

КИБЕРСИГУРНОСТТА ОТ ГЛЕДНА ТОЧКА НА ПОТРЕБИТЕЛИТЕ

Иван Михайлов¹

¹ Икономически университет – Варна/Катедра „Информатика“, Варна, България,

imihaylov@ue-varna.bg

РЕЗЮМЕ

В съвременните условия значителна част от човешката дейност се осъществява с помощта на информационните технологии. Съхраняваните и обработвани в информационните системи данни не само се увеличават като обем, но и се променят в качествено отношение. Те са ценен обект за гражданите и за обществото. В този контекст сигурността на комуникационните структури и на информационните системи се превръща в необходимо и предварително условие за по-нататъшен прогрес. Образователните институции разполагат с лични данни за своите служители и обучавани лица, както и с данни за постигнатите резултати. Тези данни са ценен ресурс, който трябва да бъде опазван, подобно на финансовите активи. С две основни директиви на Европейския съюз – от 2016 и от 2022 година, се цели повишаване на общото ниво на киберсигурност в Съюза. В документите се обръща сериозно внимание на реакциите след настъпване на киберинциденти. Следователно може да се заключи, че информираността и комуникацията са едни от важните фактори за осигуряването на информационна сигурност. Основните постановки от директивите са включени и в текста на действащия от 2018 г. в България Закон за киберсигурността. Целта на настоящия доклад е въз основа на анализ на резултатите от анкета, която изследва опита на студентите с киберинциденти и на техните последващи действия, да се определи нивото на информираност на студентите относно добрите практики в тези случаи и за осведомеността им относно адекватните реакции при възникване на такива ситуации. Получените знания ще спомогнат за по-доброто разбиране на нуждата от мерки за повишаване на киберсигурността и за управление на рисковете в контекста на университетските информационни ресурси.

КЛЮЧОВИ ДУМИ: киберсигурност, кибератаки, информационна сигурност, киберинциденти

CYBERSECURITY FROM THE USERS' PERSPECTIVE

Ivan Mihaylov¹

¹ University of Economics – Varna, Department of Informatics, Varna, Bulgaria,

imihaylov@ue-varna.bg

ABSTRACT

In modern conditions, a significant part of human activity is carried out with the help of information technology. The data stored and processed within information systems not only grows in volume but also changes in quality, becoming a valuable asset for both citizens and society. In this context, the security of communication infrastructures and information systems becomes a necessary prerequisite for further progress. Educational institutions hold personal data about their employees and students, as well as information on academic achievements. This data is a valuable resource that must be safeguarded in the same way as financial assets. Two key European Union directives from 2016 and 2022 aim to increase the overall level of cybersecurity across the Union, placing significant emphasis on responses following cyber incidents. Therefore, awareness and communication are essential factors for ensuring information security. The main provisions of these directives are also included in the Bulgarian Cybersecurity Act, effective since 2018.

The purpose of this report is to determine students' level of awareness regarding best practices and appropriate responses in cases of cyber incidents, based on an analysis of survey results examining students'

experiences with cyber incidents and their subsequent actions. The knowledge gained will contribute to a better understanding of the need for enhanced cybersecurity measures and risk management in the context of university information resources.

KEYWORDS: *Cybersecurity, Cyber Attacks, Information Security, Cyber Incidents*

ВЪВЕДЕНИЕ

Понятието „информационна сигурност“ не е ново. То се отнася до защитата на автоматизирано обработваната информация срещу неправилен достъп, случайно или нарочно видоизменяне, унищожаване или разкриване на съдържанието ѝ. Още през 1998 г. в България е приета „Концепция за национална сигурност на Република България“¹. В точка 43 от Концепцията се казва, че „Опазването на националната сигурност изисква да не се допуска използването на информацията, за да се манипулира масовото съзнание. Приоритет е и да се гарантира със специален закон защитата на държавния информационен ресурс от изтичане на важна за страната политическа, икономическа, научно-техническа и друга информация.“ Също така в Концепцията ясно е казано, че ефективността на органите, които имат за задача да се грижат за информационната сигурност, зависи от „мотивацията на човешкия фактор и от наличието и точността на информация за заплахите и опасностите“. През 2011 г. е приета „Стратегия за национална сигурност на Република България“, която е актуализирана през 2018 г. и е приета „Актуализирана стратегия за национална сигурност на Република България“ с времеви хоризонт до 2025 г. В нея има раздел „Политика за киберсигурност“, който се препраща към Национална стратегия за киберсигурност „Киберустойчива България 2020“, която е актуализирана през 2021 г. – Актуализирана Национална стратегия за киберсигурност „Киберустойчива България 2023“². В т.6.3. Осведоменост, образование и обучение се акцентира на повишаването на киберкултурата чрез добавяне на аспектите на киберсигурността и отговорното и безопасно използване на интернет и новите технологични предизвикателства в програмите за начално и средно образование. Такива усилия са положени и например в учебната програма по информационни технологии за X клас е включена „Тема 3. Решаване на проблеми и безопасност“ и по-конкретно „решение на проблем, свързан с операционната система, приложения и антивирусни програми, и достъп до мрежови услуги, които се използват на конкретно работно място. Посочва начини за надеждна дигитална идентификация при използване на публични услуги.“³

