COVID-19 И КИБЕРПРЕСТЪПЛЕНИЯТА СРЕЩУ ЗДРАВЕОПАЗВАНЕТО

ПРОФ. Д-Р ГАБРИЕЛА БЕЛОВА, ДОЦ. Д-Р НИКОЛАЙ МАРИН,
ГЛ. АСИСТЕНТ ДОКТОР ЙОСИФ КОЧЕВ





Проф. д-р Габриела БЕЛОВА *е завършила специалност „Право" в СУ „Св. Климент Охридски" и LLM in International and Commercial Law, University of Buckingham, UK. През 2004 г. Придобива ОНС „доктор", през 2007 г. е избрана за доцент, а през 2014 г. – за професор в катедра "Международно право и международни отношения" на ЮЗУ "Неофит Рилски" – Благоевград. През периода 2010 г. - 2019 г. е декан на Правно-историческия факултет на ЮЗУ "Неофит Рилски". От 2017 г. до момента е ръководител на катедра "Международно право и международни отношения". От м. ноември 2019 г. е заместник-декан на факултета и Председател на Общото събрание на ЮЗУ "Неофит Рилски".*

Автор е на монографии и на редица статии и студии в областта на международното право, правото на Европейския съюз, правата на човека и др. Била е ръководител на национални проекти и участник в европейски и международни проекти. Участвала е обучителни семинари в Академията по европейско право, гр. Трир, Германия. Била е лектор в модул V Operational aspects of European Police Cooperation в рамките на CEPOL European Joint Master Programme "Policing in Europe". Член е на Българската асоциация по международно право, на Българската асоциация по европейско право и на Българската асоциация за европейски изследвания.

Доц. д-р Николай Марин *завършва специалност „Право" в Правно-историческия факултет на ЮЗУ „Неофит Рилски" – Благоевград. През 2007 г. му е присъдена ОНС „доктор" по Международно право и международни отношения, а от 2011 г. е доцент по „Международно право и международни отношения. В периода 2011 г.- 2019 г. е бил заместник-декан на Правно-историческия факултет. Преподавател по Международно право и по международни отношения в Академията на МВР. От м. октомври 2019 г. и понастоящем е Декан на Правно-историческия факултет. Има редица публикации в областта на международното публично право и правото на Европейския съюз у нас и в чужбина. Специализирал е в Съда на Европейския съюз, Института Макс Планк за международно и европейско право, Люксембург, а също и в Аристотеловия университет, Солун и в Европейския център за професионално обучение (CEDEFOP). Участвал е в редица български и международни научни и образователни проекти. Преподавал е в международна магистърска програма в модул V Operational aspects of European Police Cooperation в рамките на CEPOL European Joint Master Programme "Policing in Europe". Член е на редколегиите на научните списания „Международна политика" и „Европейски правен преглед". Член е на Управителния съвет на Българската асоциация за европейско право, член е на Българската асоциация за европейски изследвания.*



Гл. ас д-р Йосиф Йорданов Кочев *е завършил бакалавърска степен специалност „Европеистика” и магистърска степен специалност „Международни отношения” в ЮЗУ „Неофит Рилски“ – Благоевград. През 2015 година придобива образователната и научна степен „доктор” след успешна защита на дисертационен труд на тема: „Политиката на Европейския съюз по проблемите на киберсигурността”. От 2017 година е главен асистент в катедра „Международно право и международни отношения” към Правно-историческия факултет на ЮЗУ „Неофит Рилски”. Автор е на редица статии в областта на киберсигурността и е участвал в национални и европейски проекти. През м. юни 2013 г. е приет за член на Съюза на учените в България в секция „Сигурност”.*

Резюме: *Едва ли е изненадващо, че киберпрестъпниците се опитват да проникнат във все повече компютърни мрежи. Това е така всеки път, когато има световно събитие. В миналото олимпийските игри и влизането в сила на GDPR провокираха засилена хакерска дейност. Днес се използват човешките слабости по повод на пандемията Covid-19. Атаката срещу Университетската болница в гр. Бърно (Чешка Република), която се случи на 13 март 2020 г. и доведе до отмяна на плановите операции е най-големият и притеснителен инцидент досега, но далеч не е единственият по време на пандимията. Досега никога не е имало кибератака срещу здравно или лечебно заведение, която директно да е довела до загуба на човешки живот, но според експерти по киберсигурност е само въпрос на време това да се случи.*

