МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
РІВНЕНСЬКИЙ ДЕРЖАВНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ
КАФЕДРА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА МОДЕЛЮВАННЯ

Кіндрат П.В.

О С Н О В И К І Б Е Р Б Е З П Е К И

конспект лекцій

Рівне 2025

Затверджено на засіданні кафедри інформаційних технологій та моделювання
Протокол від «29» квітня 2025 року № 5

Схвалено навчально-методичною комісією факультету математики та інформатики
Протокол від «30» квітня 2025 року № 4

Рецензент:
Бойчура М.В. к.т.н., доцент.

Кіндрат П.В. Основи кібербезпеки: конспект лекцій [Електронний ресурс] Рівненський державний гуманітарний університет. Рівне. 2025. 119 с.

Конспект лекцій орієнтований на допомогу в отриманні та засвоєнні знань з курсу «Основи кібербезпеки» студентам спеціальностей 121 «Інженерія програмного забезпечення» та 122 «Комп'ютерні науки». Схема конспекту акцентує увагу студентів на закріпленні основних фахових знань, формуванні відповідних умінь і в цілому отриманні ними кваліфікаційних компетентностей.

ЗМІСТ

ЛЕКЦІЯ 1 ПОНЯТТЯ КІБЕРБЕЗПЕКИ ТА КІБЕРЗАГРОЗ

1.1 Кібербезпека як складова міжнародної, регіональної та національної безпеки

Поступовий перехід у розвитку людської формації "інформаційного суспільства" до "високотехнологічного суспільства" обумовлює еволюцію підходів до забезпечення безпеки у нових умовах на різних рівнях. Відбувається поступова трансформація концепції інформаційної безпеки громадянина, суспільства, держави до необхідності її доповнення новою концепцією – кібербезпека.

Виходячи з дефініції "кібернетична безпека", єдиною й об'єднуючою ознакою в усі епохи розвитку людської цивілізації, яка однозначно характеризуєявища та факти пов'язані з проблематикою її забезпечення, є безумовно ознака, яка визначає наявність систем та процесів управління. Виокремлення кібербезпеки в окремий вид безпеки сталося порівняно недавно. Вперше у світі в 1996 р. у військовій доктрині США "Concept Force XXI" на законодавчому рівні визнано необхідність захисту кіберпростору.

З урахуванням того, що проблема кібербезпеки носить глобальний характер, важливою є позиція міжнародних організацій. Так, Міжнародний союз електрозв'язку (ITU) визначає, що **кібербезпека** – це набір засобів, стратегії, принципи забезпечення безпеки, гарантії безпеки, керівні принципи, підходи до управління ризиками, дії, професійна підготовка, практичний досвід, страхування і технології, які можуть бути використані для захисту кіберсередовища, ресурсів організації та користувача. Загальні завдання безпеки у кіберсередовищі включають забезпечення ***доступності, цілісності, конфіденційності*** інформації. Глобальна програма включає п'ять стратегічних напрямів та сім стратегічних цілей, що їх слід враховувати при створенні системи кібероборони, причому вимога щодо уніфікації глобального законодавства у сфері кібербезпеки розглядається як головна стратегічна ціль.

За поглядами американських військових фахівців до цього часу **кібербезпека США** розглядалася як комплекс заходів, спрямованих на захист комп'ютерів, електронних даних і мереж їх передачі від несанкціонованого доступу (конфіденційність), та інших дій, пов'язаних з маніпулюванням або крадіжкою, блокуванням (доступність), псуванням (спотворення), руйнуванням і знищенням (цілісність) умисного і випадкового характеру. Згідно зі Словником, виданого у січні 2019 року **кібербезпека** (безпека кіберпростору) – це дії, вжиті в захищеному кіберпросторі для запобігання несанкціонованому доступу, експлуатації або пошкодженню комп'ютерів, електронних систем зв'язку та інших інформаційних технологій, включаючи інформаційні технології платформи, а також інформацію, що міститься в ній, для забезпечення її ***доступності, цілісності***, аутентифікації, ***конфіденційності*** і неспростовності. Зазначений приклад наданий з метою підтвердження зміни базового термінологічного апарату МО США в сфері кібербезпеки на 25-30%, що свідчить про гнучкість термінологічної системи сфери кібербезпеки США. Українське ж законодавство комплекс цих заходів однозначно визначає як - технічний захист інформації (ТЗІ).

В Україні термін "кібербезпека" вперше використано у 2007 році , але лише в контексті необхідності "розробки та впровадження національних стандартів та технічних регламентів застосування інформаційно- комунікаційних технологій, гармонізованих з відповідними європейськими стандартами, у тому числі згідно з вимогами ратифікованої Верховною Радою України Конвенції про кіберзлочинність". З 2016 року кібербезпека України визначається як стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі. Відповідно до Закону України , **кібербезпека** – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.

При цьому має місце процес розмежування різних видів безпеки за геополітичними рівнями та усвідомлення ролі кібербезпеки на кожному з них. Необхідність такого усвідомлення ролі кібербезпеки покликана, в першу чергу, активізацією міжнародних

терористичних, екстремістських організацій та злочинних угруповань, окремих держав, які здійснюють кібервпливи на громадян, суспільство, держави з метою реалізації своїх інтересів. Тому, забезпечення кібербезпеки на міжнародному, регіональному та національному рівнях є однією з найважливіших складових системи забезпечення національноїбезпеки для будь-якої держави.

Трансформація суспільства та глобалізація світових процесів фундаментально впливає на всі геополітичні рівні безпеки – міжнародний, регіональний та національний. Після першого прообразу кібервійни, яка відбулася в Естонії у квітні 2007 р., провідні країни світу в системі безпеки суттєвого значення стали надавати кіберкомпоненті.

За допомогою такої компоненти "невідомий і невидимий противник" у будь-який час з будь-якої точки світу має можливість здійснення кібервпливів через кіберпростір на фізичне, матеріальне та ідеологічне становище будь-якої країни або групи країн. Тому, усвідомлення ролі і місця кібербезпеки та реальності кіберзагроз для безпеки на усіх рівнях поступово відбувається у більшості країн світу.

На міжнародному рівні кібербезпека є транснаціональною задачею. Вона не може забезпечуватися однією державою або групою держав. Це задача усіх цивілізованих країн. Тільки сумісні зусилля з питань забезпечення кібербезпеки матимуть інтегральний ефект та сприятимуть підвищенню рівня міжнародної безпеки в кіберсфері, як окремо взятої держави, так і світового співтовариства в цілому. Досягнення такої мети потребує пошуку нових шляхів побудови такої системи міжнародних інститутів, механізмів, заходів і гарантій, які у своїй сукупності мінімізуватимуть ймовірність реалізації кіберзагроз та нейтралізуватимуть їх.

Кібербезпека на міжнародному рівні формується на основі національних стратегій кібербезпеки окремих держав, регіональної (субрегіональної) безпеки груп держав і регіонів світу та інтегрується до рівня глобальної міжнародної кібербезпеки, коли мова йде про кіберзахист і реалізацію загальнолюдських інтересів від загроз планетарного характеру, які за своїми масштабами і наслідками виходять за національні межі держав і здатні впливати на безпеку людства.

Кібербезпека на регіональному рівні визначається в рамках якої-небудь частини країни, її окремих адміністративно-територіальних одиниць, стосовно декількох сусідніх районів, областей тієї або іншої держави, у масштабі групи країн, що входять до певної географічної зони. До особливостей забезпечення кібербезпеки на регіональному рівні належать: її обмеженість певною територією зі своїми неоднаковими природно-географічними, соціально- економічними, культурно-історичними й іншими умовами життєдіяльності; специфічність інтересів, що склалися саме в даному життєвому середовищі соціально-територіальної спільності людей; зміст і форми прояву суперечностей між цією спільністю і центром, іншими регіонами, світовоюспільнотою.

На регіональному рівні кібербезпека реалізується на основі низки принципів, до яких належать: територіальна організація кіберзахисту населення, місця існування та об'єктів з критичною інформаційноюінфраструктурою; інтегральний комплексний підхід до створення системи кібербезпеки в регіоні; нероздільність безпеки і стійкого розвитку; безперервність зусиль, включаючи організацію постійного спостереження і контролю за станом захищеності суспільства, природного середовища і потенційно небезпечних об'єктів від цілеспрямованого кібервпливу тощо.

Кібербезпека окремо взятого регіону не може бути достатньою мірою забезпечена поза рамками систем кібербезпеки більш високого рівня. Але слід зазначити, що саме на регіональному рівні закладаються фундаментальні основи кібербезпеки міждержавних утворень, націй і народів, їх стійкого та стабільного розвитку.

Інколи, коли мова йде про кібербезпеку у масштабах кількох географічно близьких країн регіону, кібербезпека регіонального рівня трансформується у кібербезпеку субрегіонального рівня.

1.2. Кіберінциденти: історичний огляд (передумови скоєння та наслідки)

Еволюція кібератак, яка спостерігається за останні кілька років, показує, що докорінно

змінюються не тільки суб'єкти та об'єкти кібервпливу, а змінюються й їх цілі та мета – від примітивних кібератак на компанію конкурента, до міждержавного протистояння у кіберпросторі. Кардинальні зміни, що обумовлені найбільш відомими інцидентами останніх років у кіберпросторі та навколо нього, ставлять перед воєнним та політичним керівництвом провідних країн світу нетривіальні задачі, ефективність знаходження розв'язання яких визначатиме найближчі перспективи розвитку людської цивілізації. Кіберпростір та пов'язані з ним нові виклики та загрози, що спричинили виникненню нової сфери протиборства з метою вироблення єдиної стратегії протидії, потребують ґрунтовного аналізу найвідоміших кіберінцидентів, що мали місце за останні роки. Серед таких кіберінцидентів, які позначилися на розвитку порядку денного подій в усьому світі, за оцінками фахівців, стали ті, що відбулися в Естонії у травні 2007 р., в Грузії у серпні2008 р., в Ірані в липні 2010 р., у Франції в грудні 2010 р., у М'янмі (Бірмі) в 2010 р., у Бельгії в березні 2011 р., на Близькому Сході в 2012 р., в Україні у 2014 та 2017 р. Але перед тим, як дослідити передумови скоєння даних кіберінцидентів та наслідків, до яких вони призвели, доцільно встановити початок ери кіберінцидентів в комп'ютерних мережах.

Кібератаки проти Естонії (2007) – перші відомі масовані кібератаки спрямовані проти національної безпеки країни. Кібератаки відбувались в декілька хвиль на тлі розхитування російськими спецслужбами суспільно- політичної ситуації в країні під приводом "протестів" "проти" перенесення пам'ятника "Бронзовий солдат" у Таллінні. Пік атак припав на 9 травня 2007 року. Зловмисникам вдалось вчинити "дефейс" деяких сайтів, урядові та банківські сервери і служби були виведені з ладу внаслідок масованих атак на відмову в обслуговуванні.

Скоординовані кібератаки на комп'ютерні системи державних установ Естонії почалися 27 квітня 2007 року під час загострення російсько-естонських відносин, пов'язаних з перенесенням пам'ятника Бронзовому солдату у Таллінні. Скоординована атака хакерів вивела на деякий час з ладу сайти парламенту Естонії, міністерств, банківських установ, засобів масової інформації. На думку деяких оглядачів, кібератака на Естонію належала до одних з найкраще організованих та масових в історії Інтернету.

Події розгортались у три хвилі: перші атаки були зареєстровані 28 квітня, наступна, потужніша хвиля була зареєстрована 4 травня, найпотужніша, третя хвиля була зареєстрована 9 травня 2007 року. Інтернет-трафік із закордону зріс вчетверо, що зробило недоступними атаковані сайти. Через атаки до 90% банківських транзакцій в Естонії зазнали проблем в обробці або не змогли бути завершені в нормальному режимі. На піку, створений зловмисниками трафік сягав 100 Мб/с. Для здійснення атак були використані ресурси мережі Storm. Дещо згодом, коли відбувались процеси над учасниками заколотів квітня 2007 року, боти BlackEnergy були використані для атаки на сайт видання delfi.ee.

З початку естонська сторона звинуватила РФ в організації кібератак, однак пізніше міністр оборони країни спростував ці звинувачення за відсутності доказів. Однак, пізніше того ж року, депутат Державної думи Росії Сергій Марков на прес-конференції визнав, що один з його помічників був причетним до організації кібератак. У 2007 році лідер руху "Наші" у Придністров'ї Костянтин Голоскоков визнав причетність цієї організації до атак проти Естонії. У відповідь Естонія проголосила Сергія Маркова і лідера руху "Наші" Василя Якименка персонами "нон ґрата". Оскільки Придністров'я залишається невизнаним жодною країною світу, не існувало можливості притягнути до відповідальності організаторів кібератак з цього регіону.

Кібератаки проти Грузії (2008), які відбувались спільно зі збройною агресією Російської Федерації проти країни. Умовно кібератаки поділені на дві хвилі. Перша хвиля розпочалась 7 серпня 2008 року – за день до початку гарячої фази збройної агресії проти Грузії. Перевага була віддана DDoS-атакам (атакам типу відмови в обслуговуванні) на урядові веб-сайти та засоби масової інформації. Під час другої хвилі вже відбувались дефейси різних сайтів, а також DoS-атаки проти ширшого кола сайтів (великих приватних підприємств тощо).

Кібератака проти Ірану (2010). Кіберінцидент в Ірані з мережним хробаком "Stuxnet" заслуговує на особливу увагу. Різні дослідження висувають різні версії щодо цільового

призначення “Stuxnet”, але щодо передумов виникнення кіберінциденту та наслідків від його реалізації точка зору більшості експертів збігається.

Технічна складність зі створення мережного хробака “Stuxnet” вимагає значних ресурсів, надати під силу які у повному масштабі здатен тільки уряд або декілька зацікавлених урядів розвинених держав. Об’єктом кібернападу даного шкідливого програмного забезпечення є іранські ядерні об’єкти (системи контролю та збору даних (SCADA)), які було виготовлено компанією “Siemens”. Якщо звернути увагу на активізацію діяльності США в кіберпросторі (у 2009 році створено Кіберкомандування США) та врахувати політичну ситуацію на Близькому Сході (бажання Ізраїлю призупинити ядерну загрозу, що надходить від Ірану), то відповідь на питання щодо розробника та замовника даного кіберінциденту є очевидною. Про це свідчать такі факти. По- перше, США є однією з найбільш розвинених держав світу, а відповідно вона й найбільш залежить від якісного функціонування кібернетичних систем різного цільового призначення у різних сферах. По-друге, США здійснює послідовну внутрішню політику щодо створення та нарощування потужності власного Кіберкомандування. Виконання завдань за призначенням таким органом воєнного управління неможливе без розроблення спеціалізованих засобів кібервпливу та кіберзахисту. По-третє, програма під кодовою назвою “Олімпійські ігри ” розроблена в адміністрації попереднього Президента США Д. Буша та підтримана й нарощена адміністрацією Президента Б. Обами передбачає нарощення кількості та технологічної складності кібератак проти Ірану.

Як наслідок, у кінці вересня 2010 року урядом Ірану офіційно визнано, що у програмному забезпеченні системи управління Бушерської атомної електростанції (АЕС) виявлено серйозні збої, які тривали протягом двох діб. У результаті розслідування спеціалістами було встановлено, що шкідливе програмне забезпечення знищило не лише деякі спеціальні дані й пошкодило програмні коди, а й призвело до виникнення передумов для виходу з ладу реального обладнання цього дуже важливого для економіки Ірану енергетичного об’єкта. Наслідки даного кіберінциденту мали суттєвий інформаційно-психологічний вплив на уряди інших держав, у яких розвиваються ядерні програми. Таким чином, світові, на прикладі Ірану, вперше без застосування військової сили та інших засобів врегулювання міжнародних політичних неузгодженостей було продемонстровано уразливість окремої промислової галузі від прихованих кібервпливів.

Кібератаки проти України (2013 - по теперішній час)

На особливу увагу заслуговує низка кіберінцидентів, що почалися в Україні з 2013 року. Перші атаки на інформаційні системи приватних підприємств та державні установи України фіксували ще під час масових протестів у 2013 році. Російсько-український конфлікт став першим конфліктом в кіберпросторі, коли була здійснена успішна атака на енергосистему з виведенням її з ладу. Мали місце атаки проти інформаційної системи “Вибори” під час виборів Президента, численні атаки на відмову обслуговування, дефейси, кібершпигунство тощо.

У лютому 2014 року розпочалась російська збройна агресія проти України, яка велась також і в кіберпросторі. Майбутній директор американського Агентства національної безпеки Майкл Роджерс з цього приводу зазначає, що разом з військовою операцією із захоплення Криму, Росія розпочала проти України кібервійну.

Кіберзагрози Українській державі та суспільству умовно можна поділити на два ключових рівні. Перший – “класичні” кіберзлочини – як абсолютно оригінальні, так і звичайні, для своєї реалізації вони потребують лише сучасних інформаційних технологій.

Другий – злочини, характерні для геополітичної боротьби (або такі злочини на місцевому рівні, які мають потенціал вплинути на політичне становище держави): хактивізм, кібершпигунство та кібердиверсії. Водночас техніки здійснення атак в обох випадках демонструють чимало спільного. Наприклад, фішингові техніки можуть бути використані як для заволодіння коштами громадян, так і з метою кібершпигунства.

Першим масованим випадком хактивізму, з яким зіткнулася Україна, були події довкола закриття файлообмінного сервісу ex.ua. Після спроб правоохоронних органів втрутитися в роботу файлообмінного сервісу було здійснено DDoS-атаки на понад 10

інтернет-сайтів органів державної влади, зокрема, на сайт Президента України та сайт Міністерства внутрішніх справ України. Події довкола ex.ua вперше наочно продемонстрували, наскільки Українська держава не готова ані ідеологічно, ані технічно до подібних атак. Саме відсутність прямих економічних збитків стала причиною того, що реальних висновків тих подій так і не було зроблено, а країна виявилась непідготовленою до ефективного протистояння агресії Російської Федерації в кіберпросторі.

Наступна хвиля хактивізму сталася на тлі політичного протистояння ужовтні 2013 року – лютому 2014 року (події Євромайдану). Це протистояння активно відбувалось у соціальних мережах, де спостерігався значний сплеск зацікавленості проблемою. З першого дня Євромайдану невідомі особи почали масово використовувати нетботи з метою засмічення інформаційного поля, введення людей в оману та поширення чуток. Наприклад, у Twitter, де можна відслідковувати всі події за хештегом #євромайдан, десятки нетботів вкидали різноманітне інфосміття.

Також були використані механізми ускладнення традиційних комунікацій, зокрема мобільного зв'язку (через автоматичні дзвінки на телефони певних активістів чи політиків, що унеможливило використання їхніх мобільних телефонів у роботі).

Після початку збройної агресії Російської Федерації проти України, компанії, що спеціалізуються на наданні послуг кібербезпеки, стали реєструвати зростання кількості кібератак на інформаційні системи в країні. Зазвичай, кібератаки були спрямовані на приховане викрадення важливої інформації, ймовірніше для надання Росії стратегічної переваги на полі бою.Жертвами російських кібератак ставали урядові установи України, країн ЄС, Сполучених Штатів, оборонні відомства, міжнародні та регіональні оборонні та політичні організації, аналітичні центри, засоби масової інформації, дисиденти. З початком російсько-української війни стали з'являтись загони антиукраїнських хактивістів, які йменують себе “Кіберберкутом” та проукраїнська “Кіберсотня Майдану”, “Анонімусами” з російською або українською “пропискою” тощо. Попри складності у визначенні ступеня співпраці хакерських угруповань з державними органами, спираючись на зібрані докази можна стверджувати, що проросійські хакерські угруповання перебувають на території Росії, і що їхня діяльність відбувається на користь

кремлівського режиму.

Можна стверджувати, що з початку Російсько-української війни в середовищі дослідників кібербезпеки поліпшились можливості виявлення, відстеження та захисту від угруповань російських хакерів. Серед можливих пояснень можна навести те, що із загостренням протистояння російським хакерам бракує часу на вчасне оновлення та вдосконалення тактики, технологійта методів діяльності.

Дослідники компанії FireEye виокремили два угруповання російських хакерів, які активно проявили себе у Російсько-українській кібервійні: так звана APT29 (також відома як Cozy Bear, Cozy Duke) та APT28 (також відома як Sofacy Group, Tsar Team, Pawn Storm, Fancy Bear).

В період між 2013 та 2014 роками деякі інформаційні системи урядових установ України були уражені комп'ютерним вірусом, відомим як Snake/Uroborus/Turla. Даний різновид шкідливого програмного забезпечення надзвичайно складний, стійкий до контрзаходів та ймовірно створений в 2005 р. Починаючи з 2013 розпочалась “операція Армагедон” – російська кампанія систематичного кібершпигунства за інформаційними системами урядовихустанов, правоохоронних та оборонних структур. Здобута в такий спосіб інформація ймовірно могла сприяти Росії й на полі бою. Істотним відхиленням від цього правила стала кібердиверсія – атака на “Прикарпаттяобленерго”.

Операція “Змія”

Дослідники британської фірми BAE Systems Applied Intelligence зафіксували в 2013—2014 роках сплеск виявлених випадків зараження інформаційних систем приватних підприємств та державних установ України комп'ютерним хробаком (з руткітом), який вони назвали “Змія” (англ. snake). Дослідники з німецької фірми GData назвали цього хробака “уроборос”, англ. uroborus (також англ. ouroborus – гадюка в грецькій міфології, або англ. sengokuта англ. snark). На думку дослідників обох фірм, цей хробак можливо пов'язаний та

був створений на основі хробака Agent.BTZ, який у 2008 році уразив інформаційні системи Центрального Командування ЗС США.

Пік виявлення атак із використанням хробака "уроборос" збігся з розвитком масових протестів. Протягом січня 2014 року було зафіксовано 22 випадки інфікування інформаційних систем, при цьому протягом 2013 року "уроборос" був виявлений не більше 8 разів. В Україні зловмисники із застосуванням "уроборос" отримували повний доступ до уражених систем. На думку британських експертів, є всі підстави вважати, що за "уроборос" стоять спецслужби Російської Федерації.

Атака на "Вибори"

21 травня 2014 року зловмисники з угруповання КіберБеркут здійснили успішну кібератаку на інформаційну систему "Вибори" Центральної виборчої комісії України. Їм вдалось вивести з ладу ключові мережеві вузли корпоративної мережі та інші компоненти інформаційної системи ЦВК. Майже

20 годин поспіль програмне забезпечення, яке мало показувати поточні результати підрахунку голосів, не працювало як слід. В день виборів, 25 травня,за 12 хвилин до закриття виборчих дільниць (19:48 EET), зловмисники розмістили "картинку Яроша" на серверах ЦВК.

Увечері 25 травня фахівцями CERT-UA було отримано інформацію про те, що на російських телеканалах анонсували новину про нібито виграш Дмитра Яроша на "президентських перегонах". З метою підтвердження цієї інформації на російському ТБ було продемонстровано картинку, яку в мережі вже назвали як "Картинка Яроша". 25 травня, о 20:16:56 було зафіксоване перше звернення

до веб-сайта ЦВК виключно за IP-адресою внутрішнього веб-сервера з вказівкою у GET-запиті повного шляху до картинки "result.jpg" з IP-адреси 195.230.85.129. Ця адреса входить до діапазону IP-адрес телеканалу ОРТ.

В результаті атаки "Перший канал" російського телебачення повідомив своїм глядачам про те, що найбільшу кількість голосів виборців в першому турі на виборах Президента України набрав лідер "Правого сектора" Дмитро Ярош. Про це йшлося у випуску вечірніх новин, присвяченому позачерговим виборам Президента України. Ведуча повідомила, що незважаючи на дані екзит-полів, які свідчать про перемогу Петра Порошенка в першому турі, на сайті ЦВК з'явилася "дивна картинка" (так звана "Картинка Яроша"). За їхньою інформацією, Дмитро Ярош набрав 37,13 % голосів виборців, натомість за фаворита Петра Порошенка проголосувало лише 29,63 %.

Рано вранці наступного дня, 26 травня, сервери системи "Вибори", які приймали та обробляли дані про підрахунок голосів, зазнали розподіленої DoS- атаки, та були недоступні в проміжку між 1-3 годинами ранку.

Окрім інформаційної системи ЦВК, кібератак зазнали інші організації, які мали дуже віддалений зв'язок до виборів, жертвою міг стати сайт, який містив сторінку зі словом "вибори". Однак більшість атак проти таких сайтів відрізнялись низьким рівнем технічної реалізації. Натомість, атака проти ЦВК відрізнялась високою складністю та технологічністю. За словами Миколи Коваля, тогочасного голови CERT-UA, атака на інформаційну систему ЦВК стала однією з найскладніших кібератак, які йому тоді довелось розслідувати.

І хоча відповідальність за атаки взяло на себе угруповання начебто хактивістів КіберБеркут, Микола Коваль припускає, що значна складність атаки може свідчити про те, що за нею стояли підрозділи іншої держави. Також, у мережі ЦВК було виявлене шкідливе програмне забезпечення, яке пов'язують з угрупованням APT28/Sofacy Group.

Опитані американською газетою Christian Science Monitor фахівці з комп'ютерної безпеки назвали атаку на інформаційною систему "Вибори" надзвичайно небезпечною, а також попередженням на майбутнє про уразливість комп'ютерних систем, залучених у виборчий процес. Можливість зриву виборів, або маніпуляція результатами виборів, набула нової ваги під час виборів Президента США 2016 року після успішної кібератаки проти Демократичної партії.

Атака на "Прикарпаттяобленерго"

23 грудня 2015 року сталась перша у світі підтверджена атака, спрямована на

виведення з ладу енергосистеми: російським зловмисникам вдалось успішно атакувати комп'ютерні системи управління в диспетчерській “Прикарпаттяобленерго”, було вимкнено близько 30 підстанцій, близько 230 тисяч мешканців залишались без світла протягом однієї-шести годин. Атака відбувалась із використанням троянської програми BlackEnergy.

Водночас синхронних атак зазнали “Чернівціобленерго” та “Київобленерго”, але з меншими наслідками. За інформацією одного з обленерго, підключення зловмисників до його інформаційних мереж

відбувалося з підмереж глобальної мережі Internet, що належать провайдерам в Російській Федерації.

Загалом кібератака мала комплексний характер та складалась щонайменше з таких складових:

– попереднє зараження мереж за допомогою підроблених листів електронної пошти з використанням методів соціальної інженерії;

– захоплення управління АСДУ з виконанням операцій вимикань на підстанціях;

– виведення з ладу елементів IT інфраструктури (джерела безперебійного живлення, модеми, RTU, комутатори);

– знищення інформації на серверах та робочих станціях (утилітою KillDisk);

– атака на телефонні номери кол-центрів, з метою відмови в обслуговуванні знеструмлених абонентів.

Масштабна хакерська атака, що відбувалась у декілька етапів, розпочалась щонайменше 14 квітня 2017 року з компрометації системи оновлення програми M.E.Doc. Останній етап, з використанням різновиду вірусу Petya, відбувся 27 червня 2017 року, та спричинив порушення роботи українських державних підприємств, установ, банків, медіа тощо. Внаслідок атаки була заблокована діяльність таких підприємств, як аеропорт “Бориспіль”, ЧАЕС, Укртелеком,Укрпошта, Ощадбанк, Укрзалізниця та низка інших великих підприємств.

Жертвою вірусу також стали телеканал “Інтер”, медіахолдинг ТРК “Люкс”, до складу якого входять “24 канал”, “Радіо Люкс FM”, “Радіо Максимум”, різні інтернет-видання, а також сайти Львівської міської ради, Київської міської державної адміністрації. Трансляції передач припинили канали “Першийавтомобільний” та ТРК “Київ”.

28 червня 2017 року Кабінет Міністрів України повідомив, що атака на корпоративні мережі та мережі органів влади була зупинена.

Масштабна деструктивна атака різновидом вірусу Petya (також відомого як NotPetya, Eternal Petya, Petna, ExPetr тощо) стала можливою завдяки компрометації системи оновлення програми M.E.Doc та встановлення прихованого бекдору. Таким чином, масштабною деструктивною атакоюзловмисники закрили собі наявний в них завдяки бекдору доступ до комп'ютерів та комп'ютерних мереж у близько 80% українських підприємств (в тому числі – представництв закордонних компаній). Є підстави вважати, що зловмисники пішли на такий крок оскільки або здобули надійніший доступ до інформаційних систем важливих для них жертв, або ж вважають, що зможуть доволі просто відновити його.

В цих умовах, забезпечення кібербезпеки стає нагальною проблемою не тільки для кожної окремої країни, але й в міжнародному масштабі. Сьогодні у світі діє величезна кількість різних міжнародних програм співробітництва, які тою або іншою мірою стосуються забезпечення кібербезпеки. Їхніми відправними точками стали відповідні міждержавні угоди, конвенції, інші документи ООН та ЄС.

1.3 Загрози у сфері кібербезпеки

1.3.1 Зміст, класифікація та ознаки кіберзагроз

Події, які відбулися в квітні-травні 2007 року в Естонії наочно продемонстрували всьому цивілізованому світові уразливість окремо взятої держави від нового класу загроз для національної безпеки. Характер прояву таких загроз значною мірою був обумовлений абсолютною залежністю практично усіх систем державного управління та приватного сектору Естонії, у тому числі банківських структур, закладів торгівлі, засобів масової інформації тощо від інфокомунікаційних та інших електронних засобів та програмних

продуктів. Різноманітні прояви загроз їх правильному функціонуванню набули нової форми й отримали у сфері національної безпеки назву «кіберзагроз».

Зважаючи на провідну роль та місце інфокомунікацій та різноманітних електронних засобів і програмних продуктів у житті сучасного високотехнологічного суспільства будь-якої розвиненої держави, прийняття практично в усіх країнах курсу на інформатизацію та інтенсифікацію процесів впровадження ІТ-інновацій в усі без виключення сфери життя, очевидним залишається факт того, що кіберзагрози та їх прояви матимуть місце і в майбутньому. Саме тому, при побудові ефективної системи кібербезпеки важливо знати перелік тих загроз, яким вона повинна протистояти. При цьому, процес виявлення кіберзагроз вимагає глибокого аналізу їх сутності з подальшою систематизацією набутих знань. Якщо враховувати ще й те, що кіберзагрози можуть мати найрізноманітніший характер – від підліткового вандалізму до цілком спланованих державних кібероперацій, визріває нагальна потреба у чіткому розмежуванні таких загроз за різними класифікаційними ознаками. У такому разі основну увагу слід акумулювати на тому, що спектр кіберзагроз породжений феноменом кіберпростору є досить обмеженим, а множина їх проявів залишається практично безмежною. Отже, упорядкування можливих кіберзагроз за певними класифікаційними ознаками дозволить забезпечити необхідний рівень достовірності їх ідентифікації та створить передумови для організації ефективної протидії їх проявам.

