in the virtual world.

Въведение

В доклада се анализират възможностите за повишаване на киберосведомеността и киберхигиената на потребителите, тъй като тя може да се разглежда като аспект при проявяванията на кибер етиката във виртуалния свят в условията на информационното общество. Целта е да се синтезират възможности, както за изследване на кибер осведоменост на служителите, така и да се дефинират информационни услуги свързани с подобряване тяхното етично поведение в киберпространството. Етичното поведение в виртуалното пространство е в зависимост от киберосведомеността. Тя от своя страна е предпоставка за добра киберхигиена.

За реализирането на информационната услуга свързана с изследване на нивото на киберосведоменост на служителите се предлага използването на метод на анкетно проучване. За да може да се реализират останалите информационни услуги свързани с подобряване на компетенциите за кибер осведоменост на потребителите от публичния сектор и тяхното етично поведение във виртуалния свят се предлага методология, която включва и разработена уеб платформа.

Изследване на кибер осведоменост на служителите чрез метод на анкетно проучване.

Изследване на кибер осведоменост на служителите чрез метод на анкетно проучване подпомага създаване на съответни информационни услуги и условия в интерес на гражданите и бизнеса в съвременното е-Управление. Последователният метод за изследване на кибер осведоменост на служителите, чрез метод на анкетно проучване, се явява предпоставка за разработване на методология, както и съответно решение за подобряване на компетенциите за кибер



осведоменост на потребителите от публичните административни структури при работа в киберпространството. Кибер хигиената е инициатива на образованието и осведомеността за информационна сигурност (ISEA) [3] за разпространяване на осведомеността относно добрите цифрови практики за безопасно онлайн изживяване [2].

. Синтезът на възможности за въвеждане и контрол на ефективни регулаторни мерки за защита на информацията, както и създаването на условия в интерес на гражданите и бизнеса в съвременното е-Управление е от изключителна важност.

Първо, от редица изследвания е доказано, че половината от пробивите в сигурността на данните са причинени от грешки на обикновените бизнес потребители, което опровергава схващането, че хакерите са тези, които стоят зад повечето пробиви. Друго ключово наблюдение от проучванията е, че човешките грешки водят до повече инциденти отколкото от злонамерените действия. Това налага извода, че вниманието трябва да се насочи към човешкия фактор.

Нещо повече, в изминалата COVID-пандемична ситуация много потребители предпочитаха да работят по така наречения модел "работа от дома/хоум офис" „Work From Home“ (WFH). Това изисква по-подробни изследвания за киберсигурността и повишаване на кибер осведомеността и компетентността на потребителя. Според проучването Covid-19 на ISACA, около 90% от участниците вярват, че рязък преход от мястото на работа към така наречения начин на работа в домашен офис би увеличил риска за поверителността на данните и би създал проблеми.

На второ място, ключов аспект на човешкия фактор е свързан и с управлението на идентичността, което е важен елемент от системата за киберсигурност в рамките както на публичните административни структури, така и в сектора на бизнеса. По отношение на управлението на цифровата идентичност, основни въпроси са сигурността и поверителността. Тъй като кибератаките свързани с кражбата на самоличност са широко разпространена в киберпространството, то мерките за идентифициране и валидиране на цифрови самоличности са от решаващо значение за управлението на мрежата и сигурността на информацията.

На трето място, проблемът е изследван от гледна точка на потребителя чрез прилагане на методология за изследване чрез метода на анкетното проучване. Той дава възможност да се направи избор на ключови показатели за изследване, свързани с кибер осведомеността. Те са изследвани и анализирани и след това са определени критерии за оценка. Целта на проучването е да се подпомогне постигането на пакет от способности при работа в киберпространството и изграждане на концептуален модел за етично поведение. Изследването има за цел да помогне на потребителите да получат определени умения, когато работят в киберпространството. Проведено е проучване и са анализирани и обобщени резултатите от анкетата. Резултатите от анкетното проучване се използват за разработване на информационни услуги, които биха повишили кибер информираността на потребителите, дигиталните компетенции за етично поведение, както и за поддържане на високо ниво на киберхигиена сред служителите от организациите на публичния сектор.

Задачи на анкетното проучване са следните:

1. Да се дефинират изискванията при работа на длъжностните лица и отделните потребители при работа в групова среда, както и в условия на пандемия при модела WFH.
2. Да се подпомогне постигане на пакет от способности за етично поведение в киберпространството.
3. Да се дефинират функционалностите за отделните потребители и публични административни структури по постигане високо ниво на сигурност на информацията относно личните данни и тези, касаещи структурата.
4. Да се проучи онлайн етичното поведение на служителите при отдалечен достъп по време на пандемията.
5. Да изследва уязвимостите на потребителите и възможния риск от кражба на самоличност.

