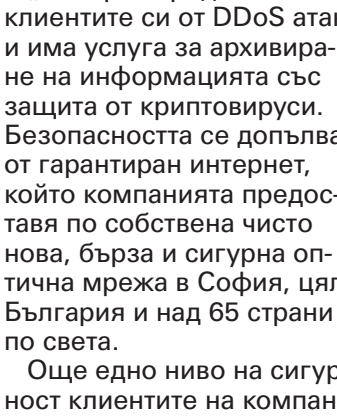
Фирми дали на мошеници 22 млн. лева за година

■ На 15-а стр.

Бандити мамят хората да пратят данни за банковите си карти



■ На 16-а стр.

2024 - заплахи и иновации в дигиталната ера

ТОКЕН ТЕЙЛС, MEDIUM

Какви да са отбранителните ни стратегии, за да опазим парите си

2024 г. носи множество предизвикателства и възможности в сферата на киберсигурността. Нараства и заплахите, които дебнат в сенките на виртуалния свят. Ето тенденциите в киберсигурността, които се очаква да оформят отбранителни стратегии както на организациите, така и на отделните лица през 2024 г.

1. Интеграция на изкуствен интелект и машинно обучение: Една от най-известните тенденции в киберсигурността е интегрирането на изкуствения интелект (AI) и машинното обучение (ML) в протоколите за сигурност. Тъй като киберзаплахите стават все по-сложни, необходимостта от адаптивни и интелигентни защитни механизми никога не е била по-голяма. AI и ML технологиите могат да анализират огромно количество данни в реално време, позволявайки по-бързо откриване на заплахи и реагиране.

Тези напреднали технологии не се ограничават само до защитни мерки; киберпрестъпниците също използват AI, за да подобрят ефективността и стелта на своите атаки. Пейзажът на киберсигурността сега е бойно поле, където интелигентните алгоритми се състезават, за да надхитрят един друг.

2. Заплахи от квантовите изчисления: Въпреки че квантовото изчисление генерира огромни очаквания за решаване на сложни проблеми, то също представлява значителна заплаха за настоящите стандарти за криптиране. Тъй като квантовите компютри стават по-мощни, те биха могли потенциално да разбият широко използваните алгоритми за криптиране, което прави традиционните мерки за сигурност остарели. В очакване на това организациите проучват квантово устойчиви криптографски решения, за да гарантират поверителността на чувствителната информация в постквантовата ера.

3. Архитектура с нулево доверие: Архитектурата с нулево доверие се наложи като основна концепция за киберсигурност. В модела с нулево доверие нито един субект, независимо дали е вътре, или извън мрежата, не се доверява по подразбиране. Всеки потребител, устройство и приложение трябва да удостовери и потвърди самоличността си, преди да получи достъп до ресурси. Този подход минимизира риска от неоторизиран достъп и странично движение в рамките на мрежата, съобразявайки се с принципа на най-малко привилегии.

4. **Предизвикателства пред сигурността в облака:**

Продължаващата миграция към услуги, базирани на облак, въведе нови предизвикателства пред киберсигурността. Организациите трябва да се справят с проблеми като неправилно конфигурирани облачни настройки, несигурни интерфейси за програмиране на приложения (API) и нарушения на данните, произтичащи от уязвимости в облака. Тъй като бизнесите все повече разчитат на облачна инфраструктура, осигуряването на тези среди става от първостепенно значение за предотвратяване на изтичане на данни и неоторизиран достъп.

(Продължава на 14-а стр.)

Киберсигурност от **кабела през сървъра до облака**

DDoS атаките и криптовирусите, които зачестиха напоследък в България, са сред най-разпространените и разрушителни видове кибератаки. Те са

сериозен бизнес риск,

а не само IT проблем. Могат да доведат до прекъсване на услугите, загуба на данни и финансови щети.

Неслучайно всички банки, медии, успешни корпорации и фирми с онлайн магазини ползват услуги за киберсигурност. Много от тях се доверяват на „Нетера" – глобална телекомуникационна компания с близо 30 години опит, която предлага

комплексна защита

„Нетера" предпазва клиентите си от DDoS атаки и има услуга за архивиране на информацията със защита от криптовируси. Безопасността се допълва от гарантиран интернет, който компанията предоставя по собствена чисто нова, бърза и сигурна оптична мрежа в София, цяла България и над 65 страни по света.

Още едно ниво на сигурност клиентите на компанията постигат, като разположат сървърите си в

защитената среда

на един от 4-те дейта центъра на „Нетера", два от които са в София.

