ТЕМА 2. ГАРАНТУВАННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ

1) Стратегія як основний док-т у сфері гарантування кібербезпеки, історія документу.

Стратегія кібербезпеки була затверджена 15 березня 2016 року указом Президента України. Попередньо 27 січня 2016 Рада національної безпеки і оборони України розглянула та схвалила проект поданий Кабінетом Міністрів України. Прийняттю цього документа передували неодноразові кібератаки різного рівня та масштабів, кількість яких постійно зростала.

Стратегія є основним документом, оскільки документує основні поняття та положення та є підґрунтям для розробки та створення повноцінної нормативно-правової бази, що буде регламентувати дії у площині кіберзлочинності.

Ця Стратегія базується на положеннях Конвенції про кіберзлочинність, ратифікованої Законом України від 7 вересня 2005 року, законодавства України щодо основ національної безпеки, засад внутрішньої та зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом та спрямована на реалізацію до 2020 року Стратегії національної безпеки України, затвердженої Указом Президента України від 26 травня 2015 року «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про Стратегію національної безпеки України"».

2) Мета Стратегії та її реалізація.

Метою Стратегії є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави.

Для досягнення цієї мети необхідними є:

- створення національної системи кібербезпеки;
- посилення спроможностей суб’єктів сектору безпеки та оборони для забезпечення ефективної боротьби із кіберзагрозами воєнного характеру, кібершпигунством, кібертероризмом та кіберзлочинністю, поглиблення міжнародного співробітництва у цій сфері;
- забезпечення кіберзахисту державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, а також інформаційної інфраструктури, яка знаходиться під юрисдикцією України та порушення сталого функціонування якої матиме негативний вплив на стан національної безпеки і оборони України (критична інформаційна інфраструктура).

Тобто, метою є захист та створення безпечного простору для функціонування різних об’єктів та суб’єктів, що має бути реалізованим внаслідок створення комплексної системи кібербезпеки.

3) Основні загрози кібербезпеки України.

Сучасні інформаційно-комунікаційні технології можуть використовуватися для здійснення інформаційних терористичних актів. Дедалі частіше об’єктами кібератак та кіберзлочинів стають інформаційні ресурси фінансових установ, підприємств транспорту та енергозабезпечення, державних органів, які гарантують безпеку, оборону, захист від надзвичайних ситуацій.

Основними загрозами кібербезпеки в Україні є:

- невідповідність інфраструктури електронних комунікацій держави, рівня її розвитку та захищеності сучасним вимогам;
- недостатній рівень захищеності критичної інфраструктури, державних електронних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, від кіберзагроз;
- безсистемність заходів кіберзахисту критичної інфраструктури;
- недостатній розвиток організаційно-технічної інфраструктури забезпечення кібербезпеки та кіберзахисту критичної інфраструктури та державних електронних інформаційних ресурсів;
- недостатня ефективність суб'єктів сектору безпеки і оборони України у протидії кіберзагрозам воєнного, кримінального, терористичного та іншого характеру;
- недостатній рівень координації, взаємодії та інформаційного обміну між суб'єктами забезпечення кібербезпеки.

Аналізуючи основні фактори загрози, можна стверджувати, що вони є типовими для усіх країн, які перебували на етапі становлення у регулюванні цього напрямку інформаційної безпеки. Зважаючи на це, при розробці стратегічного плану щодо впровадження затвердженої Стратегії варто зважати на досвід інших країн, які вже пройшли цю ланку.

4) Основні суб’єкти забезпечення кібербезпеки.

Відповідно до Стратегії основу національної системи кібербезпеки становитимуть Міністерство оборони України, Державна служба спеціального зв’язку та захисту інформації України, Служба безпеки України, Національна поліція України, Національний банк України, розвідувальні органи, на які мають бути покладені в установленому порядку такі основні завдання:

