00:00:00  
*Speaker 1:* Коли. Краще буде проводити інтерв'ю українською та англійською для вас.

00:00:07  
*Speaker 2:* Якщо можна українською буде трішки перехворіти Тяжко.

00:00:15  
*Speaker 1:* Добрянського? Тоді можете розказати, чим ви займаєтеся. Трошки про себе інформації.

00:00:23  
*Speaker 2:* Ну, я заступник декана факультету інформатики Могилянської академії. Не знаю. Консультант з кібербезпеки, з цифрових перетворень, З розробки. Не знаю. Різноробочий, айтішник. Можна так мене занести, Будь ласка.

00:00:43  
*Speaker 1:* Звичайно. Як, на вашу думку, змінилося як кібер стан нашої країни з початку повномасштабного вторгнення кібер атак?

00:00:55  
*Speaker 2:* Ви маєте на увазі наш кіберзахисту? Що саме по британцям дуже широке слово. Як це?

00:01:05  
*Speaker 1:* Тобто як? Наприклад, як змінилася кількість кібератак?

00:01:11  
*Speaker 2:* Ну дивіться, Вочевидь, їх кількість виросла, тому що це стало пріоритетом для Росії. Але ж ну, Росія нас три тижні року і так дуже активно атакує. Це просто, знаєте, типу, грубо кажучи, якісь останні останні зовсім бар'єри для неї стали. І це перше. Друге це те, що росіяни намагаються дуже активно масштабувати всю свою діяльність. Типу залучаючи будь яких взагалі учасників, намагаючись імітувати дуже ніби велику активність. Ну знову ж таки, щоб залучати учасників. Да. Тобто, якщо дивитися нещодавно не згадаю, читав дослідження. І це не перша думка, що от ці хакерські угрупування типу сонце плювок, а не ти там, блін. Я кажучи, що це одні і ті ж самі ГРУшників, розвідка їхня та, яка просто імітує ніби їх дуже багато, грубо кажучи, для створення ефекту. Але разом з тим тут варто розуміти, що є і реальні наслідки цього всього. Да. Тобто там Путін і закони намагався приймати для ніби як легалізації етичного характеру з метою підвищення кібербезпеки. Але ну, відверто кажучи, приватної кібербезпеки на Росії немає. Що я маю на увазі під цим? Це те, що будь хто, хто працює в кібер на Росії, вони ну, там з імовірністю, якщо вони, якщо вони ще й професіонали, вони з імовірністю на вісімдесят відсотків Проурядові хакери не хакери, але проурядові щонайменше. Так що ну зросла кількість. Ну, інтерес зріс до нас і відповідно, внаслідок діяльність теж значно зросла. Тому що якщо раніше там намагались хоч якось тіпа я не знаю, скромніше будь я що сказать, то зараз немає жодного обмеження. Ну що можуть, те й роблять.

00:03:30  
*Speaker 1:* Тобто які уроки винесла спільнота кібербезпеки з кібератак та інфраструктуру України і як лікарні можуть підготуватися до подібних загроз?

00:03:41  
*Speaker 2:* Так давайте друге питання. Не дуже хочу, але давайте спершу почну. Ну, найважливіше це те, що всі почали жити рамкою кібербезпеки Якихось організацій чи ще чогось. Використовується термін, що англійською звучить як Березін, тобто кібер стійкість. І це перш за все про підхід. Про те, шо не можна шоб тіпа урядові компанії наприклад були не захищені, а приватні захищені чи навпаки. А про те що є загальна рамка країни, да і відповідно коли хтось з усіх ланок вразливий, чи то держава вразлива, чи то приватні компанії вразливі, то в результаті цього програють всі. Тому зараз, з одного боку, держава дуже активно допомагає приватному бізнесу, який ну не кібер. Я маю на увазі от якийсь зовсім лівий приватний. Там магазини якісь нова пошта, да так і навпаки. Приватний бізнес, які беруть, Петрук намагається допомогти державі бути кращим в культурі. Це відповідь на перше питання які уроки винесла японцям? Мабуть, найсильніше підкреслив був урок. А можете? Друге питання, якщо ваша ласка, повторите.

00:05:08  
*Speaker 1:* Як лікарні можуть підготуватися до подібних загроз у лікарні? Тобто у лікарнях наразі досить багато медичного обладнання, тобто проводяться багато операцій. І у зв'язку з тим, що багато медичного обладнання зв'язують до Інтернету. Тобто.