Методологията за събиране на данни се основава на онлайн анкетно проучване, съставено от въпроси, които обхващат аспекти като поверителност и управление на самоличността, бизнес дейност, етика и др. Редица въпроси в проучването включват опции за отговори с множество възможности за



избор. Следователно някои от визуализираните резултати могат да надхвърлят 100%. Първоначалният анализ включва описателна статистика на ключови въпроси от проучването, като по този начин предоставя общ преглед на ключовите характеристики на високо ниво.

Дизайнът на анкетата позволява автоматично пропускане на някои въпроси, в зависимост от тяхното значение за конкретен участник. В резултат на това, някои заключения са валидни само за по-малък брой респонденти от общия брой на тях.

Придобиването на способности за наблюдение, откриване и разпознаване на киберзаплахите в екосистемата на публично административната структура е свързано с допълване в информационната инфраструктура на структурите с елементи като сървъри по сигурността на информацията, антивирусни сървъри и други хардуерни и софтуерни средства, които са част от инфраструктура.

Тези способности дават възможност за обединяване на системи, сензори и изпълнителски звена (обекти), с което се увеличава ефективността в работата на публични административни структури. Това се постига, чрез осигуряване на съгласуваност на интерфейсите, оборудването, приложенията и услугите на компонентите от състава на информационната инфраструктура на организациите. Придобиването на способности за наблюдение е свързано и с получаването на данни и изображение в „реално време“, чрез подсистема за наблюдение, откриване и разпознаване на киберинциденти. Това предполага наличие на система от сензори и камери в информационната инфраструктура на комуникационните и информационни системи на системата за ръководство и управление на административната структура.

Придобиването на способности за ефективен обмен и обработка на информация между центрове за отговор на инциденти (SIRC - Security Incident Response Centers) е свързано със създаване на автоматизирана информационна среда за събиране и предаване на сензорна информация за управление на обектите от системата за кибер сигурност.

Изграждането на етичен модел на поведение в киберпространството е свързано с споделяне на данни в реално време чрез подсистема за откриване на кибер инциденти. Изгражданата интегрираната информационна среда за пренос и обработка на информация е предпоставка за непрекъснатото циркулиране на адекватните информационните потоци в рамките на публичните административни структури.

В допълнение, предложеният последователен метод за изследване на кибер осведоменост, мениджмънт на идентичността и предлагане на решение за повишаване на компетенциите на потребителите за етично поведение в киберпространството, може да бъде приложен успешно, както на национално ниво, така и в други информационни домейни от публичния сектор и бизнеса.

Анализът на резултатите от анкетата се бъде използва при разработването на решение за повишаване на киберхигиената. Методологията за изследване на кибер осведоменост на служителите и метод за подобряване на компетенциите за киберосведоменост и етично поведение включва следните стъпки:

1. Изследване на киберосведоменост на потребителите
 - Метод на анкетно проучване
 - избор на ключови индикатори за изследване
 - дефиниране на критерии за оценка
2. Разработване и изпълнение на анкетно проучване
 - избор на технология за провеждане на анкетното проучване
 - разработване на анкетна форма
 - изпълнение на проучването сред избраните реципиенти
 - обработка и анализ на резултатите
3. Методология за подобряване на компетенциите за кибер осведоменост и етично поведение на потребителите от публичния сектор
 - Дефиниране на цел и задачи на методиката
 - Избор на технологии за реализация на Методиката - система за управление на съдържание CMS (Content Management System)

4. Методика за разработване на портал - уебсайт „Кибер осведоменост“

- концепцията и архитектурата на уебсайта,
- визуалният дизайн и изборът на тема на уебсайта
- внедряването и разработването на уебсайта
- прилагане и осигуряване на сигурността на портала
- създаването и управлението на съдържанието и публикуване

Методика за повишаване на компетенциите за етично поведение.

Разработването на методиката се налага като резултат от проведеното изследване с помощта на метода на анкетното проучване. Проучването е извършено между потребители - служители в публичния сектор. Анализът на резултатите от проучването показва, че анкетираните потребители като цяло не се чувстват достатъчно подготвени за справяне с кибератаки, предотвратяване на киберзаплахи, като особено необходимостта от такива компетенции се засилва при работа в режима „работа от дома“ в условията на пандемия. Изводите от проучването показват, че нивото на киберосведоменост на служителите в организациите от публичния сектор е доста слабо. 45% от служителите посочват, че не им е провеждано обучение за сигурност на информацията при работа в киберпространството и особено за дистанционен режим на работа. 74,2% от тях смятат, че пробивите в сигурността по-често се дължат на човешки фактор в организацията. 75,9% смятат, че относно увеличилите се атаки насочени към персоналните устройства, мерките за информационна сигурност не са адекватни, а 8,6% от анкетираните не знаят към кого да се обърнат при възникване на киберинцидент. Само 11,4% от всички служители са преминали през повишаване на професионалната квалификация по киберсигурност и защита на информацията в съответната структура.

Методиката има два аспекта - информационен и изследователски. Основната цел е да се подпомогне постигането на способности за етично поведение и работа в киберпространството в условията на пандемия. Това се постига като се подобри киберосведомеността и компетенциите на потребителите, работещи в организации, както от публичния сектор, така и в бизнеса.