- на Міністерство оборони України, Генеральний штаб Збройних Сил України відповідно до компетенції – здійснення заходів з підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони);
- на Державну службу спеціального зв'язку та захисту інформації України – формування та реалізація державної політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту критичної інформаційної інфраструктури, державний контроль у цих сферах;
- на Службу безпеки України – попередження, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, які вчиняються у кіберпросторі; здійснення контррозвідувальних та оперативно-розшукових заходів, спрямованих на боротьбу з кібертероризмом та кібершпигунством, а також щодо готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів;
- на Національну поліцію України – забезпечення захисту прав і свобод людини та громадянина, інтересів суспільства і держави від злочинних посягань у кіберпросторі; запобігання, виявлення, припинення та розкриття кіберзлочинів; підвищення поінформованості громадян про безпеку в кіберпросторі;
- на Національний банк України – формування вимог щодо кіберзахисту критичної інформаційної інфраструктури у банківській сфері;
- на розвідувальні органи України – здійснення розвідувальної діяльності щодо загроз національній безпеці України у кіберпросторі, інших подій і обставин, що стосуються сфери кібербезпеки.

Стратегією передбачено, що держава сприятиме залученню наукових установ, навчальних закладів, організацій, громадських об’єднань і громадян до розробки та реалізації заходів із кібербезпеки і кіберзахисту.

Тобто, на зазначені суб’єкти покладені права щодо розробки, впровадження, підтримки та вдосконалення Стратегії кібербезпки у рамках їх основних повноважень. Аналізуючи положення документу варто вказати, що ці установи будуть одночасно і об’єктами і суб’єктами кібербезпеки, оскільки з одного боку вони будуть однією із ланок, що гарантує дотримання цієї стратегії, а з іншого – самі будуть знаходитись під впливом решти організацій.

5) Напрями забезпечення кібербезпеки.

Попередньо визначено чотири основних напрямки, на яких на теперішньому етапі буде сфокусовано увага у площині кібербезпеки:

- розвиток безпечного, стабільного і надійного кіберпростору;

- кіберзахист державних електронних інформаційних ресурсів та інформаційної інфраструктури, призначеної для обробки інформації, вимога щодо захисту якої встановлена законом;
- кіберзахист критичної інфраструктури;
- розвиток потенціалу сектору безпеки і оборони у сфері забезпечення кібербезпеки передбачатиме здійснення в установленому порядку.

Тобто визначені напрямки є пріоритетними у впроваджені концепції кібербезпеки. Проте ефективність залежить від упровадження комплексної координації правоохоронних органів щодо боротьби з кіберзлочинністю та підготовка суддів, слідчих та прокурорів для роботи з доказами, що стосуються злочину, отриманими в електронній формі, з урахуванням особливостей кіберзлочинів.

6) Різновиди кіберзлочинів

Кіберзлочинність – незаконні дії, які здійснюються людьми, що використовують інформаційні технології для злочинних цілей.

Серед основних видів кіберзлочинності виділяють поширення шкідливих програм, злом паролів, крадіжку номерів кредитних карт і інших банківських реквізитів, а також поширення протиправної інформації через Інтернет.

Класифікація кіберзлочинів:

1) правопорушення проти конфіденційності, цілісності і доступності комп'ютерних даних і систем, зокрема:

2) правопорушення, пов'язані з комп'ютерами, включаючи підробку і шахрайство, вчинені з використанням комп'ютерів;

3) правопорушення, пов'язані зі змістом інформації, зокрема, дитяча порнографія, расизм і ксенофобія;

4) правопорушення, пов'язані з порушенням авторських та суміжних прав, наприклад незаконне відтворення і використання комп'ютерних програм, аудіо/відео та інших видів цифрової продукції, а також баз даних і книг.

Кіберзлочинність – незаконні дії, які здійснюються людьми, що використовують інформаційні технології для злочинних цілей.

Серед основних видів кіберзлочинності виділяють поширення шкідливих програм, злом паролів, крадіжку номерів кредитних карт і інших банківських реквізитів, а також поширення протиправної інформації через Інтернет.

З 1991 за класифікатором Інтерполу інформаційні злочини поділяються на:

- несанкціонований доступ та перехоплення;
- зміна комп'ютерних даних;

- комп’ютерне шахрайство;
- незаконне копіювання;
- комп’ютерний саботаж;
- інші комп’ютерні злочини.

В Україні у законодавстві немає подібних класифікацій, лише у КК є розділ про «Злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку».