Відповіді **Павла Родіонова** – доповідача вебінару “29 років. Від черв’яка Морріса до “поганого кролика”. Чому нас все ще зламують?” 29.11.2017 р.

Який етикет чи кодекс хакерів? Чи існує він ?	Так, він існує. Точніше існує не кодекс хакерів, а кодекс спеціалістів з кібербезпеки. Його можна знайти тут: https://www.isc2.org/Ethics
У вебінарі основна увага приділялась кібератакам на комп'ютерні мережі, а як щодо мобільних пристроїв? Адже їх кількість зараз перевищує кількість ПК і на мобільних пристроях часто зберігається інформація фінансового характеру, яка може бути цікава хакерам. Чи мобільні пристрої менш вразливі до подібних атак і дана проблема не є настільки актуальною?	Проблема дуже актуальна, на жаль в рамках вебінару неможливо було адекватно освітити питання захисту мобільних пристроїв.
Чи можливо вчителю інформатики зробити систему захисту даних для шкільних комп'ютерів? Якщо так, як можна це зробити на вищому рівні?	Це можливо, і для цього треба використовувати загальні правила кібербезпеки. Я рекомендую звернутись до загальних рекомендацій з кібербезпеки, включити також цей документ https://www.cisecurity.org/controls/
Чи безпечно зберігати важливі дані в public cloud storages як Google Drive та Dropbox?	Так, це досить безпечно. Але завжди треба розглядати відповідні ризики. Втрата доступу до облікового запису або можливість втрати даних
Есть ли какие-то практические решения и советы по кибербезопасности от Cisco для IoT устройств?	Да, есть. Они описаны тут https://www.cisco.com/c/en/us/about/security-center/secure-iot-proposed-framework.html. Простой поиск в Google IoT Security выдает большое количество рекомендаций
В чому полягає найбільша вразливість IoT пристроїв?	Виробники пристроїв не піклуються про безпеку, і продаюсь незахищене обладнання. Це не є проблемою для будь-якого промислового обладнання, але пристрої для звичайних користувачів повинні мати кращих захист
Враховуючи необізнаність населення України у проблемах кібербезпеки, як Ви вважаєте, чи було б доцільним введення ОБОВ'ЯЗКОВОГО навчального курсу для учнів та студентів?	Це було б непогано, але хто буде вести такі курси?
MacOS, Linux і Windows: що краще в плані безпеки? Яка ОС більш бажана для кібератак?	Зараз це Windows, але не тому, що вона менш захищена, а тому, що більш розповсюджена.
Як захистити ноутбук від несанкціонованого доступу до веб-камери та мікрофону?	Є багато рекомендацій, рекомендую ці https://github.com/sapran/dontclickshit/
Топ 3 речі, які необхідно виконати звичайному, некваліфікованому користувачу Windows, для запобігання популярних кібервразливостей.	Рекомендую прочитати https://github.com/sapran/dontclickshit/

Как бороться с миллионным количеством эксплоитов, которые есть в открытом доступе для разных систем? (https://www.exploit-db.com/) Не говоря уже о закрытых подписках, которые даже в компаниях антивиров не все знают))	https://github.com/sapran/dontclickshit/
В связи с участившимися атаками на компьютерные устройства и на крупные предприятия, как вы думаете, возможен ли в будущем взлом и угон таким способом электромобилей? Ведь мы все знаем, что компания "Тесла" активно занимается разработкой автопилота.	Возможно, но безопасность зависит от Tesla.
Насколько программирование применимо в сфере кибербезопасности? Какие языки актуальны для работы в этой области?	Более чем применимо, это использование и автоматизация управления оборудованием по безопасности, дополнения к инструментам безопасности, создание и использование API, машинное обучение и многое другое. Достаточно поискать "Machine Learning in Cybersecurity"
На скільки широко в Україні використовуються модулі TPM та технологія Intel "Trusted Execution Technology", яка їх використовує?	Це не питання використання технології в Україні, скоріш за все питання імплементації її різними венодрами. Повний список тут https://www.intel.com/content/dam/www/public/us/en/documents/datasheets/trusted-execution-technology-server-platforms-matrix.pdf
Як ви оцінюєте ступінь захисту Office 365? Сучасні хмарність сервіси мають широке застосування в навчальному процесі. Намагаємося вчити учнів та вчителів використовувати сервіси Microsoft та Google. Наскільки захист цих компаній є сильним?	Завжди можливі помилки, але ці компанії слідкують за захищеністю своїх хмарних технологій
Преимущества и недостатки SMARTnet	SmartNet -- это всего лишь сервисный контракт, который предусматривает определнный уровень обслуживания. У него нет понятия "преимущества" или "недостатки", это соглашение сторон, которое должно выполняться.
В чём отличие современной криптографии от классической ?	Таких понятий нет. Для прочтения рекомендую книгу Брюса Шнайера "Прикладная криптография"
Чи зможе технологія блокчейну суттєво ускладнити хакерам проводити атаки на компьютерні мережі та забезпечити високу безпеку будь-якій інформації?	Ні
На скільки широко в Україні використовуються модулі TPM та технологія Intel "Trusted Execution Technology", яка на них базується? Чи може використання даної технології захистити від загроз, схожих на Petya-A.	Це залежить від імплементації цих технологій відповідним вендором. https://www.intel.com/content/dam/www/public/us/en/documents/datasheets/trusted-execution-technology-server-platforms-matrix.pdf