В предишно наше проучване са анализирани и проучени редица нормативни актове и стандарти, засягащи въпроса за киберсигурността и информационната сигурност. Актуално и изчерпателно изследване на въпросите с киберсигурността е предложено от Юлиана Хаджичонева и Пламен Мандаджиев (2023). Авторите засягат и въпроса за необходимост от обучение както на потребителите на информационните системи, така и на ИТ специалистите в организацията.

По време на проведените проучвания стана видно, че съществуват и периодично се актуализират или публикуват нови нормативни документи, касаещи въпросите за киберсигурността както на ниво Европейски съюз, така и на национално ниво. Това се дължи на факта, че

¹ Концепция за национална сигурност на Република България, <https://www.strategy.bg/StrategicDocuments/View.aspx?lang=bg-BG&Id=655>

² <https://iaieu.egov.bg/wps/portal/agency-iaieu/cybersecurity>

³ <https://www.mon.bg/obshto-obrazovanie/uchebni-planove-i-programi-2/uchebni-planove-i-programi-poklasove/uchebni-programi-za-x-klas/>

България като пълноправен член на съюза трябва да прилага неговото законодателство като разработва необходимите нормативни документи.

Образователните институции обработват не само лични данни, но и данни, за резултатите от обучението на ученици и студенти. Освен това те са място за провеждане на научни изследвания. В този смисъл те попадат в обхвата на Директивата на ЕС 2022/2555 – приложение II Други критични сектори, сектор 7. Научни изследвания, Вид субект – Научноизследователски организации. Нарастващата заплаха кибератаки в този сектор е дискутирана от Димитров и Андреев (2023).

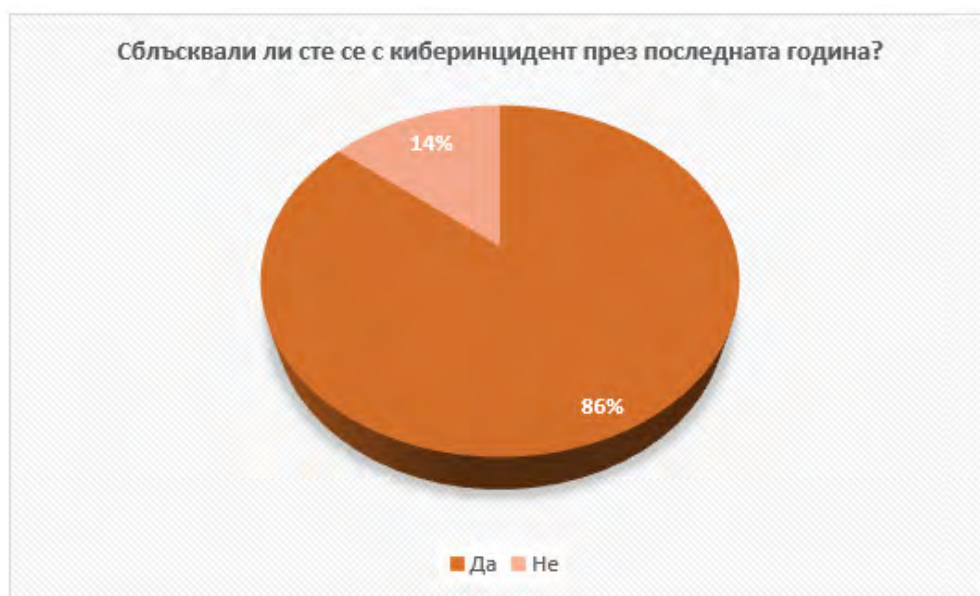
Университетите, разглеждани в ролята им на такива организации, трябва да предприемат действия за разработване и прилагане на политики за информационна сигурност. Откъде обаче трябва да се започне, кои са рисковите фактори за сигурността, които се намират вътре в организацията? Може би отговор дава Н. Димитров (2022) в предложеното от него определение за „Вътрешен контекст (на организация) – включва всички вътрешни параметри на околната среда и фактори, които влияят върху начина, по който организацията управлява риска и се опитва да постигне целите си. Той включва: вътрешните заинтересовани страни, подхода към управлението, договорните отношения, способности, култура и стандарти. Управлението включва: структурата, политиките, целите, ролите, отчетността и процеса на вземане на решения на организацията, а способностите включват: нейните знания и човешки, технологични, капиталови и системни ресурси.“ В това определение също се включват човешките ресурси.

1. ИЗЛОЖЕНИЕ

В настоящия доклад се обръща специално внимание на основните потребители на информационните системни в университетите – студентите. Те са представители на поколението Z, което, както всяко поколение, има своите специфични черти. Както казва Д. Георгиева (2022) „Основна характеристика на поколението Z е, че те правят всичко през смартфона си – учат, работят, комуникират, забавляват се. Те категорично считат, че новите технологии подпомагат и облекчават живота на хората.“

С цел набиране на данни относно киберинцидентите, с които се сблъскват студентите и техните последващи реакции, разработихме онлайн анкета. Тя е анонимна и включва основни въпроси относно конкретния вид на инцидента, реакцията на потребителите, комуникацията с други потребители и информиране относно случилото се.

Анкетата бе изпратена на студенти, обучаващи се в образователна и квалификационна степен „бакалавър“ (от 1 до 4 курс) в Икономически университет – Варна. Отзоваха се 71 студенти, които отговориха изчерпателно на поставените въпроси. Делът на тези от тях, които са имали проблем със сигурността е притеснително висок. Според В. Димитров (2022) липсата на информираност за кибератаки и защитата от хакери може да доведе до тежки последствия. След успешна злонамерена кибератака резултатите може да бъдат катастрофални. Възможните последствия включват загуби на активи, репутация, доверие и времето, което е необходимо за възстановяване след атаката. На фиг. 1 е представен дела на студентите, които са претърпели киберинцидент през последната година.



Фигура 1. Отговори на въпроса „Сблъскали ли сте се с киберинцидент през последната година?“

Източник: Собствена разработка

Всички от отговорилите са на възраст между 18 и 24 години, което означава, че са представители на поколението Z, което „живее“ в мобилните устройства. Това е обяснение и на резултатите на отговора „Къде се случи инцидентът?“ – 66% от анкетираните отговарят, че инцидентът е станал на мобилно устройство.

Важно е да се анализира и вида на инцидента. Резултатите показват, че най-чести са инцидентите, свързани с фишинг атаки (36%), загуба на парола или акаунт (33%), заразяване със зловреден софтуер (16%), непозволен достъп до лични данни (13%) и хакване на профил в социалните мрежи (2%). Важно е да се уточни, че респондентите са посочвали по няколко отговора на този въпрос (фиг. 2).



Фигура 2. Отговори на въпроса „Какъв вид инцидент сте преживели?“

Източник: Собствена разработка

По отношение на това дали са идентифицирали причината за настъпване на инцидент, респондентите отговарят, че не знаят, не могат да уточнят защо се е случило събитието. Това подсказва за липса на технически знания и за ниско ниво на дигитална грамотност. След анализ на отговорите може да се направи извода, че основно инцидентите се дължат на отваряне на подозрителни линкове, слаби пароли и използване на несигурни мрежи.

Комуникацията и споделянето за настъпили инциденти е важно действие с цел предотвратяване на подобни инциденти с други потребители. Реално обаче голям брой от анкетираните (45%) са предприели единствено мерки като смяна на паролата и считат, че това е достатъчно действие в отговор на киберинцидента. Едва 37% са потърсили помощ от ИТ специалист. Тези данни показват ниско ниво на доверие или липса на знания за възможностите за подкрепа.

Необходимостта от повишаване на знанията на потребителите относно защитата и възможностите за превенция на техните данни е изведена и в проучване на Mailok и колектив (2023). И в настоящото изследване се стига до извода, че е налице значителен дефицит в знанията на студентите относно основните методи на защита. Едва 12.5% от респондентите се определят като „много добре информирани“ за основните принципи на киберсигурността. Половината от участниците не знаят какво е двуфакторна автентикация и считат, че използването на „силни“ според тях пароли е достатъчна мярка за защита срещу кибератаки. В друго проучване на Garba и колектив (2020) авторите също достигат до необходимостта от обучения на студентите по основни елементи от киберсигурността и липсата на активни образователни програми за повишаване на знанията им.