„Нетера" предлага и облачни услуги, които отговарят на най-високите стандарти за киберзащита. Това се потвърждава от факта, че компанията е

сертифицирана по ISO 27018 – стандарта за сигурност

на облачните услуги.

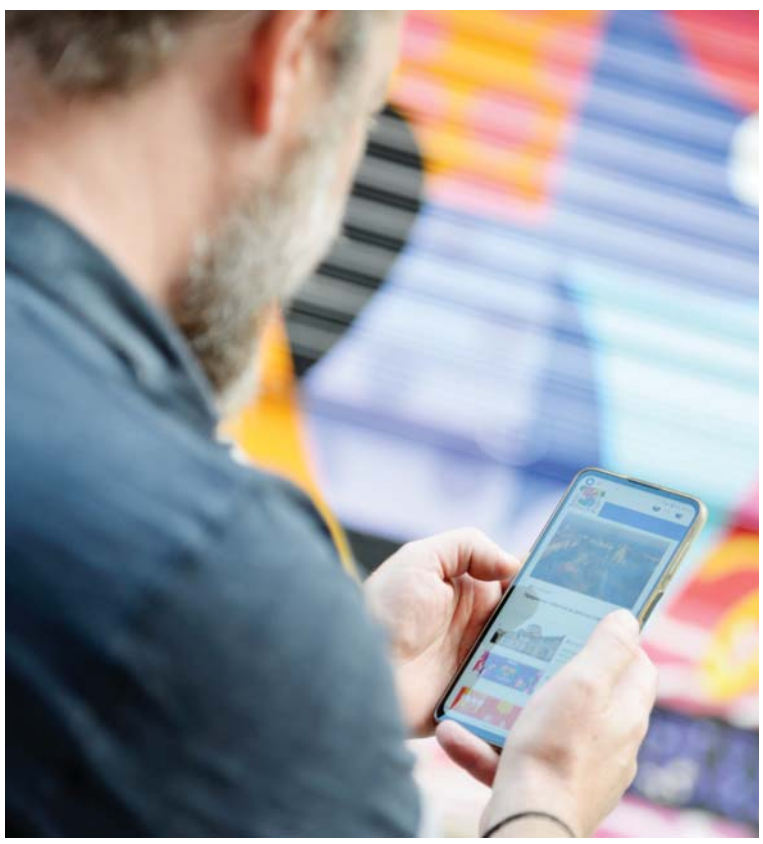
Компанията е сертифицирана и по всички други нужни за бизнеса ѝ и важни за клиентите ѝ ISO стандарти, както и по международния сертификат за финансова сигурност PSI DSS.

Атаките към български организации и фирми зачестяват, „Нетера" предпазва бизнеса от повишения риск

Ако имате нужда от защита на системите и данните си, свържете се с „Нетера". Ще ви консултират безплатно.

Новият хит – измамите с криптовалута

Благодарение на технологиите се правят и фалшиви видеоматериали



ДИМИТЪР МАРТИНОВ

Най-новият вид измами са свързани с инвестициите в криптовалута. При тях хората биват убеждавани, че сключват сделка, чиято възвръщаемост е над 300 процента. Често в схемите се ползват образите на известни личности.

В миналото това ставаше с текст на фалшиво интервю. В последно време обаче благодарение на технологиите, се правят фалшиви видеоматериали.

В тях глас на популярна личност разказва как само за месец е успял да изкара над 100 000 лева, а е инвестирал едва 300. Често това е станало чрез купуване на акции в „Епъл“, „Тесла“ и дори популярния изкуствен интелект ChatGPT.

„Една-две жертви имаме на седмица, които са видели в интернет реклама на платформа за търговия, в която се казва, че ако инвестираш определена валута в крипто, сумата ще се удвои, утрои, дори учетвори бързо и сигурно.

„Това уж е таен интернет сайт, на който се подава тайна информация за бързи инвестиции. А всъщност става въпрос за обикновена интернет измама. Имаме по една-две жертви седмично, измамени със суми, вариращи от 10 до 100 хил. евро“, разказа още старши комисар Димитров.

2024 - заплахи...

(*Продължение от 13-а стр.)*

5. Еволюция на Ransomware: Ransomware атаките се превърнаха в изключително сложни операции. Участниците в заплахата използват тактики като двойно изнудване, при което откраднатите данни не само са криптирани, но също така има заплаха да бъдат изтеглени, освен ако не бъде платен откуп.

