Гавриш О.С.
викладач кафедри економічної та інформаційної безпеки
Дніпропетровського державного університету внутрішніх справ

Останнім часом все більше зростає питання захисту програмного забезпечення від зломів. Регулярно з'являються повідомлення про великі витоки даних за підсумками кібератак. У минулому році говорили про кібервикрадення 80 млн. доларів з банку в Бангладеш. Також великою історією стали два витоки даних у Yahoo, що ледь не призвело до зриву продажу Yahoo.

Це тільки деякі прояви діяльності чорного хакерського ринку, на якому продаються викрадені цифрові продукти. У міру поширення цифрових технологій в повсякденному житті проблема буде тільки рости. Якщо раніше в основному крали електронні гроші з електронних рахунків, то тепер до мережі підключається величезна кількість пристроїв, аж до автомобілів. Для хакерів тут відкриваються нові можливості.

Звичайно, противагою цьому може бути зустрічний процес - технологічне вдосконалення захистів. Проблема в тому, що виробники погано мотивовані до впровадження такого роду удосконалень. Вони більше зацікавлені в розробці нових продуктів, що означає більшу кількість коду, що потребує ретельного тестування. В середньому кожен новий програмний продукт налічує 14 вразливостей. Кожна з вразливостей може бути використана для нелегального доступу.

Сучасний комп'ютер, являє собою комбінацію компонентів, що походять з різних джерел - починаючи з комплектуючих і операційних систем і закінчуючи додатками. Кожен з компонентів може містити в собі несправності (допущені помилково або навмисно), які в сукупності створюють вразливість.

Вразливість виникає з основ, на яких стоять інформаційні технології, з культури розробки програмного забезпечення, а також із суперечливих інтересів урядів. Однак зараз бурхливий розвиток кіберзлочинності починає змушувати компанії, уряди і наукові інститути до дій.

Основні тези кібербезпеки сьогодення :

Сучасним атакам практично не можна запобігти, тому зараз не менше зусиль потрібно направляти на підготовку команд реагування на інциденти.

Кіберзлочинці - це не одинаки, це добре підготовлені, добре мотивовані і добре фінансовані організації.

Вся інформація, яку ви знаєте про свою мережу і техніку - ніщо, якщо ви не знаєте, хто вам протистоїть. Тому вам потрібно встати на місце хакера і зрозуміти, що йому може бути цікаво в вашій компанії і як він може це отримати.

Головне порушення кібербезпеки сьогодні - це відсутність комплексного підходу (люди, системи, процеси), ігнорування питань кібербезпеки з боку CEO, зайва впевненість у безпеці.

Раніше зловмисники атакували для шантажу або заволодіння грошовими коштами, сьогодні це використання інфраструктури жертви для атаки на третіх осіб, маніпулювання виборами або техногенні катастрофи.

Кібербезпеку неможливо купити - її можна тільки побудувати.

Всі погоджуються, що актуальність кібератак зростає. До 2007 року кібербезпека фінансувалася за залишковим принципом, тепер ми переходимо в стадію кіберстійкості. Зараз найбільш просунуті програми впроваджують ген кібербезпеки в кожен процес і пристрій, адже навіть кавоварка може бути використана для кібератак.

Кіберризиків як таких не існує - всі вони пов'язані з ризиками втрати грошей, техногенної безпеки тощо. Обсяг світового ринку кібербезпеки за підсумками 2017 року сягне $ 120 млрд. За останні 13 років він виріс в 35 разів.

Література:

1. Проблеми кіберзлочинності [Електронний ресурс]. – Режим доступу: http://kontinentusa.com/kiberbezopasnost-problemy
2. Системный инженер Cisco[Електронний ресурс]. – Режим доступу:https://delo.ua/tech/10-vazhnyh-tezisov-dlja-kiberbezopasnosti-329632/?supdated_new=1510515414

Державне управління у сфері забезпечення кібернетичної безпеки в Україні

Гончаров М.В.
магістр Донецького юридичного інституту МВС України

Необхідною умовою розвитку інформаційного суспільства є високий рівень кібербезпеки. Саме тому ефективне державне управління інформаційними ресурсами є важливою умовою забезпечення кібернетичної безпеки та реалізації виваженої державної політики у сфері інформатизації.