Положително може да се оцени факта, че интересът към подобряване на знанията уменията по киберзащита и възможностите за спазване на киберхигиена сред студентите е висок. Резултатите показват, че 82% от анкетираните заявяват, че биха се включили в обучения или семинари по киберсигурност. Бариера може да се окаже цената. Университетите, които предлагат специалности, свързани с информационните технологии, вероятно разполагат с преподаватели, които под натиска на съвременната ситуация, в някаква степен се интересуват и са запознати с добрите практики в областта на информационната сигурност. В тези университети може да се разработят и предложат такива обучения. Те могат да бъдат и част от някои изучавани от студентите дисциплини. Освен това, благодарение на все по-тесните партньорства между различните университети в страната и между университетите и гимназиите, може да се предприемат такива съвместни инициативи.

На проведената през месец октомври 2024 г. Осма национална кръгла маса „ИТ иновации във висшето образование 2024“⁴ в ИУ – Варна, присъстваха представители на различни университети от страната. В резултат на работата по време на научния форум участниците стигнаха до извода, че осигуряването на високо ниво на информационната сигурност и на киберзащитата е непосилна за отделните организации задача. Освен това индивидуалните действия не биха били толкова ефективни, колкото съвместните усилия, комуникацията и непрекъснатото сътрудничество между образователните институции.

ЗАКЛЮЧЕНИЕ

Анализът на резултатите спомага за идентифицирането на области, където е необходимо да се насърчи обучението и осведомеността за киберсигурността сред студентите. Добива се

⁴ Осма национална кръгла маса „ИТ иновации във висшето образование 2024“, <https://ue-varna.bg/bg/news/natsionalna-kragla-masa-it-inovatsii-vav-vissheto-obrazovanie-2024/2948>

представа за нагласите и преживяванията на студентите относно киберсигурността и рисковете в онлайн пространството. В тази връзка настоящото изследване може да помогне на образователните институции (и не само) при разработването на политики за информационна сигурност. Наличието и спазването на такива политики е сериозно предизвикателство и са необходими значителни усилия, време и финансови средства за постигане на работещи инструменти. Сериозно внимание трябва да се обърне на осведомеността на потенциалните потребители на информационните системи, техните отговорности относно опазването и защитата на данните.

БЛАГОДАРНОСТИ

Това изследване е направено в рамките на НПД-334 „Изграждане на облачна инфраструктура за целите на дигиталната трансформация в условията на смесено обучение“.

REFERENCES / ИЗПОЛЗВАНА ЛИТЕРАТУРА

1. Георгиева, Д. (2022) Поколението Z, бъдещите специалисти в областта на счетоводството. Сборник с доклади от научно-практическа конференция „Счетоводното образование като комплекс от знания, умения и компетентности“. <https://www.cceol.com/search/chapter-detail?id=1117530>
2. Димитров, В. (2022) Основи на киберсигурността. София: Авнгард Прима.
3. Димитров, Д., Андреев, Е. (2023) Нарастващата заплаха от кибератаки срещу научния сектор. SES 2023 Nineteenth International Scientific Conference SPACE, ECOLOGY, SAFETY 24 – 26 October 2023, Sofia, Bulgaria. https://www.researchgate.net/publication/375160133_THE_GROWING_THREAT_OF_CYBER_ATTACKS_AGAINST_THE_SCIENTIFIC_SECTOR
4. Димитров, Н. (2022) Управление на риска за сигурността в центъра за компетентност КВАЗАР. Изд. Висше военноморско училище „Н. Й. Вапцаров“, Варна. https://www.researchgate.net/publication/376892279_UPRAVLENIE_NA_RISKA_ZA_SIGURNOSTTA_V_CENTRA_ZA_KOMPETENTNOST_KVAZAR
5. Хаджичонева, Ю., Мандаджиев, П. (2023) Управлението на киберсигурността: мисията става спешна. Международна научна конференция „Права и сигурност“. https://www.researchgate.net/publication/375547778_UPRAVLENIETO_NA_KIBERSIGURNOSTTA_MISIATA_STAVA_SPESNA_MANAGING_CYBER_SECURITY_THE_MISSION_BECOMES_URGENT#fullTextFileContent
6. Garba, A., A., Siraj, M., M., Othman, S., H. Musa, M., A. (2020) A Study on Cybersecurity Awareness among Students in Yobe State University, Nigeria: A Quantitative Approach. International Journal on Emerging Technologies, 11(5), 41-49. https://www.researchgate.net/publication/343600853_A_Study_on_Cybersecurity_Awareness_Among_Students_in_Yobe_A_Quantitative_Approach
7. Mailok, R., Hassan, H., Said, C.S., Hashim, M. (2023) Assessing the levels of knowledge of personal data protection among students. International Journal on Social and Education Sciences (IJonSES), 5(4), 879-892. <https://doi.org/10.46328/ijonSES.610>