Ключови думи: *киберсигурност, здравеопазване, Covid-19, болнични заведения, рансъмуер.*

COVID-19 AND CYBER CRIMES AGAINST HEALTHCARE

PROF. DR. GABRIELA BELOVA, ASSOC. PROF. DR. NIKOLAY MARIN, CH. ASSISTANT PROFESSOR DR. YOSIF KOCHEV

Abstract: *It is hardly surprising that cybercriminals are trying to penetrate increasingly computer networks. This is so every time there is a world event. In the past, the Olympic Games and the entry into force of the GDPR provoked a heightened hacker activity. Today, human weakness is being used in the context of the Covid-19 pandemic. The attack on the University Hospital in the city of Brno (Czech Republic), happened on March 13, 2020 and led to the abolition of planned operations, was the biggest and worrying incident, but far from being the only one during the pandiemia. To date, there has never been a cyberattack against a health or medical institution that has directly led to a loss of human life, but according to cybersecurity experts it is only a matter of time before this happens.*

Key words: *Cybersecurity, health care, Covid-19, hospital facilities, ransomware.*

Тъй като страховете от коронавирусната инфекция с бързи темпове завладяха съзнанието на световното население, киберпрестъпниците се стремят да използват всяка възможност да извлекат всякакъв вид ползи от жертвите си по повод на услуги и продукти, свързани с Covid-19.

Едва ли е изненадващо, че киберпрестъпниците се опитват да проникнат във все повече компютърни мрежи. Това е така всеки път, когато има световно събитие. В миналото олимпийските игри и влизането в сила на GDPR провокираха засилена хакерска дейност. Днес се използват човешките слабости по повод на пандемията Covid-19. Секретарят на Интерпол Юрген Сток заявява: „Болници и медицински организации по целия свят работят без прекъсване, за да се запази благосъстоянието на индивидите, поразени с коронавируса. Те са се превърнали в цели за безмилостни киберпрестъп-

ници, които се опитват да реализират печалба за сметка на болни пациенти”[1].

Най-големият и притеснителен инцидент досега се случи на 13 март 2020 г. в Университетската болница в гр. Бърно (Чешка Република), която понесе изключително сериозна кибератака в разгара на епидемията от коронавирусната инфекция, довела до прекратяването на планираните операции[2].

Вследствие на кибератаката болницата в Бърно е била неспособна да прехвърли информация от ключови клинични системи в своята база данни и е принудена да изключи ИТ системите си и да прехвърли спешните пациенти към друго медицинско заведение в града. Следва да се има предвид, че болницата е вторият по големина национален обект със стратегическо значение в сферата на здравеопазването и по време на атаката е била сред най-важните центрове за тестване на COVID-19 в Чехия.

“Системата за обществено оповестяване в болницата започна да повтаря съобщението, че целият персонал трябва незабавно да затвори всички компютри поради „кибернетична атака”, информира изследовател в областта на киберсигурността, който по същото време чака в болницата за операция[3]. Кибератаката не се отразява върху работата, свързана с изследванията за коронавирус, но причинява смущения в изключително напрегнатия и натоварен график на болницата.

Въпреки че точната природа на атаката е неизвестна, признаците сочат към възможността ИТ инфраструктурата на болницата да е криптирана от рансъмуер[4]. Инцидентът бе потвърден от Чешкия национален офис за киберсигурност и информационна сигурност (NÚKIB), който през цялото време си сътрудничи с правоприлагащите органи и болничния персонал, за да успее да върне съоръжението в пълна готовност за работа.

Чешката болница не е единствената лечебна институция, атакувана от киберпрестъпниците. В Съединените щати уебсайтът на отдел за обществено здравеопазване в Илинойс, към който има повече от 200 000 регистрирани лица, също излиза офлайн след рансъмуер атака. По аналогичен начин хакерска група атакува компютърните системи на британската компания Hammursmith Medicine Research, (която извършва опити за създаване на ваксина срещу Covid-19), заплашвайки да публикува здравните данни на хиляди бивши пациенти, ако компанията не заплати сумата на изнудването. По данни на френската агенция за киберсигурност, болница в Париж също е била обект на провалена кибератака.