Відомі підходи до класифікації кіберзагроз в основному зорієнтовані на їх розгляд у площині інформаційних загроз, загроз безпеці інформації, загроз розподіленим системам обробки даних тощо. Тобто основний акцент у таких класифікаціях розставлено на інформаційній складовій загрози, а не на кібернетичній. Ситуація, що склалася обумовлена відсутністю єдиного розуміння сутності дефініції кіберзагрози.

Відповідно до Закону України “Про основні засади забезпечення кібербезпеки України” це визначення має наступне тлумачення.

Кіберзагроза – наявні та потенційно можливі явища і фактори, що створюють небезпеку життєво важливим національним інтересам України укіберпросторі, справляють негативний вплив на стан кібербезпеки держави,кібербезпеку та кіберзахист її об’єктів.

На даний час цією проблематикою займається багато вчених, як в нашій державі, так і за її межами. Наступне визначення більш повно описує це явище, з наукової точки зору.

Кіберзагроза – фактори (події, явища), які мають місце або можуть виникнути в інформаційній, комунікаційній, комп’ютерно-мережній та соціотехнічній складових кіберпростору (або їх комбінації у певному поєднанні), за умови умисного цілеспрямованого або випадкового впливів та створити небезпеку порушення процесів управління і передачі інформації, що відбуваються у кібернетичних системах різних сфер (соціальної, технічної, соціотехнічної), або можуть зашкодити елементам таких систем.

Під ***кібернитичною системою*** (cybernetic system) (за редакцією Глушкова В.М.) будемо розуміти множину взаємопов’язаних об’єктів, які є елементами системи, що здатні сприймати, запам’ятовувати тапереопрацьовувати інформацію, а також здійснювати її обмін.

Виходячи зі сформульованого визначення обов’язковими ознаками будь- якої кіберзагрози є:

– об’єкт, щодо якого може бути реалізована загроза, – носій або виразник того чи іншого інтересу, який підлягає захисту;

– суб’єкт або носій загрози, – іноземна держава, вітчизняні й іноземні організації, групи осіб, самоорганізовані технічні системи тощо, дії (функціонування) яких можуть негативно вплинути на реалізацію інтересів об’єкта у будь-якій сфері;

– методи та способи реалізації загроз – дія чи послідовність узгоджених дій, яка може завдати шкоди інтересам об’єкта, що підлягають захисту;

– причини виникнення кіберзагроз – комплексна ознака, що поєднує у собі наявність відповідних можливостей і намірів суб’єкта загрози та уразливостей об’єктів захисту;

– можливі наслідки або негативні результати, до яких може призвести реалізація загрози – негативні зміни або відсутність позитивних змін у стані об’єкта захисту, що відповідають меті та поставленим цілям суб’єкта загрози.

Впорядкування наданих ознак дозволяє подати їх узагальненою схемою вигляду

рис. 1.1.

Таким чином, будь-якій кіберзагрозі можуть бути поставлені увідповідність притаманні їй ознаки, за якими її можна ідентифікувати, а виявлення сукупності таких ознак або певної їх частини, забезпечить виявлення образу тієї чи іншої загрози та дозволить сформулювати судження про її зміст.

Виявлення кіберзагрози дозволяє у подальшому оцінити її рівень та сформувати пропозиції щодо відповідних заходів нейтралізації та запобігання (якщо загроза ще не реалізується) чи стримування та протидії (якщо реалізація загрози уже відбувається у формі кібервпливу).

Отже, визначення поняття “кіберзагроза” на основі критичного поєднання існуючих тлумачень, дозволяє формулювати основні загрози у сфері кібербезпеки та виявляти ознаки таких загроз, за якими вони можуть бути виявлені.

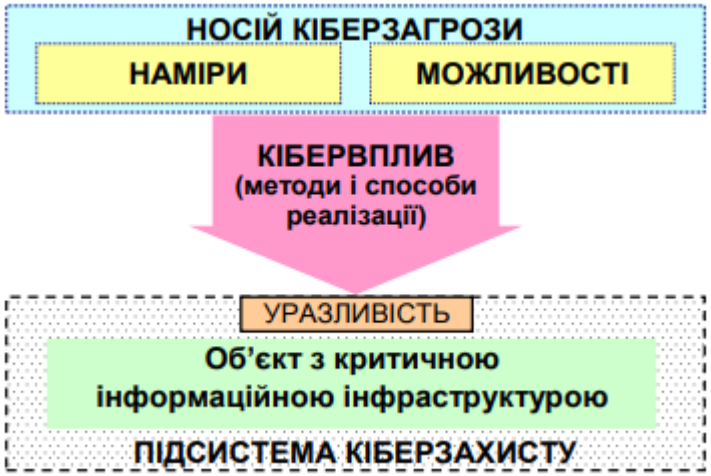


Рис. 1.1. Узагальнена схема ознак кіберзагрози

Відомо, що до складу будь-якої кібернетичної системи входять такі елементи: об’єкт управління, суб’єкт управління та канал передачі даних. Природа усієї системи визначається її призначенням та, зазвичай, є комбінованою. При цьому, природа окремих елементів може бути абсолютно різною: біологічною, технічною або соціальною. Кожен із трьох зазначених вище елементів кібернетичної системи, у свою чергу, може також розглядатися як кібернетична система, але нижчого за ієрархією рівня, але вже така, що складається зі своїх елементів. Особливості процесів управління, які відбуваються у кібернетичній системі, обумовлені специфікою алгоритмів перетворення вхідної дії, яка надходить через рецептори і видозмінюється на виході системи у вихідну дію. Порушення будь-якого з етапів таких алгоритмів може призвести до дезорганізації усього процесу управління та невиконання системою її функцій.

Середовище передавання інформації є однією із найбільш уразливих складових, що забезпечують функціонування кібернетичної системи. Під час передавання інформації вона може перехоплюватися, модифікуватися або взагалі знищуватися. Властивості середовища передачі інформації характеризуються видом фізичного середовища, у якому поширюється інформація, і визначаються при оцінюванні можливості реалізації кіберзагрози тій або іншій системі.

Можливості джерел (суб’єктів) кіберзагрози обумовлені сукупністю способів доступу (проникнення, впливу) до елементів кібернетичної системи, в результаті якого можливе порушення їх функціонування або виведення зі станунормальної роботи.

Спираючись на подане визначення кіберзагрози та враховуючи особливості функціонування комп’ютерних (інформаційних) систем, булазастосована класифікація їх за такими ознаками:

– вид кібернетичної системи (КС), на яку спрямована кіберзагроза;
– елемент КС, на який безпосередньо спрямована реалізація кіберзагроз;
– уразливості (системи та її елементів), що використовуються;

- розташування джерела (суб'єкта) кіберзагроз;
- способ реалізації кіберзагроз;
- середовище поширення;
- умисність;
- походження;
- повторюваність появи;
- прихованість прояву;
- масштаби наслідків від реалізації загрози;
- ієрархія управління, що відбувається у КС;
- доцільність реалізації кіберзагроз;
- час появи кіберзагроз;
- умовність реалізації.

Розглянем кожну ознаку більш детально.

За видом КС (її фізичною природою), на яку спрямовані кіберзагрози,розрізняють:

- технічні;
- біологічні;
- соціальні;
- комбіновані.

Слід зазначити, що вид КС, яка підлягає захисту, обмежує не лише діапазон її потенційних загроз, а й значною мірою можливі заходи протидії таким загрозам. Так, наприклад, при розгляді суто технічних КС, можна знехтувати загрози біологічної або соціальної природи, що дозволить скоротити перелік можливих заходів захисту та протидії.

За елементом КС, на який безпосередньо спрямовані (або через який здійснюється) кіберзагрози, можна виділити такі класи загроз:

- загрози об'єкта управління;
- загрози суб'єкта управління;
- загрози каналу передачі даних;
- комплексні загрози.

Класифікація за такою ознакою як елемент КС, на який спрямована загроза, дозволяє підвищити ефективність протидії за рахунок раціонального використання сил та засобів (ресурсів) захисту. Завчасне зосередження ресурсів захисту на певній складовій КС, щодо якої існує загроза, дозволяє забезпечити необхідний рівень захисту всієї системи із найменшими витратами.

За уразливостями (системи та її елементів), що використовуються, маютьмісце такі загрози:

- загрози, що реалізуються за рахунок уразливостей складових КС;
- загрози, що реалізуються за рахунок використання уразливостей підсистеми захисту КС (за наявності такої підсистеми);
- загрози, що реалізуються із застосуванням недоліків в алгоритмах управління та обробки інформації (сигналів).

Класифікація загроз за уразливістю, що використовується, дозволяєпідвищити точність локалізації небезпеки та мінімізувати витрати на проведення заходів захисту КС.

За розташуванням джерела (суб'єкта) кіберзагроз відносно об'єкта, на який вона спрямована, слід виділяти загрози:

- зовнішні;
- внутрішні.

Об'єкти, з якими взаємодіють КС, що підлягають захисту, виступають джерелом зовнішніх загроз, а складові таких систем – внутрішніх.

Зовнішні кіберзагрози, у свою чергу, поділяються на загрози від середовища функціонування КС та загрози від конкуруючих (протидіючих) систем. До загроз першого підкласу можна віднести стихійні лиха, революції тощо. Прикладом загроз другого підкласу

можуть бути загрози протиборчих сторін одна одній у військовому конфлікті.

Клас внутрішніх кіберзагроз розгалужується з урахуванням складу конкретної КС. Наприклад, для сучасних інформаційно-управляючих систем до внутрішніх кіберзагроз можуть належати загрози від носіїв інформації; технічних засобів; програмних засобів; засобів захисту інформації (апаратних, алгоритмічних, програмних); людини-оператора (обслуговуючого персоналу)тощо.

Завчасне визначення джерела загрози дозволяє застосовувати відносно нього активні (превентивні) заходи протидії.

Спосіб реалізації кіберзагроз залежить від конкретного об'єкта та його особливостей (технічних, соціальних, біологічних, психологічних), але взагальному випадку виділяються:

– загрози, що передбачають активне втручання у процес функціонування КС (активні кіберзагрози);

– загрози, що безпосередньо не впливають на роботу КС (пасивні кіберзагрози);

– загрози із комплексним характером впливу.

За середовищем поширення загрози виділяються класи, що відповідають існуючим небезпечним середовищам:

– інформаційному;

– комунікаційному;

– комп'ютерно-мережному;

– соціотехнічному.

Середовище поширення кіберзагроз не в останню чергу визначає форми та способи протидії таким загрозам. Наприклад, недоцільно (хоча й можливо) застосовувати фізичне знищення комунікаційних каналів для захисту від атаки типу "відмова в обслуговуванні", а від завдання превентивного удару по противнику, що готується до збройної агресії, можна вважати ефективним.

За умисністю загрози бувають:

навмисними;

ненавмисними.

Навмисні загрози передбачають цілеспрямований намір заподіяння шкодиКС або її елементам. Ненавмисні загрози виникають і реалізуються безвідносно до волі носія (джерела) загрози.

За походженням можна виділити загрози:

– штучного походження (антропогенні, техногенні);

– природного походження.

Загрози штучного походження є наслідком діяльності людини або функціонування технічних систем. Загрози ж природного походження виникають внаслідок природних процесів, що відбуваються у живій та неживій природі.

За повторюваністю появи виділяються загрози:

– повторювані (періодичні, аперіодичні);

неповторювані.

Віднесення тієї або іншої загрози до класу повторюваних дозволяє ефективніше протидіяти їй у майбутньому за рахунок формування образу такої загрози та застосування відпрацьованого алгоритму протидії. Неповторювані ж загрози вимагають залучення більш значних ресурсів для їх усунення через необхідність додаткового вивчення та моделювання. Показник повторюваності може бути визначений, наприклад, кількістю випадків появи тієї чи іншої кіберзагрози за деякий проміжок часу.

За прихованістю прояву виділяються:

– приховані;

– неприховані.

Рівень прихованості загроз визначає складність алгоритмів їх ідентифікації, що неодмінно позначається на тривалості виявлення загроз та врешті-решт визначає принципову можливість такого виявлення за допустимийчас.

Реалізація однієї із кіберзагроз наведених класів або їх сукупності може призвести до

наслідків різного масштабу для КС або її елементів. Відповідно й кіберзагрози можна поділити на:

- локальні;
- частковосистемні;
- загальносистемні.

Локальні загрози характеризуються несуттєвим ускладненням роботи окремого елемента КС, що не позначається на функціонуванні КС у цілому.

Загрози частковосистемного характеру призводять до порушення роботи кількох елементів або сегмента КС, що здатне негативно позначитися на виконанні КС частини своїх функції або призначення в цілому з можливістю відновлення ураженого сегмента.

Загальносистемні загрози спрямований на ураження кількох сегментів системи або ключових її елементів, що неодмінно призводить до відмови функціонування КС у цілому без можливості відновлення її роботи.

За ієрархією управління, що відбувається у КС, виділяються кіберзагрози:

– вищого (стратегічного) рівня;
– середнього (оперативного) рівня;
– нижчого (тактичного) рівня.

На вищому (стратегічному) рівні управління приймаються та реалізуються найбільш важливі рішення для КС у цілому. Очевидно, що загрози цього рівня найбільш небезпечні для функціонування КС.

Проміжний (оперативний) рівень забезпечує управління ходом окремих операцій (оперативне управління), а тому є не просто буфером між вищою та нижчою ланками управління, а відіграє вкрай важливу роль у виконанні КС свого призначення. Порушення управління у проміжній ланці здатне призвести до дезорганізації КС, а тому загрози на проміжному рівні управління також становлять небезпеку.

Нижча (тактична) ланка управління, як правило, найбільш чисельна (що дозволяє застосовувати в управлінні дублювання та резервування), тому загрози на цьому рівні не становлять значної небезпеки, а можуть лише вплинути на реалізацію певної часткової функції КС. Проте одночасна реалізація деякої сукупності кіберзагроз відносно критичних елементів на нижчому рівні управління може призвести до синергетичного ефекту, тому безпекою цієї ланки управління КС також не слід нехтувати.

Прийняття рішення про *доцільність реалізації* КЗ можливо за критерієм "ефективність/вартість". Тобто, якщо отриманий від реалізації кіберзагроз ефект перевищує витрати на її підготовку і здійснення, є сенс розглядати можливість такої загрози. В іншому випадку реалізація кіберзагроз недоцільна. Відповідно до цього виділимо такі класи кіберзагроз:

– гіпотетично можливі, але малоймовірні;
– з високою ймовірністю реалізації.

Важливим фактором, що впливає на ймовірність реалізації тієї чи іншої кіберзагрози, є її залежність від певних подій. Тобто реалізація одних кіберзагроз можлива лише за умови, якщо відбудеться відповідна сприятлива подія (або група подій), а реалізація інших не вимагає виконання такої умови.

Відповідно *за умовністю реалізації* виділимо кіберзагрози:

- умовні;
- безумовні.

За часом появи кіберзагрози виділимо:

– загрози, які закладено при створенні КС;
– загрози, які виникають у процесі функціонування КС.

Недосконалості у структурі та конструкції КС або її окремих елементів є уразливими місцями, які потенційно можуть використовуватися для порушення сталої роботи системи. Такі уразливості закладаються під час створення системи або проявляються у процесі її функціонування (для комп'ютерних систем це "загрози нульового дня"). Виявлення закладених при створенні КС уразливостей дозволяє значно підвищити захист таких систем

від кіберзагроз уже на ранніх етапах експлуатації. Уразливості, що проявляються з часом, більш небезпечні, оскільки їх виникнення складно передбачити чи спрогнозувати, а тому протидія загрозам, що використовують такі уразливості, украй складна.

Застосований для класифікації кіберзагроз ознаковий принцип дозволяє описати будь-яку загрозу множиною якісних та кількісних ознак, які можуть бути використані при моделюванні та подальшій ідентифікації такої загрози.

Надана класифікація кіберзагроз передбачає можливість доповнення та розгалуження на підкласи, що досить зручно при розробці переліку загроз для кожної конкретної КС, залежно від рівня необхідної деталізації.

Розглянемо, наприклад, деяку КС, що належить до класу інформаційно- управляючих систем, які на даний час набули найбільшого поширення. Такі системи складаються із інформаційних та програмно-апаратних елементів, а також операторів, що їх експлуатують.

Основними елементами такого класу КС є:

– масиви даних як сукупність інформації та її носіїв;

– технічні засоби, які автоматизують процеси, що відбуваються у системі (засоби обчислювальної техніки, інформаційно-обчислювальні комплекси і мережі, засоби і системи передачі, прийому та обробки інформації та команд, інші виконавчі технічні засоби, засоби і система охоронної та пожежної сигналізації, засоби і система оповіщення і сигналізації, контрольно- вимірювальна апаратура, засоби кондиціонування, електропостачання, зв'язку, оргтехніка тощо);

– програмні засоби (операційні системи, системи управління базами даних тощо);

– засоби захисту інформації (апаратні, алгоритмічні, програмні);

– людина-оператор (обслуговуючий персонал) з усіма притаманними психофізіологічними станами та реакціями.

З огляду на інформацію, яка забезпечує функціонування інформаційно- управляючої системи, запропоновану класифікацію можна розширити і у класі загроз каналу зв'язку (інформації, командам, що передаються) виділитипідкласи:

– за видом інформації, яка передається;

– за видом властивості інформації, що порушується; за метою здійсненнязагрози тощо.

Зважаючи на присутність у контурі управління інформаційно-управляючоїсистеми операторів, можна виділити такі *способи реалізації кіберзагроз*:

– інформаційно-психологічний вплив;

– психогенний вплив;

– психоаналітичний вплив;

– нейролінгвістичний вплив;

– психотронний вплив;

– психотропний вплив.

Якщо розглядати особливості процесів управління та обміну інформацією, які відбуваються у таких системах, то слід зазначити, що на даний момент вони здійснюються згідно з еталонною моделлю взаємодії відкритих систем ISO/OSI,викладеною у стандарті *ISO 7498*. Кіберзагроза як фактор, що впливає на процеси управління та передачі інформації, може бути спроектована на еталонну модель. Тому клас кіберзагроз, який характерний відкритим

системам, можна розширити такими підкласами:

– загрози фізичного рівня;

– загрози канального рівня;

– загрози мережного рівня;

– загрози транспортного рівня;

– загрози сеансового рівня;

– загрози рівня представлення;

– загрози прикладного рівня.

Таким чином, така класифікація кіберзагроз дозволяє вирішувати такіосновні завдання:

– встановлювання основних зв’язків між існуючими та потенційнимикіберзагрозами;

– формування достовірних прогнозів щодо виникнення і розвитку новихзагроз;

– визначення ефективних способів захисту кібернетичних систем та їхскладових від деструктивних кібервпливів та протидії кіберзагрозам;

– забезпечення подальших досліджень впливу кіберзагроз на відповідні об’єкти захисту .

1.3.2 Основні характеристики кіберзагроз

Оцінюючи високий ступінь кіберзагроз для держави, орієнтуючись на провідні держави світу в Україні впродовж останніх років значно інтенсифікується діяльність щодо прийняття та внесення змін до низки нормативно-правових актів, які стосуються кібербезпеки.

– Указом Президента України №287/2015 “Про рішення Ради національної безпеки і оборони України” від 6 травня 2015 року “Про Стратегію національної безпеки України” була затверджена “Стратегія національної безпеки України”. В Стратегії національної безпеки України були визначені актуальні Загрози національній безпеці України, серед яких є загрози інформаційній безпеці, загрози кібербезпеці і безпеці інформаційних ресурсівта загрози безпеці критичної інфраструктури. Відповідно до загроз визначені Основні напрями державної політики національної безпеки України.

– Указом Президента України №96/2016 “Про рішення Ради національної безпеки і оборони України” від 27 січня 2016 року “Про Стратегію кібербезпеки України” була затверджена “Стратегія кібербезпеки України” та визначений робочий орган Ради національної безпеки і оборони України – Національний координаційний центр кібербезпеки. Це документ довгострокового планування, в якому визначаються пріоритети національних інтересів України у сфері кібербезпеки, наявні та потенційно можливі кіберзагрози життєво важливим інтересам людини і громадянина, суспільства та держави в кіберпросторі, пріоритетні напрями, концептуальні підходи до формування та реалізації державної політики щодо безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави,

підвищення ефективності основних суб’єктів забезпечення кібербезпеки, насамперед суб’єктів Сектору безпеки і оборони, щодо виконання завдань у кіберпросторі, а також потреби бюджетного фінансування, достатні для досягнення визначених цілей і виконання передбачених завдань, та основнінапрями використання фінансових ресурсів.

– Указом Президента України №240/2016 “Про рішення Ради національної безпеки і оборони України” від 20 травня 2016 року “Про Стратегічний оборонний бюлетень України” був затверджений “Стратегічний оборонний бюлетень України”. Де на підставі положень Стратегії національної безпеки України, Воєнної доктрини України та Концепції розвитку Сектору безпеки і оборони України визначені стратегічні цілі.

Наприклад. Оперативна ціль 1.5. Удосконалення системи кібербезпеки та захисту інформації. Очікуваний результат: створено в Міністерстві оборони України, інших складових сектору оборони, підрозділи з кіберзахисту, протидії технічним розвідкам, впровадження заходів із захисту інформації відповідно до вимог нормативно-правових актів України та з урахуванням стандартів НАТО і ISO/IEC.

– Закон України “Про основні засади забезпечення кібербезпеки України” від 5 жовтня 2017 року (набув чинності 9 травня 2018 року), в якому визначено правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.

Також зроблено низку змін в інші нормативно-правові акти: “Про Державну службу спеціального зв’язку та захисту інформації України”, “Про захист інформації в інформаційно-телекомунікаційних системах”, “Про оборону України”, “Про засади

внутрішньої і зовнішньої політики", "Про об'єкти підвищеної небезпеки" тощо.

Враховуючи вищезазначене були сформовані основні кіберзагрози у найважливіших сферах та їх характеристики:

– кіберзагрози у сфері державного управління та у сфері управління об'єктами з критичною інформаційною інфраструктурою;

– кіберзагрози в інформаційній безпеці;

– загрози кібертероризму;

– кіберзагрози в енергетичній сфері;

– кіберзагрози у воєнній сфері.

Кіберзагрози у сфері державного управління та у сфері управління об'єктами з критичною інформаційною інфраструктурою. Системі державного управління приділяється ключова роль в управлінні державою. Це визначається тим, що державне управління, з одного боку, є конкретним специфічним видом управлінської діяльності державними інститутами зі своєю компетентнісною та функціональною специфікою, яка суттєво відрізняє його

від інших видів управлінської діяльності. З іншого боку, державне управління є прерогативою спеціальних суб'єктів управління – органів державного управління, які згідно зі своїм функціональним призначенням здійснюють управління державними процесами у межах свої компетенції. Важливо також відзначити дві обставини. Перша: системі державного управління властива ієрархічна структура, яка визначається прийнятою у тій чи іншій державі технологією побудови вертикалі влади. Друга: для системи державного управління зберігаються усі базові принципи управління, прийняті в теорії управління.

Навіть поверхневий аналіз сфери державного управління у таких провідних країн світу як США, Китай, ФРН та ін. показує, що система державного управління, незалежно від територіального розміщення держави, прийнятої у ній політичної ідеології та інших особливостей державного устрою, охоплює такі основні складові елементи, як:

– суб'єкти державного управління (органи виконавчої влади);

– об'єкти державного управління (усі сфери життєзабезпечення суспільства та держави, у тому числі й об'єкти з критичною інформаційною інфраструктурою, що перебувають в компетенції управління держави);

– процеси управління державою (суспільні відносини, що виступають регулятором прямих та зворотних зв'язків між суб'єктами та об'єктами управління).

Зважаючи на наявність у системі державного управління типових ознак кібернетичної системи, таких як суб'єктів управління, об'єктів управління та середовища для обміну процесами управління у подальшому її декомпозицію здійснюватимемо саме з позицій кібернетичної системи.

У широкому розумінні під кіберзагрозами у сфері державного управління та у сфері управління об'єктами з критичною інформаційною інфраструктурою розуміються потенційно можливі кібервпливи природного, технічного або антропогенного характеру, які можуть спричинити небажані наслідки для суб'єктів і об'єктів системи та процесів управління нею. Виникнення будь-якої кіберзагрози у сфері державного управління характеризується наявністю уразливості у системі державного управління. Чим більше уразливостей має система державного управління, тим більша кількість кіберзагроз їй загрожує. Зважаючи на те, що усі кіберзагрози не можуть бути піддані повному описові, розглянемо головні з них.

Головна кіберзагроза у сфері державного управління та у сфері управління об'єктами з критичною інформаційною інфраструктурою для будь-якої держави – це загроза через кібервплив протиборчої сторони на свідомість, підсвідомість, інформаційні ресурси, інфосферу об'єктів з критичною інформаційною інфраструктурою держави нав'язати людині, суспільству й державі бажану (для іншої сторони) систему цінностей, поглядів, інтересів і рішень у сфері державного управління та управління об'єктами з критичною інформаційною інфраструктурою, керувати їх поведінкою і розвитком у бажаному для іншої сторони напрямі. Тому очевидним є факт того, що держави

з вищим ступенем економічного, політичного, соціального та інших рівнів розвитку намагаються через сферу державного управління інших держав з нижчим рівнем керувати їх розвитком у своїх інтересах під постійним інформаційним контролем.

При реалізації кіберзагроз у сфері державного управління також переслідується ціль, яка полягає у зміні правлячого режиму шляхом руйнування базових основ системи державного управління. Означена мета досягається не за рахунок руйнування економічного або військового потенціалу держави, а за рахунок реалізації таких кіберзагроз, які здійснюються у вигляді масованого кібервпливу, що як наслідок призводять до змін в морально- психологічному стані її населення та керівництва держави. Кіберзагрози при цьому спрямовуються для вирішення таких цілей:

– створення атмосфери бездуховності та аморальності, негативного відношення до органів державної влади;

– маніпулювання громадською свідомістю і політичною орієнтацією соціальних прошарків населення держави в інтересах створення політичної напруги та хаосу;

– дестабілізація політичних відносин між політичним партіями, громадськими об'єднаннями та рухами з метою провокації конфліктів, розпалювання атмосфери недовіри та підозрілості;

– загострення політичної боротьби, провокування репресій проти опозиції;

– розв'язування у суспільстві громадянської війни;

– зниження рівня керованості органів державної влади і органів управління з метою утруднення прийняття важливих державних рішень;

– дезінформація населення про роботу органів державної влади, підрив їх авторитету, дискредитація органів управління;

– провокування соціальних, політичних, національних і релігійних сутичок;

– ініціювання страйків, масових безладів й інших акцій економічного протесту;

– підрив міжнародного авторитету держави, його співпраці з іншими державами;

– нанесення втрат життєво важливим інтересам держави в політичній, економічній, оборонній, інформаційній, науково-технологічній та інших сферах.

Досвід більшості держав, де відбулись так звані "кольорові революції", свідчить про те, що такі держави не були у змозі не тільки протистояти негативним кібервпливам, але й виявляти сам факт такої агресії. Такий стан справ можна пояснити тим, що оперативність і якість управлінських рішень напряму залежать від повноти та достовірності вхідної та вихідної інформації, викривлення та маніпулювання якою є однією з головних задач інформаційної війни.

До джерел загроз кібербезпеці у сфері державного управління та у сфері управління об'єктами з критичною інформаційною інфраструктурою належать:

– руйнування об'єктів з критичною інформаційною інфраструктурою у результаті кібервпливів, що можуть призвести до виникнення техногенних катастроф або спалаху воєнних конфліктів;

– інформаційна ізоляція держави та блокування діяльності системи державного управління у результаті цілеспрямованих кібервпливів іноземних держав, неадекватної зовнішньої та внутрішньої політики у різних сферах;

– діяльність іноземних спецслужб;

– діяльність державних та недержавних політичних та економічних структур, спрямованих проти системи державного управління та об'єктів з критичною інформаційною інфраструктурою;

– недосконаліть систем виявлення кібервпливів та попередження їх наслідків, недостатній рівень кваліфікації персоналу відповідних систем;

– "віртуалізація" процесів державного управління та управління об'єктами з критичною інформаційною інфраструктурою через кіберпростір без приділення належного рівня уваги організації заходів щодо забезпечення їх гарантованої захищеності;

– міжнародний кібертероризм;

– недосконаліть нормативно-правової бази щодо протидії негативним кібервпливам

на системи державного управління та об'єкти з критичною інформаційною інфраструктурою;

– зниження темпів науково-технічного розвитку у результаті неадекватної внутрішньої та зовнішньої політики держави в інформаційній сфері.

До об'єктів загроз кібербезпеці систем державного управління та у сфері управління об'єктами з критичною інформаційною інфраструктурою належать різні управлінські аспекти діяльності системи державного управління, а саме:

– система формування суспільної свідомості через формування у суб'єктів певного менталітету, світогляду, політичних поглядів, моральних цінностей тощо;

– механізми прихованого управління індивідуальною свідомістю та підсвідомістю суб'єктів державного управління, що є потенційними мішенями цілеспрямованого кібервпливу;

– управління об'єктами з критичною інформаційною інфраструктурою, що включають відповідну інфраструктуру (системи накопичення, обробки та аналізу інформації, комутаційні канали, системи та мережі тощо).

Кіберзагрози у сфері державного управління та у сфері управління об'єктами з критичною інформаційною інфраструктурою можутьреалізовуватися за різними напрямами. До основних напрямів реалізації впливукіберзагроз можна віднести такі, як:

– цілеспрямоване використання засобів масової інформації з позицій, що суперечать інтересам системи державного управління;

– маніпулювання інформацією (дезінформація, приховування або спотворення інформації та процесів управління);

o порушення процесів управління за рахунок несанкціонованого доступу сторонніх суб'єктів до процесів прийняття управлінських рішень або необґрунтованого обмеження доступу легальних суб'єктів управлінської діяльності;

– деструктивний вплив на національний сегмент кіберпростору з метою використання його в антидержавних інтересах;

– формування нових "підставних" суб'єктів державного управління з метою реалізації через них кібервпливів деструктивного характеру на систему державного управління та об'єкти з критичною інформаційною інфраструктурою;

– різні види кібервпливів;

– реалізація помилкової (нав'язаної із зовні) економічної та науково- технічної політики у процесі управління державною системою та об'єктами з критичною інформаційною інфраструктурою.