Използването на усъвършенствани алгоритми за криптиране и насочването към критична инфраструктура са ескалирали въздействието на атаките с ransomware. Защитата изисква многостранен подход, съчетаващ стабилни стратегии за архивиране, обучение на служители и усъвършенствани инструменти за откриване на заплахи.

6. Уязвимости на интернет на нещата (IoT): Разпространението на IoT устройства разшири повърхността за атака на киберпрестъпниците. През 2024 г. можем да очакваме увеличаване на атаките, насочени към IoT устройства, използвайки уязвимости в техните често неадекватни мерки за сигурност. Тъй като тези устройства стават неразделна част от нашето ежедневие, защитата им е от решаващо значение за предотвратяване на потенциални прекъсвания и защита на поверителността на потребителите.

7. Правила за повишена сигурност: Правителствата и регулаторните органи по света признават ескалиращите киберзаплахи и реагират с по-строги разпоредби за киберсигурност.

През 2024 г. можем да очакваме въвеждането на всеобхватни рамки, които упълномощават организациите да прилагат стабилни мерки за сигурност и да докладват инциденти своевременно. Спазването на тези разпоредби ще бъде не само законово изискване, но и от съществено значение за поддържане на доверието на клиентите и заинтересованите страни.

Заключение: *Обсъдените по-горе тенденции подчертават динамичния характер на киберзаплахите и необходимостта от постоянни иновации в отбранителните стратегии.*

През 2024 г. организациите и отделните лица трябва да останат бдителни, да се адаптират към възникващите предизвикателства и да инвестират в най-новите технологии, за да останат една крачка пред непрекъснато развиващия се пейзаж на киберзаплахите.

Специалистите по киберсигурност на Висшето училище по телекомуникации и пощи **не отстъпват** пред изкуствения интелект - те го управляват!

„С интензивната практическа подготовка и интердисциплинарните познания специалностите на ВУТП водят промяната, а не я следват“, казва ректорът проф. д-р Миглена Темелкова

„Ако има образователна институция, която със специалностите си да върви крачка преди изкуствения интелект – това със сигурност е Висшето училище по телекомуникации и пощи!“, казват неговите студенти. Проверката в рейтинговата система показва, че вече няколко години Висшето училище по телекомуникации и пощи е символ на високи стандарти за качество на обучението, тъй като интегрира в учебните си планове последните достижения в киберсигурността. Този университет е едно от най-старите висши училища в България и вече 142 години е еталон в работата си в полза на националната сигурност на страната, за нейната икономическа и образователна система.

„Киберсигурността е безспорно човешка дейност. Нея не бива да поверяваме на изкуствения интелект. Затова и предизвикателството пред нашия университет е изграждането на специалисти, по-добри от опциите, които предоставя и ще ни предоставя изкуственият интелект“, казва ректорът на университета проф. д-р Миглена Темелкова.

„Комуникационни мрежи и киберразследване“ е магистърската програма

с топрейтинг, разработена с оптимално съотношение между фундаментални знания, теория и практика. Учебният план е построен в съответствие с изискванията на Израелския директорат по киберсигурност и е част от концепцията на Българската академия за сигурност. Съществена част от лекциите се провежда от водещи израелски експерти на академията. Едно от големите преимущества на програмата е, че студентите преминават обучение на киберсимулатора от последно поколение CyberRange, като в края на обучението полагат на него изпит, което най-обективно може да даде оценка относно усвоения учебен материал и степен на тяхната подготовка. Успешно завършилите програмата получават престижен съвместен сертификат от Българската академия за сигурност и Центъра за иновации и киберсигурност на Израел.

„Българската академия за сигурност е

единствена на Балканите, която разполага с такъв тип симулатор

Той позволява в максимална степен да се пресъздаде реалната среда на киберпространството. С този тип симулатор тренират служители от правителствени и силови структури на водещи държави“, обяснява председателят на академията Владимир Бронфенбренер.

Университетът предлага и няколко бутикови специалности без аналог в България: „Киберсигурност на високите технологии“ в ОКС „професионален бакалавър“, „Киберсигурностна комуникационните технологии“ и „Киберсигурност в бизнеса“ в ОКС „бакалавър“, в които преподават доказани експерти в областта на киберсигурността и специалисти, работещи в националната служба за борба с организираната престъпност.

Висшето училище по телекомуникации и пощи приоритетно акцентира върху безспорните си конкурентни предимства: отлична теоретична подготовка на студентите, но и много практика. Университетът разполага с лаборатории и симулационни зали, оборудвани от най-големите телекомуникационни и ИТ глобални компании.