Кибератаката срещу болницата в Бърно буди сериозна загриженост сред специалистите, поради факта, че досега онлайн престъпността, свързана с COVID-19, бе ограничена преди всичко до фишинг атаки (насочени имейли с помощта на привличащи вниманието заглавия и прикачени файлове, съдържащи злонамерен софтуер) и кампании за дезинформация. След инцидента в Чехия експертите предупреждават, че разпространението на коронавирусната инфекция осигурява плодородна почва за киберпрестъпления от всякакъв вид. Така например, Flavius Plesu, основател на разузнавателната платформа за човешки рискове OutThink, смята, че престъпниците ще видят в пандемията COVID-19 шанс и възможност да се възползват от слабите звена в системите за сигурност[5].

Медии в САЩ анонсират, че атаките срещу сектора на здравеопазването са се увеличили само с 150% през последния месец[6]. Очевидно е, че оптимизирането на киберсигурността на болниците не може да чака. От решаващо значение е да се действа бързо, за да се гарантира безопасността на пациентите, поверителността на личните данни и непрекъснатото здравно обслужване.

Днес болниците, както никога досега, са свързани с облачни, мобилни и „Интернет на нещата” (IoT) технологии, които подобряват тяхната ефективност и качество на обслужването. Същевременно обаче, тези промени създават нови проблеми пред „добрия стар периметър на сигурността” и отварят повече възможни входове, към които хакерите се насочват. По данни на американската здравна администрация през 2019 г. приблизително 40 милиона пациентски досиета са изтекли, като здравните организации продължават да понасят увеличение на броя на технологичните пробиви с всяка изминала година[7].

Може би т. нар. рансъмуер атаката е най-широко разпространената заплаха за кибурсигурността на лечебните заведения и медицинските организации. През м. юни 2019 г. пет американски здравни доставчици съобщават за рансъмуер атаки само в рамките на една седмица[8]. По време на пандемията COVID-19 доставчици на здравни услуги в

световен мащаб са били сигнализирани, че са възможни рансъмуер атаки, прикрити под формата на официални съвети от правителствени агенции. Най-често получените съобщения в електронната поща или в социалните мрежи (от фалшиви или компрометирани/хакнати профили) насърчават получателя да отвори прикачен файл, който след това може да зарази софтуера и да заключи цялата критична IT система. От своя страна, блокирането на критичните системи на болниците не само би забавило бързата медицинска реакция, необходима в тези безпрецедентни времена, но и би могло директно да доведе до смъртни случаи. Неслучайно, Интерпол съветва болници и здравни заведения да бъдат бдителни към подозрителни имейли, както и да гарантират, че антивирусните системи се актуализират, а уязвимите места в сигурността своевременно се отстраняват. От огромно значение за сигурността на мрежите на лечебните заведения е те да бъдат ограничени за ползване само от определени устройства и лица. В противен случай, достъпът до Wi-fi мрежите от пациенти създава предпоставки за злоупотреби и компрометиране на цялата мрежа.

Световната здравна организация (СЗО) също предупреждава за подозрителни имейл съобщения, които се опитват да се възползват от извънредната ситуация с Covid-19, като крадат парични средства или чувствителна за обществеността информация. Според по-нови доклади обаче, по време на епидемията от коронавирус са се увеличили и опитите за хакерство срещу собствените компютърни системи на СЗО и тези на партньорите на организацията[9].

Тревожната тенденция на увеличени киберпрестъпления представлява значителна финансова тежест за болничните заведения не само от гледна точка на възстановяване на вредите, свързани със софтуера и хардуера, но и с оглед на разходите, свързани с възстановяването на увредена репутация, които могат да бъдат огромни. Според една от водещите компании IBM средната цена на пробив в сигурността в сектора на здравеопазването е 6,45 милиона щатски долари, което означава с около 65% по-високи от средните разходи за възстановяване на щетите във всички останали отрасли на индустрията[10].

Неслучайно пробивът в сигурността на медицинските заведения е окачествяван от някои автори като „перлата на короната за хакерите”[11].