В информационен аспект методиката има за цел да:

- разшири знанията в областта на киберхигиената и киберсигурността;
- подпомага потребителите на услугите му да извършват превантивни действия за намаляване на рисковете от инциденти в информационната сигурност
- осигурява достъп до онлайн приложения за тестване на различни информационни ресурси.
- осигурява достъп до информационни ресурси относно новини, събития, специализирани издания и научни публикации относно киберосведомеността и сигурността
- осъществява непосредствена поддръжка, като предоставя информация при разрешаването на вече възникнали киберинциденти
- предоставя възможност за подаване на сигнали за потенциални киберинциденти от страна на потребителите

В изследователски аспект методиката има за цел да:

- Изследва различни аспекти на онлайн етичното поведение на служителите при достъпване на услуги с отдалечен достъп, както и режим на работа от дома (WFH – Work From Home - модел).
- Изследва уязвимостта на служителите и възможните потенциални рискове от кражба на идентичност.
- Изследва нивото на компетенциите свързани с киберхигиената и киберетиката посредством възможност за решаване на съответни тестове.
- Предоставя функционалност за извършване на специализирани анкетни проучвания сред професионалисти относно инфраструктурата и др.

Методиката е реализирана посредством използването на съвременните информационни технологии и системите за управление на съдържание CMS (Content Management System), като е разработено уеб базирано приложение – уебсайт „Кибер осведоменост“. Той е проектиран и развит



като информационен уебсайт. Като целева аудитория за него може да се посочи широк кръг от потребители от публичния сектор, които са различни по отношение на компетенциите и уменията си в областта на информационната, компютърната и киберсигурността. Групата на потенциалните потребители обхваща както специалисти - професионалисти с високо ниво на квалификация, като служители по сигурността на информацията, системни, мрежови и други администратори, специалисти по киберсигурност и други; така и служители – неспециалисти. Те чрез услугите на уебсайта могат да постигнат безопасно пребиваване в киберпространството. Сайтът може да бъде полезен и на ръководния състав, мениджърите и служителите по сигурността на информацията и по киберсигурността (CISO) във връзка с проверка и подобряване на киберхигиената и компетенциите на потребителите в областта на сигурността на компютърните системи и мрежи, както и за рискове и заплахи в киберпространството.

Основната цел на сайта „Кибер осведоменост“ е да повиши способностите за кибер осведоменост и компетенциите за етично поведение на потребителите, работещи в организации от публичния сектор за работа в киберпространството. В него се предвижда да са публикувани и предоставени като информационни ресурси национални и международни документи за киберсигурност и информационна сигурност. Уебсайтът предоставя възможности за тестване на компетенциите по киберсигурност на потребителите. В допълнение в средата е осигурена възможност за участие от страна на потребителите в изследване, реализирано с метода на анкетното проучване, което изследва различни индикатори и служи като основа за последващ анализ. свързан с кибератаки, споделяне и обмен на информация, мнения и полезни практики за кибер инциденти, което би подпомогнало разработването на модел за етично поведение.

Заключение

В заключение може да се обобщи, че е предложена изследователска методология, която се фокусира върху оценката на компетентността за етично поведение на персонала в публичния сектор да работи ефективно в рамките на сигурно и безопасно работно място. Методологията, приложена в това проучване, се основава на изследователски подход на проучване, който е насочен конкретно към лица, работещи в публичното киберпространство. Въз основа на анализирания резултати от проучването авторите предлагат решения за подобряване на компетенциите и етичното поведение на потребителите във виртуалния свят и повишаване на тяхната кибер осведоменост. Като вариант на реализация на предложената методология, авторите предлагат разработен портал за киберосведоменост. Основната му цел е да осигури информация и ресурси относно киберсигурността и информационната сигурност, за да служи като централен хъб за достъп до знания в тази област. както и да подкрепят етичното поведение на потребителя в съвременна виртуална среда. Онлайн платформата допълнително предлага на потребителите да оценят уменията си по теми, свързани с киберсигурността, да се включат в обществени проучвания, свързани с киберсигурността, както и да разпространяват и обменят информация, перспективи и ефективни методологии относно киберинциденти и експертиза в киберсигурността.

Благодарности. Докладът е написан благодарение на финансиране от Министерство на образованието и науката в изпълнение на Националната стратегия за развитие на научните изследвания 2017 – 2030 по Национална научна програма „Сигурност и отбрана“, приета с решение на Министерски съвет № 731 от 21 октомври 2021 г.

Литература

- [1] Насоки относно етичните аспекти за надежден ИИ, независима експертна група на високо равнище, по въпросите на изкуствения интелект (ЕГВР ИИ), Европейската комисия, b-1049 Брюксел, 2019 г.
- [2] MeitY,G, Cyber Hygiene by ISEA, , <https://play.google.com/store/apps/details?id=com.cyberhygiene&hl=bg>
- [3] Information security Education and awareness (ISEA), <https://isea.gov.in>