Бизнесът участва пряко в образователния процес

чрез интегриране опита на водещи свои експерти в обучителния процес, в практическите занимания и в интердисциплинарните умения, които сферата на високи технологии изисква.

„Актуализираме учебните си планове в комуникация с бизнеса. Изискванията му се променят и ние като университет, чиято философия е предоставянето на качествени технически умения и компетенции в баланс с теоретични познания, се стараем учебните ни планове винаги да са адекватни и да отговарят на очакванията на работодателите и пазара на труда. Само така можем да изпреварим развитието на изкуствения интелект“, коментира проф. Темелкова.

Атестат за качеството и високия стандарт на образование във Висшето училище по телекомуникации и пощи е, че 88% от студентите работят по специалността си още от втори курс, а към специалностите се отчита сериозен интерес и от чуждестранни студенти.

„Добрата новина е, че нашите програми по киберсигурност не подготвят тесни специалисти, които ще паднат жертви на изкуствения интелект, а инженери с комплексни познания и високо ниво на практическа подготвеност, които ще са специалистите, наблюдаващи и калибриращи работата на изкуствения интелект“, заключава проф. Темелкова.

Много опции с един доверен IT партньор – LIREX

LIREX е водеща българска група от IT компании, една от най-експертните организации на европейския пазар в информационните и комуникационни технологии.

С над 30 години опит във високотехнологичната индустрия, LIREX е водеща в реализацията на цялостни решения и професионални услуги за организации от много сфери на икономиката както в корпоративния, така и в публичния сектор.

От експертизата на LIREX в областта на IT решенията се възползват клиенти от сектори образование, енергетика, промишленост, отбрана и сигурност, търговия и финанси.

Системният интегратор LIREX е партньор с устойчиви принципи, ценности, екип и подход.

В LIREX знаят, че IT е сложен бизнес, който изисква внимателно планиране, организиране и синхронизиране на IT дейностите във всяка организация, затова предлаганите IT решения са прецизирани и ефективни. Всеки реализиран проект е персонализиран според потребностите на клиента.

Иновативното мислене е ДНК-то на LIREX. В компанията действат предприемчиво и въвеждат смели IT решения.

Екипът от експерти на LIREX работи съгласувано съвместно с клиента във всички фази на проекта - от идеята, дизайна и разработката до внедряването и поддръжката.

Принципите, основните пет ценности и клиентският подход са много важни за екипа специалисти по системна интеграция, управляеми услуги, дигитална трансформация, доставка и поддръжка на LIREX, защото са лично свързани с всяка възможност, всяко решение, всяка услуга и обещание, които предоставят на своите клиенти.

LIREX поддържа високо ниво на експертиза и квалификации с над 500 сертификата по програми на Cisco, Microsoft, HPE, VMware, Veeam, ITIL, PMP, Agile, Scrum, ISACA и други.

LIREX предлага технологии на топпроизводители, персонализирани решения и услуги, IT експертиза в съчетание с високо ниво на обслужване.

Групата компании LIREX включват: LIREX BG, LIREX BS, LIREX HIGH TECH, LIREX ST.

Фирми дали на мошеници 22 милиона лева за година, **изкуствен интелект програмира умни вируси**

Всяка седмица българска фирма става жертва на кибератака, при която компанията губи поне 20 000 евро. Това става с подмяна на айбана, а зад схемата стоят нигерийски престъпни групи.

Хакерите изпращат мейл до обща поща на компанията, до която имат достъп поне 10 души. В писмото обикновено се казва, че човек трябва да въведе потребителското си име и парола, в противен случай акаунтът му ще бъде изтрит. Има и линк, където това да стане. Ако го натисне, човек отива на сайт, който изглежда досущ като този на оригиналната поща. Обаче е различен - например вместо .info пише .imfo.

Ако човек попълни данните си, ги праща на киберпрестъпниците. Оттам нататък те започват да следят кореспонденцията. Изчакват завършването на сделка с контрагент и подменят айбана, на който българската фирма трябва да изпрати парите.

За трансфер към новата сметка трябва потвърждение с есемес. Понякога самите български компании го правят. А има и случаи, при които хакерите директно мамят така, че да получат данните за вход в онлайн банкирането. Тогава им трябва кода от есемеса, за да потвърдят транзакцията.