Цената на едно от откраднати електронни здравни досиета може да достигне в т.нар. darknet до хиляда щатски долара. За сравнение, номерата на социалните осигуровки или информацията от кредитните карти обикновено варира между един и сто и десет щатски долара[12]. Отчасти това е така, тъй като електронните здравни досиета (в държавите, където съществуват) съдържат информация, която е по-трудна за възстановяване след кражба (лична информация, наличие на застраховка, номер на полица, медицински диагнози, информация за фактури и др.). Тази информация често се използва от престъпници за създаване на фалшиви лични документи, за закупуване на медицинско оборудване или наркотици, или за подаване на фалшива застрахователна претенция. От подобен вид е кибератаката, която Националната здравна служба на Обединеното кралство претърпя през 2017 г. с вируса WannaCry.

Друг проблем, който би могъл да бъде очертан представлява фактът, че медицинските кадри нямат осведоменост за проблемите, свързани с киберсигурността. И това е естестено, тъй като спасяването на човешки животи и лечението на пациентите е основен приоритет за персонала в болниците, което ги прави по-склонни към непредпазливо поведение, когато става въпрос за спазването на правилата и политиките за сигурност в медицинските заведения. За съжаление, когато болничният персонал трябва преди всичко да се стреми да ограничи разпространението на коронавируса, той не мисли приоритетно за киберсигурността. Хакерите знаят това и се насочват конкретно към сектора на здравеопазването.

Освен това, обучението на медиците в тази насока също е от изключителна важност. А дори данните от по-развитите държави показват, че почти една трета от медицинския персонал в здравеопазването (или около 32%) никога не са били обучавани относно киберсигурността на работното си място, каквато квалификация би трябвало да притежават[13]. Подобна липса на информираност, съчетана с нарастващото използване на мобилни устройства, таблети и лаптопи води до неправилно боравене и съхранение на пациентските досиета и облекчаване на средата за кражба на идентификационни данни чрез фишинг атаки, изтегляне или разпространение на злонамерени файлове и др. В бързината на ежедневието – и въ-

преки най-добрите усилия на обучителите в областта на киберсигурността – хората все още са изключително податливи да отварят имейли, които им изглеждат убедителни. Много често разликата между автентичния имейл и фалшифия фишинг имейл е една буква в електронния адрес на подателя, което ги прави почти идентични. В случаите, когато медицинския персонал действа под стрес или други фактори, влияещи върху концентрацията на хората, той много лесно би могъл да бъде заблуден и да стане жертва на различни кибератаки. След като хакерите получат достъп до мрежата на лечебното заведение, е въпрос на креативност и умения да бъдат нанесени колосални материални и нематериални щети, дори такива, свързани с живота и здравето на пациентите.

Обикновено се счита, че свързаните устройства са най-слабото звено на болниците. В САЩ броят на свързаните медицински устройства и IoT може да достигне до 15-20 на болнично легло - от инфузионни помпи и монитори на пациента до апарати за ядрено-магнитен резонанс. Тези устройства, както и пейсмейкъри или други имплантирани, свързани с интернет, устройства, обикновено работят при legacy операционни системи, което ги прави силно уязвими и лесни за хакване. Тази пропаст в сигурността на IoT остава без надзор, тъй като болниците рядко могат да си позволят системите им да функционират на временен режим – дори само за няколко часа. При тях достъпът 24/7 е от решаващо значение.

На следващо място, въвеждането на режим на социална дистанцираност в много държави, както и на т. нар. отдалечени работни места или home office също води до повишаване на заплахите пред киберсигурността. В този смисъл, организациите и компаниите следва да бъдат особено бдителни в периода на пандемия, за да гарантират, че тези, с които се свързват от разстояние, не представляват риск за киберсигурността в обществото. „Днешните неочаквани и извънредни мерки увеличават киберриска по много начини, които никога преди това не сме виждали", изтъква Лукаш Олейник, независим изследовател и консултант в областта на киберсигурността[14].

Според специалисти към днешна дата никога не е имало кибератака срещу здравно или лечебно заведение, която директно да е довела до загуба на живот. Британският национален център по киберсигурност обаче заявява, че е само въпрос на време да се случи.