00:05:30  
*Speaker 2:* Ну ну, по перше, це може бути так собі. Вам факт цікавий, але Росія перед ударом ракетних Охматдиту зламала його мережу. Ну, але вони ламали це не як лікарню, а як. Ну, у кожного свої припущення. Це вже давно відомо, що вони так роблять перед ракетними ударами. Але менше з тим. Ну, лікарні насправді. Ну, це ті ж лікарні. Грубо кажучи, запит на кібербезпеку приблизно такий само, як і всіх. Тільки питання в його критичності чи як це сказати? Та тому, що якщо в якійсь приватній фірмі інтернет не працює годину це одна історія, а якщо в лікарні, то це зовсім інше. Тому ну я просто лікарняний готувався, знаєте, на рівні критичної інфраструктури. Просто. Ну це і є той рівень. В принципі, насправді так просто придумувати. Ну мені прям повністю алгоритм про говорить, чи цього достатньо?

00:06:36  
*Speaker 1:* Ну якщо можете проговорити алгоритм буде цікаво подивіться.

00:06:42  
*Speaker 2:* По перше, я дуже раджу різним непрофесійним організаціям у лікарні, зокрема, наприклад, під цю категорію потрапляють непрофесійні, я маю на увазі не зі світу кібератак. Я дуже раджу намагатися пограти. В цю гру вилетіло з голови. Архітектуру нульової довіри я маю на увазі підходити до всіх компонентів своєї цифрової інфраструктури з міркування а що, якщо ось цей вузол чи цей елемент зламано? Як ми будемо діяти відповідно? Виходячи з такого підходу, одразу треба робити план дій. Так, разом з цим ти будеш автоматично опрацьовувати якийсь базовий план протидії і туди йти відповідно. Ну саме базове це план поновлення мають щонайменше. А далі я б дуже радив би. Зараз сучасний тренд на кібер операції і на їх виявлення лежить не просто в площині вияву того, що, здається хтось когось зламає, грубо кажучи, а лежить в площині того, наскільки швидко ти зможеш зрозуміти, що тебе зламали вже. Так що тут от якраз таке концентрувати увагу не стільки на кіберзахисту, скільки на вияві втручання в мережу. Бо якось так.

00:08:25  
*Speaker 1:* От тактика кібер війни Росії в Україні включала атаки на енергомережі, зв'язок і критичну інфраструктуру. Як ви думаєте, ці тактики можуть бути адаптовані для атак на медичні установи?

00:08:43  
*Speaker 2:* Ну, це ви зараз заходите на слизьку стежину, тому що зараз за це. Ну, Червоний Хрест давно вже намагається з цим щось робити в рамках кібервійни. Так як адаптовано. Ну. Можна кібер операції ділити за їхнім наслідком. Так, вочевидь, є такі, які приносять результат безпосередній військовий. Так от, наприклад, якщо в зламають, наприклад, Міністерство оборони з їхніми там таємними певними системами, вочевидь, їхня логістика там просяде. То що сьогодні є політичні діяння? І от політичні причини це широкі. Це не тільки, знаєте, От про якийсь активізм з надання йому самої ідеї. Тепер про широкі політичні мотиви, Що, наприклад, коли ти з Згадайте, коли зламали міністерство. Та ну навіщо ці чотири міністерства, що ці регістри не працювали? Тут же не тільки питання в регістрах. Це ну неприємно, але ну від цього не вмирають. Але тут ще питання того, як це сприймається суспільством. Є теорія саботажу. Дуже вам радив би з нею ознайомитися. І от це в тому числі про такий вплив. От.

00:10:17  
*Speaker 1:* Тобто ви хочете сказати, що як кібератака вона діє не тільки як фізично, але й ментально на суспільство?

00:10:25  
*Speaker 2:* Так так, так так. І от. І оці атаки на медичну, ну, грубо кажучи, що буде від того, що зламали? Зламали лікарню. Уявімо. Обладнання перестало працювати від слова зовсім. І що? І що з цього? Ну, конвенція не Нічого, тому що це буде Конвенції. Маленька кількість людей у нас. Я, щоправда, не знаю. Я не впевнений, що в Україні є лікарні на тисячу прям людей. Знаєте, як в Америках не туди йти, але менше з тим це кілька сотень. Ну це неправильно. Це трішки не етично. Так кажуть про людей, але рамками війни це нічого, грубо кажучи, да. Але моральний ефект буде значно більший, тому що це прийняти суспільство дуже сильно. Це підніме страх. Там припустимо, як ми можемо почувати себе в безпеці. Це підірве, підриває довіру загалом до медичної, ще не до медичної системи. Бо чи варто мені йти в лікарню, якій я можу вмерти, тому що там перестануть всі прилади працювати, викручуються. Ну, тут треба завжди думати про кібер операції, кібер операції. Тут треба розуміти їхню природу. Кібер операція сама по собі не конвенційних. Тобто такі операції не можеш зробити бабах! Тобі кібер операція може щось доповнювати. Це помічний інструмент. Це я б радив подивитись в бік інформаційної безпеки того, як роблять інформаційні атаки. Потім зрозуміти, що кібер операції це в контексті повномасштабної війни. Так, це теж інструментарій для того, щоб доповнювати якісь інші цілі військово політичні. Господи, прости чи ті, які на полі бою? Ну але ну, це ніколи. Ну, майже ніколи не самодостатня діяльність, тому що в рамках самодостатньої діяльності вона дуже мало змістовна. Ну зламав ти лікарню і шо? От.

