Співробітники кафедри безпеки інформаційних технологій Національного авіаційного університету, менеджер з інформаційної безпеки компанії "Інфопульс Україна" Гліб Пахаренко і один з колишніх керівників підрозділу по боротьбі з комп'ютерною злочинністю СБУ Костянтин Корсун ініціювали створення першої в Україні університетської команди реагування на комп'ютерні інциденти. Не секрет, що кількість кіберзлочинів в Україні, як і в багатьох інших країнах, зростає і це стало можливим внаслідок виникнення і розвитку глобального інформаційного простору. І незважаючи на відсутність точної статистики про рівень кіберзлочинності у країні, кожен з нас знає, якому ризику ми піддаємося, використовуючи, наприклад, свої банківські картки для оплати в мережі Інтернет.

"Кіберзлочинність - це як глобальне потепління - з ним не можна боротися тільки в рамках однієї країни, тут потрібні спільні зусилля" - говорить Гліб Пахаренко. "І Україна, з її європейськими прагненнями, не може залишатися осторонь. Саме тому й був створений CERT (скорочено від Computer Emergency Response Team) на базі НАУ, основною метою якого є координація заходів щодо ефективної протидії несанкціонованим діям в комп'ютерних мережах НАУ".

Саме глобальний характер технічної бази кібертерпреступленій та їх доступність визначили особливі риси цього виду злочинів:

- Високу ефективність кібератак, наслідки, яких можуть мати глобальний характер;
- Просторову невизначеність джерела кібератаки;
- Часову невизначеність та невідповідність в часі власне кібератаки та процесу її підготовки;
- Можливість організації складних кібератак одночасно на різні інформаційні системи з різних напрямків;
- Анонімність злочину (для здійснення провозаконного акту зловмисникові немає необхідності перетинати кордони держав та перебувати безпосередньо на місці злочину);
- Зниження рівня морально-психологічного тиску на суб'єкт кібератаки, пов'язане з просторово-часовою віддаленістю від об'єкта кібератаки (вся боротьба для суб'єктів кібератаки відбувається у віртуальному кіберпросторі);
- Доступність технічних засобів для вчинення злочину (в більшості випадків для цього необхідний тільки комп'ютер з доступом в інформаційну систему);
- Акти кіберзлочинів відбуваються людьми з високим інтелектуальним потенціалом.

Таким чином, можна сказати, що кіберзлочинність - це застосування певних методів для підриву безпеки або реалізації загрози характеристикам безпеки ресурсів інформаційних

систем за допомогою використання їх уразливості. І для того щоб забезпечити певний рівень безпеки ресурсів інформаційних систем і був створений CERT.

Університет був вибраний не випадково. Там є все необхідне - численні повноцінні комп'ютерні мережі, широкосмуговий доступ в Інтернет, і талановиті люди. У найближчому майбутньому планується підключити до проекту й інші ВНЗ, між якими буде встановлено регулярний обмін даними про інциденти, статистикою, а також напрацюваннями щодо запобігання існуючих проблем. Таким шляхом йшли в США, Європі, і багатьох інших країнах, де на основі існуючих CERT навчальних закладів створювалися вже комерційні організації, здатні вирішувати серйозні проблеми в сфері IT і взаємодіяти як одне ціле з подібними командами з інших країн.