У сфері управління об'єктами з критичною інформаційною інфраструктурою потенційно кіберзагрози можуть бути спрямовані на: інформаційно-телекомунікаційні системи державного управління та приватногосектору, що забезпечують функціонування та безпеку стратегічних інститутів, систем і об'єктів держави (органів центрального та місцевого управління, систем управління енергетикою, транспортом, зв'язком, банківським сектором, підприємств, під час діяльності яких використовуються та (або) виробляються небезпечні речовини тощо) і безпеку громадян (системи управління правоохоронних структур й оборонного сектору тощо), несанкціоноване втручання в роботу яких може загрожувати економічній, екологічній, соціальній та іншим видам безпеки або завдати шкоди міжнародному іміджу держави. До таких об'єктів з критичною інформаційною інфраструктурою можна віднести такі групи об'єктів, як:

– державні електронні інформаційні ресурси;

– автоматизовані системи управління або електронні інформаційні ресурси де обробляється (зберігається) інформація, яка є власністю держави, або інформація, несанкціоновані дії щодо якої можуть створювати загрозу національній безпеці та обороноздатності держави (у тому числі відкрита інформація);

– автоматизовані системи управління, що використовуються суб'єктами воєнної організації держави;

– телекомунікаційні системи загального користування та спеціальні телекомунікаційні

системи;

– автоматизовані системи управління, що здійснюють керування виробничими та (або) технологічними процесами на об’єктах підвищеної небезпеки та інші інформаційно-телекомунікаційні системи та автоматизовані системи управління.

Наслідки впливу кіберзагроз у визначених сферах проявляються на всіх рівнях, оскільки найбільш уразливими об’єктами кібервпливів виступають механізми управлінської діяльності індивідів, що відповідають за формування

їх ментальності, свідомих та підсвідомих сфер мислення та поведінки. На рівні суб’єкта реалізація визначених кіберзагроз призводить до формування викривленого поняття про навколишню дійсність, права, свободи, життєві цінності, державний устрій тощо, що призводить до втрати відчуття самореалізації. Як результат створюються передумови для реалізації кібервпливів деструктивного характеру, ускладнюються соціальні процеси, загострюються протиріччя між різними соціальними прошарками, зростає політична напруженість у суспільстві, знижується ступінь керованості суспільством та державою.

Вплив кіберзагроз на систему державного управління, що регулює процеси, які безпосередньо впливають на безпеку держави, рівень та якість життя населення, як показує світовий досвід, призводить до катастрофічних наслідків і для держави, і для суспільства. Результатом пливу кіберзагроз на систему державного управління є спотворення процесів управління державою таким чином, що унеможливлюються усталені процеси управління державою та об’єктами з критичною інформаційною інфраструктурою. Наслідком порушенням таких процесів може бути втрата державою суверенітету.

Реалізація кіберзагроз має й інші, не менш негативні наслідки. Це наслідки економічного характеру, що охоплюють усю сукупність процесів від втрати керованості державою до повної руйнації її критичної інформаційної інфраструктури. Втрата керованості унеможливлює прийняття найважливіших політичних та економічних рішень. На етапі формування основ державної політики реалізація визначених кіберзагроз призводить до підриву авторитету системи державного управління не тільки у суспільстві, а й на міжнародній арені. Порушення процесів управління у системі державного управління ускладнює контроль та управління об’єктами з критичною інформаційною інфраструктурою. У результаті порушуються баланс у відносинах між суспільством і державою, уповільнюються темпи економічного, соціального та культурного розвитку.

У сфері державного управління та у сфері управління об’єктами з критичною інформаційною інфраструктурою кіберзагрози можуть бути спрямовані на:

– посягання на державний суверенітет держави та її територіальну цілісність, на прояв територіальних претензій з боку інших держав;

– здійснення спроб втручання у внутрішні справи будь-якої держави з боку інших держав;

– провокування воєнно-політичної нестабільності, яка може призвести до розпалювання регіональних та локальних війн;

– створення сприятливих умов для розвідувально-підривної діяльності іноземних спецслужб;

– поширення корупції у системі державного управління, створення умов для налагодження співпраці між бізнесом, політикою й організованою злочинністю;

– поширення кібертероризму та кіберзлочинності;

o несанкціоноване використання об’єктів з критичною інформаційною інфраструктурою з метою вчинення техногенних аварій та катастроф;

– створення сприятливих умов для використання в інтересах протиборчої сторони діяльності військових формувань і правоохоронних органів держави;

– зародження та провокування проявів сепаратизму та екстремізму;

– створення умов для порушення системою державного управління норм діючого законодавства;

– розбалансування системи державного управління внаслідок порушення усталених процесів управління те регулювання державних механізмів;

– формування несприятливих умов, що призводять до критичної залежності системи державного управління та об'єктів з критичною інформаційною інфраструктурою від закордонних високотехнологічних розробок в IT- сфері;

– створення підґрунтя на тлі якого в управлінській діяльності системи державного управління превалюватимуть особистісні інтереси над загальнонаціональними;

– створення передумов для моральної та духовної деградації суспільства;

– зведення до мінімуму ефективності державної інноваційної політики;

– обмеження свободи слова та доступу громадян до інформації;

– поширення засобами масової інформації культу насильства, жорстокості, порнографії;

– розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави;

– маніпулювання суспільною свідомістю шляхом поширення недостовірної, неповної або упередженої інформації;

– провокування інформаційної війни.

1.3.3 Кіберзагрози в інформаційній безпеці

Питанням дослідження впливу проявів кіберзагроз на інформаційну безпеку останнім часом приділяється значна увага наукової спільноти. Це пов'язано не лише з високотехнологічністю суспільства, а й з тими новими викликами та загрозами, що породжуються у інформаційній сфері внаслідок її розвитку. У силу політичного та економічного протистояння держав породжені новими викликами та загрозами проблеми з часом тільки загостюються. Змінюються цілі протистояння, нового обрису набувають об'єкти та суб'єкти впливу. Для прикладу: основною ціллю реалізації кіберзагрози в інформаційній сфері, незалежно від її виду, є здійснення таких кібервпливів, які призводять до управління масовою та індивідуальною свідомістю таким чином, що протиборча сторона (інколи навіть не знаючи про це) діє всупереч власним інтересам. При цьому, суб'єктом впливу кіберзагроз у вузькому сенсі завжди виступає людина та її психіка, а у більш широкому – масова свідомість. Ці кібервпливи, незалежно від того усвідомлювані вони чи ні, призводять до серйозних порушень психічного та фізичного здоров'я, поступового розмивання природних і культурних норм поведінки, до нагнітання соціальної напруженості у суспільстві та виникнення непередбачуваних критичних ситуацій.

Для визначення кіберзагроз в інформаційній сфері та з'ясування джерел їх появи досить важливо правильно вміти виокремлювати об'єкти кібервпливу від суб'єктів кібервпливу. До об'єктів кібервпливу в інформаційній сфері відносяться ті об'єкти, у відношенні яких можуть бути реалізовані кіберзагрози у вигляді кібервпливів, що, як наслідок, призводять до модифікації властивостей таких об'єктів як кібернетичних систем. При цьому, ключовою ознакою об'єкта, що дозволяє розглядати його як об'єкт кібервпливу є наявність у ньому процесів управління. Конкретизуючи такі об'єкти, до них можна віднести такі системи, як: систему соціальних відносин; систему політичних відносин; систему психологічних відносин. Об'єктом кібервпливів в інформаційній сфері може бути також будь-який компонент або сегмент кіберпростору, в якому відбуваються процеси управління. Наприклад, масова та індивідуальна свідомість, соціально-політична система, критична кібернетична інфраструктура, психологічні ресурси (система цінностей, психологічне здоров'я) тощо.

Суб'єктами кібервпливу в інформаційній сфері можуть виступати держави, їх союзницькі утворення і коаліції, міжнародні утворення, незаконні збройні формування, терористичні та екстремістські організації, транснаціональні компанії, різні соціальні мережі, медіа-корпорації, віртуальні коаліції та ін. Головними ознаками, що дозволяють відносити розглядувані утворення до суб'єктів кібервпливу в інформаційній сфері, є такі:

– суб'єкти мають власні цілі та інтереси;

– суб'єкти у своєму складі мають соціальні утворення, що можуть бути використані

для здійснення інформаційно-психологічних впливів;

– суб'єкти спроможні до розробки або розробляють кіберзброю для здійснення інформаційно-психологічного впливу;

– суб'єкти спроможні здійснювати контроль над визначеним сегментом кіберпростору у рамках якого вони спроможні встановлювати регуляторні норми інформаційно-психологічних відносин;

– наявність у суб'єкта спеціальної ідеології (доктрини або стратегії), що передбачає правила його участі в заходах інформаційно-психологічного протиборства.

Встановивши відмінність між суб'єктами та об'єктами впливу в інформаційно-психологічній сфері можна помітити, що кіберзагрози для них можуть спрямовуватися на:

– особистість, суспільство, державу;

– масову свідомість;

– індивідуальну свідомість.

Кіберзагрози для особистості проявляються у двох основних аспектах. Перший аспект проявляється при впливі на особистість, як суб'єкта політичного життя, носія певного світогляду співвимірного з його життєвими

та особистісними ціннісними установками й духовними ідеалами, що володіє правом вираження політичного волевиявлення, і другий – при вивченні особистості як свідомого індивіда, що піддається різним маніпуляціям із застосуванням кібервпливів, що призводять до реалізації загроз щодо втрати ним фізичного та психічного здоров'я.

У першому випадку реалізація кіберзагрози щодо особистості, як суб'єкта політичного життя, призводить до побудови між цим суб'єктом, суспільством та державою такої лінії поведінки, яка набуває рис екстремізму, що загрожують існуванню політичної системи в державі й сприяють утвердженню політичної байдужості суспільства.

У другому випадку – при впливі на особистість, як свідомого індивіда, кіберзагрози проявляють себе як цілеспрямовані довготривалі кібервпливи, що призводять до формування бажаної для зацікавленої сторони морально- психологічної атмосфери, яка сприяє зародженню кіберзлочинності, кібертероризму і, як наслідок, призводить до порушень фізичного та психічного здоров'я. Зважаючи на те, що для конкретного індивіда головними системоутворюючими рисами є цілісність (тенденція до стійкості) та розвиток (тенденція до зміни), то перекручування або руйнування цих рис призводить до припинення його існування, як соціального суб'єкта. Це говорить про те, що вплив кіберзагроз на індивідуальну свідомість індивіда слід розцінювати з двох позицій – з позиції збереження індивіда як особистості та з позиції руйнування його, як цілого. Прикладом небезпек при впливі на особистість, як свідомого індивіда, може бути цілеспрямований процес поширення порнографічної продукції, що ображає суспільну мораль, руйнує дитячу психіку та призводить до спонукання індивіда до здійснення протиправних вчинків.

Кібервпливи можуть ісуттєво змінювати масову (суспільну) свідомість і поводження великих соціальних груп, навіть незважаючи на той факт, що такий вид свідомості формується насамперед у процесі історичного розвитку нації, народності, великої соціальної групи. Велика соціальна група – це необмежена за кількістю певна соціальна спільнота, яка має стійкі цінності, норми поведінки і соціально-регулятивні механізми. Їх прикладом можуть бути партії, етнічні групи, виробничо-галузеві та громадські організації. Соціально-психологічними регуляторами життєдіяльності великих груп є: групова свідомість, менталітет, звичаї, традиції тощо. Велика група характеризується низкою групових факторів до яких відносять психічний склад групи, групову психологію та групову свідомість. Остання, у свою чергу, впливає на формування у носіїв цієї групи відповідного типу особистості, що обов'язково враховується і використовується при здійсненні інформаційно-психологічних впливів. Метою впливів на масову свідомість суспільства є виклик особливої, конфліктної поведінки його в різних життєвих ситуаціях. Наприклад, ініціювання паніки у суспільстві, примус до здачі у полон, мобілізація мітингувальників тощо. Такі підходи та механізми їх реалізації знайшли грунтовне відображення у спеціалізованій науковій літературі.

Наслідки впливу кіберзагроз для суспільства зокрема та держави в цілому

проявляються у локальному (регіональному) та загальнонаціональному масштабах. Маніпулювання масовою свідомістю досягається у результаті цілеспрямованого інформаційно-психологічного впливу у вигляді потужного психологічного і морального тиску на суспільство на фоні його бідності та соціальної незахищеності, що призводять до проявів непокори діючій системі державного управління. Окремі види інформаційно-психологічного впливу, які спрямовуються на визначені цілі (суспільство чи окремих індивідів) здатні до серйозного порушення нормального функціонування державних інститутів.

Прояв кіберзагроз на індивідуальну свідомість призводить до того, що в ній відбуваються дві взаємопов'язані зміни. Це зміни у психіці та психічному здоров'ї та зміни у життєвих цінностях, орієнтирах та світогляді. У першому випадку втрачається адекватне сприйняття світу та подій, які у ньому відбуваються. Притупляються усі психічні реакції, відбувається деградація особистості, здійснюється перехід від потреб вищого рівня (духовного) до потреб нижчого рівня (фізіологічного). У другому випадку зміна життєвих цінностей спонукає здійснення антисоціальних вчинків, які становлять небезпеку не тільки для самого суб'єкта, а й суспільства та держави в цілому.

Масова свідомість також уразлива до проявів кіберзагроз, навіть не зважаючи на те, що її підвалини в першу чергу, формуються насамперед життєвим досвідом, а вже потім внаслідок кібервпливу. У психології мас, згідно з французьким психологом Г. Лебоном, інформаційні процеси та процеси управління можуть розглядатися у трьох формах при впливі на населення, натовп та колектив. При цьому, основними джерелами, що дозволяють впливати на масову свідомість, а відповідно і керувати масами для населення, є ЗМІ та чутки, для натовпу – не обов'язково грамотний, але обов'язково харизматичний і бажано фанатичний лідер та його найближче оточення, для колективу – офіційна інформація від посадових осіб та неформального (обраного або призначеного) лідера.

Таким чином, метою реалізації кіберзагроз у інформаційно-психологічній сфері може бути реалізація кібервпливів спрямованих на:

– нанесення шкоди психічному здоров'ю особи;

– порушення традиційних устоїв особистості, суспільства, держави;

– порушення стійкості процесів управління в кіберпросторі;

– цілеспрямований кібервплив на особистість та суспільство, спрямований на блокування вільного волевиявлення, штучне нав'язування йому синдрому залежності і здійсненням ним через ці обставини протиправних дій;

– розробку, створення і застосування спеціальних технічних і програмних засобів інформаційно-психологічного впливу на психіку особистості;

– цілеспрямоване втручання іноземних спецслужб у роботу державнихкібернетичних систем;

– управління масовою свідомістю з використанням спеціалізованих засобів інформаційно-психологічного впливу;

– підготовку до кібервійн з використанням кіберзброї.

Потенційними джерелами виникнення та поширення кіберзагроз для визначених суб'єктів та об'єктів впливу є:

– ЗМІ і спеціальні засоби, що мають інформаційно-пропагандистську спрямованість. Сучасні ЗМІ (радіо, газети, телебачення) виконують роль засобів комунікацій між суб'єктами та об'єктами кіберпростору. З одного боку ЗМІ, як потенційні джерела поширення кіберзагроз в інформаційно- психологічній сфері, можуть бути стримуючим фактором при розв'язанні кібервійн, з іншого – як їх ініціатор та підсилювач. Засоби інформаційно- психологічної спрямованості (мобільні телерадіомовні пропагандистські центри) на відміну від ЗМІ мають менше за територіальними ознаками охоплення цільової аудиторії, але характеризуються конкретним, спрямованим на певний регіон (територію) контентом, який поширюється, як приховано, так і з використанням засобів телерадіомовлення та друкованої продукції (флаєрів, листівок, плакатів тощо);

– мережа Інтернет та спеціалізоване програмне забезпечення прискореного поширення

відповідних впливів. Мережа Інтернет, яка має високу ресурсоспроможність на сьогодні перетворюється в нове соціальне середовище (*e*-середовище) та досить динамічно набуває вигляду базису дієвої медіатехнології прихованого кібервпливу світового масштабу. Спеціалізоване програмне забезпечення прискореного поширення кібервпливів тільки сприяє підсиленню дієвості таких впливів, причому без порушення законів та при повній безконтрольності з боку держави;

– спеціальні технічні пристрої та програмні засоби, що здатні модифікувати (порушувати цілісність) інформації, на основі якої приймаються стратегічнірішення;

– засоби віртуальної реальності;

– чутки;

– засоби підпорогового психосемантичного впливу;

– фізичні особи, що від природи наділені здатністю неусвідомленого кібервпливу на особистість, суспільство, державу, масову та індивідуальну свідомість;

– релігійні та інші об’єднання громадян;

– нові зразки зброї на нетрадиційних принципах дії (наприклад, генератори фізичних полів та випромінювань тощо).

ЛЕКЦІЯ 2. КЛАСИФІКЦІЯ ДІЙ У КІБЕРПРОСТОРІ

2.1 Дії у кіберпросторі та їх особливості

2.1.1 Сутність, цілі та задачі кібердій

До останнього часу вважалось, що бойові дії ведуться в чотирьох проекціях простору: на суші, на морі, в повітрі і в космосі. При цьому, інформаційні технології відігравали допоміжну роль: зв'язок, автоматизація управління, облік тощо.

Однак у сучасних умовах вже можна говорити про перенесення значної частки бойових дій безпосередньо в кіберпростір, тобто він вже може розглядатись як окремий простір ведення бойових дій. Його винятковість пов'язана з тим, що він єдиний з усіх п'яти наразі опанованих людиною просторів є екстериторіальним, адже практично позбавлений географічних обмежень. При цьому, залежність сучасної людини від кіберпростору є лише трохи меншою, ніж від інших. Саме від кіберпростору, від його стану, функціональності, передбачуваності та прогнозованості залежить стабільність світової економіки, безпека людей, всезагальне зростання добробуту,суспільний розвиток.

Кібердії, як специфічний вид протиборства, можна охарактеризувати такими особливостями:

– кібердії відбуваються у кіберпросторі, який вже сьогодні віднесений до нового театру воєнних дій поряд з космічним, морським, повітряним та наземним театрами;

– кібердії в переважній більшості мають асиметричний характер (наприклад, держава з достатньо малими за чисельністю Збройними Силами спроможна нанести серйозних втрат державі чисельність Збройних Сил у якій єзначно більшою);

– наслідки від дій в кіберпросторі або безпосередньо, або опосередковано впливають на процеси глобалізації, що відбуваються у світі (економіку, фінанси, зброю та системи управління озброєнням, промисловість тощо);

– кібердії впливають на когнітивні та емоціональні процеси у соціумі, на адекватність сприйняття та правильність оцінювання ним подій, що відбуваються, та якість рішень, які ним приймаються;

– кібердії не мають єдиної загальноприйнятої стратегії та характеризуються великим ступенем невизначеності щодо задач, місця та часу їх проведення;

– на практиці досить складно розпізнавати факти здійснення кібердій цілеспрямованого або випадкового характеру;

– ведення дій у кіберпросторі потребує створення, впровадження та супроводження дієвої системи кібербезпеки. Ключовими елементами такої системи мають бути сили та засоби кіберрозвідки, захисту та впливу, які за сферами відповідальності об'єднується під егідою єдиного державного міжвідомчого координуючого органу із широким залученням громадськості, бізнесу, освітньої та наукової компонент тощо;

– кібердії обмежуються границями кіберпростору, але не обмежуються географічними та часовими рамками;

– кібердії на відміну від інших видів воєнних дій здійснюються протиборчими сторонами приховано та мають високий ступінь анонімності;

– джерело кібердій, як правило, складно піддається аналізу та виявленню;

– кібердії ґрунтуються на методології комплексного застосування усіх наявних сил та засобів, а також сил та засобів їх забезпечення або пов'язаних з їх застосуванням.

Успішне досягнення цілей кібердій та якісне вирішення задач, що стоять перед ними, безпосередньо пов'язані з чітким усвідомленням їх суб'єктами

усього спектра з виконання необхідних та достатніх умов для їх успішного здійснення. Саме тому у ході кібердій їх цілі та задачі, форми та способиздійснення можуть варіювати та носити різносторонній характер. Наприклад:

– розвідувальна форма кібердій має на меті добування усіма наявними засобами відомостей про процеси управління у воєнній, економічній, політичній, культурній та інших сферах діяльності суспільства та держави протиборчої сторони;

– кібердії набувають руйнуючої форми у випадку переслідування мети спрямованої на

знищення, придушення або видозмінення з їх використанням процесів управління у кібернетичних системах протиборчої сторони, що можуть призвести до виведення з ладу її об'єктів з критичною інформаційною інфраструктурою частково або в цілому.

Цілі та задачі кібердій можуть полягати у:

– паралізації або взятті під контроль в найкоротші терміни об'єктів з критичною інформаційною інфраструктурою протиборчої сторони та його основних сил і засобів без нанесення фатальних втрат промисловості та території;

– дезорганізації функціонування органів державної влади та органів військового управління протиборчої сторони, об'єктів з критичною інформаційною інфраструктурою військового (стратегічних ядерних сил, систем попередження про ракетний напад, систем контролю космічного простору тощо), цивільного (атомної енергетики, хімічної та нафтопереробної промисловості тощо), подвійного призначення (об'єктів зі зберігання відходів ядерної та хімічної промисловості);

– перешкоджанні всіма наявними засобами нормальній роботі функціонування органів державної влади та органів військового управлінняпротиборчої сторони;

– повному оволодінні стратегічною ініціативою, збереженні стійкого державного і військового управління своїх військ (сил);

– забезпеченні переваги на землі, морі, повітрі, космосі та в кіберпросторі;

– досягненні інформаційної переваги над протиборчою стороною шляхом реалізації кібервпливів на інформацію управління та команди управління інформаційними системами з одночасним захистом власної критичної інформаційної інфраструктури від аналогічних дій.

2.1.2 Класифікація форм і способів кібердій

Входження людства в епоху високотехнологічного суспільства обумовлює значні зміни в характері і в способах ведення збройної боротьби сучасності. Використання та контроль кіберпростору в національних інтересах потребує докорінного перегляду військових доктрин та стратегій застосування Збройних сил. У світі у низці держав, наприклад США, Франції, Естонії, Німеччині, Великобританії та ін., здійснюються спроби формування нової теорії збройної боротьби – теорії ведення бойових дій в кіберпросторі. Створення такої теорії неодмінно призведе до змін у військовому мистецтві.

Нік Харві, міністр збройних сил Великобританії, в інтерв'ю газеті "The Guardian" 31.05.2001 р. заявив: "Cyber weapons 'now integral part of Britain's armoury'". Також він сказав, що: "Кібердії стануть частиною бойовищ майбутнього, що проводитимуться паралельно з більш традиційнимиморськими, наземними та повітряно-космічними операціями. Кіберзброя стане невід'ємною частиною арсеналу держави".

Дії в кіберпросторі на сьогодні ще не набули визначеної в класичному розумінні форми збройної боротьби. Поряд з тим, зважаючи на останні збройні конфлікти та локальні війни, в яких мало місце протиборство в кіберпросторі, можна виділити такі форми ведення кібердій: кіберакції, кіберзаходи, кібероперації та кіберкампанії.

Отже, визначення поняття "кібератака" відповідно до Закону України "Про основні засади забезпечення кібербезпеки України" має наступне тлумачення:

Кібератака – спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно- комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби й обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту.

Кібероперація – це скоординована й узгоджена за масштабом, місцем і часом паралельна або послідовна кібердія розвідувального, оборонного та (або) наступального характеру, яка має на меті завоювання переваги в кіберпросторі за рахунок нанесення збитків

суб'єктам та об'єктам з критичною інформаційною інфраструктурою протиборчої сторони та захисту власних кібернетичних систем від аналогічних дій у відповідь .

При цьому така категорія, як кібервійна більшістю військових експертів нівелюється. Наприклад, у "Концептуальному плані розвитку можливостей сухопутних військ з ведення кібероперацій в кіберпросторі на період з 2016 по 2028 роки", опублікованому у 2010 році Командуванням навчально-наукового центру з розбудови сухопутних військ США, вона підміняється категорією "бойова операція в кіберпросторі" (Cyber Warfare Operations). Але, якщо не виключати ймовірність виникнення такого явища у майбутньому, то у першому наближенні можна запропонувати наступне трактування категорії кібервійна.

Кібервійна – це складне суспільно-політичне явище, що протікає у вигляді конфлікту в кіберпросторі між протиборчими сторонами (державами, коаліціями держав тощо) з використанням кібернетичних систем.

У найближчому майбутньому кібервійна може бути окремою й самостійною частиною широкомасштабних бойових дій із застосуванням

наземної, повітряної, космічної та морської компонент. Під веденням бойових дій в кіберпросторі слід розуміти кібердії, що здійснюються з метою забезпечення дій командувань на різних театрах воєнних дій.

Згідно з системою форм кібердій можна виділити три базові форми протистояння в кіберпросторі: розвідувальна, оборонна та наступальна, також можуть мати подвійне призначення.

Основною формою дій у кіберпросторі прийнято вважати кібероперації. Розглянемо базові формі відповідно до кібероперації.

Розвідувальна кібероперація – це вид кібердій у кіберпросторі, що передбачає цілеспрямований процес добування даних, а також інформації про управління в кібернетичних системах протиборчої сторони. Процес добування даних, що становлять інтерес, їх аналіз та інтерпретація спрямовані на виявлення організаторами кібероперації уразливих місць протиборчої сторони та знаходження точок прикладання основних зусиль.

Добування інформації про кіберзагрози власним кібернетичним системам являє собою найбільш важливу проблему для розвідувального співтовариства. Розвідка у кіберпросторі, або кіберрозвідка використовує нові джерела, форми і способи добування даних, нові технології і технологічні прийоми. Проблемним питанням при організації розвідувальних кібероперацій залишається якісне укриття слідів на зворотному шляху доставляння розвідувальних даних. Дана обставина свідчить про те, що: по-перше, докорінного перегляду потребує усталена роками розвідувальна інфраструктура будь-якої держави світу; по- друге, розробленню підлягають нові форми і способи здійснення розвідувальних кібердій; по-третє, удосконалення потребують розвідувальні засоби та технології.

Оборонна операція в кіберпросторі – це кібердії з боку держави, спрямовані на застосування нею наявних кіберзасобів в інтересах захисту власних кібернетичних систем та процесів управління, які в них протікають, від кібердій з боку протиборчої сторони. Оборонна кібероперація ґрунтується на комплексному застосуванні можливостей власної системи кіберозброєння з метою своєчасного виявлення, відслідковування, аналізу, припинення та протидії кібервпливам протиборчої сторони, спрямованим на критичну інформаційну інфраструктуру держави. При формуванні оборонної стратегії кібероперації обов'язковому урахуванню підлягає порядок проведення процедур та заходів, спрямованих на мінімізацію наслідків кібердійпротиборчої сторони.

Наступальна кібероперація – це форма ведення кібердій в кіберпросторі. Такі дії, як правило, спрямовуються на викривлення, блокування, знищення інформації управління та інші дії з інформацією та процесами управління, що циркулюють в кібернетичних системах протиборчої сторони.

Кількість кібероперацій, що проведено у світі до сьогоднішнього дня, є достеменно невідомою. З відкритих джерел принаймні відомо три кібероперації, які отримали світовий резонанс та піддалися ґрунтованому

науковому дослідженню з боку військових експертів. Це: розвідувально- наступальна кібероперація "Олімпійські ігри", організована спецслужбами та представниками Збройних

Сил США та Ізраїлю за підтримки відповідних урядів; розвідувальна кібероперація "Червоний жовтень" (державна належність та виконавець невстановлені); розвідувальна кібероперація "Мережниймандрівник" (державна належність та виконавець невстановлені).

Довідково.

Кібероперація "Олімпійські ігри" ініційована адміністрацією 43-го Президента США (Д. Буша) та підтримана його наступником Б. Обамою мала на меті знищення або досягнення суттєвого стримування іранської ядерної програми, а також недопущення ескалації збройного конфлікту на Близькому Сході між Ізраїлем та Іраном. Інструментом досягнення мети в кібероперації виступила кіберзброя Stuxnet та Flame.

Кібероперація "Червоний жовтень" мала на меті незаконне отримання та передавання інформації, що становить державну таємницю, а також добування конфіденційної інформації з баз даних приватних мереж та мобільних засобів. Серед держав, що найбільш підпали під цілі даної кібероперації, були переважно держави в минулому СРСР (Україна, Росія, Білорусь та ін), а також держави Східної Європи (Словакія, Угорщина Молдова, Чехія та ін).

Кібероперація "Мережний мандрівник" ("NetTrave/et або інші назви "Travnef, "Netfile") проводилася з метою незаконного добування інформації про стан аерокосмічних досліджень, нанотехнологій, лазерної фізики, досліджень у галузі ядерної фізики, медичної справи, нафтопереробних та телекомунікаційних компаній 40 країн світу. Серед країн, які стали ціллю даноїкібероперації були США, РФ, Україна, Канада, Монголія, Індія, Іспанія, Німеччина, Японія, Іран та ін.

Кібероперації можуть бути: тактичними, стратегічними, легальними та спеціальними.

Тактичні кібероперації здійснюються з метою демонстрації протиборчій стороні уразливостей її критичної інформаційної інфраструктури від сторонніх кібервпливів, що призводить до деморалізації населення та особового складу Збройних сил, нав'язування їм ідеї явної переваги протиборчої сторони і неминучої поразки у звичайній війні, у разі її початку.

Під час тактичних кібероперацій вирішуються такі основні задачі:

– ускладнення або вибіркова зупинка діяльності засобів телекомунікацій телекомпаній, операторів стільникового зв'язку, провайдерів Інтернету, відомчих мереж тощо;

– тимчасова зупинка або ускладнення діяльності систем управління життєзабезпеченням населення та Збройних Сил та порушення діяльності систем управління банківської та фінансової сфер. Прикладом тактичної кібероперації може бути естонський кіберінцидент у 2007 році.

Стратегічні кібероперації здійснюються з метою нанесення реальних збитків протиборчій стороні, які проявляються у руйнуванні системи

управління органів державної влади, системи управління національною економікою, а також створенні передумов до виникнення техногенних аварій та катастроф, що можуть призвести до появи значної кількості жертв серед особового складу збройних сил та мирного населення.