ДИМИТЪР МАРТИНОВ
DMARTINOV@24CHASA.BG

Подменят банковата сметка на компании, преди да платят на контрагенти

За целта измамникът ползва сайт в тъмния интернет. В него се вкарва мобилният номер. Той лъже доставчика, че телефонът е в роуминг и за да си получи съобщенията, трябва да ги даде на сайта. Така мошениците реално четат всеки есемес. Услугата е валидна за 15 минути, което е предостатъчно.

„На всеки четири дни имаме българска фирма, която е жертва на този вид престъпления“, посочва главен комисар Явор Серафимов - директор на ГДБОП.

Общо за миналата година има такива 65 измами. Загубите са за 22 млн. лева, а най-голямата, за която „24 часа“ ексклузивно съобщи, бе за 12,3 млн. лева през юли. Пострада фирма от топ 10 на българския бизнес. Най-малката пък е за 2000 лева. От дирекция „Киберпрестъпност“ на ГДБОП съветват да внимавате при всеки превод, а ако забележите, че сметката е нова, да проверите по алтернативен начин реална ли е промяната.

И зад най-голямата хакерска атака срещу българска фирма стоят нигерийци, съобщи шефът на дирекция „Киберпрестъпност“ към ГДБОП старши комисар Владимир Димитров. „Това са нигерийски организирани престъпни групи, които влизат в мейлите на български компании. В избран момент подменят банковата сметка, по която българската фирма да изпрати следващото плащане, и така се ощетяват български компании с десетки хиляди евро“, обясни Димитров.

Общото между всички нигерийски измами е какво става, след като парите са дадени. Бандите използват други престъпни групи, които да изперат средствата. Така една и съща сума минава през различни бушони, познати и като финансови мулета. Ролята им е срещу дребна сума да си отворят сметка, в която да получат средствата. След това се прави верига от преводи, понякога не през банки, а компании за трансфер на пари. Целта е следата да се маскира и парите да изчезнат.

Често обаче фирми стават жертва и на друг тип атака. При нея всичките им данни биват криптирани, а за да ги отключат, киберпрестъпниците искат откуп, обичайно в биткойни. Вирусът влиза или през мейл, или през сайтове за гледане на пиратски филми например.

Според повечето доклади рансъмуерът е основният риск за малкия и средния бизнес. Новите му варианти намаляват, но са още по-сложни за премахване. Проблем е, че го ползват и за друго - кражба на данни, с които кибербандитите си осигуряват достъп до чувствителна информация, например банкови сметки.

В последно време подобни вируси се създават не от хора, а с помощта на изкуствен интелект. Подобен злонамерен софтуер майсторски убягва на технологиите за засичане и разкриване, налични в традиционните антивирусни модели. Наблюдаваните от компаниите за киберсигурност крайни устройства събират ценни данни за това как работят киберпрестъпниците и помагат да се разпознае как някои атаки са станали по-интелигентни, по-усъвършенствани и по-трудни за откриване.

В България от подобен вирус пострада БНР. Архивът на радиото бе изцяло криптиран и до днес не е възстановен.

Най-големият икономически университет обучава магистри и бакалаври как да управляват сигурността в дигиталното пространство, изгражда своя надеждна защита и консултира важни държавни структури в управлението на тези процеси

Проф. д-р Димитър Димитров е учен икономист. Ректор е на Университета за национално и световно стопанство от декември 2019 г. През декември 2023 г. е преизбран за втори мандат. Завършва ВИИ „К. Маркс“ през 1988 г., специалност „Икономика и управление на промишлеността“.

Придобива научната степен „доктор“ (2004). Научните му интереси са в областта на икономиката на отбраната и сигурността, икономическия анализ в отбраната, защитата на критичната инфраструктура и ядрената сигурност. Специализирал е в авторитетни европейски и американски университети. Има над 104 публикации.

Ръководител е на множество проекти за модернизация на висшето образование. Председател е на Националната мрежа за решения за устойчиво развитие SDSN Bulgaria и е ръководител за България на Европейския университет ENGAGE.EU. Работи активно по Националната научна програма „Сигурност и отбрана“. Създател е на единствената в света международна магистърска програма „Ядрена сигурност“ към катедрата, която ръководи – „Национална и регионална сигурност“.

Представител е на УНСС в Международния институт за сигурност и сътрудничество, член е на международни организации по ядрена сигурност. Участва в работни групи, които подготвят документи и формират държавната политика в областта на сигурността, защитата при бедствия, отбранителната индустрия.

Ректорът проф. д-р Димитър Димитров:

За УНСС думата на годината е киберсигурност

- Проф. Димитров, ако трябва да определите дума на годината за УНСС, каква ще е тя?