Яка платформа для розгортання корпоративної хмари на вашу думку є більш захищеною (Office 365 чи G Suit)?	Це залежить від вимог компанії, немає явних рекомендацій
Безопасны ли сети провайдеров, которые предоставляют услуги "транспорта трафика"? Возможна ли кража трафика у этих провайдеров?	Да, возможна. Поэтому рекомендуется дополнительно шифровать трафи
Як буде виглядати чи як зміниться кіберпростір після створення квантового комп'ютера? З якими загрозами зіткнуться в першу чергу кіберзахисники?	Він просто перейде на новий рівень. Вже зараз починаються використовуватись протоколи шифрування, що розраховані на теоретичні можливості квантових комп'ютерів, тому мало що зміниться. Безпека залежить від людей, а наявність квантового комп'ютера людей не змінить.
Чи вважаєте Ви обґрунтованою заборону використання DrWeb в Україні, притому що навіть в Пентагоні використовують AV Kaspersky?	Так, повністю обґрунтованою. Kaspersky зараз заборонений для використання в держустановах США
Скільки сертифікованих спеціалістів високого рівня в Україні по кібербезпеці?	В мене немає такої інформації
Яка антивірусна програма встановлена на Вашому комп'ютері? Чим аргументований вибір саме цього ПЗ?	В мене встановлений Cisco AMP for Endpoints для MAC. Я її вважаю оптимальною.
Чи можна вважати JS бібліотеку Coinhive - вірусом/черв'яком чи взагалі чимось шкідливим, з точки зору кібербезпеки?	Наразі це скоріш за все не явно шкідливе, скоріше "потенційно непотрібне" (Potentially unwanted) програмне забезпечення. Воно не шкодить компьютеру, але використовує його ресурси для виконання своїї завдань.

- - зеленим кольором помічені питання, які експерт визнав найкращими. Інформація про цих учасників подана нижче.

Name	Назва навчального закладу	Питання	Відповідь експерта
Yaroslav Mozghovyi Ярослав Мозговий	Sumy State University	У вебінарі основна увага приділялась кібератакам на комп'ютерні мережі, а як щодо мобільних пристроїв? Адже їх кількість зараз перевищує кількість ПК і на мобільних пристроях часто зберігається інформація фінансового характеру, яка може бути цікава хакерам. Чи	Проблема дуже актуальна, на жаль в рамках вебінару неможливо було адекватно освітити питання захисту мобільних пристроїв.

		мобільні пристрої менш вразливі до подібних атак і дана проблема не є настільки актуальною?	
Oleg Pisarenko Писаренко Олег	Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»	Есть ли какие-то практические решения и советы по кибербезопасности от Cisco для IoT устройств?	Да, есть. Они описаны по тут https://www.cisco.com/c/en/us/about/security-center/secure-iot-proposed-framework.html. Простой поиск в Google IoT Security выдает большое количество рекомендаций
Daria Loziienko	ОНУ імені І. І. Мечникова	Насколько программирование применимо в сфере кибербезопасности? Какие языки актуальны для работы в этой области?	Более чем применимо, это использование и автоматизация управления оборудованием по безопасности, дополнения к инструментам безопасности, создание и использование API, машинное обучение и многое другое. Достаточно поискать "Machine Learning in Cybersecurity"