Під час стратегічних кібероперацій вирішуються такі основні задачі:

– злам та розкрадання найважливіших державних кодів і алгоритмів шифрування, паролів та кодів доступу, перехоплення переговорів перших осіб держави;

– проникнення у системи управління критичною інформаційною інфраструктурою, інформаційні системи різного цільового призначення та державні бази даних;

– розкрадання, навмисне спотворення або знищення інформації в базах даних спецслужб, силових міністерств та відомств, органів державної влади, центрального банку тощо;

– пошкодження завантажувальних програм (біосів) мікропроцесорів комп'ютерів і знищення баз даних операторів стільникового зв'язку, провайдерів Інтернету, відомчих комп'ютерних мереж, комп'ютерних мереж військового призначення, систем управління життєзабезпеченням, що призводить до можливості виникнення серії великих техногенних аварій та катастроф на об'єктах з критичною інформаційною інфраструктурою (атомних електростанціях, підприємствах хімічної-, нафто- і газопереробних галузей тощо).

Прикладом стратегічної кібероперації може бути кіберінцидент з мережевим хробаком “Stuxnet” на Бушерській АЕС в Ірані.

Легальні кібероперації здійснюються представниками спецслужб з метоюприхованого впливу на політику держави протиборчої сторони. Вони проводяться за такими основними напрямами:

– кібервплив на представників органів державної влади;

– кібервплив на населення;

– кібервплив на економічні та фінансові процеси в державі.

Кібервплив на представників органів державної влади проявляється в інформаційному терорі (компрометації, залякуванні, введенні в оману), який спрямовується проти патріотично налаштованих національних лідерів, їх найближчого оточення, родичів, друзів тощо та в інформаційній підтримці “агентів впливу” шляхом створення їх сприятливих умов для політичного зростання.

Кібервплив на населення здійснюється з метою формування негативної громадської думки проти органів управління державною владою, насамперед, силових структур, і патріотичних громадських організацій шляхом поширення компрометуючої інформації та панічних чуток.

Кібервплив на економічні та фінансові процеси в державі здійснюється приховано. По-перше, штучно стимулюється ажіотаж на ринку на речі першої необхідності. По-друге, приховано створюються такі умови, які у невигідному положенні для держави провокуватимуть коливання курсами валют, енергоносіїв тощо. Як правило, такий кібервплив під час легальної

кібероперації здійснюється через радіо і телевізійні супутникові або звичайні канали ЗМІ, а також електронну пошту, каналами стільникового зв’язку, соціальних мереж тощо.

Спеціальні кібероперації – це кібердії, що проводяться спеціальними підрозділами Збройних Сил з метою знищення стратегічних озброєнь протиборчої сторони.

Вони полягають у:

– прихованому проникненні у системи управління стратегічною зброєю з подальшим несанкціонованим її спрацюванням, що призводить до виникнення техногенних аварій та катастроф й знищення відповідної інфраструктури;

– блокування систем управління військами, передача у війська помилкових наказів і директив у найважливіші моменти бойових дій;

– дезорганізація орбітального угруповання протиборчої сторони (за його наявності);

– блокуванні запуску стратегічних ракет, зміні польотного завдання ракет шляхом їх перенацілювання на власні об’єкти з критичною інформаційною інфраструктурою або об’єкти іншої держави тощо.

2.1.3 Основні форми і способи кібердій:

– Поширення спеціально підібраної інформації (дезінформації), в першу чергу, у соціальних Інтернет-сервісах. Її реалізація виявляється у такий спосіб:

– розсилка електронних листів;

– організація новинних груп;

– створення сайтів з елементами інтерактивної взаємодії їх відвідувачів(чати, on-line-голосування);

– розміщення інформації на приватних за змістом веб-ресурсах (блоги, соціальні мережі), в електронних версіях періодичних видань і мережевого мовлення (трансляції передач радіо- і телестанцій), або в мультимедійних архівах (Youtube) .

– Повне або часткове наповнення інформаційних ресурсів шляхом підміни їх змісту, шляхом несанкціонованого доступу. З метою залучення уваги до суб’єкта кібервпливу та демонстрації своїх можливостей. Особлива роль при реалізації даної форми кібердій відводиться семантичним атакам, що полягають у проникненні до ресурсів сайта й подальшому непомітному розміщенні на них дезінформації. Подібним атакам піддаються найпопулярніші інформаційні сторінки, змісту яких користувачі цілком довіряють.

– Створення “двійників” інформаційних ресурсів схожих на оригінальні

– цілеспрямована реєстрація у пошукових системах, з метою перенаправлення (підміна) посилань на інші інформаційні ресурси протилежного змісту.

– Зниження ефективності функціонування структурних елементів каналів передачі даних між елементами кібернетичних систем:

– “бомбардування” мережі електронними листами – “спам” ;

– DoS (DDoS)-атаки (атака типу “відмова в обслуговуванні”);

– впровадження мережних комп'ютерних вірусів;

– розміщення інформації на приватних за змістом веб-ресурсах (блоги, соціальні мережі), в електронних версіях періодичних видань і мережевого мовлення (трансляції передач радіо- і телестанцій), або в мультимедійних архівах (Youtube) .

– Віддалене приховане управління ресурсами мережі:

– активація процесу прихованого управління здійснюється при використанні механізмів:

– “часових бомб” – за часом;

– “логічних бомб” – за діями, що безпосередньо здійснюються над операційною системою;

– “троянських коней” – за ключовими повідомленнями. Дозволяє створювати ботнет мережі.

– Захист власних ресурсів – динамічний захист комп'ютерних систем та мереж від кібератак та захист соціуму від деструктивного контенту.

Динамічний захист від кібератак передбачає реалізацію процедур завчасного виявлення кіберзагроз ресурсам мережі й побудови відповідної моделі дій з урахуванням виявлених уразливостей та ужиття заходів (у тому числі й активних), спрямованих на забезпечення заданих показників захищеності. Сутність захисту від деструктивного контенту полягає в перекритті доступу до “небажаної” інформації.

Отже, до суб’єктів кібердій можна віднести:

– окремих громадян та осіб без громадянства, соціальні утворення або угруповання громадян, що мають на меті залякування суспільства, створення атмосфери напруженості з метою вирішення окремих політичних, релігійних, національних, економічних або соціальних проблем;

– держави або їх коаліції з економічними і політичними цілями. Основними об’єктами кібердій при цьому можуть бути:

– кібернетичні системи державних урядових органів, фінансових установ, підприємств енергетичної галузі;

– системи управління повітряним рухом, рухом залізничного транспорту та підприємств критичних галузей промисловості;

– системи управління військами та зброєю;

– інші кібернетичні системи, які призначені для збирання, обробки, збереження та видачі інформації тощо, кібервпливи, які можуть призвести до порушення в них процесів управління;

– програмне та інформаційне забезпечення;

– програмно-апаратні, телекомунікаційні та інші засоби інформації тауправління;

– канали зв’язку, що забезпечують циркуляцію інформаційних потоків між кібернетичними системами;

– інтелект людини та масова свідомість.

2.2 Система кібердій

У XXI столітті людство живе у той час, коли темпи науково-технічного прогресу досить динамічно змінюють усі сфери його життя. Зміни відбуваються практично в усьому – від техніки, до моральних цінностей суспільства. Цілком очевидним є факт того, що сьогодні відбувається безперервний процес адаптації людської цивілізації до власних

високотехнологічних здобутків, які чинять на неї не тільки позитивний вплив, а й інколи мають негативні прояви, наслідки від яких мають планетарний характер.

Усвідомлюючи стратегічну важливість захисту від нових викликів та загроз, поява яких обумовлена високотехнологічними здобутками, в провідних країнах світу здійснюється активна робота щодо створення систем протидії таким викликам та загрозам. Наприклад, в США та ін. розвинених державах стрімкими темпами здійснюється підготовка збройних сил та приватного сектору до ведення кібероперацій, роль яких при досягненні воєнно-політичних цілей поставлених перед державою з часом тільки зростає. Інтенсивно удосконалюється категоріальний апарат у сфері боротьби в кіберпросторі, розробляється нова система боротьби в кіберпросторі – система кібердій.

Враховуючи ступінь розуміння ролі й місця кібербезпеки для України в системі національної безпеки, в державі вживається низка заходів з покращення ситуації, що склалася. На державному рівні здійснюються заходи спрямовані на усунення дефініційної невизначеності, здійснюються кроки спрямовані на налагодження належної координації між відповідними відомствами та приватним сектором та інші спеціальні заходи тощо. Але б яка б не була їх кількість, їх завжди буде недостатньо для створення ефективної системи кібербезпеки держави. Це пов'язано з низкою причин, однією з яких є відсутність в державі єдиної системи поглядів на систему кібердій в кіберпросторі, розробці якої і присвячено даний розділ.

Система кібердій – це сукупність взаємопов'язаних підсистем кіберрозвідки, кіберзахисту, кібервпливу та кіберконтррозвідки, які утворюють цілісну єдність, на яку покладаються функції із забезпечення кібербезпеки.

Метою системи кібердій є забезпечення стану кіберзахищеності.

2.2.1 Основи кіберрозвідки

Розвідка є однією з найдавніших професій. З плином часу змінювалися тільки способи та засоби її ведення. Нині розвідка перемістилася у новий вимір кіберпростір й посіла важливе місце у системі кібердій. При цьому, вона може виступати, як окремим їх видом, так і бути супроводжуючим елементом інших складових системи кібердій – кібервпливу та кіберзахисту.

Зростання ролі й місця кіберрозвідки обумовлено низкою факторів, середяких основними можна вважати:

– постійне збільшення взаємозалежності між секторами та об'єктами з критичною інформаційною інфраструктурою;

– постійне зростання кількості кіберзагроз кібернетичним системам управління різного рівня;

– поява принципово нових засобів і способів несанкціонованого доступу доінформації про процеси управління в кібернетичних системах тощо.

Відповідно до Закону України "Про основні засади забезпечення кібербезпеки України" під **кіберрозвідкою** розуміють діяльність, що здійснюється розвідувальними органами у кіберпросторі, або з його використанням.

У більш широкому сенсі під кіберрозвідкою слід розуміти таке визначення. **Кіберрозвідка –** процес добування усіма наявними технічнимизасобами розвідки (космічної, повітряної, радіоелектронної, мережної, програмно-комп'ютерної, розвідки систем управління тощо) й засобами розвідки з відкритих джерел (*OSINT*-розвідка) інформації наявної в кіберпросторі про протиборчу сторону та подальша її обробка, що здійснюються за єдиним задумом і планом з метою викриття процесів управління, які протікають в кібернетичних системах під час їх функціонування та формування вихідних даних для здійснення заходів кіберзахисту та кібервпливу на фізичні, соціальні, інформаційні та інші кібернетичні системи.

Або коротко, **кіберрозвідка** – сукупність заходів, спрямованих на забезпечення всебічної обізнаності щодо дій у кіберпросторі, або з його використанням.

До *основних функцій* кіберрозвідки можна віднести такі функції, як:

– постійний пошук і добування розвідувальної інформації про процеси управління в

кібернетичних системах протиборчої сторони, що становлять інтерес з використанням усіх наявних технічних засобів розвідки й засобів розвідки з відкритих джерел інформації з кіберпростору;

– обробка, узагальнення та аналіз добутої розвідувальної інформації;

– підготовка розвідувальної інформації на підставі проведеного аналізу для прийняття обґрунтованих управлінських рішень;

– формування вихідних даних для здійснення кібервпливу на кібернетичні системи протиборчої сторони;

– прогнозування можливих проявів кіберзагроз та їх наслідків.

Згрупувавши функції кіберрозвідки, можна виділити дві основні групи задач. Перша група задач – це задачі, що пов'язані з добуванням інформації; друга – це задачі прогнозування кіберзагроз.

Відповідно до масштабів і характеру розвідувальних завдань кіберрозвідка може бути стратегічною, оперативною та тактичною.

Стратегічна кіберрозвідка проводиться з метою підготовки та проведеннястратегічних операцій та війни в цілому у "класичному розумінні" й кібероперацій та кіберкампаній у рамках системи кібердій. Стратегічною ціллю такого виду розвідки також є досягнення воєнної, політичної, промислової, технологічної та іншої переваги над протиборчою стороною за рахунок викриття процесів управління в кібернетичних системах протиборчої сторони.

Оперативна кіберрозвідка вирішує завдання розвідки в інтересах ведення спеціальних операцій в межах заданого операційного району.

Тактична кіберрозвідка здійснюється силами і засобами спеціальних підрозділів кіберрозвідки в інтересах успішного ведення кібердій у ході їх підготовки та безпосереднього ведення.

Кіберрозвідка має низку особливостей. Основними з них є такі:

– порівняно з іншими видами розвідки роль кіберрозвідки постійно зростає. При правильному підході до організації кіберрозвідки, а також раціональному застосуванні сил та засобів кіберрозвідки у мирний час можливо добувати від35 до 95% інформації про об'єкти або суб'єкти, що становлять інтерес;

– добуваюча та обробляюча складові процесу кіберрозвідки мають взаємозалежний тісний зв'язок;

– підвищується роль знань на заключному етапі процесу кіберрозвідки, який на відміну від інших видів розвідки не завершується підготовкою розвідувальних даних для визначених органів. Заключний етап кіберрозвідки полягає у приведенні розвідувальних даних у вищий ступінь готовності до їх застосування у процесі прийняття управлінських рішень – у вигляді набутих знань;

– під час кіберрозвідки роль, місце та функції людини, як на етапі добування, так і на етапі обробки змінюються за рахунок зменшення об'єму працевитрат;

– сутність кіберрозвідки в основному зводиться на здійснення діяльності, спрямованої на досягнення або утримання переваги в кіберпросторі над протиборчою стороною;

– складність територіальної та державної ідентифікації належності суб'єктаабо об'єкта кіберрозвідки, що суттєво ускладнює процес добування розвідувальної інформації та забезпечення її достовірності.

До кіберрозвідки висувається низка вимог системного характеру, таких як:

– підсистеми кіберрозвідки повинні мати розвинену інфраструктуру, що дозволить здійснювати постійний моніторинг процесів управління різної природи у системах управління різного цільового призначення та ієрархічної складності з метою досягнення синергетичного ефекту;

– підсистеми кіберрозвідки мають бути максимально автоматизованими, а звітні результати повинні подаватися у стандартизованій формі, яка доступна усім підсистемам;

– система кіберрозвідки повинна мати централізований банк даних для збереження розвідувальної інформації та добутих знань.

Кіберрозвідка включає три основні фази:

– організацію кіберрозвідки;
– ведення кіберрозвідки;
– інформаційна робота.

Організація кіберрозвідки передбачає визначення цілей і завдань розвідки, виділення необхідних сил і засобів, планування її заходів, постановку завдань виконавцям, організацію їх підготовки та інші питання. Ведення кіберрозвідки

має безпосередній зв'язок з добування розвідувальної інформації. Інформаційна робота являє собою збір, обробку розвідувальної інформації, її узагальнення та доведення до зацікавлених осіб.

2.2.2 Основи кіберзахисту

Невід'ємною складовою системи кібердій є підсистема кіберзахисту, призначена для реалізації заходів із забезпечення кібербезпеки. При цьому,категорія "кіберзахист" у даному випадку уживається виходячи з такого її тлумачення, яке подано в Законі України "Про основні засади забезпечення кібербезпеки України".

Кіберзахист – сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від інформаційних та кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних та соціосистем.

Основними видами кіберзахисту є (рис. 2.1):

– апаратно-програмний захист;
– технічний захист інформації;
– радіоелектронний захист (радіоелектронна протидія);
– інформаційно-психологічна протидія;
– інші заходи організаційного та нормативно-правового захисту.

Рис. 2.1. Види кіберзахисту

Апаратно-програмний захист – це комплексне застосування апаратних та програмних засобів для забезпечення кіберзахисту комп'ютерної системи. Незважаючи на те, що сучасні операційні системи, такі як операційні системи лінійки *Windows, Linux* та ін. мають власні базові системи захисту, актуальність у здійсненні апаратно-програмного захисту зберігається. Це пов'язано з тим,що інформація при мережному обміні, як правило, піддається деструктивним впливам з боку протиборчої сторони.

Апаратно-програмний захист буває двох видів та містить п'ять груп.

Перший вид – це апаратний захист. Апаратний захист – це захист комп'ютерної системи з використанням технічних пристроїв. Другий вид – це програмно-математичний захист, що забезпечує захист комп'ютерної системи на основі використання програм розмежування доступу (паролів доступу, режимів доступу користувачів тощо).

Основними групами апаратно-програмного захисту є:

– системи ідентифікації (розпізнавання) й автентифікації (перевірки істинності) користувачів;

– системи шифрування даних дискового простору;

– системи шифрування даних, що передаються мережею;

– системи атентифікації електронних даних.

– засоби управління криптографічними ключами.

Технічний захист інформації в кібернетичних системах – це вид захисту, що спрямовується на забезпечення інженерно-технічними заходамиконфіденційності, цілісності та доступності інформації управління. На технічний захист інформації покладаються завдання з виявлення і блокування каналів витоку інформації (радіоканал, ПЕМВ, акустичні канали, оптичні канали тощо). Ефективність вирішення задач з технічного захисту інформації передбачає наявність фахівців в області захисту інформації та їх відповідного технічного оснащення спеціальною технікою виявлення і блокування каналів витоку. Вибір спецтехніки для вирішення завдань технічного захисту інформації визначається на основі аналізу ймовірних загроз і ступеня захищеності об'єкта.

Радіоелектронний захист – це комплекс заходів щодо забезпечення стійкої роботи радіоелектронних засобів від порушення штатних режимів їх роботи.

Інформаційно-психологічна протидія – це складова інформаційно- психологічної боротьби, спрямована на власну аудиторію, яка одночасно є мішенню для пропаганди (психологічних операцій) опозиції (противника), з метою нейтралізації або зведення до мінімуму ефекту від стороннього інформаційно-психологічного впливу. Вона включає комплекс заходів, спрямованих на захист певної системи світоглядних орієнтирів, настанов, стереотипів, на основі яких ґрунтується високий морально-психологічний стан суб'єктів впливу та здатність соціуму, як такого до опору агресору. За американською класифікацією такий вид діяльності відноситься до "консолідуючої пропаганди".

Для підвищення психологічної стійкості особового складу доцільно виявляти лідерів, створювати неформальні групи військовослужбовців, які б формували відповідні стереотипи про армію противника, були б носіями високого морально-психологічного стану. Створення зазначених груп слід здійснювати завчасно, ще в ході психологічного відбору при формуванні миротворчого контингенту. При виконанні завдань в оперативному районі може виникнути необхідність призначення у кожному підрозділі відповідальних осіб, в частинах – спеціальних команд по збору і знищенню агітаційно-пропагандистських матеріалів противника. Зарубіжні фахівці вважають листівки найбільш ефективним засобом психологічного впливу на соціум, тому закриття цього каналу впливу на військовослужбовців дозволить значно знизити ефективність психологічного впливу на особовий склад.

Особлива увага при організації протидії повинна приділятися вивченню змісту, тез та аргументів друкованої та телерадіомовної пропаганди суб'єкта впливу, а також аналізу можливого негативного психологічного впливу на соціум з помітною нервово-психічною нестійкістю, високою "недовірливістю" і тривожністю, які у складних ситуаціях нерідко стають індукторами паніки.

Організаційні заходи захисту передбачають виконання таких функцій:

– визначення технологічних процесів обробки інформації;

– обґрунтування та вибір завдань захисту;

– розробку та впровадження правил реалізації заходів захисту інформації;

– визначення та встановлення обов'язків підрозділів і осіб, що беруть участь в обробці інформації;

– вибір засобів забезпечення захисту інформації;

– оснащення структурних елементів кібернетичної системи нормативними документами і засобами забезпечення захисту інформації;

– встановлення порядку впровадження засобів обробки інформації, програмних і технічних засобів захисту інформації та контролю їх ефективності;

– визначення зон безпеки інформації;

– обґрунтування структури та технології функціонування систем захисту інформації;

– розробку правил та порядку контролю функціонування системи захисту інформації;

o встановлення порядку проведення атестації технічних засобів та систем обробки інформації, систем зв'язку та передачі даних, технічних засобів та систем, що розташовані в приміщеннях, де вона циркулює, приміщень для засідань, а також усієї кібернетичної системи у цілому на відповідність вимогамбезпеки інформації.

Нормативно-правовий захист – це вид захисту, що ґрунтується на низці державних указів, законів, постанов, розпоряджень та відповідних міжнароднихдокументів.

Основні цілі кіберзахисту показано на рис. 2.2.

Рис. 2.2. Основні цілі кіберзахисту

Таким чином, підсистема кіберзахисту також як і підсистема кіберрозвідки, є однією з трьох ключових і невід'ємних складових системи кібербезпеки. Отже, тільки комплексна взаємодія компонентів підсистеми кібербезпеки забезпечить захист інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем, систем управління об'єктів та суб'єктів з критичною інформаційною інфраструктурою, автоматизованих систем управління, гарантуватиме своєчасне виявлення, упередження та нейтралізацію спроб реалізації різноманітних кібердій зі сторони суб'єктів кібервпливу.

2.2.3 Основи кібервпливу

Зі вступом людства в епоху високотехнологічного розвитку кібервпливи дедалі частіше стають чи не найбільш дієвими механізмами контролю процесів управління, що протікають у кібернетичних системах різного цільового

призначення та різного ієрархічного рівня. Тому наслідки від проявів кібервпливів у міжнародній політиці дедалі частіше проявляються, в першу чергу, не в силовому досягненні політичних цілей, а в прихованому і зовні цілеспрямовано-керованому процесі зміни легітимних урядів, політичного, економічного та духовного підкорення окремих народів, країн територій тощо. Слід зазначити також, що кібервпливи можуть бути спрямовані на будь-які об'єкти кіберпростору, включаючи соціум, соціотехнічні системи, технічні системи (комп'ютерні системи та мережі, системи зв'язку та автоматизовані системи управління (АСУ), управляючі елементи систем озброєння і військової техніки та небезпечних і критичних об'єктів, програмне забезпечення, бази даних тощо), у вигляді інформаційних,

психологічних та різноманітних фізичних деструктивних впливів. Причому останнім часом у світі досить інтенсивно розвиваються спеціальні технології психологічного кібервпливу на масову свідомість людей та технології кібервійн. Саме тому роль кібервпливів у сучасній системі протиборства дедалі все частіше стає визначальною, а у системі кібердій їм відводиться чільне місце.

Нині існує багато визначень категорій "кібервплив" та "активні дії у кіберпросторі", але остаточно визнаних та прийнятих ще й досі не існує. У міру розвитку науки і техніки з'являються все нові й нові її тлумачення, отже, маємо такі визначення.

Кібервплив – це цілеспрямований процес застосування усього наявного комплексу засобів та заходів впливу на визначені елементи кіберпростору з метою порушення процесів управління в кібернетичних системах протиборчої сторони шляхом зміни нормальних режимів їх функціонування з подальшим, або співвимірним у часі впливу взяттям їх під власне управління та контроль.

Активні дії у кіберпросторі – заходи деструктивного (руйнівного) впливу на автоматизовані системи управління, системи зв'язку, навігації й управління зброєю, мережнокомп'ютерні та соціотехнічні системи противника.

Безумовно, що кібервпливи є успішними тільки за виконання низки умов. Однією з основних умов є умова існування в сторони, що планує здійснити кібервплив повної інформаційної бази даних про об'єкти впливу за всіма сферами життєдіяльності (суспільно-політичне становище, паролі доступу до комп'ютерних систем та мереж управління збройними силами, систем управління об'єктами атомної енергетики, транспорту, банківської системи, державних органів управління тощо).

Сучасні інформаційні технології дозволяють здійснювати проникнення не лише у відкриті системи, а також у локальні закриті системи, що не мають виходу до загальних мереж. Для цього використовуються будь-які можливості доступу до них, в тому числі безпровідні засоби прийому-передачі інформації. Проникнення у локальні мережі використовується не лише для контролю за потоками інформації та її збору, а також з метою нанесення кіберударів за яких забезпечується порушення нормального функціонування у визначений час за допомогою заздалегідь вмонтованих програмних та апаратних закладок операційних систем, так званої "оболонки" комп'ютера або повного виведення зі строю його апаратних засобів – "ядра".

Об'єктами кібервпливу можуть бути органи управління та системиуправління кібернетичних систем живої та неживої природи, а саме:

- технічні системи різного призначення;
- соціум;
- соціотехнічні системи.

У свою чергу, в технічних системах об'єктами кібервпливу виступатимуть АСУ озброєнням і військовою технікою, АСУ критичною інформаційною інфраструктурою (системи життєзабезпечення), АСУ технологічними процесами тощо, комп'ютерні системи з їх базами даних, програмним та апаратним забезпеченням тощо, різні види комп'ютерних систем тощо. Об'єктами кібервпливу серед соціуму є індивідуальна та групова свідомість. Соціотехнічні кібервпливи здійснюються, як на технічні системи, так і на соціотехнічні системи засобами масової комунікації – телебаченням, радіомовленням, Інтернет-мережею тощо.

Спираючись на об'єкти кібервпливу можна виділити його основні види:

- комп'ютерний вплив;
- фізичний вплив;
- радіоелектронний вплив;
- інформаційно-психологічний вплив тощо.

Таким чином, як випливає з вищесказаного – підсистема кібервпливу є ще однією невід'ємною складовою системи кібербезпеки.

Невід'ємною складовою всіх кібердій на цей час стає кіберконтррозвідка. Кіберконтррозвідку можна визначити та охарактеризувати, як особливий вид діяльності,

підпорядкований вирішенню завдань забезпечення кібербезпеки та кібероборони, спрямований на адекватну протидію кіберзагрозам національній безпеці, що виникають або можуть виникнути внаслідок кіберрозвідувальної та кібердеструктивної діяльності спеціальних органів іноземних держав (розвідки, контррозвідки), недержавних розвідувальних і контррозвідувальних структур, організацій та окремих осіб. Має на меті запобігання, виявлення та припинення деструктивної діяльності з використанням кіберконтррозвідувальних (та інших) сил і засобів, форм і методів, обумовлених необхідністю своєчасного прийняттязаходів, адекватних характеру та масштабам кіберзагроз національним інтересам. Тому функціонування системи кібербезпеки хоча б без однієї зі складових її компонентів, не гарантуватиме досягнення бажаного стану безпеки процесів управління в різних сферах.

Отже, спираючись на передовий світовий досвід у галузі кібербезпеки та ґрунтуючись на отриманих нових наукових результатах встановлено, що система кібердій, що складається з підсистем – кіберрозвідки, кіберзахисту, кібервпливу та кіберконтррозвідки, зі своїми складовими, на сьогодні стає ефективним регулятором процесів управління у різних сферах і на різних рівнях, виступає дієвим інструментом ведення міжнародної та регіональної політики несиловими методами. Саме тому її роль і місце у системі кібербезпеки й надалі тільки актуалізуватиметься.

ЛЕКЦІЯ 3
ЗАГАЛЬНІ КРИТЕРІЇ - ISO / IEC 15408

3.1 Історія створення Загальних критеріїв - ISO / IEC 15408

У 1990 році робоча група WG3 підкомітету SC27 об'єднаного технічного комітету JTC1 Міжнародної організації зі стандартизації (ISO) і Міжнародної електротехнічної комісії (IEC) приступила до розробки «Критеріїв оцінки безпеки інформаційної технології» (англ. Evaluation Criteria for IT Security, ECITS).

Трохи пізніше, в 1993 році, урядові організації 6 країн - Канади, США, Великобританії, Німеччини, Нідерландів і Франції зайнялися складанням так званих «Загальних критеріїв оцінки безпеки інформаційних технологій» (англ. Common Criteria for IT Security Evaluation, CCITSE). За цим документом історично закріпилося більш коротку назву - Загальні критерії (ЗК).

Офіційний сайт ЗК: commoncriteriaportal.org.

У 1996 році з'явилася перша версія ЗК, яка була схвалена ISO / IEC. В результаті спільних зусиль усіх зацікавлених сторін 1 грудня 1999 року було введено в дію міжнародний стандарт ISO / IEC 15408-1999 «Критерії оцінки безпеки інформаційної технології».

В даний момент чинною є версія 3.1 ЗК (варіант 4), прийнята у вересні 2012 року, а остання версія міжнародного стандарту ISO / IEC 15408 прийнята в 2009 році.

Критерії призначені служити основою при оцінці характеристик безпеки продуктів і систем IT. Закладені в стандарті набори вимог дозволяють порівнювати результати незалежних оцінок безпеки. На підставі цих результатів споживач може приймати рішення про те, чи достатньо безпечні IT-продукти або системи для їх застосування із заданим рівнем ризику.

3.2 Стек стандартів ISO/IEC 15408

Стек стандартів **ISO/IEC 15408 включає в себе наступні стандарти:**

ISO/IEC 15408-1/2/3:2017 Інформаційні технології. Методи захисту. Критерії оцінки:

Частина 1. Вступ та загальна модель (ISO/IEC 15408-1: 2022, IDT).

Частина 2. Функціональні вимоги (ISO/IEC 15408-2: 2022, IDT).

Частина 3. Вимоги до гарантії безпеки (ISO/IEC 15408-3: 2022, IDT).

Стандарт містить загальний набір вимог до функцій безпеки IT-продуктів і систем, а також до заходів гарантії, застосованих до них під час оцінки безпеки.

Якщо взяти європейські стандарти, відносно яких відбувається гармонізація, то їх вже 5:

ISO/IEC 15408-1:2022. Інформаційна безпека, кібербезпека та захист конфіденційності. Критерії оцінки IT-безпеки. Частина 1. Вступ і загальна модель

Цей документ встановлює загальні концепції та принципи оцінювання безпеки IT і визначає загальну модель оцінювання, що надається різними частинами стандарту, який у цілому призначений для використання в якості основи для оцінки властивостей безпеки IT-продуктів.

Цей документ містить огляд усіх частин серії ISO/IEC 15408. Він описує різні частини серії ISO/IEC 15408; визначає терміни та скорочення, які слід використовувати в усіх частинах стандарту; встановлює основну концепцію мети оцінювання (TOE); описує контекст оцінювання та описує аудиторію, якій адресовані критерії оцінювання. Дано вступ до основних концепцій безпеки, необхідних для оцінки IT-продуктів.

Цей документ представляє:

- ключові поняття профілів захисту (PP), модулів PP, конфігурацій PP, пакетів, цілей безпеки (ST) і типів відповідності;
- опис організації компонентів безпеки по всій моделі;
- різні операції, за допомогою яких функціональні компоненти та компоненти

гарантії, наведені в ISO/IEC 15408-2 та ISO/IEC 15408-3, можуть бути налаштовані шляхом використання дозволених операцій;

- загальну інформацію про методи оцінювання, наведені в ISO/IEC 18045;
- настанова щодо застосування ISO/IEC 15408-4 для розробки методів оцінювання (EM) і діяльності з оцінювання (EA), виведених із ISO/IEC 18045;
- загальну інформацію про попередньо визначені рівні гарантії оцінювання (EAL), визначені в ISO/IEC 15408-5;
- інформація щодо обсягу схем оцінювання.