00:12:27  
*Speaker 1:* А от яку роль відіграє вихідний шкідливий софт ресивер у конфлікті в Україні і як ця загроза може вплинути на безпеку Суспільства.

00:12:40  
*Speaker 2:* Ви дуже влучно потрапили питанням, тому що ну, на Росії загалом по кібер вони не ну вони нормальні, але вони не дуже сильні в плані наступального, кібер в плані, що от знайти якусь вразливість і ламають через неї. А вони зато дуже добре вміють. Розводить людей і з вірусами в них непогано. Тому це один з їх прям буквально ключових інструментів. У них є непогані експерти в написанні вірусів. Можна тільки згадати, що тільки Лабораторія Касперського тільки чого коштує. Та вона ж розумієте, що Ну той, хто робить захист, той точно має розуміти, як щось працює. Згодні, то відповідно це дуже ефективно працює. Росія Комбінує атаки соціальної інженерії разом з вірусами. Згадайте, скільки існує прикладів того, як наші співгромадяни та знаходили посилки. За машинку проголосувати в телеграмі чи ще за якусь руду тему. Це прям один з їх інструментів, який показує. Я б навіть сказав гарний результат.

00:14:03  
*Speaker 1:* От які тактики кібервійни, Наприклад, шкідливу шкідливе безе, знищуючи Вайпер, малює дідусь. Атаки та фішингові кампанії, найімовірніше, будуть використовуватися проти критичних інфраструктур. І як їм можна протидіяти?

00:14:23  
*Speaker 2:* Ну дивіться, дідусь атаки навряд чи. Хоча б тільки один раз була. І то не зовсім так, коли діти йому ламали Закарпаттяобленерго. Так це в ну відомий прецедент, то не зовсім достали. Менше з тим. Почали телефонним номером обдзвонювати їхню гарячу лінію, щоб доповнити операцію. Ну так ви описуєте. Ну це ж ви розумієте, що фішинг, що мова це все частини соціальної інженерії. Тобто фішинг це інструмент, що в мене чи людини пароль? Але ти ж фішинг. Ну не можеш ти, ти не можеш зламати фішинг. Тобі треба встановити спершу контакт з людиною, а потім вже її намагатися цю ссилку кинуть. Шкідливу, наприклад, те ж саме з вірусом. Ти ж не можеш, просто вакуумно, як сферичний кінь в вакуумі, просто матеріалізувати вірус на чомусь комп'ютері. Ти треба, щоб хтось його запустив. А тут я кажу тут якраз таки це поле діяльності росіян. де вони гинуть, там якраз дуже активно і в принципі доволі ефективно займаються тим, що випалюють віруси фішингу і туди тепер.

00:15:47  
*Speaker 1:* А от які країни або хакерські групи становлять найбільші загрози кібервійни для критичної інфраструктури України?