- За УНСС думата на годината е киберсигурност, защото започнахме да виждаме проблемите с киберсигурността навсякъде около нас. Особено с навлизането на изкуствения интелект, с предстоящото навлизане на квантовите компютри, които могат да разбиват много бързо пароли, с развитието на информационните технологии, които буквално са навсякъде около нас – умни телефони, умни телевизори, дори хладилници, чрез които може да бъде извършена такава атака. Знанието на хората, които се занимават с лоши неща в тази област, също нараства. Така че киберсигурността

ще бъде все по-важна

през следващите години.

- Какво прави вашият университет по линия на киберсигурността?

- Въпросът ясно се появи преди 2–3 години, когато челно се сблъскахме с него. Имахме проблеми със защитата на нашите информационни масиви. Но за радост минахме с минимални щети. Разбрахме на практика колко сериозен може да бъде този въпрос за един голям университет с близо 20 000 студенти, силно дигитализиран, с въведени електронни книги, протоколи, архиви, документи. По време на ковид учебният процес беше изцяло онлайн. Пораженията при една кибератака при нас могат да са огромни.

Това ни принуди бързо

да организираме работата така, че да намалим риска

За наша радост бизнесът много помогна. Няколко големи технологични фирми ни консултираха безплатно и помогнаха да решим временно нещата. Но разбрахме, че трябва да извървим нашия път към по-организирана киберзащита. Създадохме специална позиция на зам.-ректор по дигитализация и киберсигурност, която се среща по-рядко в университетите и е признание за приоритета, който отдаваме на тази област.

- Сега с каква защита разполага УНСС?

- Предприели сме конкретни мерки, но може би е по-добре да не ги казваме. За няколко години организирахме ресурсите си и миналия месец на 14 декември получихме сертификат за информационна сигурност ISO 27001:2022. УНСС е

първият и единственият университет в България, който има такъв сертификат

Това не е просто една грамота, а предполага наличието на много организационни, физически и нормативни мерки, свързани с киберсигурността, които са внедрени и работят. Сертификатът официално бе връчен от „Бюро Веритас“, световен лидер в акредитацията, с присъствие в над 140 държави. След дълъг процес на проучване и на база изводите, които направи, ние получихме този сертификат.

- Предлагате ли обучение по киберсигурност?

- От няколко години провеждаме обучение по магистърската програма „Управление на киберсигурността“ и тя се радва на голям интерес. В нея участват и хора от практиката - ГДБОП, МВР, БАН и други структури, които обучават нашите студенти. Имаме прием по програмата и през септември, и през януари. Отзивите от студентите са много добри.

Аз самият до известна степен съм специалист в тази област. Миналата и по-миналата година по два семестъра преминах обучение по киберсигурност в САЩ с Фулбрайт стипендия. Посетих редица институции, занимаващи се с киберсигурност, имах възможност да почерпя опит от водещите в областта, представен бе огромният мащаб на проблема и всички негови аспекти. Не става въпрос само за софтуерни и технически специалисти. Има нужда от хора, които управляват процесите, разработват и спазват нормативната уредба. Именно тук е

ролята на УНСС като бизнес управленски университет

Магистърската ни програма е за хора, които управляват процесите. Не е задължително да са софтуерни експерти или да пишат кодове.

- Разкажете повече за бакалавърската програма по киберсигурност.

- Стартирахме подготовката на бакалавърска програма „Киберсигурност и електронно управление“. Засега срещаме проблеми с акредитацията, тъй като Картата за висше образование поставя

изисквания, които не са в унисон с важността на проблема

Киберсигурността се приравнява към всички възможни специалности по информатика и има определени капацитети, които трудно се запълват на национално ниво. Надявам се, че Министерството на образованието и науката и Националната агенция по оценяване и акредитация ще проявят разбиране в тази посока, защото интересът е изключително голям. Имаме над 50 студенти, които в момента изучават киберсигурност платено обучение, а не можем да получим акредитация за нормално обучение по информатика държавна поръчка.

Продължаваме усилията и миналата година разкрихме съвместна програма с Тракийския университет. Получава се добра синергия между нас и нашите партньори. Бизнесът активно помага в тези дейности. Когато създавахме бакалавърската програма по киберсигурност, над 50 компании изпратиха писма за подкрепа и заявиха нуждата от подобни кадри.

Необходимостта от такива специалисти е буквално навсякъде,

особено с навлизането на изкуствения интелект.

- Каква добавена стойност има обучението при вас по тази специалност?