ISO/IEC 15408-2:2022. Інформаційна безпека, кібербезпека та захист конфіденційності. Критерії оцінки IT-безпеки. Частина 2. Функціональні компоненти безпеки.

Цей документ визначає необхідну структуру та зміст функціональних компонентів безпеки з метою оцінки безпеки. Він містить каталог функціональних компонентів, який відповідає загальним вимогам безпеки багатьох IT-продуктів.

ISO/IEC 15408-3:2022. Інформаційна безпека, кібербезпека та захист конфіденційності. Критерії оцінювання IT-безпеки. Частина 3. Компоненти забезпечення безпеки.

Цей документ визначає вимоги серії стандартів ISO/IEC 15408. Він включає окремі компоненти гарантії, з яких складаються рівні гарантії оцінки та інші пакети, що містяться в ISO/IEC 15408-5, а також критерії для оцінки профілів захисту (PP), конфігурацій PP, модулів PP та цілей безпеки (STs).

ISO/IEC 15408-4:2022. Інформаційна безпека, кібербезпека та захист конфіденційності. Критерії оцінки IT-безпеки. Частина 4. Структура для специфікації методів оцінювання та діяльності

Цей документ забезпечує стандартизовану структуру для визначення об’єктивних, повторюваних і відтворюваних методів оцінювання та діяльності з оцінювання. Цей документ не визначає, як оцінювати, приймати або підтримувати методи оцінювання та діяльність з оцінювання. Ці аспекти є справою для тих, хто розробляє методи оцінювання та діяльність з оцінювання в їхній конкретній сфері інтересів.

ISO/IEC 15408-5:2022. Інформаційна безпека, кібербезпека та захист конфіденційності. Критерії оцінювання IT-безпеки. Частина 5. Попередньо визначені пакети вимог до безпеки.

Цей документ надає пакети забезпечення безпеки та функціональні вимоги безпеки, які були визначені як корисні для підтримки загального використання зацікавленими сторонами.

Приклади наданих пакетів включають рівні гарантії оцінювання (EAL) і складені пакети гарантій (CAP).

Цей документ представляє:

- сімейство пакетів *рівня гарантії оцінки (EAL),* які визначають попередньо визначені набори компонентів гарантії безпеки, на які можна посилатися в PP та ST, і які визначають відповідні гарантії безпеки, які необхідно надати під час оцінювання цілі оцінки (TOE);
- сімейство пакетів *гарантії композиції (CAP),* які вказують набори компонентів гарантії безпеки, що використовуються для визначення відповідних гарантій безпеки, які мають бути надані під час оцінювання складених TO;
- пакет *складеного продукту (COMP),* який визначає набір компонентів гарантії безпеки, що використовуються для визначення відповідних гарантій безпеки, які мають бути надані під час оцінювання TOE складеногопродукту;
- сімейство пакетів *гарантії профілю захисту (PPA),* які вказують набори компонентів гарантії безпеки, що використовуються для визначення відповідних гарантій безпеки, які мають надаватися під час оцінювання профілю захисту;
- сімейство пакетів *гарантії цільової безпеки (STA),* які вказують набори компонентів гарантії безпеки, що використовуються для визначення відповідних гарантій безпеки, які мають бути надані під час оцінки цільової безпеки.

Серед користувачів цього документа можуть бути споживачі, розробники та оцінювачі безпечних IT-продуктів.

Опис стандарту 15408

У стандарті, що отримав назву «Загальні критерії оцінки безпеки інформаційних технологій » (The Common Criteria for Information Technology Security Evaluation), докладно розглянуто загальні підходи, методи та функції забезпечення захисту інформації в організаціях.

Функції системи інформаційної безпеки забезпечують виконання вимог конфіденційності, цілісності, достовірності та доступності інформації. **Всі функції представлені у вигляді чотирирівневої ієрархічної структури**: клас – сімейство

- компонент – елемент.

За аналогією представлені вимоги якості. Подібна градація дозволяє описати будь-яку систему інформаційної безпеки і зіставити створену модель з поточним станом справ.

У стандарті виділені 11 класів функцій:

- аудит;
- ідентифікація та аутентифікація;
- криптографічний захист;
- конфіденційність;
- передача даних;
- захист даних користувача;
- управління безпекою;
- захист функцій безпеки системи;
- використання ресурсів;
- доступ до системи;
- надійність засобів.

Оцінка інформаційної безпеки базується на моделях системи безпеки, що складаються з перерахованих у стандарті функцій. У ISO 15408 міститься **ряд зумовлених моделей** (так званих **профілів),** що описують стандартні модулі системи безпеки. З їх допомогою можна не створювати моделі поширених засобів захисту самостійно, винаходячи велосипед, а користуватися вже готовими наборами описів, цілей, функцій і вимог до цих засобів. Простим прикладом профілів може служити модель міжмережевого екрану.

Сертифікований профіль являє собою повний опис певної частини (або функції) системи безпеки. У ньому міститься аналіз внутрішнього і зовнішнього середовища об’єкта, вимоги до його функціональності і надійності, логічне обгрунтування його використання, можливості та обмеження розвитку об’єкта.

Стандарт ISO 15408 вигідно відрізняє **відкритість.** Описує ту чи іншу область системи безпеки профіль можна створити самостійно за допомогою розробленої в ISO 15408 структури документа. У стандарті визначена також послідовність дій для самостійного створення профілів.

Загальні критерії узагальнили зміст і досвід використання Помаранчевої книги, розвинули рівні впевненості Європейських критеріїв, втілили в реальні структури концепцію профілів захисту Федеральних критеріїв США.

Стандарт ISO/IEC 15408 «Загальні критерії оцінки безпеки інформаційних технологій» (англ. Common Criteria for Information Technology Security Evaluation) описує інфраструктуру (Framework) в якій користувачі комп’ютерної системи можуть описати вимоги, розробники можуть заявити про властивості безпеки продуктів, а експерти з безпеки визначити, чи задовольняє продукт заявам. Таким чином цій стпндарт дозволяє бути впевненим, що процес опису, розробки та перевірки продукту був проведений в строгому порядку.

У “Загальних критеріях” (ЗК) проведена класифікація широкого набору функціональних вимог і вимог довіри до безпеки, визначені структури їх групування і принципи цільового використання

Загальні критерії дозволяють підвищити довіру до засобів захисту і самої інформації, що захищається за рахунок трьох основних якостей:

1. Можливості гнучкого завдання вимог до засобів захисту інформації з урахуванням їх призначення і умов застосування.
2. Більш повного і обгрунтованого набору вимог безпеки.

3. Наявності методології оцінки, що забезпечує об'єктивність і порівнянність результатів.

Загальні критерії являють собою набір з п'яти окремих взаємопов'язаних частин. До них відносяться:

- Введення і загальна модель.
- Функціональні вимоги безпеки.
- Вимоги до надійності захисних механізмів.
- Попереднє визначення профілі захисту.
- Процедури реєстрації профілів захисту.

Основними відмітними рисами ЗК є наступні:

1. Перш за все, ЗК – це певна методологія та система формування вимог і оцінки безпеки ІТ. Системність простежується, починаючи від термінології та рівнів абстракції представлення вимог аж до їх застосування при оцінці безпеки на всіх етапах життєвого циклу продуктів і систем ІТ.
2. Загальні критерії характеризуються найбільш повною на сьогоднішній день сукупністю вимог безпеки ІТ.
3. У ЗК проведено чіткий поділ вимог безпеки на функціональні вимоги і вимоги довіри до безпеки. **Функціональні вимоги** (11 класів, 66 родин, 135 компонентів) відносяться до **функцій безпеки** (ідентифікації, аутентифікації, управління доступом, аудиту і т. д.), а **вимоги довіри** (8 класів,

44 сімейства, 93 компонента) – до досягнення **впевненості в коректності реалізації та ефективності функцій безпеки** шляхом оцінки технології розробки, тестування, аналізу вразливостей експлуатаційної документації, постачання і супроводу продуктів та систем ІТ.

4. Загальні критерії включають шкалу довіри до безпеки (оціночні рівні довіри – ОРД), яка може використовуватися для отримання різного ступеня впевненості у безпеці продуктів і систем ІТ
5. Систематизація і класифікація вимог щодо ієрархії «клас» – «сімейство» –

«компонент» – «елемент» з унікальними ідентифікаторами вимог забезпечує зручність їх використання.

6. Компоненти вимог в родинах і класах ранжовані за ступенем повноти і строгості, а вимоги довіри згруповані в пакети вимог
7. Гнучкість у підході до формування вимог безпеки для різних типів продуктів і систем ІТ та умов їх застосування забезпечується можливістю цілеспрямованого формування необхідних наборів вимог у вигляді певних в ЗК стандартизованих структур (пакетів вимог, профілів захисту і завдань з безпеки).
8. Загальні критерії володіють відкритістю і розширюваністю, тобто дозволяють уточнювати існуючі і вводити додаткові вимоги.

Як показують оцінки фахівців у галузі інформаційної безпеки за рівнем систематизації, повноті і можливостям деталізації вимог, універсальності і гнучкості в застосуванні ЗК представляють найбільш досконалий з існуючих в даний час стандартів. Причому, що дуже важливо, в силу особливостей побудови він має практично необмежені можливості для розвитку і являє собою базовий стандарт, що містить методологію завдання вимог і оцінки безпеки ІТ, а також систематизований каталог вимог безпеки. Як функціональних стандартів, в яких

формулюються вимоги до безпеки певних типів продуктів і систем ІТ, передбачається використання профілів захисту (ПЗ), що створюються за методологією і на основі каталогу вимог ЗК. У ПЗ можуть бути включені ібудь- які інші вимоги, які є необхідними для забезпечення безпеки конкретного типу продуктів або систем ІТ.

3.3 Структура та основні положення стандарту ISO / IEC 15408

Стандарт встановлює основні поняття і принципи оцінки безпеки ІТ, а також визначає загальну модель оцінки, яким присвячені різні частини стандарту, призначеного в цілому для використання в якості основи при оцінці характеристик безпеки продуктів ІТ. Стандарт ISO/IEC 15408 складається з трьох частин.

Частина 1 «Введення і загальна модель» встановлює загальний підхід до формування вимог безпеки й оцінки безпеки, на їх основі розробляються основні конструкції (профіль захисту та завдання з безпеки) уявлення вимог безпеки в інтересах споживачів, розробників і оцінювачів продуктів і систем ІТ. Вимоги безпеки об'єкта оцінки (далі - ОО) за методологією стандарту визначаються, виходячи з цілей безпеки, які ґрунтуються на аналізі призначення ОО і умов середовища його використання (загроз, припущень, політики безпеки).

Частина 2 «Функціональні вимоги безпеки» містить універсальний каталог функціональних вимог безпеки (далі - ФВБ) і передбачає можливість їх деталізації і розширення за певними правилами.

Частина 3 «Компоненти довіри до безпеки» включає в себе систематизований каталог вимог довіри, що визначають заходи, які повинні бути прийняті на всіх етапах життєвого циклу продукту або системи ІТ для забезпечення впевненості в тому, що вони задовольняють пред'явленим до них функціональним вимогам. Тут же містяться оціночні рівні довіри, що визначають шкалу вимог, які дозволяють зі зростаючою ступенем повноти і строгості оцінити проектну, тестову і експлуатаційну документацію, правильність реалізації функцій безпеки ОО, уразливості продукту або системи ІТ, стійкість механізмів захисту і зробити висновок про рівень довіри до безпеки об'єкту оцінки.

Узагальнюючи вищесказане, можна відзначити, що каркас безпеки, закладений частиною 1 стандарту, заповнюється складовими з класів, сімейств і компонентів в частині 2, а частина 3 визначає, як оцінити міцність всієї «будови».

Основні ідеї стандарту зображені на рис. 3.1.

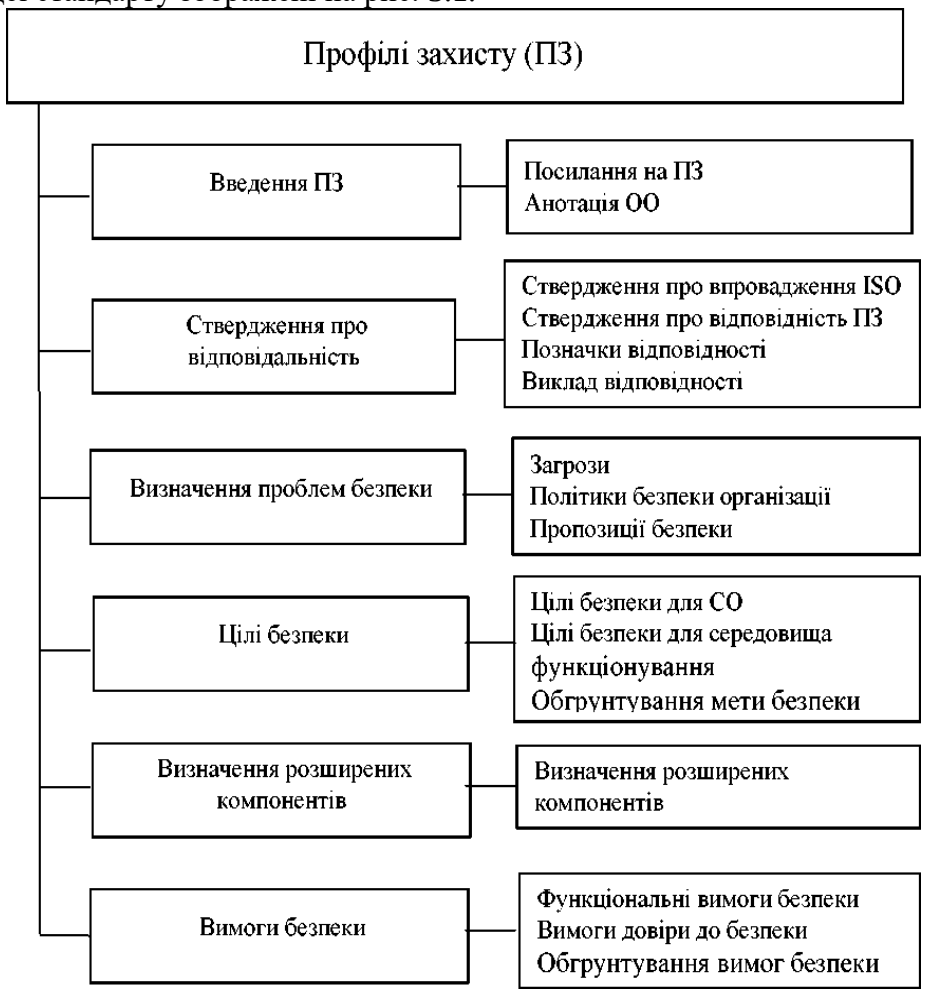


Рис. 3.1 Основні ідеї стандарту ISO / IEC 15408

Під ОО розуміється набір програмних, програмно-апаратних та / або апаратних засобів, можливо супроводжуваних посібниками.

В оцінці характеристик безпеки ОО зацікавлені в основному 3 групи користувачів: споживачі, розробники і оцінювачі.

Споживачі за результатами оцінки зможуть вирішити, чи задовольняє ОО їх потреби в

безпеці. Ці потреби зазвичай визначаються як наслідок аналізу ризиків, а також спрямованості політики безпеки. Споживачі можуть також використовувати результати оцінки для порівняння різних ОО.

Стандарт надає споживачам, особливо тим, що входять в групи і спільноти з єдиними інтересами, незалежну від реалізації структуру, яка називається профілем захисту (далі - ПЗ), для однозначного виразу їхніх вимог безпеки.

Стандарт призначений для підтримки розробників при підготовці до оцінки своїх ОО і сприяння в її проведенні, а також при встановленні вимог безпеки, яким повинні задовольняти ці ОО.

Дані вимоги містяться в залежною від реалізації конструкції, іменованої завданням з безпеки (далі - ЗБ). Ці ЗБ можуть базуватися на одному або декількох ПЗ, щоб показати, що ЗБ відповідають вимогам безпеки, пред'явлених споживачами, які встановлені в даних ПЗ.

Стандарт містять критерії, призначені для використання оцінювачами ОО при формуванні висновку про відповідність об'єктів оцінки пред'явленим до них вимогам безпеки.

Відповідно до стандарту безпека пов'язана із захистом активів. Активи - це сутності, що представляють цінність для кого-небудь. Середовище, в якому розміщуються ці активи, називається середовищем функціонування.

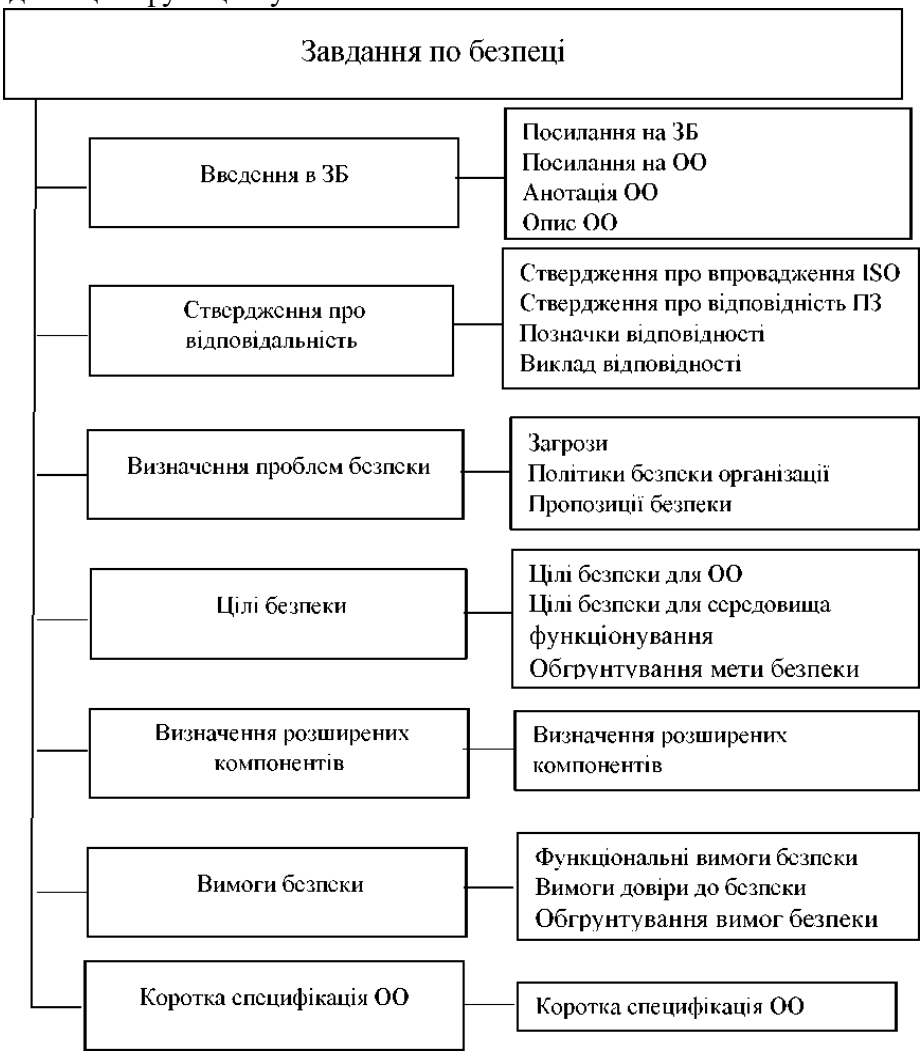


Рис. 3.2 Високорівневі поняття безпеки та їх взаємозв'язок

Багато активів представлені у вигляді інформації, яка зберігається, обробляється і передається продуктами ІТ таким чином, щоб задовольнити вимоги власників цієї інформації. Власник інформації має право вимагати, щоб доступність, поширення і модифікація будь-якої такої інформації суворо контролювалися і активи були захищені від загроз контрзаходами. Рис. 3.2 ілюструє високорівневі поняття безпеки та їх взаємозв'язок.

Багато власників активів не мають знань, досвіду та ресурсів, необхідних для

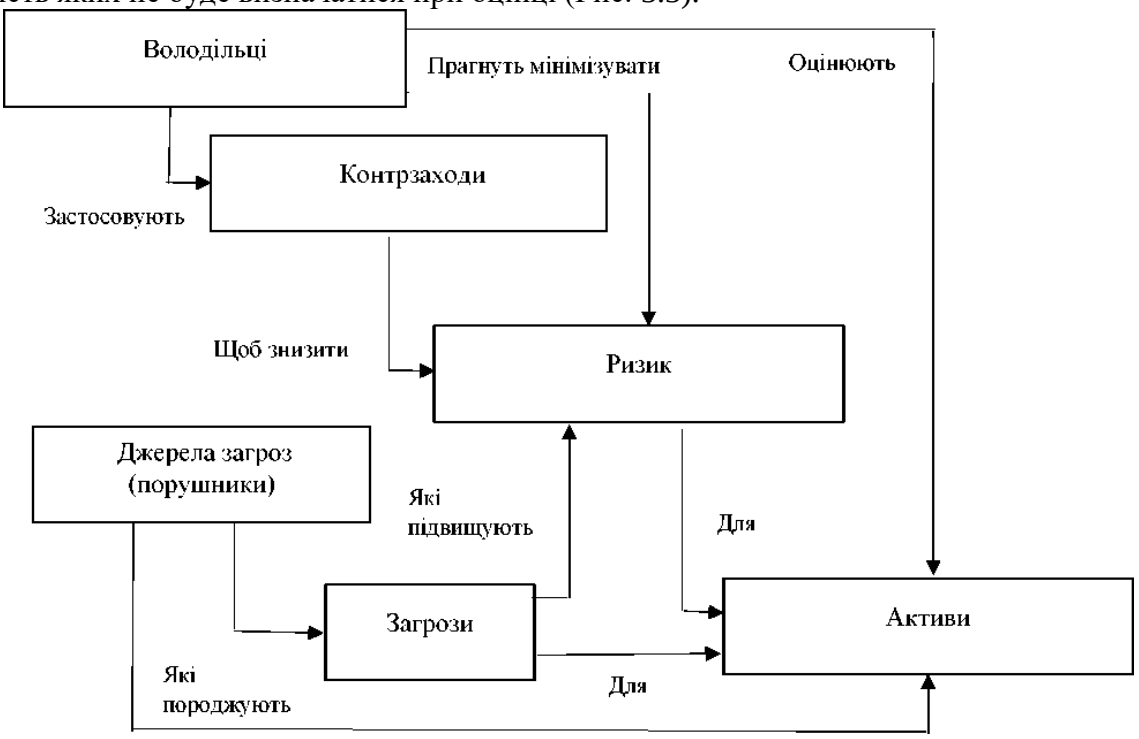
винесення судження про достатність і коректності контрзаходів, і при цьому вони можуть не захотіти покладатися виключно на затвердження розробників цих контрзаходів. Внаслідок цього дані споживачі можуть захотіти підвищити свою впевненість в достатності і правильності деяких або всіх контрзаходів шляхом замовлення оцінки цих контрзаходів. Рис 3.2 показує також поняття, використовувані при оцінці, і їх взаємозв'язок.

При оцінці достатність контрзаходів аналізується через конструкцію, звану ЗБ. Воно починається з опису активів і загроз цим активам. Потім в ЗБ описуються контрзаходи (в формі цілей безпеки) і демонструється, що дані контрзаходи є достатніми, щоб протистояти описаним загрозам: якщо контрзаходи здійснюють те, що заявлено по відношенню до них, то забезпечено протистояння загрозам.

Далі в ЗБ контрзаходи діляться на дві групи:

а) цілі безпеки для ОО: вони описують контрзаходи, коректність яких буде визначатися при оцінці (Рис. 3.2);

б) цілі безпеки для середовища функціонування: вони описують контрзаходи, коректність яких не буде визначатися при оцінці (Рис. 3.3).



Хочуть зловживати та/або можуть нанести збитків

Рис. 3.3 Цілі безпеки для об’єкта оцінки

В ЗБ для ОО, коректність контрзаходів ІТ якого будуть оцінювати в процесі оцінки, потрібна подальша деталізація цілей безпеки для ГО в функціональних вимогах безпеки (далі - ФВБ).

Таким чином, в ЗБ демонструється, що:

- ФВБ задовольняють цілям безпеки для ОО;
- цілі безпеки для ОО та цілі безпеки для середовища функціонування

протистоять загрозам;

- і ФВБ, і цілі безпеки для середовища функціонування протистоять загрозам.

З цього випливає, що коректний ОО (задовольняє ФВБ) в поєднанні з коректним середовищем функціонування (задовольняє цілям безпеки) буде протистояти загрозам.

Для визначення коректності ОО можуть виконуватися різні види діяльності, такі як:

- тестування ОО;
- дослідження різних проектних уявлень ОО;
- дослідження фізичної безпеки середовища розробки ОО.

ЗБ забезпечує структурований опис цих видів діяльності для визначення коректності в формі вимог довіри до безпеки (далі - ВДБ).

За стандартом визнають два типи оцінки: оцінка ЗБ / ОО і оцінка ПЗ.

Оцінка ЗБ / ОО проходить в два етапи:

- оцінка ЗБ: на цьому етапі визначають достатність ОО і середовища функціонування;
- оцінка ОО: на цьому етапі визначають коректність ОО; як зазначалося раніше, оцінка ОО не включає оцінку коректності середовища функціонування.

Результатом процесу оцінки ОО буде:

- яке твердження, що не всі ВДБ задоволені, і тому не досягнуть заданий рівень довіри до того, що ОО задовольняє ФВБ, які викладені в ЗБ;
- яке твердження, що все ВДБ задоволені, і тому досягнутий заданий рівень довіри до того, що ОО задовольняє ФВБ, які викладені в ЗБ.

Щоб дати можливість зацікавленим групам або співтовариствам споживачів висловити свої вимоги безпеки і полегшити розробку ЗБ, стандарт надає дві спеціальні конструкції: пакети і ПЗ.

Пакет - це певний набір вимог безпеки.

Пакети можуть бути двох видів, що містять:

- тільки ФВБ;
- тільки ВДБ.

У той час, як ЗБ завжди описує конкретний ОО (наприклад, міжмережевий екран Х-2, версія 3.1), ПЗ призначений для опису типу ОО (наприклад, міжмережеві екрани прикладного рівня). Тому один і той же ПЗ можна використовувати в якості шаблону для безлічі різних ЗБ, які будуть використовувати в різних оцінках.

Зазвичай ЗБ описує вимоги для ОО та його формує розробник ОО, в той час як ПЗ описує загальні вимоги для деякого типу ОО.

Тому ПЗ зазвичай розробляється:

- спільнотою користувачів, які прагнуть прийти до консенсусу щодо вимог для даного типу ОО;
- розробником ОО або групою розробників подібних ОО, які бажають встановити мінімальний базис для конкретного типу ОО;
- урядовою організацією або великою корпорацією, що визначають свої вимоги як частина процесу закупівлі.

ПЗ визначає допустимий тип відповідності ЗБ профілем захисту. Тобто в ПЗ встановлюють, які типи відповідності є допустимими для ЗБ, а саме:

- якщо в ПЗ встановлено, що потрібно «сувора відповідність», то ЗБ має в суворій формі відповідати ПЗ;
- якщо в ПЗ встановлено, що потрібно «демонстрована відповідність», то ЗБ має або строго відповідати ПЗ, або його відповідність ПЗ може бути продемонстровано.

Порядок отримання результатів оцінки ПЗ і ЗБ/ОО зображено на рис. 2.4. Очікувані результати оцінки ПЗ і ЗБ/ОО наступні:

- оцінки ПЗ дозволяють створювати каталоги (реєстри) оцінених ПЗ;
- оцінка ЗБ дає проміжні результати, які потім використовуються при оцінці ОО;
- оцінки ЗБ / ГО дозволяють створювати каталоги (реєстри) оцінених ОО.

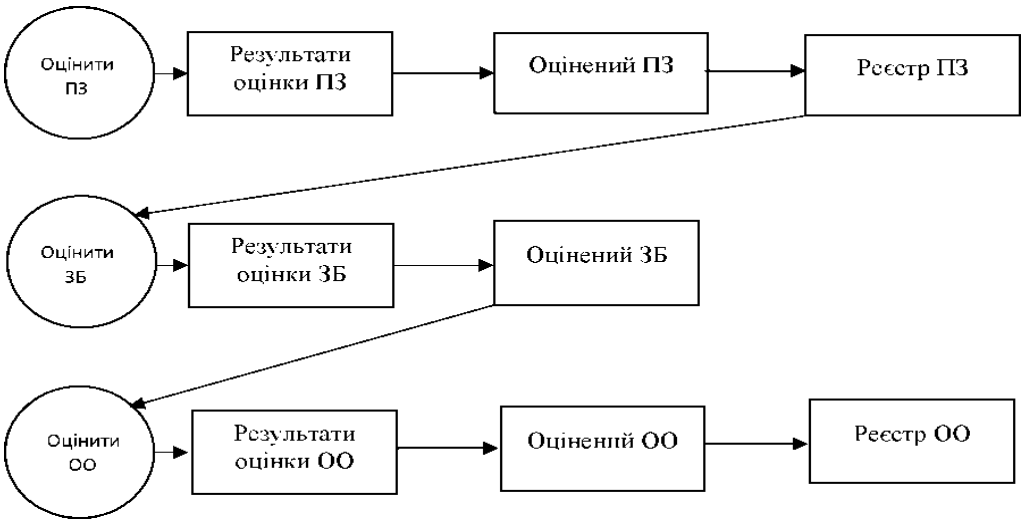


Рис. 3.4 Порядок отримання результатів оцінки ПЗ і ЗБ/ОО

Необхідно, щоб оцінка приводила до об'єктивних і повторюваних результатів, на які потім можна посилатися як на свідчення навіть при відсутності абсолютно об'єктивної шкали для представлення результатів оцінки безпеки ІТ. Наявність сукупності критеріїв оцінки є необхідною попередньою умовою для того, щоб оцінка приводила до значимого результату, надаючи технічну основу для взаємного визнання результатів оцінки різними органами оцінки.

Після оцінки ЗБ і ОО у власників активів є довіра (як визначено в ЗБ) до того, що ОО разом із середовищем функціонування протистоять конкретним загрозам. Результати оцінки можуть бути використані власником активів при прийнятті рішення про прийняття ризику, пов'язаного із схильністю активів впливу конкретних загроз.

Після введення оціненого ОО в експлуатацію зберігається можливість прояву в ОО раніше невідомих помилок або вразливостей. В цьому випадку розробник може внести зміни в ОО (щоб усунути уразливості) або змінити ЗБ, щоб виключити уразливості з області оцінки. У будь-якому випадку колишні результати оцінки можуть виявитися вже недійсними. Якщо виявиться необхідним відновити впевненість, то буде потрібно переоцінка.