00:15:58  
*Speaker 2:* Ну, насправді ви маєте розуміти, що дуже мало держав офіційно визнають свої кібер війська. Якщо навіть і визнають, то частіш за все. Ну інформації про це нуль, Я не знаю. Ви знайомі з вірусом? Так, сьогодні от я дуже радив би і по ньому є книжки і фільми. Є доволі непоганий документальний. Була операція, яка, якщо коротко пояснить, зірвала Ірану. підготовку ядерного реактора. Ну не могли, грубо кажучи, ядерний реактор. Ну як ти? Фізично це об'єкт дуже захищений. Тому його, грубо кажучи, вірусом ламали. Це якраз таки історія про це. Все це текст. І відповідно, ну, ламали. Операція, блін, в чотирнадцятому році вона була. Але ж ви розуміли, що досі ніхто за неї відповідальності на себе не взяв. Да. Хоча це, вочевидь, знаєте, боротьба добра зі злом ніхто ні відповідальності не взяв. У нас дуже великі проблеми з міжнародним законодавством в контексті цього кібервійни. Тому що якщо уважно почитати, так би мовити, букви закону, то можна зауважити, що такого поняття, як кібер війна не існує. У мене є свої погляди. Чому так і. Ну то може, зашкодить. Ну, вочевидь, це відмороження від зла, яка в принципі не надто приховує свої зусилля. Це ті, хто заробляє цим гроші. От, наприклад, ця Північна Корея. Так. Ну це ж Азаров груп, так званий. Це ж нікому не секрет, що це Північна Корея, наприклад. Та що вони таким чином собі буквально долар в країну мусять. От подивіться, справа за розробку. Це буде дуже показово. Іран. Ну, вони ну, вони не. Вони дуже хочуть, але не можуть. У них це не систематично, низьким рівнем результатами буває подекуди, але. Ну але ну слабенько. І от. Ну і Китай це теж дуже непогано в плані відбору, але Китаю ОДЕК. Якщо рахувати від урожайності, то я думаю, що Китай буде найменше від мороженої, потім Росія. Відмороження шийної відмороження. Ну, не дивлячись на всю ситуацію, календар і Іран, і тільки КНДР і Іран визнає свої кібер війська і туди тепер хоче навіть КНДР і навіть КНДР не визнає. Так що ну одну з загроз цього дві зла КНДР, Іран, Росія, Китай.

00:19:02  
*Speaker 1:* А от не зараз в нас геополітична ситуація між Україною та США починає бути дуже нестабільна. Чи вважаєте ви, що США стає на одну полицю з Росією, Китаєм та КНДР?

00:19:23  
*Speaker 2:* Раптове питання Чи стає на одну полицю? Та ні. Ну як вам сказати я? Ну, Я просто думаю, що Україна апріорі має бути сильна, незалежна, без Америки. І шо? Ну мені, звісно дуже неприємно і дуже сумно. Боляче. Та я навіть з гранатою сидів, коли злетів ця вся ситуація. Але, об'єктивно кажучи, ну не знаю. В словах Трампа є доля правди. Ну, як мінімум для нашого власного планування. Тому що ну ти можеш покладатись на кого хочеш, але розраховувати завжди краще виключно на себе. Ну моя така думка і в кіберпанку воно в принципі теж так само. Ну у нас є можливість захищатись. Слава Богу. І це головне.

00:20:17  
*Speaker 1:* А от як співпрацю України в сфері кібербезпеки із західними країнами вплинуло на геополітичний баланс.

00:20:27  
*Speaker 2:* Кібербезпеці не геополітичний баланс. Знову ж таки, ми повертаємося до того, що кібер операції не мають яскраво вираженої кінетичної дії. Тобто, скоріш за все, якщо операції і існують взагалі українські, то вони не є стоп, Це фігури СБУ визнавали там якісь уявні хакерські групи. Якщо ви уважно прочитайте про те, що визнавали ГУР і СБУ, ви побачите, що частіш за все це або якась повна оренда. Ну, по наслідкам, якщо задатися питанням про після прочитання новини і шо? Ну ти читаєш новину шо там той то той там зламав тет а тет. А потім теологічне питання і шо то стає зрозуміло, що? Ну мабуть, по перше, все ж таки кібервійни якась не існує, але результатів чомусь дуже і не видно. Поясню чому. Тому що частіш за все в більшості випадків ми будемо бачити або на полі бою. Але ми ніколи в житті не співставити в голові, що оце от що тут відбулося. Це результат кібер операції. Да або ну воно буде відбуватися, як от, наприклад, при зламі цих реєстрів воно буде відбуватися в головах наших співгромадян у форматі ті побили надцять наших зламали. Ну дибіли, ну кошмар. Хочемо поділитися з вами наших реєстрів. Стало відомо, що китайські хакери в американській інфраструктурі усувалися місяцями, але наших фізичних експертів кібербезпеки не хвилює. Та й таке.

00:22:19  
*Speaker 1:* А от яку роль відіграє кібер війна в сучасній стратегії гібридної війни?

00:22:31  
*Speaker 2:* Яку роль поки що не належну? Але я думаю, що нарівні з дронами в майбутньому це теж стане одним з стовпів війни повномасштабної та очікує на краще. Але поки це воно себе випробовує, випробовує, тому що дрони по факту не те що не до кінця. Вони тільки на перших етапах, навіть не дивлячись на те, що ніби скільки всього вже зроблено, які ми успіхи класні маємо. Але все одно це тільки початок розвитку технології. То з кіборгами, думаю, щось буде подібне. Просто будуть. Варто очікувати нових цих твітів про участь кіборга в чомусь, наприклад.