Следва да се има предвид, че здравеопазването като сектор от икономиката претърпява вреди не само при атаки, насочени към конкретни медицински обекти, но и при киберпрестъпления от по-общ характер. NotPetya е една от най-големите кибератаки на всички времена. Атаката през м. юни 2017 г. е причинила щети от 10 милиарда долара на дружества от различни области на обществения живот, включително и здравеопазването. Засегнати са компютри по целия свят, включително тези на базираната в Масачузетс компания за медицински услуги Nuance. Системите на компанията са затворени в продължение на седмици, което поставя хиляди здравни организации в невъзможност да използват своите програми. Неслучайно, тогава Генералният секретар на НАТО Йенс Столтенберг настоя алианса да укрепи киберотбраната си, като заяви, че кибератаката може да задейства принципа на колективната отбрана по член 5[15].

Не на последно място, възможността за трансгранично предоставяне на здравни услуги, особено в рамките на Европейския съюз, също допринася за по-голямата уязвимост на здравната инфраструктура.

На 24 март 2020 г. Председателят на Европейската комисия Урсула фон дер Лайен също предупреждава, че киберпрестъпността в ЕС се е увеличила поради епидемията от коронавируса. Киберпрестъпниците се възползват от нарастващото време, което хората прекарват онлайн поради новите мерки, предприети от държавите членки за спиране на разпространението на вируса, като същевременно се възползват и от самата здравна криза. „Те ни следват онлайн и се възползват от притесненията ни за коронавируса. Страхът ни се превръща във възможност за бизнес за тях", посочва фон дер Лайън във видео обръщение[16].

Междувременно комисарят по вътрешния пазар Тиери Бретон се консултира с телекомуникационните оператори относно защитата на мрежите на ЕС от кибератаки. Според комисията Европейската мрежа на екипите за реагиране при инциденти с компютърната сигурност (ЕРИКС) също повиши нивото на внимание, като през този период се призовава за силна киберустойчивост.

Въпреки че целите на тези атаки са неясни, може да се предположи, че има множество мотиви за кибератаки срещу авторитетни здравни организации по време на пандемията. По същия начин, докато се борят срещу коронавируса, болниците и изследователските центрове в Европа се превръщат в цел за киберпрестъпниците, които търсят информация, разузнаване и достъп до системата.

Киберпрестъпниците например биха могли да търсят информация относно лечението, тестовете или ваксините, свързани с коронавируса, за да ги продават на черния пазар, да криптират чувствителни данни и да ги държат за откуп, или просто да нарушат оперативната съвместимост на институцията.

Според K. Raiu (Костин Райу), ръководител на глобалните изследвания и анализи в компанията Kaspersky, разрушителна или рансъмуер атака срещу болница или друга здравна организация би могла да бъде „твърде опасна", тъй като излага на риск преди всичко пациентите. „В крайна сметка това може да доведе до загуба на човешки живот, или защото ресурсите, необходими за лечението им, вече не са налични; или защото процесите в болницата са силно забавени", изтъква Raiu, добавяйки, че е изключително важно болниците да бъдат защитени и да могат да защитят данните на пациентите си[17].

Тъй като общият брой на глобалните случаи на Covid-19 непрекъснато се увеличава, хакерите повишават активността си и се опитват да се възползват от кризата с удари не само срещу болничните заведения, но и производството, ангажирано в борбата срещу пандемията. „Виждаме съгласувани атаки срещу производството, фармацевтичните продукти, пътуванията, здравеопазването и застраховането", обяснява Шерод де Грипо (Sherrod DeGrippo), старши директор в областта на изследванията на заплахите и откриването на киберсигурността във фирмата Proofpoint. „Когато казвам производство, много пъти те могат да бъде насочена срещу подмножества от производства, състоящи се от производители, които създават болнични легла, медицинско оборудване, всички неща, които бихте свързали със здравеопазването", продължава експертът[18].

В заключение, данните показват, че рансъмуер и другите видове кибератаки се увеличават, а здравеопазването е една от най-привлекателните цели. Въпреки нарастващата заплаха, по-голямата част от болниците и лекарите не са подготвени да се справят със заплахите за киберсигурността, въпреки че последните представляват сериозен проблем за общественото здраве.