ЛЕКЦІЯ 4
ІСТОРІЯ РОЗВИТКУ СТАНДАРТІВ УПРАВЛІННЯ ІБ. СТАНДАРТ ISO/IEC 27000

4.1. Історія розвитку стандартів управління ІБ в Європі

Сьогодні безпека цифрового простору показує новий шлях національної безпеки кожної країни. Відповідно до ролі інформації як цінного товару в бізнесі, її захист, безумовно, необхідний. Для досягнення цієї мети, кожній організації, в залежності від рівня інформації (з точки зору економічної цінності), потрібна розробка системи управління інформаційною безпекою (далі - СУІБ), захисту своїх інформаційних активів.

В організаціях, існування яких в значній мірі залежить від інформаційних технологій (далі - ІТ), можуть бути використані всі інструменти для захисту даних. Проте, безпека інформації необхідна також для споживачів, партнерів по співпраці, інших організацій і уряду. У зв'язку з цим, для захисту цінної інформації, необхідно щоб кожна організація прагнула до тієї чи іншої стратегії та реалізації системи безпеки на її основі.

СУІБ є частиною комплексної системи управління, заснованої на оцінці та аналізі ризиків, для розробки, реалізації, адміністрування, моніторингу, аналізу, підтримки та підвищення ІБ і її реалізації, отриманих з цілей організації і вимоги, вимоги безпеки, які використовуються процедур і розмірах і структурі її організації.

Зародження принципів і правил управління ІБ почалося в Великобританії в 1980-х роках. У ті роки Міністерство торгівлі і промисловості Великобританії (англ. Department of Trade and Industry, DTI) організувало робочу групу для розробки зводу кращих практик щодо забезпечення ІБ.

У 1989 році «DTI» опублікувало перший стандарт в цій області, який називався PD 0003 «Практичні правила управління ІБ». Він представляв собою перелік засобів управління безпекою, які в той час вважалися адекватними, нормальними і хорошими, застосовними як до технологій, так і середовищ того часу. Документ «DTI» був опублікований як керівний документ британської системи стандартів (англ. British Standard, BS).

У 1995 році Британський інститут стандартів (англ. British Standards Institution, BSI) прийняв національний стандарт BS 7799-1 «Практичні правила управління ІБ». Вона описував 10 областей і 127 механізмів контролю, необхідних для побудови СУІБ (англ. Information Security Management System, ISMS), визначених на основі кращих прикладів зі світової практики.

Цей стандарт і став прабатьком всіх міжнародних стандартів СУІБ. Як і будь-який національний стандарт BS 7799 в період 1995-2000 років користувався, скажімо так, помірною популярністю тільки в рамках країн британської співдружності.

У 1998 році з'явилася друга частина цього стандарту - BS 7799-2 «СУІБ. Вимоги та настанови щодо застосування», що визначила загальну модель побудови СУІБ і набір обов'язкових вимог, на відповідність яким повинна проводитися сертифікація. З появою другої частини BS 7799, що визначила, що повинна з себе представляти СУІБ, почався активний розвиток системи сертифікації в галузі управління безпекою.

В кінці 1999 року експерти Міжнародної організації зі стандартизації (англ. International Organization for Standardization, ISO) і Міжнародної електротехнічної комісії (англ. International Electrotechnical Commission, IEC) прийшли до висновку, що в рамках існуючих стандартів відсутній спеціалізований стандарт управління ІБ. Відповідно, було прийнято рішення не займатися розробкою нового стандарту, а за погодженням з «BSI», взявши за базу BS 7799-1, прийняти відповідний міжнародний стандарт ISO / IEC.

В кінці 1999 року обидві частини BS 7799 були переглянуті і гармонізовані з міжнародними стандартами систем управління якістю ISO / IEC 9001 та екологією ISO / IEC 14001, а рік по тому без змін BS 7799-1 був прийнятий як міжнародний стандарт ISO / IEC 17799 2000 «Інформаційні технології (далі - ІТ). Практичні правила управління ІБ ».

У 2002 році була оновлена і перша частина стандарту BS 7799 - 1 (ISO / IEC 17799), і друга частина BS 7799-2.

Що ж стосується офіційної сертифікації по ISO / IEC 17799, то вона спочатку не була передбачена (повна аналогія з BS 7799). Була передбачена тільки сертифікація по BS 7799-2,

який представляв собою ряд обов'язкових вимог (що не увійшли в BS 7799-1) і в додатку перелік умовно обов'язкових (на розсуд сертифікатора) найбільш важливих вимог BS 7799-1 (ISO / IEC 17799).

На території СНД першою країною, яка в листопаді 2004 року прийняла стандарт ISO / IEC 17799: 2000 у якості національного, була Білорусь.

У складі ISO / IEC за розробку сімейства міжнародних стандартів з управління ІБ відповідає підкомітет № 27, тому була прийнята схема нумерації даного сімейства стандартів з використанням серії послідовних номерів, починаючи з 27000 (27k).

У 2005 році підкомітет SC 27 «Методи захисту ІТ» Об'єднаного технічного комітету JTC 1 «ІТ» ISO / IEC розробив сертифікаційний стандарт ISO / IEC 27001 «ІТ. Методи захисту. СУІБ. Вимоги », що прийшов на зміну BS 7799-2, і тепер сертифікація проводиться вже по ISO 27001.

В Україні ISO / IEC 27001: 2005 в якості національного стандарту введений в дію тільки з 1 липня 2012 року.

У 2005 році на основі ISO / IEC 17799 2000 був розроблений ISO / IEC 27002: 2005 «ІТ. Методи захисту. Звід норм і правил управління ІБ ».

На початку 2006 року був прийнятий новий британський національний стандарт BS 7799-3 «СУІБ. Керівництво з управління ризиками ІБ», який в 2008 році отримав статус міжнародного стандарту ISO / IEC 27005« ІТ. Методи захисту. Управління ризиками ІБ ».

У 2004 році Британським інститутом стандартів було опубліковано стандарт ISO / IEC TR 18044 «ІТ. Методи захисту. Управління інцидентами ІБ ». У 2011 році на його базі був розроблений стандарт ISO / IEC 27035 «ІТ. Методи захисту. Управління інцидентами ІБ ».

У 2009 році був прийнятий стандарт ISO / IEC 27000 «ІТ. СУІБ. Загальний огляд і термінологія». Він надає огляд систем управління ІБ і визначає відповідні терміни. Словник ретельно сформульованих формальних визначень охоплює більшість спеціалізованих термінів, пов'язаних з ІБ і використовуваних в стандартах групи ISO / IEC 27.

25 вересня 2013 року було опубліковано нові версії стандартів ISO / IEC 27001 та 27002. З цього моменту стандарти серії ISO / IEC 27k (управління ІБ) повністю інтегровані до стандартів серії ISO / IEC 20k (управління ІТ-сервісами). Вся термінологія з ISO / IEC 27001 перенесена в ISO / IEC 27000, який визначає загальний термінологічний апарат для всього сімейства стандартів ISO / IEC 27k.

В Україні впровадженням міжнародних стандартів у національні стандарти, узагальненням світового досвіду в галузі стандартизації та впровадженням міжнародних стандартів в Україні займається Технічний комітет зі стандартизації № 20 (далі - ТК-20) «Інформаційні технології», який функціонує на базі Міжнародного науково-навчального центру ІТ і систем Національної академії наук і Міністерства освіти і науки України.

ТК-20 є активним учасником підкомітетів Міжнародної організації з стандартизації та Міжнародної електротехнічної комісії (ISO / IEC), Європейської організації зі стандартизації (CEN), а також Європейського комітету зі стандартизації в галузі електротехніки (CENELEC). ТК-20 також здійснює формування напрямків розвитку науково-технічної політики України в сфері міжнародної стандартизації в галузі ІТ та ЕЦП.

Офіційний сайт Центру: http://www.irtc.org.ua.

В даний час в Україні в якості національних впроваджені такі міжнародні стандарти:

1) Затверджені наказом Держспоживстандарту від 31.10.2003 № 189:

- ДСТУ ISO / IEC TR 13335-1: 2003 Інформаційні технології. Настанови з керування безпеки інформаційних технологій. Частина 1. Концепції та моделі безпеки інформаційних технологій (ISO / IEC TR 13335-1: 1996, IDT);
- ДСТУ ISO / IEC TR 13335-2: 2003 Інформаційні технології. Настанови з керування безпеки інформаційних технологій. Частина 2. Керування та планування безпеки інформаційних технологій (ISO / IEC TR 13335-2: 1997, IDT);
- ДСТУ ISO / IEC TR 13335-3: 2003 Інформаційні технології. Настанови з керування безпеки інформаційних технологій. Частина 3. Методи керування захист інформаційних технологій (ISO / IEC TR 13335-3: 1998, IDT)
- 2) Затверджені наказом Держспоживстандарту від 03.03.2005 № 57:

• ДСТУ ISO / IEC TR 13335-4: 2005 формаційні технології. Настанови з управління безпеки інформаційних технологій. Частина 4. Вибирання засобів захисту (ISO / IEC TR 13335-4: 2000, IDT);

• ДСТУ ISO / IEC TR 13335-5: 2005 ^формаційні технології. Настанови з управління безпеки інформаційних технологій. Частина 5. Настанова з управління. Мережна безпека (ISO / IEC TR 13335-5: 2001, IDT);

3) Затверджені наказом Держспоживстандарту від 28.12.2010 № 631:

• ДСТУ ISO / IEC 27001: 2010 ^формаційні технології. Методи та засоби Досягнення

інформаційної безпеки. Системи керування інформаційною безпеки. Вимоги (ISO / IEC 27001: 2005, IDT).

28 жовтня 2010 постановою Правління Національного банку України № 474 вступили в силу такі стандарти з управління інформаційною безпекою в банківській системі України:

• СОУ Н НБУ 65.1 СУІБ 1.0: 2010 року Методи захисту в банківській діяльності. Система управління інформаційною безпеки. Вимоги (ISO / IE 27001: 2005, MOD);

• СОУ Н НБУ 65.1 СУІБ 2.0: 2010 року Методи захисту в банківській діяльностіI. Звід правил для управління інформаційною безпеки (ISO / IE 27002: 2005, MOD).

Крім того, 25 грудня 2014 року спільним наказом Адміністрації Держспецзв'язку та Міністерства юстиції України № 2170/5/703 був оновлений перелік міжнародних стандартів для їх подальшого впровадження в Україні:

«Перелік міжнародних та європейських стандартів, інших АКТІВ технічного регулювання для гармонізації з метою реформування, розвитку та забезпечення інтероперабельності системи ЕЦП»

1. ISO / IEC 27000 до: 2013 Information technology - Security techniques - Information security management systems - Overview and vocabulary
2. ISO / IEC 27001: 2013 Information technology - Security techniques - Information security management systems - Requirements
3. ISO / IEC 27002: 2013 Information technology - Security techniques - Code of practice for information security management
5. ISO / IEC 27005: 2011 Information technology - Security techniques - Information security risk management
6. ISO / IEC 27006: 2007 Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems
7. ISO / IEC 27007: 2011 Information technology - Security techniques - Guidelines for information security management systems auditing
8. ISO / IEC TR 27008: 2011 Information technology - Security techniques - Guidelines for auditors on information security management systems controls
9. ISO / IEC 27010 до: 2012 Information technology - Security techniques - Information security management for inter-sector and inter-organizational communications
16. ISO / IEC 27035: 2011 Information technology - Security techniques - Information security incident management »

4.2 Стандарт ISO/IEC 27000. Основні характеристики.

Останнє оновлення стандарту ISO / IEC 27000 «IT. СУІБ. Загальний огляд і термінологія» відбулося у 2016 році.

Стандарт складається з наступних розділів:

• - Вступ;
• - сфера застосування;
• - терміни та визначення;
• - системи управління ІБ;
• - сімейство стандартів СУІБ.

3.2.0. Вступ

3.2.0.1 Огляд

Міжнародні стандарти системи управління ІБ представляють собою модель для налагодження і функціонування системи управління. Ця модель включає в себе функції, за якими експерти дійшли згоди на підставі міжнародного досвіду, накопиченого в цій області.

При використанні сімейства стандартів СУІБ організації можуть реалізовувати і вдосконалювати СУІБ і підготуватися до її незалежної оцінки, яка застосовується для захисту інформації, такої як фінансова інформація, інтелектуальна власність, інформація про персонал, а також інформація, довірена клієнтами або третіми особами. Ці стандарти можуть використовуватися організацією для підготовки незалежної оцінки своєї СУІБ, застосовуваної для захисту інформації.

3.2.0.2 Сімейство стандартів СУІБ

Сімейство стандартів СУІБ, що має загальну назву «Information technology. Security techniques» (Інформаційна технологія. Методи захисту), призначене для допомоги організаціям будь-якого типу і розміру в реалізації і функціонуванні СУІБ і складається з наступних міжнародних стандартів:

- ISO / IEC 27000 СУІБ. Загальний огляд і термінологія;
- ISO / IEC 27001 СУІБ. вимоги;
- ISO / IEC 27002 Звід правил з управління ІБ;
- ISO / IEC 27003 Керівництво по реалізації СУІБ;
- ISO / IEC 27004 УІБ. вимірювання;
- ISO / IEC 27005 Управління ризиками ІБ;
- ISO / IEC 27006 Вимоги для органів, що забезпечують аудит і сертифікацію СУІБ;
- ISO / IEC 27007 Керівництво по проведенню аудиту СУІБ;
- ISO / IEC TR 27008 Керівництво з аудиту механізмів контролю ІБ;
- ISO / IEC 27010 УІБ для міжсекторальних та міжорганізаційних комунікацій;
- ISO / IEC 27011 Керівництво по УІБ для телекомунікаційних організацій на основі ISO / IEC 27002;
- ISO / IEC 27013 Керівництво по інтегрованій реалізації стандартів ISO / IEC 27001 та ISO / IEC 20000-1;
- ISO / IEC 27014 Управління ІБ вищим керівництвом;
- ISO / IEC TR 27015 Керівництво по УІБ для фінансових сервісів;
- ISO / IEC TR 27016 УІБ. Організаційна економіка;
- ISO / IEC 27035 Управління інцидентами ІБ (в стандарті не вказано).

Міжнародний стандарт, що не мають загальної назви:

- ISO 27799 Інформатика в охороні здоров'я. УІБ за стандартом ISO / IEC 27002.

Стандарт надає огляд СУІБ і визначає відповідні умови.

Сімейство стандартів СУІБ містить стандарти, які:

- визначають вимоги до СУІБ і сертифікації таких систем;
- містять пряму підтримку, детальне керівництво і роз'яснення цілого процесу створення, впровадження, супроводу та поліпшення СУІБ;
- включають в себе галузеві керівні принципи для СУІБ;
- керують проведенням оцінки відповідності СУІБ.

4.2.1 Сфера застосування

Стандарт представляє собою огляд СУІБ, а також умов і визначень, які широко використовуються в стандартах СУІБ. Стандарт застосовується до всіх типів і розмірів організацій (наприклад, комерційні підприємства, урядові установи, неприбуткові організації).

4.2.2 Терміни та визначення

Розділ містить визначення 89 термінів, наприклад:

- інформаційна система - додатки, сервіси, IT активи та інші компоненти обробки інформації;
- -нформаційна безпека (ІБ) - збереження конфіденційності, цілісності та доступності інформації;

- доступність - властивість бути доступним і готовим до використання за запитом уповноваженої особи;
- конфіденційність - властивість інформації бути недоступною або закритою для неуповноважених осіб;
- цілісність - властивість точності і повноти;
- неспростовність - здатність засвідчувати настання події або дії котрі створюють суб'єкти;
- подія ІБ - виявлене стан системи (сервісу або мережі), що вказує на можливе порушення політики або заходів ІБ, або невідома ситуація, яка може стосуватися безпеки;
- інцидент ІБ - одне або кілька подій ІБ, які зі значним ступенем вірогідності призводять до компрометації бізнес-операцій і створюють загрози для ІБ;
- управління інцидентами ІБ - процеси виявлення, оповіщення, оцінки, реагування, розгляду і вивчення інцидентів ІБ;
- система управління - набір взаємопов'язаних елементів організації для встановлення політик, цілей і процесів для досягнення цих цілей;
- моніторинг ІБ - визначення статусу системи, процесу або дії;
- політика ІБ - спільний намір і напрямок, офіційно виражене керівництвом;
- загроза ІБ - можлива причина небажаного інциденту, який може завдати шкоди;
- вразливість ІБ - нестача активу або заходи захисту, яке може бути використано однією або декількома загрозами.

4.2.3. Системи управління ІБ

Розділ «СУІБ» складається з наступних основних пунктів:

- опис СУІБ;
- впровадження, контроль, супровід і поліпшення СУІБ;
- переваги впровадження стандартів сімейства СУІБ.

3.2.3.1 Вступ

Організації всіх типів і розмірів:

- збирають, обробляють, зберігають і передають інформацію;
- усвідомлюють, що інформація і пов'язані процеси, системи, мережі і люди є важливими активами для досягнення цілей організації;
- стикаються з цілою низкою ризиків, які можуть вплинути на функціонування активів;
- усувають передбачуваний ризик за допомогою впровадження заходів і засобів ІБ.

Вся інформація, що зберігається і обробляється організацією, є об'єктом для загроз атаки, помилки, природи (наприклад, пожежа або повінь) і т.п. і об'єктом вразливостей, властивих її використання.

Зазвичай поняття ІБ базується на інформації, що розглядається як цінність активів і вимагає відповідного захисту (наприклад, від втрати доступності, конфіденційності та цілісності). Можливість отримати своєчасний доступ уповноважених осіб до точної і повної інформації є каталізатором бізнес-ефективності.

Ефективний захист інформаційних активів шляхом визначення, створення, супроводу і поліпшення ІБ є необхідною умовою для досягнення організацією своїх цілей, а також підтримки та поліпшення правової відповідності та репутації. Ці координовані дії, спрямовані на впровадження належних заходів захисту і обробку неприйнятних ризиків ІБ, загальновідомі як елементи управління ІБ.

У міру зміни ризиків ІБ і ефективності заходів захисту в залежності від зиінних обставин організації слід:

- контролювати і оцінювати ефективність впроваджених заходів та процедур захисту;
- ідентифікувати виникаючі ризики для обробки;
- вибирати, впроваджувати і покращувати відповідні заходи захисту належним чином.

Для взаємозв'язку і координації дій ІБ кожної організації слід сформувати політику і цілі ІБ і ефективно досягати цих цілей, використовуючи систему управління.

3.2.3.2 Опис СУІБ

Опис СУІБ передбачає наступні складові:

- положення і принципи;
- інформація;
- інформаційна безпека;
- управління;
- система управління;
- процесний підхід;
- важливість СУІБ.

Положення і принципи

СУІБ складається з політик, процедур, керівництв і відповідних ресурсів і дій, колективно керованих організацією, для досягнення захисту своїх інформаційних активів. СУІБ визначає систематичний підхід до створення, впровадження, обробки, контролю, перегляду, супроводу і поліпшенню ІБ організації для досягнення бізнес-цілей.

Вона базується на оцінці ризику і прийнятних рівнях ризику організації, розроблених для ефективної обробки і управління ризиками. Аналіз вимог захисту інформаційних активів і застосування відповідних заходів захисту, щоб забезпечити необхідний захист цих активів, сприяє успішній реалізації СУІБ.

Наступні основні принципи сприяють успішній реалізації СУІБ:

- - розуміння необхідності системи ІБ;
- - призначення відповідальності за ІБ;
- - об'єднання зобов'язань керівництва та інтересів зацікавлених осіб;
- - зростання соціальних цінностей;
- - оцінки ризику, що визначають відповідні заходи захисту для досягнення допустимих рівнів ризику;
- - безпеку як невід'ємний елемент ІС і мереж;
- - активне попередження і виявлення інцидентів ІБ;
- - забезпечення комплексного підходу до УІБ;
- - безперервна переоцінка і відповідне поліпшення ІБ.

Інформація

Інформація - це актив, який поряд з іншими важливими бізнес-активами важливий для бізнесу організації і, отже, повинен бути відповідно захищений. Інформація може зберігатися в різних формах, включаючи такі як цифрова форма (наприклад, файли з даними, що зберігаються на електронних або оптичних носіях), матеріальна форма (наприклад, на папері), а також в нематеріальному вигляді в формі знань співробітників.

Інформація може бути передана різними способами, включаючи кур'єра, електронну або голосову комунікацію. Незалежно від того, в якій формі представлена інформація і яким способом передається, вона повинна бути належним чином захищена.

У багатьох організаціях інформація залежить від інформаційної та комунікаційної технології. Ця технологія є істотним елементом в будь якій організації і полегшує створення, обробку, зберігання, передачу, захист і знищення інформації.

Інформаційна безпека

ІБ включає в себе три основних виміри (властивості): конфіденційність, доступність і цілісність. ІБ передбачає застосування та управління відповідними заходами безпеки, які включають в себе розгляд широкого діапазону загроз, з метою забезпечення тривалого успіху і безперервності бізнесу та мінімізації впливів інцидентів ІБ.

ІБ досягається застосуванням відповідного набору заходів захисту, визначеного за допомогою процесу управління ризиками і керованого з використанням СУІБ, включаючи політики, процеси, процедури, організаційні структури, програмні та апаратні засоби, щоб захистити ідентифіковані інформаційні активи.

Ці заходи захисту повинні бути визначені, реалізовані, проконтрольовані, перевірені і

при необхідності поліпшені, щоб гарантувати, що рівень ІБ відповідає бізнес-цілям організації. Відповідні заходи і засоби ІБ слід органічно інтегрувати в бізнес-процеси організації.

Управління

Управління включає в себе дії по керівництву, контролю і безперервному вдосконаленню організації в рамках відповідних структур. Управлінська діяльність включає в себе дії, методи або практику формування, обробки, напрямки, спостереження і контролю ресурсів. Величина управлінської структури може варіюватися від однієї людини в невеликих організаціях до управлінської ієрархії в великих організаціях, що складаються з багатьох людей.

Щодо СУІБ управління включає в себе спостереження і вироблення рішень, необхідних для досягнення бізнес-цілей за допомогою захисту інформаційних активів. Управління ІБ виражається через формулювання і використання політик ІБ, процедур та рекомендацій, які потім застосовуються повсюдно в організації всіма особами, пов'язаними з нею.

Система управління

Система управління використовує сукупність ресурсів для досягнення цілей організації. Система управління організації включає в себе структуру, політики, планування, зобов'язання, методи, процедури, процеси і ресурси.

У частині ІБ система управління дозволяє організації:

- - задовольняти вимоги безпеки клієнтів та інших зацікавлених осіб;
- - покращувати плани і діяльність організації;
- - відповідати цілям ІБ організації;
- - виконувати нормативи, законодавство і галузеві накази;
- - організовано управляти інформаційними активами для сприяння постійному поліпшенню і корекції поточних цілей організації.

Процесний підхід

Організації потрібно вести різні види діяльності і управляти ними для того, щоб функціонувати ефективно і результативно. Будь-який вид діяльності, який використовує ресурси, потребує управлінні для того, щоб забезпечити можливість перетворення входів в виходи за допомогою сукупності взаємопов'язаних дій, - це також називається процесом.

Вихід одного процесу може безпосередньо формувати вхід наступного процесу, і зазвичай така трансформація відбувається в планованих і керованих умовах. Застосування системи процесів у рамках організації разом з ідентифікацією і взаємодією цих процесів, а також їх управлінням може бути визначено як «процесний підхід».

Додаткова інформація щодо процесного підходу (В стандарті відсутня)

Родоначальником процесного підходу до управління якістю прийнято вважати американського вченого Уолтера Шухарта. Його книга починається з виділення 3-х стадій в управлінні якістю результатів діяльності організації:

1) розробка специфікації (технічне завдання, технічні умови, критерії досягнення цілей) того, що потрібно;

2) виробництво продукції, що задовольняє специфікації;

3) перевірка (контроль) виробленої продукції для оцінки її відповідності специфікації.

Специфікації ► Виробництво ► Перевірка

Шухарт одним з перших запропонував лінійне сприйняття зазначених стадій замкнути в цикл, який він ототожнив з «динамічним процесом набуття знань».

Після першого циклу результати перевірки повинні бути основою вдосконалення специфікації на продукцію. Далі виробничий процес коригується на основі уточненої специфікації, а новий результат виробничого процесу знову ж піддається перевірці і т. д.

Американський вчений Едвардс Демінг трансформував цикл Шухарта в форму, яка найбільш часто зустрічаються сьогодні. Він, щоб перейти від контролю якості до управління якістю, дав більш загальні назви кожному з етапів, і, крім того, додав ще один, 4-й етап, за допомогою якого він хотів звернути увагу американських менеджерів на те, що вони недостатньо аналізують отриману на третьому етапі інформацію і не покращують

процес. Саме тому цей етап називається «впливай» (Act), і відповідно цикл Шухарта-Демінга називають моделлю «PDCA» або «PDSA»:

Плануй (Plan) ► Роби (Do) ► Перевіряй (Check)

або Вивчай (Study) ► впливай (Act)

- *Plan - Планування - ідентифікація та аналіз проблем; оцінка можливостей, постановка цілей і розробка планів;*
- *Do - Реалізація - пошук рішення проблем і реалізація планів;*
- *Check (Study) - Оцінка результативності - оцінка результатів реалізації та висновки відповідно до поставленим завданням;*
- *Act - Поліпшення - прийняття рішень на основі отриманих висновків, корекція і поліпшення роботи.*

Модель «PDCA» для СУІБ

Планування - Реалізація - Контроль - Поліпшення

1. Планування (Розробка та проектування)	*Встановлення цілей, політик, елементів управління., процесів і процедур СУІБ для досягнення результатів, відповідних загальній політиці і цілям організації*
2. Реалізація (Впровадження та забезпечення функціонування)	*Впровадження і застосування політик ІБ, елементів управління, процесів і процедур СУІБ з оцінки та обробці ризиків та інцидентів ІБ*
3. Контроль Моніторингі аналіз функціонування)	*Оцінка результативності виконання вимог політик, цілей ІБ і ефективності функціонування СУІБ і оповіщення вищого керівництва про результати*
4. Поліпшення (Супровід та удосконалення)	*Проведення коригувальних та запобіжних дій, заснованих на результатах аудиту та аналізу з боку керівництва для досягнення поліпшення СУІБ*

Метод і цикл Шухарта-Демінга, який частіше називають циклом Демінга, зазвичай ілюструють схему управління будь-яким процесом діяльності. Він з необхідними уточненнями до теперішнього часу набув широкого застосування в міжнародних стандартах управління:

- *якістю продукції ISO 9000;*
- *охороною навколишнього середовища ISO 14000;*
- *технікою безпеки і охороною праці OHSAS 18000;*
- *інформаційними сервісами ISO / IEC 20000;*
- *безпечністю харчової продукції ISO 22000;*
- *інформаційною безпекою ISO / IEC 27000;*
- *безпекою ISO 28000;*
- *безперервністю бізнесу ISO 22300;*
- *ризиками ISO 31000;*
- *енергетикою ISO 50000.*

Важливість СУІБ

Організація повинна визначити ризики, пов'язані з інформаційними активами. Досягнення ІБ вимагає управління ризиком і охоплює ризики фізичні, людські та технологічні, пов'язані з загрозам, що стосуються всіх форм інформації всередині організації або використовуваної організацією.

Ухвалення СУІБ є стратегічним рішенням для організації, і необхідно, щоб це рішення постійно інтегрувалися, оцінювалося і оновлювалося відповідно до потреб організації.

На розробку і реалізацію СУІБ організації впливають потреби і цілі організації, вимоги

безпеки, які використовуються бізнес-процеси, а також розмір і структура організації. Розробка і функціонування СУІБ повинні відображати інтереси і вимоги ІБ всіх зацікавлених осіб організації, включаючи клієнтів, постачальників, бізнес-партнерів, акціонерів та інших третіх сторін.

У взаємопов'язаному світі інформація та пов'язані з нею процеси, системи та мережі складають критичні активи. Організації та їх ІС і мережі стикаються із загрозами безпеці з широкого діапазону джерел, включаючи комп'ютерне шахрайство, шпигунство, саботаж, вандалізм, а також пожежа і повінь. Пошкодження ІС і систем, викликані шкідливим ПЗ, діями хакерів і DoS-атаками, стали більш поширеними, більш масштабними і витонченішими.

СУІБ важлива для підприємств як державного, так приватного сектора. У будь-якій галузі СУІБ є необхідним інструментом для підтримки електронного бізнесу і важлива для дій з управління ризиком. Взаємозв'язок загальнодоступних і приватних мереж і обмін інформаційними активами ускладнюють управління доступом до інформації та її обробку.

Крім того, поширення мобільних пристроїв зберігання даних, що містять інформаційні активи, може послабити ефективність традиційних заходів захисту. Коли організації приймають сімейство стандартів СУІБ, здатність застосування послідовних і взаємопов’язаних принципів ІБ можна продемонструвати бізнес-партнерам та іншим зацікавленим сторонам.

ІБ не завжди враховується при створенні і розробці ІС. Крім того, часто вважається, що ІБ - це технічна проблема. Однак ІБ, яка може бути досягнута за допомогою технічних засобів, обмежена і може бути неефективною, не будучи підтриманою відповідним управлінням та процедурами в контексті СУІБ. Вбудовування системи безпеки в функціонально завершену ІС може бути складним і дорогим.

СУІБ включає в себе ідентифікацію наявних заходів захисту і вимагає ретельного планування і уваги до деталей. Наприклад, заходи розмежування доступу, які можуть бути технічними (логічними), фізичними, адміністративними (управлінськими), або їх комбінацією, гарантують, що доступ до інформаційних активів санкціонується і обмежується на підставі вимог бізнесу і ІБ.

Успішне застосування СУІБ важливо для захисту інформаційних активів, оскільки дозволяє:

- підвищити гарантії того, що інформаційні активи адекватно захищені на безперервній основі від загроз ІБ;
- підтримувати структуровану і всебічну систему оцінки загроз ІБ, вибору і застосування відповідних заходів захисту, вимірювання та поліпшення їх ефективності;
- постійно покращувати середовище управління організації;
- ефективно відповідати правовим і нормативним вимогам.