- Нашият потенциал в областта е много голям. 50–60 души се занимават с подобни технологии. Влязохме в изследванията по киберсигурност. Работим по изследователски проекти, финансирани по различни програми.

В същото време УНСС започна да

осъществява и консултантска дейност

Имаме договори с държавни предприятия от критичната инфраструктура на България. Извършваме одит на информационната сигурност и преглед на киберсигурността. Помагат ни натрупаните знания, възможностите, които имаме с Центъра за големи данни, Центъра за компетентност „Дигитализация на икономиката в среда на големи данни“. Участвахме на доброволна основа в проучване за слабостите на националната информационна инфраструктура и резултатите предоставихме на ГДБОП и МВР. Имаше интересни изводи, но се въздържаме от публикуване на резултатите.

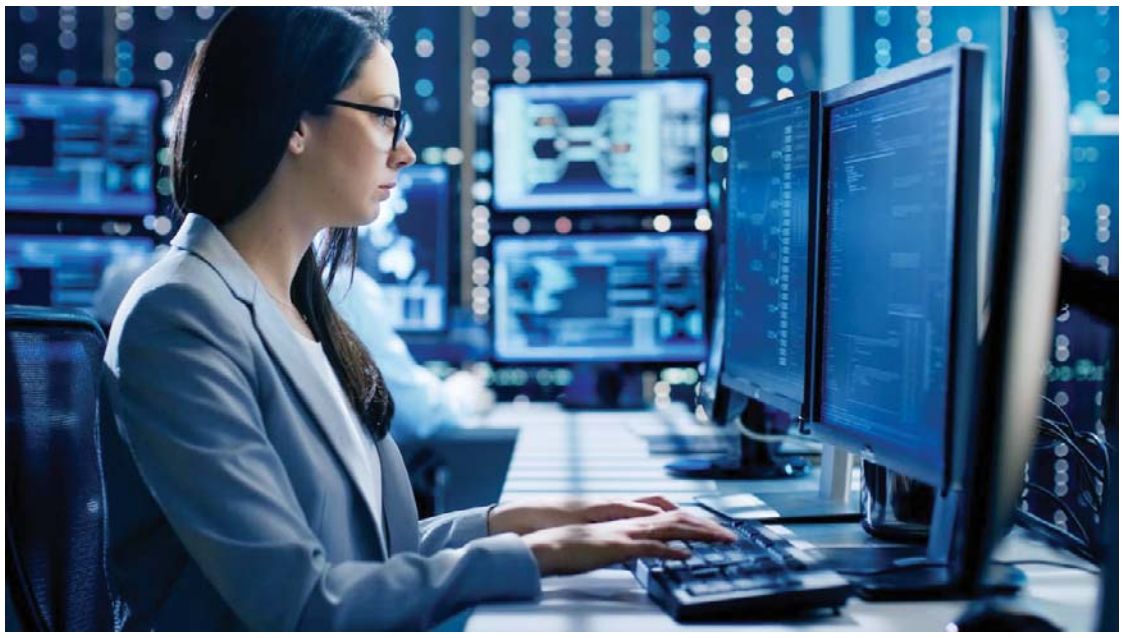
Водещите компании в тази област участват про боно като лектори. Те не идват за хонорарите, които не са и много високи, а защото усещат нуждата от кадри и необходимостта България да бъде защитена от киберзаплахи.

- Къде виждате университета в близко бъдеще в това отношение?

- Виждам УНСС като университет, който е

привлекателен и престижен за изучаване на киберсигурност

Ще продължим да работим в трите ни направления: обучение – бакалавърска и магистърска програма; научни изследвания и консултантска дейност в симбиоза с бизнеса.



Бандити мамят хората, за да си дадат данните от банковите карти, лъжат ги и с инвестиции

ДИМИТЪР МАРТИНОВ
DMARTINOV@24CHASA.BG

3 схеми за измама са популярни при мошениците, които опитват да вземат парите на хората. Лъжат ги при пазаруване, с инвестиции и ги подвеждат, че са влюбени.

Най-чести са измамите при пазаруване. Те се случват в сайтовете за публикуване на обяви и фейсбук маркетплейс, където хората обявяват неща за продан.

Петър обявява, че продава новите си дънки, защото са му малки. Иска им 50 лева. Качил е телефонния си номер. Тогава с него по вайбър се свързва мъж или жена.

Пише му съобщение, че иска да купи дънките. То е на перфектен български, не личи, че се ползва машинен превод, създаден от изкуствен интелект.