00:23:18  
*Speaker 1:* От Україна отримала міжнародну допомогу у сфері кібербезпеки, зокрема від НАТО та приватних компаній, таких як Майкрософт та Ґуґл. Наскільки важливим є зовнішнє співробітництво для стійкості кібербезпеки інших критичних інфраструктур?

00:23:40  
*Speaker 2:* Воно є надзвичайно важливим, тому що є такий вираз все більша кількість сноубордах. Да, тобто ну в тому тут речі і проблема, що кібервійни, що навіть якщо буде якась уявна якийсь уявний мир, неважливо в яких умовах, то кібер війну ти не бачиш, хто там кібер стріляє або кібер не стріляє. І тому це, звісно, ще таке відкрите питання, що буде, Але менше з тим, як я поясню на практичному прикладі хакерських угрупувань. Є так звані ті, які пішки Так текс технік. Сам процедуру можете загубили. Дмитре, а так і з високою ймовірністю не ультра професійних хакерських угрупувань. Вони від атак і до атаки подібні. І відповідно, якщо хакерські угрупування ІКС атакували там компанію і грип в країні, де були Ю. І якщо немає міжнародного обміну, то ну нічого. Нічого цікавого, скажімо так. А якщо є міжнародний обмін розвідувальною господ, розвідувальною інформацією про атаки? Та то ця інформація миттєво поширюється на всі інші країни і працює так званих агентів, тобто пошук загроз. І ти вже наперед знаєш, що висока ймовірність, що в твоїй системі почнуться ось приблизно такі можливі аналогічні, але менше з тим. Приблизно такі дії, скоріш за все тебе ламає така то така то група, наприклад. І ти зможеш ефективно протидіяти цьому.

00:25:27  
*Speaker 1:* А от наразі Україна перейшла у більш деталізовану еру. Ми використовуємо дію для того, щоб зберігати наші документи. І наразі, як більшість громадян, хто знаходиться за кордоном, вони використовують дію як основну. Інфраструктуру, де можна забрати свої документи. От наскільки діє є цей резидент.

00:26:00  
*Speaker 2:* В мене провокативні питання, задаєте зі мною він цифри не буде потім працювати після відповіді на ваші питання. Блін, вибачте, скажу. Політичне Міністерство цифрової трансформації докладає максимально зусиль для того, щоб забезпечити якомога вищий рівень захисту персональних даних українців і їх цифрової безпеки в рамках роботи в дії. От давайте так.

00:26:36  
*Speaker 1:* От напевно ви чули, що в Данії є така як програмка Міледі. Це як діджитал підпис. Чи можливо було б зробити таку ж систему аутентифікації в Україні?

00:26:54  
*Speaker 2:* Така вона є у Едді. Тобто, якщо ти клієнт якогось з дуже багатьох банків, то ти маєш собі свій цифровий Едді, яким ти можеш там підписувати щось і ще щось. Авторизація на частині державних сервісів. Це є новий власник, до речі, діє. Там теж є підпис і ще ряд речей. Так що це аж два цікавих варіанти того, як з цим можна, скажімо, працювати.

00:27:26  
*Speaker 1:* От, наприклад, от якщо заподіяти таку систему в Україні, що от у кожної людини буде свій індивідуальний номер і до цього номера буде як прив'язка документів, медичних записів. Чи можливо буде так зробити? Можливо в майбутньому?

00:27:47  
*Speaker 2:* Така в нас зараз. Знову ж таки воно все є. Ну от діє, збирає всі документи докупи і маючи ну майже дію в тебе. Ну у мене, наприклад, в мене не найкраща дія в плані, частину документів туди не підтягувати, не підтягнулися, там права. Але в мене діє закордонний паспорт, внутрішній документ. Два дипломи. Цей тех. Талон на машину. Ну типу вона вже впринципі є.

00:28:24  
*Speaker 1:* А от наскільки діє резистентність до кібератак та айдентики софт.

00:28:32  
*Speaker 2:* Та Юля ви другий раз намагаєтесь це питання задають, оскільки. Розробники і власне команди підтримки дії дотримуються найкращих світових практик з кібербезпеки для того, щоб забезпечувати найвищий рівень захисту.

00:29:03  
*Speaker 1:* Ну добре, в мене більше питань нема.

00:29:07  
*Speaker 2:* Добре, надіюсь я вам був.