4.3 ДСТУ ISO 27001, ISO 27002, ISO 27003

Система кібербезпеки, яка базується на міжнародних стандартах надзвичайно важлива у сучасному цифровому світі. Розробкою зазначених стандартів займаються Міжнародна організація з стандартизації (ISO) спільно з Міжнародною електротехнічною комісією (IEC). На сьогодні фахівцями цих організацій розроблена серія стандартів ISO/IEC 27000, яка постійно доповнюється новими документами. В Україні на даний час діють стандарти серії ДСТУ ISO/IEC 27000, які відповідно гармонізовані з ISO/IEC 27000. До них відносяться наступні:

ДСТУ ISO/IEC 27000:2019

ДСТУ ISO/IEC 27000:2019 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Огляд і словник термінів (ISO/IEC 27000:2018, IDT) – ISO/IEC 27000:2018 дає змогу переглянути системи управління інформаційною безпекою (СУІБ). Це також забезпечує терміни і визначення, як правило, використовувані в СУІБ сімейства стандартів. Цей документ є застосованим до всіх типів і розмірів організації (наприклад, комерційні організації, державні агенції, не для сприяння охоплюють

загальновживані терміни та визначення в сімействі стандартів СУІБ; не підтримують всі терміни і терміни, які застосовуються в сімействі стандартів СУІБ; не встановлює значення СУІБ у стандартах у визначенні нових термінів для використання.

ДСТУ ISO/IEC 27001:2015

ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT) – Цей стандарт визначає вимоги до проектування, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою з урахуванням обставин організації. Цей стандарт також містить вимоги для оцінювання та оброблення ризиків інформаційної безпеки, пов'язаних з потребами організації. Вимоги, наведені в цьому стандарті, є загальними та можуть бути запроваджені для всіх організацій незалежно від типу, розміру та природи. Вилучення будь-якої з вимог, наведених в розділах 4- 10 неприпустимо в разі, якщо організація прагне відповідати цьому стандарту.

Входить в групу стандартів ISO 27000 – СУІБ та тісно пов'язаний із стандартом ISO/IEC 27002.

У стандарті ISO/IEC 27001 (ISO 27001) зібрані описи найкращих світових практик в області управління інформаційною безпекою. ISO 27001 встановлює вимоги до системи менеджменту інформаційної безпеки для демонстрації здатності організації захищати свої інформаційні ресурси. Цей стандарт підготовлений в якості моделі для розробки, впровадження, функціонування, моніторингу, аналізу, підтримки та поліпшення **СистемиУправління Інформаційної Безпеки (СУІБ)**.

Система управління інформаційною безпекою СУІБ (англ. *information security management system,* ISMS) – частина загальної системи управління, яка ґрунтується на підході, що враховує ризики інформаційної безпеки як бізнес- ризики, призначена для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення інформаційної безпеки.

Для **процесів СУІБ застосована модель ПВПД** (плануй-виконуй- перевіряй- дій; англ. ***Plan-Do-Check-Act, PDCA***):

- Plan (планування) – фаза створення СУІБ, створення переліку активів, оцінки ризиків та вибору заходів;
- Do (дія) – етап реалізації та впровадження відповідних заходів;
- Check (перевірка) – фаза оцінки ефективності та продуктивності СУІБ. Зазвичай виконується внутрішніми аудиторами;
- Act (поліпшення) – виконання превентивних і коригуючих дій

Складові політики інформаційної безпеки:

- визначення критичних бізнес-процесів/банківських продуктів;
- надання доступу до інформації;
- контроль доступу;
- парольний захист;
- антивірусний захист;
- захист мережі банку;
- віддалений доступ до ресурсів мережі;
- ідентифікація та автентифікація ресурсів СУІБ;
- криптографічний захист інформації;
- політика «чистого екрана» та «чистого стола»

Мета СУІБ – вибір відповідних заходів управління безпекою, призначених для захисту інформаційних активів і гарантують довіру зацікавлених сторін.

Інформаційна безпека – збереження конфіденційності, цілісності та доступності інформації; крім того, можуть бути включені і інші властивості, такі як справжність, неможливість відмови від авторства, достовірність.

Конфіденційність – забезпечення доступності інформації тільки для тих, хто має відповідні повноваження (авторизовані користувачі).

Доступність – забезпечення доступу до інформації авторизованим користувачам, коли це необхідно (на вимогу).

Цілісність – забезпечення точності і повноти інформації, а також методів її обробки.

Саме поняття «**Захист інформації**» трактується міжнародним стандартом як забезпечення конфіденційності, цілісності та доступності інформації. Основа стандарту ICO 27001 – система управління ризиками, пов'язаними з інформацією. **Система управління ризиками** дозволяє отримувати відповіді на наступні питання:

- на якому напрямку інформаційної безпеки потрібно зосередити увагу;
- скільки часу і коштів можна витратити на дане технічне рішення для захисту інформації.

Стандарт ISO 27001 гармонізований зі стандартами систем менеджменту якості ISO 9001:2015 та ISO 14001:2015 та базується на їх основних принципах і процесному підході. Більш того, обов'язкові процедури стандарту ISO 9001 потрібні і стандартом ISO 27001. Структура документації за вимогами ISO 27001 аналогічна структурі за вимогами ISO 9001. Велика частина документації, необхідна по ISO 27001, вже могла бути розроблена, і могла використовуватися в рамках ISO 9001. Таким чином, якщо організація вже має систему менеджменту згідно, наприклад, з ISO 9001 або ISO 14001, то переважно забезпечувати виконання вимоги стандарту ISO 27001 в рамках вже існуючих систем.

Також основними принципами стандарту ISO 27001 є:

- конфіденційність інформації
- доступність інформації
- цілісність інформації

Організація може бути **сертифікована акредитованими агентствами відповідно до цього стандарту. Процес сертифікації** складається з трьох стадій:

- стадія 1 – вивчення аудитором ключових документів системи менеджменту інформаційної безпеки – положення про можливість застосування (SoA), план обробки ризиків (RTP), і ін. Може виконуватися як на території організації так і шляхом висилки цих документів зовнішньому аудитору;
- стадія 2 – детальний, глибокий аудит включаючи тестування впроваджених заходів та оцінка їх ефективності. Включає повне вивчення документів, які вимагає стандарт;
- стадія 3 – виконання інспекційного аудиту для підтвердження, що сертифікована організація відповідає заявленим вимогам. Виконується на періодичній основі.

Процедура сертифікації системи менеджменту за допомогою одного з міжнародних стандартів або їх комбінації підрозділяється на 4 етапи:

- 1 етап. Підготовка до сертифікації;
- 2 етап. Аудит 1-го ступеня (перевірка готовності до сертифікації);
- 3 етап. Аудит 2-го ступеня (сертифікаційний аудит);
- 4-ий етап. Видача сертифіката і нагляд.

ДСТУ ISO/IEC 27002:2015

ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT) – Цей стандарт встановлює настанови стосовно організаційних стандартів щодо інформаційної безпеки та загальні практики управління інформаційною безпекою, охоплюючи вибір, впровадження та управління заходами безпеки з урахуванням розгляду середовища ризиків інформаційної безпеки організації. Цей стандарт розроблено для використання організаціями, які намагаються: визначити заходи безпеки в межах процесу впровадження **системи управління інформаційною безпекою (СУІБ)** або як її ще називають **системи менеджменту інформаційною безпекою (СМІБ)** на основі ISO/IEC 27001; впровадити загальноприйняті заходи інформаційної безпеки; розробити власні настанови щодо управління інформаційною безпекою.

До 2007 року цей стандарт називався ISO/IEC 17799. Стандарт розроблений у 2005 році на основі версії **ISO 17799**, опублікованої в 2000, яка була повною копією Британського стандарту **BS 7799-1:1999**.

Стандарт надає найкращі практичні поради щодо менеджменту інформаційної безпеки для тих, хто відповідає за створення, реалізацію або обслуговування систем менеджменту інформаційної безпеки. ***Інформаційна безпека*** визначається стандартом як «збереження конфіденційності (впевненості в тому, що інформація доступна лише тим, хто уповноважений мати такий доступ), цілісності (гарантії точності та повноти інформації, а також методів її обробки) та доступності (гарантії того, що уповноважені користувачі мають доступ до інформації та пов'язаних з нею ресурсів)».

Поточна версія стандарту складається з таких основних розділів:

- Політика безпеки (*Security policy*).
- Організація інформаційної безпеки (*Organization of informationsecurity*).
- Управління ресурсами (*Asset management*).
- Безпека персоналу (*Human resources security*).
- Фізична безпека та безпека оточення (*Physical and environmental security*).
- Управління комунікаціями та операціями (*Communications and operations management*).
- Управління доступом (*Access control*).
- Придбання, розробка та підтримка систем (*Information systems acquisition, development and maintenance*).
- Управління інцидентами інформаційної безпеки (*Information security incident management*).
- Управління безперебійною роботою організації (*Business continuity management*).
- Відповідність нормативним вимогам (*Compliance*).

Цей документ описує 127 механізмів контролю, які необхідні для побудови системи управління інформаційною безпекою (СУІБ) організації, визначених на основі кращих прикладів світового досвіду (best practices) у цій галузі. Цей документ є практичним посібником зі створення СУІБ.

Британський стандарт BS 7799, на якому базується ISO/IEC 27002, рекомендує включати в документ, що характеризує політику безпеки організації, наступні розділи:

- вступний, підтверджуючий заклопотаність вищого керівництва проблемами інформаційної безпеки;
- організаційний, утримуючий опис підрозділів, комісій, груп і т.д., відповідальних за роботи в області інформаційної безпеки;
- класифікаційний, що описує наявні в організації матеріальні й інформаційні ресурси й необхідний рівень їхнього захисту;
- штатний, що характеризує міри безпеки, застосовувані до персоналу (опис посад з погляду інформаційної безпеки, організація навчання й перепідготовки персоналу, порядок реагування на порушення режиму безпеки й т.п.);
- розділ, що висвітлює питання *фізичного захисту*;
- керуючий розділ, що описує підхід до управління комп'ютерами й комп'ютерними мережами;
- розділ, що описує *правила розмежування* доступу до виробничої інформації;
- розділ, що характеризує *порядок розробки* й супроводу систем;
- розділ, що описує міри, спрямовані на забезпечення *безперервної роботи* організації;
- юридичний розділ, що підтверджує відповідність політики безпеки чинному законодавству.

Існує 3 рівня:

- Верхній.
- Середній.
- Нижній.

Верхній рівень

Програму верхнього рівня очолює особа, відповідальна за інформаційну безпеку організації. У цієї програми наступні головні цілі:

- управління ризиками (*оцінка ризиків*, вибір ефективних засобів захисту);
- *координація* діяльності в області інформаційної безпеки, поповнення й розподіл ресурсів;
- *стратегічне планування*;
- *контроль* діяльності в області інформаційної безпеки.

У рамках програми верхнього рівня приймаються стратегічні рішення по забезпеченню безпеки, оцінюються технологічні новинки. Інформаційні технології розвиваються дуже швидко, і необхідно мати чітку політику відстеження й впровадження нових засобів.

Контроль діяльності в області безпеки має двосторонню спрямованість. По- перше, необхідно гарантувати, що дії організації не суперечать законам. При цьому варто підтримувати контакти із зовнішніми контролюючими організаціями. По-друге, потрібно постійно відслідковувати стан безпеки усередині організації, реагувати на випадки порушень і допрацьовувати захисні міри з урахуванням зміни обстановки.

Варто підкреслити, що програма верхнього рівня повинна займати строго певне місце в діяльності організації, вона повинна офіційно прийматися й підтримуватися керівництвом, а також мати певний штат і бюджет.

Середній рівень

До середнього рівня можна віднести питання, що стосуються окремих аспектів інформаційної безпеки, але важливі для різних експлуатованих організацією систем. Приклади таких питань – відношення до передових (але, можливо, недостатньо перевірених) технологій, доступ в Internet (як сполучити незалежність доступу до інформації із захистом від зовнішніх погроз?), використання домашніх комп'ютерів, застосування користувачами неофіційного програмного забезпечення й т.д.

Політика середнього рівня повинна для кожного аспекту висвітлювати наступні теми:

- Опис аспекту. Наприклад, якщо розглянути застосування користувачами неофіційного програмного забезпечення, останнє можна визначити як ПЗ, що не було схвалено й/або закуплене на рівні організації.
- Область застосування. Варто визначити, де, коли, як, стосовно кого й чому застосовується дана *політика безпеки*.
- Позиція організації по даному аспекту. Продовжуючи приклад з неофіційним програмним забезпеченням, можна уявити собі позиції повної заборони, розробки процедури приймання подібного ПЗ й т.п. Позиція може бути сформульована й у набагато більше загальному виді, як набір цілей, які переслідує організація в даному аспекті. Взагалі стиль документів, що визначають політику безпеки (як і їхній перелік), у різних організаціях може сильно відрізнятися.
- Ролі й обов'язки. В «політичний» документ необхідно включити інформацію про посадові особи, відповідальні за реалізацію політики безпеки. Наприклад, якщо для використання неофіційного програмного забезпечення співробітникам потрібен дозвіл керівництва, повинне бути відомо, у кого і як його можна одержати. Якщо неофіційне програмне забезпечення використовувати не можна, варто знати, хто стежить за виконанням даного правила.
- Законослухняність. Політика повинна містити загальний опис заборонених дій і покарань за них.
- Точки контакту. Повинно бути відомо, куди варто звертатися за роз'ясненнями, допомогою й додатковою інформацією. Звичайно «точкою контакту» служать певні посадові особи, а не конкретна людина, що займає в цей момент даний пост.

Нижній рівень

Політика безпеки **нижнього рівня відноситься до конкретних інформаційних сервісів.** Вона містить у собі два аспекти – цілі й правила їхнього досягнення, тому її часом важко відокремити від питань реалізації. На відміну від двох верхніх рівнів, розглянута *політика* повинна бути визначена більш докладно. Є багато речей, специфічних для окремих видів послуг, які не можна єдиним образом регламентувати в рамках всієї організації. У той же час, ці речі настільки важливі для забезпечення режиму безпеки, що стосовні до них рішення повинні прийматися на управлінському, а не технічному рівні. Приведемо кілька прикладів питань, на які варто дати відповідь у політику безпеки нижнього рівня:

- хто має право доступу до об'єктів, підтримуваним сервісом?
- при яких умовах можна читати й модифікувати дані?
- як організований віддалений доступ до сервісу?

При формулюванні цілей політики нижнього рівня можна виходити з міркувань цілісності, доступності й конфіденційності, але не можна на цьому зупинятися. Її цілі повинні бути більше конкретними. Наприклад, якщо мова йде про систему розрахунку заробітної плати, можна поставити ціль, щоб тільки співробітникам відділу кадрів і бухгалтерії дозволялося вводити й модифікувати інформацію. У більш загальному випадку цілі повинні зв'язувати між собою об'єкти сервісу й дії з ними.

Із цілей виводяться правила безпеки, що описують, хто, що й при яких умовах може робити. Чим докладніше правила, тим більш формально вони викладені, тим простіше підтримати їхнє виконання програмно-технічними засобами. З іншого боку, занадто тверді правила можуть заважати роботі користувачів, імовірно, їх прийдеться часто переглядати. Керівництву має бути знайти розумний компроміс, коли за прийнятну ціну буде забезпечений прийнятний рівень безпеки, а співробітники не виявляться надмірно зв'язані. Звичайно найбільше формально задаються права доступу до об'єктів через особливу важливість даного питання.

Ціль програми нижнього рівня – забезпечити надійний і економічний захист конкретного сервісу або групи однорідних сервісів. На цьому рівні вирішується, які варто використовувати механізми захисту; закупаються й установлюються технічні засоби; виконується повсякденне адміністрування; відслідковується стан слабких місць і т.п. Звичайно за програму нижнього рівня відповідають адміністратори сервісів.

Програма безпеки

Після того, як сформульована політика безпеки, можна приступати до складання програми її реалізації й властиво до реалізації.

Щоб зрозуміти й реалізувати яку-небудь програму, її потрібно структурувати по рівнях, звичайно у відповідності зі структурою організації. У найпростішому й найпоширенішому випадку досить двох рівнів – верхнього, або центрального, котрий охоплює всю організацію, і нижнього, або службового, котрий відноситься до окремих послуг або груп однорідних сервісів.

Синхронізація програми безпеки з життєвим циклом систем

Якщо синхронізувати програму безпеки нижнього рівня з *життєвим циклом* сервісу, що захищається, можна домогтися більшого ефекту з меншими витратами. Програмісти знають, що додати нову можливість до вже готової системи на порядок складніше, ніж споконвічно спроектувати й реалізувати її. Те ж справедливо й для інформаційної **безпеки.**

У *життєвому циклі* інформаційного сервісу можна виділити наступні етапи:

Ініціація. На даному етапі виявляється необхідність у придбанні нового сервісу, документується його передбачуване призначення. З погляду безпеки найважливішою дією тут є оцінка критичності як самого сервісу, так і інформації, що з його допомогою буде оброблятися.

Закупівля. На даному етапі складаються специфікації, пророблюються варіанти придбання, виконується властиво *закупівля*. Зрозуміло, особлива увага повинне приділятися питанням сумісності нового сервісу з існуючою конфігурацією. Підкреслимо також, що нерідко засобу безпеки є необов'язковими компонентами комерційних продуктів, і потрібно простежити, щоб відповідні пункти не випали зі специфікації.

Установка. Сервіс установлюється, конфігурується, тестується й вводиться в *експлуатацію*. Як правило, комерційні продукти поставляються з відключеними засобами безпеки; їх необхідно включити й належним чином налаштувати. Для великої організації, де багато користувачів і даних, початкове настроювання може стати досить трудомісткою й відповідальною справою. По- друге, новий сервіс має потребу в процедурних регуляторах. Варто подбати про чистоту й охорону приміщення, про документи, що регламентують використання сервісу, про підготовку планів на випадок екстрених ситуацій, про організацію навчання користувачів і т.п.

Експлуатація. На даному етапі сервіс не тільки працює й адмініструється, але й піддається модифікаціям. Якщо безпека не підтримувати, вона слабшає. Користувачі не настільки ревно виконують посадові інструкції, адміністратори менш ретельно аналізують реєстраційну інформацію. То той, то інший користувач одержує додаткові привілеї. Здається, що в сутності нічого не змінилося; насправді ж від колишньої безпеки не залишилося й сліду. Для боротьби з ефектом повільних змін доводиться прибігати до періодичних перевірок безпеки сервісу.

Виведення з експлуатації. Відбувається перехід на новий сервіс. Тільки в специфічних випадках необхідно піклуватися про фізичне руйнування апаратних компонентів, що зберігають конфіденційну інформацію. При *виведенні даних з експлуатації* їх звичайно переносять на іншу систему, архівують, викидають або знищують.

ДСТУ ISO/IEC 27003:2018

ДСТУ ISO/IEC 27003:2018 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Настанова (ISO/IEC 27003:2017, IDT) – забезпечує висвітлення та управління на ISO/IEC 27001:2013.

ISO/IEC 27003 містить керівні вказівки щодо вимог до системи управління інформаційною безпекою (СУІБ), як зазначено у стандарті ISO/IEC 27001, і надає рекомендації, можливості та дозволи щодо них. Цей документ не передбачає надання загальних рекомендацій з усіх аспектів інформаційної безпеки. Статті 4-

10 цього документа відображають структуру ISO/IEC 27001:2013. Стандарт ISO/IEC 27003 не додає нових вимог до СУІБ та пов'язаних з ними термінів та визначень. Організації, що впроваджують СУІБ, не зобов'язані дотримуватися вказівок у цьому документі. СУІБ підкреслює важливість наступних етапів:

розуміння потреб організації та необхідності встановлення політики інформаційної безпеки та цілей інформаційної безпеки;

оцінка ризиків організації, пов'язаних з інформаційною безпекою; впровадження та керування процесами інформаційної безпеки,

контролю та іншими заходами щодо ліквідації ризиків;

моніторинг та перевірка продуктивності та ефективності СУІБ; впровадження постійного вдосконалення СУІБ.

СУІБ, подібний до будь-якого іншого типу системи управління, включає такі

ключові компоненти:

а) політика;

б) особи з визначеними обов'язками; в) процеси управління, пов'язані з:

- встановлення політики;
- забезпечення обізнаності та компетентності;
- планування;
- реалізація;
- експлуатація;

- оцінка продуктивності;
- огляд управління;
- вдосконалення;

г) документально підтверджена інформація.

СУІБ має додаткові ключові компоненти, такі як: д) оцінка ризику інформаційної безпеки;

є) обробка ризиків інформаційної безпеки, включаючи детермінацію та здійснення контролю.

Цей документ є загальним і призначений для застосування до всіх організацій, незалежно від типу (державні чи комерційні) та розміру. Організація повинна визначити, яка частина цього стандарту поширюється на неї відповідно до її специфічного організаційного контексту (Стаття 4 ISO/IEC 27001:2013). Деякі інструкції можуть бути придатними для великих організацій, але для дуже маленьких організацій (наприклад, з менш ніж 10 співробітниками) можуть бути непотрібними або неприйнятними.

4.4. Стек протоколів ДСТУ ISO/IEC 27000

Крім вищеперерахованих протоколів ДСТУ ISO/IEC 27000, 27001, 27002, 27003, до даного стеку протоколів відносяться наступні:

- **ДСТУ ISO/IEC 27004:2018 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Моніторинг, вимірювання, аналізування та оцінювання (ISO/IEC 27004:2016, IDT) –** ISO/IEC 27004:2016 містить настанови, спрямовані на допомогу організаціям в оцінюванні ефективності інформаційної безпеки та ефективності системи управління інформаційною безпекою з метою виконання вимог ISO/IEC 27001:2013, 9.1. Він встановлює: моніторинг та вимірювання ефективності інформаційної безпеки; моніторинг та вимірювання ефективності системи управління інформаційною безпекою (СУІБ), включаючи її процеси та засоби контролю; аналіз та оцінка результатів моніторингу та вимірювання. ISO/IEC 27004:2016 застосовний до організацій усіх типів і розмірів.
- **ДСТУ ISO/IEC 27005:2019 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2018, IDT) –** Цей документ містить вказівки щодо управління ризиками інформаційної безпеки. Цей документ підтримує загальні концепції, визначені в ISO/IEC 27001, і призначений для сприяння задовільній реалізації інформаційної безпеки на основі підходу до управління ризиками. Знання концепцій, моделей, процесів і термінології, описаних у ISO/IEC 27001 та ISO/IEC 27002, є важливим для повного розуміння цього документа. Цей документ застосовується до всіх типів організацій (наприклад, комерційних підприємств, державних установ, некомерційних організацій), які мають намір керувати ризиками, які можуть поставити під загрозу інформаційну безпеку організації.
- **ДСТУ ISO/IEC 27006:2015 Інформаційні технології. Методи захисту. Вимоги до органів, які надають послуги з аудиту і сертифікації систем управління інформаційною безпекою (ISO/IEC 27006:2015, IDT) –** Цей стандарт визначає вимоги та надає настанови для організацій, які надають послуги з аудиту та сертифікації систем управління інформаційною безпекою (СУІБ) додатково до вимог, що містяться в ISO/IEC 17021-1 та ISO/IEC 27001. Це, в першу чергу, спрямовано на підтримку акредитації організацій, які надають послуги із сертифікації СУІБ. Вимоги, які містить цей стандарт, необхідно продемонструвати в термінах компетентності та надійності всім організаціям, які здійснюють сертифікацію СУІБ, а настанови, долучені до цього стандарту, надають додаткову інтерпретацію цих вимог для будь- якої організації, яка виконує сертифікацію СУІБ. Цей стандарт може бути застосований як документ критеріїв для акредитації, експертного оцінювання або інших процесів аудиту.
- **ДСТУ ISO/IEC 27007:2018 Інформаційні технології. Методи захисту. Настанова щодо аудиту систем управління інформаційною безпекою (ISO/IEC 27007:2017, IDT) –** Цей документ містить вказівки щодо управління програмою аудиту системи управління інформаційною безпекою (СУІБ), щодо проведення аудитів та компетентності аудиторів

СУІБ, на додаток до вказівок, що містяться в ISO 19011. Цей документ стосується тих, хто потребує розуміння чи проведення внутрішніх чи зовнішніх аудитів СУІБ або управління програмою аудиту СУІБ.

- **ДСТУ ISO/IEC TS 27008:2019 Інформаційні технології. Методи захисту. Настанова щодо оцінювання захисту інформаційної безпеки (ISO/IEC TS 27008:2019, IDT) –** У цьому документі містяться вказівки щодо перегляду та оцінки впровадження та функціонування засобів контролю інформаційної безпеки, включаючи технічну оцінку засобів контролю інформаційної системи, відповідно до встановлених організацією вимог до інформаційної безпеки, включаючи технічну відповідність критеріям оцінки на основі вимог інформаційної безпеки, встановлених організації. У цьому документі пропонуються вказівки щодо того, як переглядати та оцінювати засоби контролю інформаційної безпеки, якими керують через систему управління інформаційною безпекою, визначену ISO/IEC 27001. Він застосовний до організацій усіх типів і розмірів, включаючи державні та приватні компанії, державні установи та некомерційні організації, які проводять огляди інформаційної безпеки та перевірки технічної відповідності.
- **ДСТУ ISO/IEC 27009:2018 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Визначення для сфери застосування ISO/IEC 27001. Вимоги (ISO/IEC 27009:2016, IDT) –** Цей документ визначає вимоги до створення галузевих стандартів, які розширюють ISO/IEC 27001 і доповнюють або змінюють ISO/IEC 27002 для підтримки конкретного сектора (домену, області застосування або ринку). Цей документ пояснює, як: включати вимоги на додаток до вимог ISO/IEC 27001: уточнювати або інтерпретувати будь-які вимоги ISO/IEC 27001; включати засоби контролю на додаток до засобів ISO/IEC 27001:2013, Додаток А та ISO/IEC 27002; модифікувати будь-які засоби управління ISO/IEC 27001:2013, додаток А та ISO/IEC 27002; додати настанови до або змінити настанови ISO/IEC 27002. У цьому документі зазначено, що додаткові чи вдосконалені вимоги не роблять вимоги ISO/IEC 27001 недійсними. Цей документ застосовується до тих, хто бере участь у розробці галузевих стандартів.
- **ДСТУ ISO/IEC 27010:2018** Інформаційні технології. Методи захисту. Управління інформаційною безпекою для міжгалузевих та міжорганізаційних комунікацій (ISO/IEC 27010:2015, IDT) – ISO/IEC 27010:2015 надає рекомендації на додаток до вказівок, наданих у сімействі стандартів ISO/IEC 27000, для впровадження управління інформаційною безпекою в спільнотах обміну інформацією. Цей міжнародний стандарт надає засоби контролю та вказівки, що стосуються, зокрема, ініціювання, впровадження, підтримки та покращення інформаційної безпеки в міжорганізаційних та міжгалузевих комунікаціях. Він містить вказівки та загальні принципи щодо того, як зазначені вимоги можуть бути виконані за допомогою встановлених повідомлень та інших технічних методів. Цей міжнародний стандарт застосовний до всіх форм обміну та спільного використання конфіденційної інформації, як загальнодоступної, так і приватної, на національному та міжнародному рівнях, у межах однієї галузі чи сектора ринку чи між секторами. Зокрема, це може бути застосовано до обміну інформацією та спільного використання, що стосується забезпечення, підтримки та захисту критичної інфраструктури організації або національної держави. Він призначений для підтримки створення довіри під час обміну конфіденційною інформацією та заохочення тим самим міжнародного зростання спільнот обміну інформацією.
- **ДСТУ ISO/IEC 27011:2018 Інформаційні технології. Методи захисту. Настанова для телекомунікаційних організацій щодо управління інформаційною безпекою на основі ISO/IEC 27002 (ISO/IEC 27011:2016, IDT) –** Сфера застосування цієї Рекомендації | ISO/IEC 27011:2016 має визначити настанови, що підтримують впровадження засобів контролю інформаційної безпеки в телекомунікаційних організаціях. Прийняття цієї Рекомендації | ISO/IEC 27011:2016 дозволить телекомунікаційним організаціям відповідати базовим вимогам управління безпекою інформації щодо конфіденційності, цілісності, доступності та будь-яких інших відповідних властивостей безпеки.
- **ДСТУ ISO/IEC 27013:2017 Інформаційні технології. Методи захисту. Настанови для інтегрованого впровадження ISO/IEC 27001 та ISO/IEC 20000-1 (ISO/IEC 27013:2015, IDT) –** ISO/IEC 27013:2021. Інформаційна безпека, кібербезпека та захист

конфіденційності – Настанови щодо інтегрованого впровадження ISO/IEC 27001 та ISO/IEC 20000-1 – Цей документ містить вказівки щодо інтегрованого впровадження ISO/IEC 27001 та ISO/IEC 20000-1 для організацій, які мають намір: запровадити ISO/IEC27001, коли вже запроваджено ISO/IEC 20000-1, або навпаки; впроваджувати як ISO/IEC27001, так і ISO/IEC 20000-1 разом; інтегрувати існуючі системи менеджменту на основі ISO/IEC27001 та ISO/IEC 20000-1. Цей документ зосереджується виключно на інтегрованій реалізації системи управління інформаційною безпекою (ISMS), як зазначено в ISO/IEC 27001, і системи управління послугами (SMS), як зазначено в ISO/IEC 20000-1.