Фалшивият клиент изобщо не се пазари за цената - нещо, което е рядкост в подобни сайтове. Всъщност не я споменава със сума. При внимателен поглед на продавача ще му направи впечатление, че купувачът нарича дънките „продуктът“. Именно заради този детайл са били предотвратени няколко измами - Петър имал няколко обяви и попитал за коя стока иде реч, но винаги получавал за отговор „продуктът“.

Тези, които нямали неговия късмет обаче, продължили комуникацията. При нея менте купувачът предложил да плати чрез суперсигурната система за плащане на сайта, в който била публикувана обявата. За целта изпращал линк. Той изглеждал точно като сайта, но имало малка разлика в името - например вместо prodavam.bg било prodavan.bg. Във фалшивата платформа продавачът трябва да даде номера на банковата си карта, докога е валидна, име и секретния трицифрен код на гърба. Вместо да си получи парите, той изпраща данните на измамника, който може да си пазарува в интернет с чуждата карта. В подобни случаи хората трябва да се усетят, че

за получаване на пари се иска айбанът, а не номер на картата

Трима българи обаче се подлъгали по празниците и олекнали средно с по хиляда лева.

Други се спасили, след като решили да се обадят на купувача по телефона. Вдигнали им хора, които нямали и представа за „сделката“. Твърдели и че нямат вайбър. Всъщност това е част от измамата - мошениците пускат приложението на български номера, за които са проверили, че нямат апликацията. За да вземат номера, се иска да го потвърдят с есемес, който се получава от телефона. Заобикалянето е просто и струва едва $ 20.

За целта измамникът ползва сайт в тъмния интернет. В него се вкарва мобилният номер. Той лъже доставчика, че телефонът е в роуминг и за да си получи съобщенията, трябва да ги даде на сайта. Така мошениците реално четат всеки есемес.

Пенсионерки са жертви на любовни измами

Други измами стават по мейла или социалните мрежи

Здравейте, аз съм адвокат на наскоро починалия африкански принц Мумбай. Той остави голямо наследсво от 20 милиона долара. Дълго търсих негови преки роднини, но това се оказа доста трудно, защото той загина в трагична катастрофа на 21 години. Така не успя да създаде семейство. Затова правителството на ЧАД е готово да прибере парите за себе си. Дългата ми проверка обаче показа, че вие сте негов далечен братовчед. Трябва само да ми преведете малка сума, за да мога да входирам молбата ви за получаване на наследството.

Горе-долу така изглеждаха първите измами, които се разпространяваха по мейла в началото на деветдесетте години на миналия век.

Разбира се, принц никога не е имало. Целта на мошениците - престъпни групи от Нигерия, бе да вземат парите на хората. Тези схеми са познати като нигерийски измами или Scam 419 (измама 419 - б.а.). Името идва от члена на Наказателния кодекс в Нигерия, който преследва компютърните престъпления.

Съобщенията идваха на английски език. Така се разпращаха до хора из цял свят. С началото на новия век мошениците почнаха да ползват и различни програми за автоматичен превод, но той беше доста лош. Затова като цяло предпочитаха да продължават с английския.

В средата на предишното десетилетие обаче машинният превод се подобри. Така изведнъж се появи

вълна от писма, уж от НАП, от различни ЧСИ-та,

непогасени дългове към фирма за бързи кредити и различни други институции. Конкретно при случая с частен съдебен изпълнител много българи получиха мейл с реално име. Затова и някои се хванаха, а от офиса на човека бяха принудени да обясняват, че не са изпращали подобно писмо. Грешката на излъганите бе, че не бяха погледнали кой е подателят на мейла. Когато задържиш върху името, което уж е ЧСИ Иван Иванов например, веднага илиза, че мейлът всъщност е регистриран в протонмейл и е с име на чужденец. Проблемът и тук, както и при менте рекламите, организирани от руснаци, е, че се правят нови пощи, дори доставчиците на услуги да са блокирали старите.

С възхода на социалните мрежи започнаха и романтичните измами. И те се правят от нигерийски групи. Схемата е елементарна. Бандитите се правят на влюбени военни на мислия в чужбина. Уж изпращат колет с бижута, но пратката е спряна на митницата. Тогава трябва да се плати, за да бъде освободена, обясни в интервю за „24 часа“ старши комисар Владимир Димитров, директор на дирекция „Киберпрестъпност“ в ГДБОП. Рекордът бил бил 500 000 лева, дадени от софиянка. Обичайно жертвите са жени над средна възраст.