Таким чином, потребує подальшого розвитку механізм захисту приватного життя особи при користуванні кіберпростором, при автоматизованій обробці персональних даних.

Глобальний кіберпростір усе більшою мірою розглядається всіма державами світу як один із найважливіших безпекових пріоритетів, оскільки його, функціонування стає визначальним чинником розвитку економіки, військового, соціального та інших секторів [1, с. 119].

Різке падіння державного управління у сфері забезпечення кібернетичної безпеки в Україні, наслідком чого може стати повна залежність економіки, армії, населення від допомоги та прихильності сильних цього світу держав. Країна, яка не береже й не підтримує кіберпростір своє держави, потрапляє у васальну залежність від науки та економіки інших країн і втрачає здатність більш менш самостійно гарантувати свою безпеку. Тому одним із головних пріоритетів діяльності державної влади в Україні має стати кібернетична безпека в країні.

Причому починати слід з системи державного управління, що забезпечує цілеспрямованість державної політики в цій галузі.

Державне управління – цілеспрямований владно-організуючий вплив у межах права відповідних органів і їх посадових осіб на регулювання, контролювання і координацію відносин, що складаються в ході виконання функцій держави.

Малиновський В.Я. вважає, що державне управління – це вид діяльності держави, суттю якого є здійснення управлінського організуючого впливу з використанням повноважень виконавчої влади через організацію виконання законів, здійснення управлінських функцій з метою комплексного соціально-економічного та культурного розвитку держави, її окремих територій, а також забезпечення реалізації державної політики у відповідних сферах суспільного життя, створення умов для реалізації громадянами їх прав і свобод, надання державних послуг громадянам [2, с. 161].

Ключовим елементом до забезпечення безпеки країни та захисту персональних даних громадян є високий рівень кібербезпеки.

На даний час ми змушені говорити про відставання нашої держави від світових показників. Для зміни цієї тенденції необхідно проводити реформи у законодавчій сфері щодо забезпечення кібернетичної безпеки в Україні

Як свідчить зарубіжний досвід, процеси реформування сектору безпеки з метою вдосконалення державного управління системою кібернетичної безпеки передбачають активізацію діяльності держави за такими напрямами: розробка та затвердження нормативних документів, переважно стратегій, положення яких визначають напрямки діяльності держави у сфері забезпечення кібернетичної безпеки; безпосереднє реформування системи управління сектором безпеки, що передбачає створення спеціалізованих підрозділів, управлінських структур з метою оперативної протидії кіберзагрозам; збільшення чисельності підрозділів, задіяних у системі гарантування кіберзахисту; проведення роз'яснювальної роботи серед населення щодо визначення реальних та потенційних кіберзагроз; сприяння розвитку міжнародного співробітництва у сфері забезпечення транснаціональної кібернетичної безпеки.

Аналіз законодавства більшість держав світу дозволяє робити висновок, що більшість з них мають фундаментальні акти законодавства - національні стратегії забезпечення кібербезпеки, положення яких визначають середньо- та довгострокові пріоритети діяльності уряду країни щодо розбудови системи захисту кіберпростору, деталізують завдання державних органів у вказаній сфері, визначають повноваження спеціальних підрозділів у складі військових формувань, які є відповідальними за гарантування захисту національного кіберпростору.

Слушно вказує О. Баранов, що практично всі національні стратегії щодо забезпечення кібербезпеки і переважна більшість експертів пов`язують проблематику кібербезпеки саме з використанням у процесі людської діяльності комп'ютерних систем і телекомунікаційних мереж (до останніх належить і мережа Інтернет) [3, с. 57].