Здравеопазването все повече разчита на технологии, които са свързани с интернет: от картони на пациентите и лабораторни резултати до радиологичната техника и болничните асансьори. От една страна, това е в полза на пациента, тъй като улеснява интегрирането на данни, ангажираността на пациентите и клиничната подкрепа. От друга страна обаче, тези технологии често са уязвими към кибератаки, които могат да източват данните на пациентите, да искат откупи в криптовалути или дори да затворят болнично заведение. Международната общност би трябвало да реагира на тези процеси чрез усъвършенстване на правната уредба, предоставяща адекватна закрила на болниците и здравната инфраструктура в мирно време, каквато е предвидена в Женевските конвеции от 12 август 1949 г. за военновременни ситуации и въоръжени конфликти.

ИЗПОЛЗВАНА ЛИТЕРАТУРА:

1 https://www.interpol.int/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware

2 Brno University Hospital in Czech Republic Suffers Cyberattack During COVID-19 Outbreak.

3 Burges, Matt *Hackers are targeting hospitals crippled by coronavirus*, Sunday 22 March 2020, *https://www.wired.co.uk/article/coronavirus-hackers-cybercrime-phishing*.

4 **Рансъмуерът** е специфичен вид злонамерен софтуер, който изтръгва финансов откуп от жертвите си, като заплашва да публикува, изтрие или затвори достъпа до важни лични данни. Последиците от рансъмуер атаката могат да бъдат катастрофални, тъй като, веднъж заразила компютъра, е трудно тя да бъде спряна. Предотвратяването на атаката е по-ефективната стратегия. Повечето форми на рансъмуер изискват между 200 и 900 долара от жертвите. Ако откупът не бъде платен в рамките на 48-72 часа, данните обикновено се изтриват завинаги. Заплащането на исканата сума най-често е посредством криптовалути. https://bg.safetydetectives.com/blog/какво-е-рансъмуер/

5 Khalili, Joel *Coronavirus hospital suspends activity over cyberattack*, March 16, 2020, https://www.techradar.com/news/coronavirus-hospital-suspends-activity-

over-cyberattack. Вж. също https://www.europapress.es/comunicados/tic-00911/noticia-comunicado-leaders-in-cybersecurity-have-united-to-combat-an-unprecedented-level-of-cyberattacks-20200316160551.html

6 Katz, Dana *Is your Hospital Prepared for the Next Cyber Attack?* https://blog.checkpoint.com/2020/04/16/is-your-hospital-prepared-for-the-next-cyber-attack/

7 U.S. Department of Health and Human Services, https://www.securitymagazine.com/articles/91909-us-health-and-human-services-department-suffers-cyberattack.

8 *Healthcare IT Security, June 19 2019; https://www.healthcareitnews.com/news/5-cybersecurity-threats-healthcare-faces-2019-and-beyond.*

9 Nicolás, Elena Sánchez *Cybercrime Rises during the Coronavirus Pandemic*, Brussels, 25. Mar, 07:07, https://euobserver.com/coronavirus/147869.

10 Source: Cost of a Data Breach Report 2019, IBM; https://www.ibm.com/security/data-breach. Вж. също https://digitalguardian.com/blog/whats-cost-data-breach-2019.

11 Katz, Dana *Is your Hospital Prepared for the Next Cyber Attack?* https://blog.checkpoint.com/2020/04/16/is-your-hospital-prepared-for-the-next-cyber-attack/.

12 https://techknowclasses.wordpress.com/2018/02/04/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.

13 https://media.kasperskydaily.com/wp-content/uploads/sites/85/2019/08/16121510/Kaspersky-Cyber-Pulse-Report-2019_FINAL.pdf.

14 Цитиран по: Nicolás, Elena Sánchez *Cybercrime Rises during the Coronavirus Pandemic*, Brussels, 25. Mar, 07:07, https://euobserver.com/coronavirus/147869.

15 NATO Warns Use of Article 5 Over Cyber Attack, Members Pledge Spending Increase https://www.haaretz.com/world-news/europe/nato-warns-use-of-article-5-over-cyber-attack-1.5489843.

16 Nicolás, Elena Sánchez *Cybercrime Rises during the Coronavirus Pandemic*, Brussels, 25. Mar, 07:07, https://euobserver.com/coronavirus/147869.

17 *Ibidem.*

18 Цитиран по: Burges, Matt *Hackers are targeting hospitals crippled by coronavirus*, Sunday 22 March 2020, *https://www.wired.co.uk/article/coronavirus-hackers-cybercrime-phishing*.