Проте ще й досі Україна остаточно не визначилася із національною стратегією забезпечення кібернетичної безпеки, а міжнародні стандарти у сфері гарантування кібернетичної безпеки, на жаль, не впроваджені в національне законодавство.

Побудова дієвої системи забезпечення кібернетичної безпеки вимагає від державних органів України чіткого визначення державної політики у цій сфері та випереджального реагування на динамічні зміни, що відбуваються у світі в сфері забезпечення кібернетичної безпеки [4].

Отже, ефективне державне управління у сфері забезпечення кібернетичної безпеки в Україні є необхідною умовою розвитку інформаційного суспільства. Тому, розбудова дієвої системи кібернетичної безпеки є однією з найнагальніших завдань забезпечення національної безпеки України.

Література:

1. Дубов Д. В. Стратегічні аспекти кібербезпеки в Україні / Д. В. Дубов // Стратегічні пріоритети № 4(29). – 2013. – С. 119.
2. . Малиновський В. Я. Державне управління: Навчальний посібник. – 3-тє вид., переробл. та допов. – К.: Атіка, 2009. – 608 с.
3. Баранов О. А. Про тлумачення та визначення поняття «кібербезпека» / О. А. Баранов // Правова інформатика. – 2014. - №2 (42). – С.54- 62.
4. Лук`янчук Р. В. Державне управління кібернетичною безпекою: шляхи вдосконалення в сучасних умовах / Р. В. Лук`янчук // Електронне наукове фахове видання «Державне управління: удосконалення та розвиток» [Електронний ресурс]. – Режим доступу: http://www.dy.nayka.com.ua/?op=1&z=893

Інформаційна безпека дитини та її забезпечення Національною поліцією України

Дручек О.М.
аспірант кафедри адміністративного
права та адміністративного процесу,ОДУВС
Науковий керівник: Коропатов О.М.
кандидат юридичних наук, доцент
професор кафедри адміністративного права та адміністративного процесу ОДУВС

Глобальною світовою тенденцією сьогоденняє розширення та поглиблення розвитку інформаційної складової життєдіяльності людини і суспільства. Інформація стає ефективним інструментом керуючого впливу на соціальні системи та індивідів за схемою «керуючий вплив – бажаний результат», і саме цим визначається її важливість як чинника формування безпечного середовища у сфері суспільних відносин. Тому однією із складових поняття безпеки у широкому розумінні наразі визнається інформаційна (кібер-) безпека – стан захищеності життєво важливих інтересів людини і громадянина, суспільства і держави, при якому запобігається завдання шкоди через неповноту, несвоєчасність та недостовірність поширюваної інформації, порушення цілісності та доступності інформації, несанкціонований обіг інформації з обмеженим доступом, а також через негативний інформаційно-психологічний вплив та умисне спричинення негативних наслідків застосування інформаційних технологій.

В Указі Президента України «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»» [1] йдеться про те, що кіберзлочинність стає транснаціональною та здатна завдати значної шкоди інтересам особи, суспільства і держави, а також про поширення в Україні випадків незаконного збирання, зберігання, використання, знищення, поширення, персональних даних, незаконних фінансових операцій, крадіжок та шахрайства у мережі Інтернет. Зазначеним нормативно-правовим актом виконання завдання забезпечення інформаційної безпеки покладається на систему державних органів, серед яких – Національна поліція України. Завданнями Національної поліції у цій сфері, зокрема, є: 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.

Особливо небезпечним інформаційний простір може стати для дітей, оскільки певні ресурси інтернету містять інформацію агресивного, жорстокого, аморального чи соціально небезпечного змісту, а надання переваги віртуального світу перед реальним справляє негативний вплив на психіку, фізичне і моральне здоров’я дитини, сприяє формуванню девіантної поведінки. Почасти підлітки, через вікові особливості психології та фізіології, поводяться у Мережі віктимно, навмисно провокуючи стосовно себе вчинення протиправних чи злочинних дій. Спеціалісти відзначають, що може йтися про встановлення незаконного контакту (грумінгу) зловмисника і дитини із метою подальших злочинних