- **ISO/IEC 27014:2020. Інформаційна безпека, кібербезпека та захист конфіденційності – Управління інформаційною безпекою** – У цьому документі містяться вказівки щодо концепцій, цілей і процесів управління інформаційною безпекою, за допомогою яких організації можуть оцінювати, спрямовувати, контролювати та передавати пов'язані з інформаційною безпекою процеси всередині організації. Цільова аудиторія цього документа: орган управління та вище керівництво; тих, хто відповідає за оцінку, управління та моніторинг системи управління інформаційною безпекою (СУІБ) на основі ISO/IEC 27001; особи, відповідальні за управління інформаційною безпекою, яке відбувається поза сферою СУІБ на основі ISO/IEC 27001, але в межах сфери управління. Цей документ застосовується до організацій усіх типів і розмірів. Усі посилання на СУІБ у цьому документі стосуються СУІБ на основі ISO/IEC 27001. Цей документ зосереджується на трьох типах організацій СУІБ, наведених у Додатку B. Однак цей документ також може використовуватися іншими типами організацій.
- **ISO/IEC TR 27015:2012. Інформаційні технології – Методи безпеки – Настанови щодо управління інформаційною безпекою для фінансових послуг** – ISO/IEC TR 27015:2012 містить інструкції з інформаційної безпеки, які доповнюють засоби контролю інформаційної безпеки, визначені в ISO/IEC 27002:2005, для ініціювання, впровадження, підтримки та покращення інформаційної безпеки в організаціях, що надають фінансові послуги.
- **ISO/IEC TR 27016:2014. Інформаційні технології – Техніка безпеки – Управління інформаційною безпекою – Економіка організації** – ISO/IEC TR 27016:2014 надає вказівки щодо того, як організація може приймати рішення щодо захисту інформації та розуміння економічних наслідків цих рішень у контексті конкуруючих вимог до ресурсів. ISO/IEC TR 27016:2014 застосовний до організацій усіх типів і розмірів і надає інформацію для прийняття економічних рішень щодо управління інформаційною безпекою вищим керівництвом, яке несе відповідальність за рішення щодо інформаційної безпеки.
- **ДСТУ ISO/IEC 27017:2017 Інформаційні технології. Методи захисту. Звід практик стосовно заходів інформаційної безпеки, що ґрунтуються на ISO/IEC 27002, для хмарних послуг (ISO/IEC 27017:2015, IDT) –** Цей стандарт надає рекомендації щодо заходів інформаційної безпеки, які застосовують для надання та застосування хмарних послуг, за допомогою формування: додаткових рекомендацій щодо впровадження для відповідних заходів безпеки, визначених в ISO/IEC 27002; додаткових заходів безпеки з рекомендаціями щодо впровадження, що конкретно стосуються хмарних послуг. У цьому стандарті наведено заходи безпеки та рекомендації щодо впровадження як для провайдерів, так і для споживачів хмарних послуг.
- **ДСТУ ISO/IEC 27018:2019 Інформаційні технології. Методи захисту. Кодекс усталеної практики для захисту персональної ідентифікаційної інформації (PII) у загальнодоступних хмарах, що діють як процесори PII (ISO/IEC 27018:2019, IDT) –** У цьому документі встановлюються загальноприйняті цілі контролю, засоби контролю та вказівки щодо впровадження заходів із захисту особистої ідентифікаційної інформації (PII) відповідно до принципів конфіденційності в ISO/IEC 29100 для загальнодоступного середовища хмарних обчислень. Зокрема, цей документ містить інструкції на основі ISO/IEC 27002, беручи до уваги нормативні вимоги щодо захисту ідентифікаційної інформації, які можуть бути застосовані в контексті середовища(ів) ризику інформаційної безпеки постачальника публічних хмарних послуг. Цей документ стосується організацій усіх типів і розмірів, у тому числі державних і приватних компаній, державних установ і некомерційних

організацій, які надають послуги з обробки інформації як процесори ідентифікаційної інформації через хмарні обчислення за контрактом з іншими організаціями. Рекомендації в цьому документі також можуть стосуватися організацій, які виконують функції контролерів ідентифікаційної інформації. Однак на контролери ідентифікаційної інформації можуть поширюватися додаткові законодавчі акти, положення та зобов'язання щодо захисту ідентифікаційної інформації, які не стосуються обробників ідентифікаційної інформації. Цей документ не призначений для покриття таких додаткових зобов'язань.

- **ДСТУ ISO/IEC 27019:2019 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою для енергопостачальних організацій (ISO/IEC 27019:2017, IDT) –** ISO/IEC 27019:2017 надає вказівки на основі ISO/IEC 27002:2013, застосовані до систем управління процесами, що використовуються в енергетиці для контролю та моніторингу виробництва або виробництва, передачі, зберігання та розподілу електроенергії, газу, нафти та тепла, а також для контролю відповідних допоміжних процесів. Це включає, зокрема, таке: технологія централізованого та розподіленого управління процесами, моніторингу та автоматизації, а також інформаційні системи, що використовуються для їх роботи, такі як пристрої програмування та параметризації; цифрові контролери та компоненти автоматизації, такі як контрольні та польові пристрої або програмовані логічні контролери (PLC), включаючи цифрові датчики та виконавчі елементи; усі додаткові допоміжні інформаційні системи, що використовуються в області управління процесом, наприклад, для додаткових задач візуалізації даних і для контролю, моніторингу, архівування даних, реєстрації історії, звітності та документації; комунікаційна технологія, яка використовується в області управління процесом, наприклад, мережі, телеметрія, програми телеконтролю та технології дистанційного управління; Компоненти розширеної інфраструктури вимірювання (AMI), наприклад розумні лічильники; вимірювальні пристрої, наприклад, для значень викидів; цифрові системи захисту та безпеки, наприклад реле захисту, ПЛК безпеки, механізми аварійного регулювання; системи енергоменеджменту,

наприклад розподілених енергетичних ресурсів (DER), інфраструктури електричних зарядок у приватних домогосподарствах, житлових будинках або промислових установках споживачів; розподілені компоненти середовища інтелектуальної мережі, наприклад, в енергетичних мережах, у приватних домогосподарствах, житлових будинках або промислових установках споживачів; усе програмне забезпечення, мікропрограми та програми, встановлені у вищезазначених системах, наприклад програми DMS (система управління розподілом) або OMS (система управління збоями); будь-які приміщення, в яких розміщено вищезазначене обладнання та системи; системи дистанційного обслуговування вищевказаних систем. ISO/IEC 27019:2017 не застосовується до області управління процесом ядерних установок. Цей домен охоплює стандарт IEC 62645. ISO/IEC 27019:2017 також містить вимогу щодо адаптації процесів оцінки та обробки ризиків, описаних у ISO/IEC 27001:2013, до вказівок, які наведені в цьому документі в секторі енергетики.

- **ДСТУ ISO/IEC 27021:2018 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги до компетенції професіоналів з управління інформацією (ISO/IEC 27021:2017, IDT**) – ISO/IEC 27021:2017 визначає вимоги до компетентності для фахівців із СУІБ, які керують або беруть участь у створенні, впровадженні, підтримці та постійному вдосконаленні одного або кількох процесів системи управління інформаційною безпекою, які відповідають ISO/IEC 27001.

- **ДСТУ ISO/IEC 27031:2015 Інформаційні технології. Методи захисту. Настанови щодо готовності інформаційно-комунікаційних технологій для неперервності роботи бізнесу (ISO/IEC 27031:2011, IDT) –** ISO/IEC 27031:2011 описує концепції та принципи готовності інформаційно- комунікаційних технологій (ІКТ) до безперервності бізнесу та надає структуру методів і процесів для ідентифікації та визначення всіх аспектів (таких як критерії ефективності, проектування та впровадження) для підвищення готовності організації до ІКТ для забезпечення безперервності бізнесу. Це стосується будь-якої організації (приватної, урядової та неурядової, незалежно від розміру), яка розробляє свою програму готовності до ІКТ для забезпечення безперервності бізнесу (IRBC), і вимагає, щоб її послуги/інфраструктури ІКТ були готові підтримувати бізнес-операції у разі виникнення

події та інциденти, а також пов’язані з ними збої, які можуть вплинути на безперервність (включаючи безпеку) критичних бізнес-функцій. Сфера застосування ISO/IEC 27031:2011 охоплює всі події та інциденти (включаючи

пов’язані з безпекою), які можуть вплинути на інфраструктуру та системи ІКТ. Він включає в себе та розширює практики обробки інцидентів інформаційної безпеки та управління ними, а також планування готовності до ІКТ та послуги.

- **ДСТУ ISO/IEC 27032:2016 Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки (ISO/IEC 27032:2012, IDT) –** Цей стандарт містить рекомендації щодо підвищення рівня кібербезпеки, розглядаючи різні

аспекти цього питання та їхній зв’язок з іншими видами безпеки, зокрема: інформаційною безпекою; мережевою безпекою; Інтернет-безпекою; захистом інформаційної інфраструктури. У стандарті розглянуто основні методи захисту зацікавлених сторін у кіберпросторі. Стандарт містить: огляд кібербезпеки; пояснення зв’язків між кібербезпекою та іншими видами безпеки; визначення зацікавлених сторін та їхньої ролі в кіберпросторі; настанова з вирішення основних питань кібербезпеки; способи взаємодії зацікавлених сторін для вирішення основних питань кібербезпеки. Цей стандарт стосується постачальників послуг у кіберпросторі. Але цільова аудиторія охоплює також споживачів, які користуються цими послугами. Якщо організації надають послуги в кіберпросторі іншим організаціям або людям для домашнього використання, то таким організаціям може знадобитися підготувати настанови на основі цього стандарту, які міститимуть додаткові пояснення або приклади, необхідні для повного розуміння читачами того, як треба діяти.

ДСТУ ISO/IEC 27033:2017. Інформаційні технології. Методи захисту. Безпека мережі. – складається з 6 частин:

- ДСТУ ISO/IEC 27033-1:2017 Інформаційні технології. Методи захисту. Захист мережі. Частина 1. Огляд і поняття (ISO/IEC 27033-1:2015, IDT) – ISO/IEC 27033-1:2015 містить огляд мережевої безпеки та відповідних визначень. Він визначає й описує концепції, пов’язані з мережевою безпекою, і надає вказівки щодо управління нею. (Мережева безпека стосується безпеки пристроїв, безпеки управлінських дій, пов’язаних із пристроями, програмами/службами та кінцевими користувачами, на додаток до безпеки інформації, що передається через канали зв’язку.) Це актуально для всіх, хто бере участь у володінні, експлуатації або використанні мережі. Це включає керівників вищої ланки та інших нетехнічних менеджерів або користувачів, на додаток до керівників і адміністраторів, які мають конкретні обов’язки за інформаційну безпеку та/або безпеку мережі, роботу мережі або які відповідають за загальну програму безпеки організації та розробку політики безпеки. Це також актуально для всіх, хто бере участь у плануванні, проектуванні та реалізації архітектурних аспектів безпеки мережі. ISO/IEC 27033-1:2015 також включає наступне: надає вказівки щодо того, як ідентифікувати та аналізувати ризики безпеки мережі та визначення вимог безпеки мережі на основі цього аналізу; надає огляд елементів управління, які підтримують архітектури технічної безпеки мережі та відповідні технічні засоби контролю, а також тих нетехнічних засобів контролю та технічних засобів контролю, які застосовуються не лише до мереж; знайомить із тим, як досягти високоякісної архітектури технічної безпеки мережі, а також аспекти ризику, дизайну та контролю, пов’язані з типовими мережевими сценаріями та областями мережевих «технологій» (які детально розглядаються в наступних частинах ISO/IEC 27033), і коротко розглядає питання, пов'язані з впровадженням і експлуатацією засобів контролю безпеки мережі, а також постійний моніторинг і перегляд їх впровадження. Загалом він містить огляд цього міжнародного стандарту та «дорожню карту» для всіх інших частин.
- ДСТУ ISO/IEC 27033-2:2016 Інформаційні технології. Методи захисту. Безпека мережі. Частина 2. Настанови щодо проектування та реалізації безпеки мережі (ISO/IEC 27033-2:2012, IDT) – ISO/IEC 27033-2:2012 містить вказівки для організацій щодо планування, проектування, впровадження та документування безпеки мережі.
- ДСТУ ISO/IEC 27033-3:2016 Інформаційні технології. Методи захисту.

Безпека мережі. Частина 3. Еталонні мережеві сценарії.

- Загрози, методи проектування та проблеми управління (ISO/IEC 27033-3:2010, IDT) – ISO/IEC 27033-3:2010 описує загрози, методи проектування та проблеми управління, пов'язані зі сценаріями еталонної мережі. Для кожного сценарію в ньому надаються детальні вказівки щодо загроз безпеці, а також методи розробки безпеки та засоби контролю, необхідні для пом'якшення пов'язаних ризиків. У відповідних випадках він містить посилання на ISO/IEC 27033- 4 –

ISO/IEC 27033-6, щоб уникнути дублювання змісту цих документів. Інформація в ISO/IEC 27033-3:2010 призначена для використання під час перегляду архітектури/проекту технічної безпеки та під час вибору та документування бажаної архітектури/проекту технічної безпеки та пов'язаних засобів контролю безпеки відповідно до ISO/IEC 27033-2. Вибрана конкретна інформація (разом з інформацією, вибраною з ISO/IEC 27033-4 до ISO/IEC 27033-6) залежатиме від характеристик мережевого середовища, що перевіряється, тобто конкретного мережевого сценарію(ів) і теми «технології». Загалом, ISO/IEC 27033-3:2010 суттєво допоможе в комплексному визначенні та реалізації безпеки для мережевого середовища будь-якої організації.

- ДСТУ ISO/IEC 27033-4:2016 Інформаційні технології. Методи захисту. Безпека мережі. Частина 4. Убезпечення комунікацій між мережами з використанням шлюзів безпеки (ISO/IEC 27033-4:2014, IDT) – ISO/IEC 27033- 4:2014 містить настанови щодо захисту зв'язку між мережами за допомогою шлюзів безпеки (брандмауер, брандмауер програм, система захисту від вторгнень тощо) відповідно до задокументованої політики інформаційної безпеки шлюзів безпеки, включаючи: виявлення та аналіз загроз мережевій безпеці, пов'язаних зі шлюзами безпеки; визначення вимог безпеки мережі для шлюзів безпеки на основі аналізу загроз; використання методів для проектування та впровадження для вирішення загроз та аспектів контролю, пов'язаних із типовими мережевими сценаріями; вирішення проблем, пов'язаних із впровадженням, експлуатацією, моніторингом та переглядом елементів управління шлюзом безпеки мережі.
- ДСТУ ISO/IEC 27033-5:2016 Інформаційні технології. Методи захисту. Безпечність мережі. Частина 5. Убезпечення комунікацій уздовж мереж із використанням віртуальних приватних мереж (VPNs) (ISO/IEC 27033-5:2013, IDT) – ISO/IEC 27033-5:2013 містить вказівки щодо вибору, впровадження та моніторингу технічних засобів контролю, необхідних для забезпечення безпеки мережі за допомогою з'єднань віртуальної приватної мережі (VPN) для з'єднання мереж і підключення віддалених користувачів до мереж.
- ДСТУ ISO/IEC 27033-6:2018 Інформаційні технології. Методи захисту. Безпека мережі. Частина 6. Забезпечення безпроводового доступу до IP-мережі

(ISO/IEC 27033-6:2016, IDT) – ISO/IEC 27033-6:2016 описує загрози, вимоги безпеки, контроль безпеки та методи проектування, пов'язані з безпроводовими мережами. Він містить вказівки щодо вибору, впровадження та моніторингу технічних засобів контролю, необхідних для забезпечення безпечного зв'язку за допомогою безпроводових мереж. Інформація в цій частині ISO/IEC 27033 призначена для використання під час перегляду або вибору архітектури/проекту технічної безпеки, які передбачають використання безпроводової мережі відповідно до ISO/IEC 27033-

2. Загалом, ISO/IEC 27033-6 значно допоможе у всебічному визначенні та реалізації безпеки для безпроводового мережевого середовища будь-якої організації. Він призначений для користувачів і розробників, які відповідають за впровадження та підтримку технічного контролю, необхідного для забезпечення безпечних безпроводових мереж.

ISO/IEC CD 27033-7. Інформаційна технологія. Безпека мережі. Частина 7. Настанови щодо безпеки віртуалізації мережі – В стадії розробки

ДСТУ ISO/IEC 27034:2017 Інформаційні технології. Методи захисту. Безпека програм. – складається з 7 частин:

- ДСТУ ISO/IEC 27034-1:2017 Інформаційні технології. Методи захисту. Безпека прикладних програм. Частина 1. Огляд і загальні поняття (ISO/IEC 27034-1:2011; Cor 1:2014, IDT) – ISO/IEC 27034 надає організаціям інструкції, які допомагають інтегрувати безпеку в

процеси, які організації використовують для управління своїми додатками. У цьому стандарті наведено загальний огляд безпеки додатків. Вона представляє визначення, принципи та процеси, які стосуються безпеки додатків. ISO/IEC 27034 можна застосовувати для додатків, розроблених в організації чи придбаних у третьої сторони, а також у разі аутсорсингу розроблення чи експлуатації додатків.

- ДСТУ ISO/IEC 27034-2:2016 Інформаційні технології. Методи захисту. Безпека прикладних програм. Частина 2. Основні нормативні положення організації (ISO/IEC 27034-2:2015, IDT) – ISO/IEC 27034-2:2015 містить детальний опис нормативної бази організації та надає керівництво для організацій щодо її впровадження.
- ДСТУ ISO/IEC 27034-3:2018 Інформаційні технології. Методи захисту. Безпека прикладних програм. Частина 3. Процес управління безпекою прикладних програм (ISO/IEC 27034-3:2018, IDT) – У цьому документі міститься детальний опис і інструкції щодо впровадження процесу управління безпекою додатків.
- ДСТУ ISO/IEC TS 27034-5-1:2019 Інформаційні технології. Захист застосунків. Частина 5-1. Структура даних управління протоколами та захистом застосунків. Схеми XML (ISO/IEC TS 27034-5-1:2018, IDT) – ISO/IEC 27034-5

описує та пояснює мінімальний набір основних атрибутів контролю безпеки додатків (ASC), а також докладно описує дії та ролі еталонної моделі життєвого циклу безпеки додатків (ASLCRM).

- ДСТУ ISO/IEC 27034-6:2018 Інформаційні технології. Методи захисту. Безпека прикладних програм. Частина 6. Вивчення випадків (ISO/IEC 27034- 6:2016, IDT) – ISO/IEC 27034-6:2016 надає приклади використання ASC для конкретних застосувань. Зазначені тут ASC надаються лише з метою пояснення, і аудиторії рекомендується створити власні ASC для забезпечення безпеки програми.
- ISO/IEC 27034-7:2018. Інформаційні технології. Безпека додатків. Частина 7. Структура прогнозування впевненості – Цей документ описує мінімальні вимоги, коли необхідні дії, визначені контролем безпеки додатків (ASC), замінюються обґрунтуванням безпеки додатків прогнозування (PASR). ASC, зіставлений із PASR, визначає очікуваний рівень довіри для наступної програми. У контексті очікуваного рівня довіри завжди існує оригінальна заявка, у якій команда проекту виконувала дії зазначеного ASC для досягнення фактичного рівня довіри. Використання обґрунтувань безпеки додатків прогнозування (PASR), визначених у цьому документі, застосовується до проектних груп, які мають визначену нормативну структуру додатків (ANF) і оригінальну програму з фактичним рівнем довіри. Прогнози щодо агрегування кількох компонентів або історії розробника щодо інших програм виходять за рамки цього документа.

ДСТУ ISO/IEC 27035:2018 Інформаційні технології. Методи захисту. Управління інцидентами інформаційної безпеки. – складається з 4 частин:

- ДСТУ ISO/IEC 27035-1:2018 Інформаційні технології. Методи захисту.

Управління інцидентами інформаційної безпеки. Частина 1. Принципи управління інцидентами (ISO/IEC 27035-1:2016, IDT) – ISO/IEC 27035-1:2016 є основою цього багатокомпонентного міжнародного стандарту. Він представляє основні концепції та етапи управління інцидентами інформаційної безпеки та поєднує ці концепції з принципами в структурованому підході до виявлення, звітування, оцінювання та реагування на інциденти, а також застосування отриманих уроків. Принципи, наведені в ISO/IEC 27035-1:2016, є загальними та призначені для застосування в усіх організаціях, незалежно від типу, розміру чи природи. Організації можуть коригувати вказівки, наведені в ISO/IEC 27035- 1:2016, відповідно до свого типу, розміру та характеру бізнесу щодо ситуації ризику інформаційної безпеки. Це також стосується зовнішніх організацій, які надають послуги з управління інцидентами інформаційної безпеки.

- ДСТУ ISO/IEC 27035-2:2018 Інформаційні технології. Методи захисту. Управління інцидентами інформаційної безпеки. Частина 2. Настанова щодо планування та підготовки до реагування на інциденти (ISO/IEC 27035-2:2016, IDT) – ISO/IEC 27035-2:2016 надає рекомендації щодо планування та підготовки до реагування на інциденти. Рекомендації

базуються на етапі «Планування та підготовка» та етапі «Здобуті уроки» моделі «Фази управління інцидентами інформаційної безпеки», представленої в ISO/IEC 27035-1. Основні моменти на етапі

«Планування та підготовка» включають наступне: політика управління інцидентами інформаційної безпеки та зобов'язання вищого керівництва політики інформаційної безпеки, включаючи ті, що стосуються управління ризиками, оновлені як на корпоративному рівні, так і на рівні системи, сервісу та мережі план управління інцидентами інформаційної безпеки створення групи реагування на інциденти (IRT) встановлювати стосунки та зв'язки з внутрішніми та зовнішніми організаціями технічне та інше забезпечення (включаючи організаційне та операційне) інструктажі та тренінги з управління інцидентами інформаційної безпеки тестування плану управління інцидентами інформаційної безпеки. Принципи, наведені в цій частині ISO/IEC 27035, є загальними та призначені для застосування в усіх організаціях, незалежно від типу, розміру чи природи. Організації можуть коригувати вказівки, надані в цій частині ISO/IEC 27035, відповідно до їх типу, розміру та характеру бізнесу щодо ситуації ризику інформаційної безпеки. Ця частина ISO/IEC 27035 також застосовується до зовнішніх організацій, що надають послуги з управління інцидентами інформаційної безпеки.

- ISO/IEC 27035-3:2020. Інформаційна технологія. Управління інцидентами інформаційної безпеки. Частина 3. Настанови щодо операцій реагування на інциденти ІКТ – У цьому документі містяться вказівки щодо реагування на інциденти інформаційної безпеки в операціях безпеки ІКТ. Цей документ робить це, по-перше, охоплюючи операційні аспекти операцій безпеки ІКТ з точки зору людей, процесів і технологій. Далі він зосереджується на реагуванні на інциденти інформаційної безпеки в операціях безпеки ІКТ, включаючи виявлення інцидентів інформаційної безпеки, звітування, сортування, аналіз, реагування, стримування, викорінення, відновлення та завершення. Цей документ не стосується операцій реагування на інциденти, не пов’язані з ІКТ, як-от втрата паперових документів. Цей документ базується на фазі «Виявлення та звітування», фазі «Оцінка та прийняття рішення» та фазі

«Відповіді» моделі «Фази управління інцидентами інформаційної безпеки», представленої в ISO/IEC 27035-1:2016. Принципи, наведені в цьому документі, є загальними та призначені для застосування в усіх організаціях, незалежно від типу, розміру чи природи. Організації можуть коригувати положення, наведені в цьому документі, відповідно до свого типу, розміру та характеру бізнесу щодо ситуації ризику інформаційної безпеки. Цей документ також стосується зовнішніх організацій, які надають послуги з управління інцидентами інформаційної безпеки.

- ISO/IEC CD 27035-4. Інформаційні технології. Управління інцидентами інформаційної безпеки. Частина 4. Координація – В стадії розробки

ДСТУ ISO/IEC 27036:2017 Інформаційні технології. Методи захисту. Інформаційна безпека у відносинах із постачальниками. – складається з 4 частин:

- ДСТУ ISO/IEC 27036-1:2017 Інформаційні технології. Методи захисту. Інформаційна безпека у відносинах із постачальниками. Частина 1. Огляд та поняття (ISO/IEC 27036-1:2014, IDT) – Цей документ є вступною частиною ISO/IEC 27036.

Він містить огляд настанов, спрямованих на допомогу організаціям у захисті їх інформації та інформаційних систем у контексті відносин з постачальниками. Він також представляє концепції, які детально

описані в інших частинах ISO/IEC 27036. Цей документ розглядає точки зору як покупців, так і постачальників.

- ДСТУ ISO/IEC 27036-2:2017 Інформаційні технології. Методи захисту. Інформаційна безпека у відносинах з постачальниками. Частина 2. Вимоги (ISO/IEC 27036-2:2014, IDT) – Цей документ визначає фундаментальні вимоги інформаційної безпеки для визначення, впровадження, експлуатації, моніторингу, перегляду, підтримки та покращення відносин постачальника та покупця. Ці вимоги охоплюють будь-яку закупівлю та постачання продуктів і послуг, таких як виробництво або складання, закупівля бізнес-процесів,

програмних і апаратних компонентів, закупівля процесу знань, створення- експлуатація-передача та послуги хмарних обчислень. Цей документ застосовується до всіх організацій, незалежно від типу, розміру та характеру. Щоб відповідати вимогам, очікується, що організація запровадила всередині ряд базових процесів або активно планує це зробити. Ці процеси включають, але не обмежуються: управління бізнесом, управління ризиками, управління операційними й людськими ресурсами та інформаційна безпека.

- ДСТУ ISO/IEC 27036-3:2017 Інформаційні технології. Методи захисту. Інформаційна безпека у відносинах з постачальниками. Частина 3. Настанови щодо безпеки ланцюга постачання інформаційних та комунікаційних технологій (ISO/IEC 27036-3:2013, IDT) – ISO/IEC 27036-3:2013 надає покупцям продуктів і послуг і постачальникам у ланцюзі постачання інформаційно-комунікаційних технологій (ІКТ) настанови щодо: отримання видимості та управління ризиками інформаційної безпеки, спричиненими фізично розосередженими та багаторівневими ланцюгами постачання ІКТ; реагування на ризики, пов'язані з глобальним ланцюгом постачання ІКТ-продуктів і послуг, які можуть мати вплив на інформаційну безпеку організацій, які використовують ці продукти та послуги. Ці ризики можуть бути пов'язані як з організаційними, так і з технічними аспектами (наприклад, введення шкідливого коду або наявність підроблених продуктів інформаційних технологій (IT); інтеграція процесів і практик інформаційної безпеки в процеси життєвого циклу системи та програмного забезпечення, описані в ISO/IEC 15288 та ISO/IEC 12207, одночасно підтримуючи засоби контролю інформаційної безпеки, описані в ISO/IEC 27002. ISO/IEC 27036-3:2013 не включає питання управління безперервністю бізнесу/відмовостійкості, пов'язані з ланцюгом постачання ІКТ. ISO/IEC 27031 стосується безперервності бізнесу.
- ДСТУ ISO/IEC 27036-4:2018 Інформаційні технології. Методи захисту. Інформаційна безпека у відносинах з постачальниками. Частина 4. Настанова щодо безпеки хмарних послуг (ISO/IEC 27036-4:2016, IDT) – ISO/IEC 27036- 4:2016 надає клієнтам хмарних послуг і постачальникам хмарних послуг рекомендації щодо отримання інформації про ризики інформаційної безпеки, пов'язані з використанням хмарних служб, і ефективне управління цими ризиками, а також реагування на ризики, характерні для придбання або надання хмарних послуг, які можуть мати вплив на інформаційну безпеку організацій, які використовують ці служби. ISO/IEC 27036- 4:2016 не включає питання управління безперервністю бізнесу/відмовостійкості, пов'язані з хмарною службою. ISO/IEC 27031 стосується безперервності бізнесу. ISO/IEC 27036- 4:2016 не надає вказівок щодо того, як постачальник хмарних послуг повинен запроваджувати, керувати та керувати інформаційною безпекою. Інструкції щодо них можна знайти в ISO/IEC 27002 та ISO/IEC 27017. Сфера застосування ISO/IEC 27036-4:2016 полягає у визначенні настанов, що підтримують впровадження управління безпекою інформації для використання хмарних служб.
- **ДСТУ ISO/IEC 27037:2017 Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів (ISO/IEC 27037:2012, IDT) –** Цей стандарт надає настанови для специфічної діяльності з оброблення потенційних цифрових доказів, такими процесами є: ідентифікація, збирання, здобуття та збереження потенційних цифрових доказів. Ці процеси потрібні під час слідства для підтримання цілісності цифрових доказів – прийнятна методологія отримання цифрових доказів, яка буде забезпечувати їхню допустимість у законодавчих та дисциплінарних судових процесах, а також інших потрібних інстанціях. Цей стандарт також надає загальні настанови стосовно збирання нецифрових доказів, які можуть буті корисними на стадії аналізування потенційних цифрових доказів. Цей стандарт також спрямовано на інформування осіб, які приймають рішення, та тих, кому потрібно визначати надійність потенційних цифрових доказів, що були їм надані. Він прийнятний для організацій, яким необхідно захищати, аналізувати та презентувати потенційні цифрові докази. Він важливий для поліцейських підрозділів, які формують та запроваджують процедури щодо цифрових доказів, часто як частину доказів більшого об'єму. Потенційні цифрові докази, розглянуті в цьому стандарті, можуть мати походження з різних типів цифрових пристроїв, мереж, баз даних тощо. Вони стосуються даних, які вже є в цифровому форматі. Цей стандарт не

намагається охопити перетворення аналогових даних у цифровий формат. Завдяки недовговічності цифрових доказів потрібно мати прийнятну методологію для гарантування цілісності та автентичності потенційних цифрових доказів. Цей стандарт не вимагає обов'язкового використання виняткових інструментів або методів. Ключовим компонентом, який забезпечує довіру в розслідуваннях, є методологія, яку застосовують протягом цього процесу, та особи, що мають кваліфікацію для виконання завдань, визначених цією методологією. Цей стандарт не стосується методології для законодавчих та дисциплінарних судових процесів, а також інших пов'язаних діяльностей під час оброблення потенційних цифрових доказів, які знаходяться поза межами сфери ідентифікації, збирання, здобуття та збереження. Запровадження цього стандарту потребує відповідності національним законам, правилам та нормативним документам. Він не повинен заміняти специфічні законодавчі вимоги будь-якої юрисдикції. Фактично, він може слугувати практичною настановою для DEFR або DES у дослідженнях, які охоплюють потенційні цифрові докази. Він не впливає на аналізування цифрових доказів та не замінює специфічних юридичних вимог, що стосуються таких питань, як визнання доказів, доказова вага, значущість та інші юридично контрольовані обмеження використання потенційних цифрових доказів у судах. Цей стандарт може допомогти у сприянні обміну потенційними цифровими доказами між юрисдикціями. Для підтримання цілісності цифрових доказів користувачам цього стандарту потрібно адаптувати та скоригувати процедури, описані в цьому стандарті, відповідно до специфічних законодавчих вимог юрисдикції для доказів. Хоча цей стандарт не охоплює судової готовності, відповідна судова готовність може бути значною мірою підтримана процесами ідентифікації, збирання, здобуття та збереження цифрових доказів. Судова готовність – це досягнення відповідного рівня здатності організації для спроможності ідентифікації, збирання, здобуття, збереження, захисту та аналізування цифрових доказів. Незважаючи на те, що процеси та діяльності, описані в цьому стандарті, є в основному реактивними заходами, використовуваними в розслідуваннях інциденту після того, як він вже трапився, судова готовність є проективним процесом спроби планування процесу дослідження інциденту. Цей стандарт відповідає ISO/IEC 27001 та ISO/IEC 27002, зокрема вимогам заходів щодо безпеки стосовно потенційних цифрових доказів за допомогою надання додаткової настанови щодо запровадження. Крім того, цей стандарт має застосування в контексті, незалежному від ISO/IEC 27001 та ISO/IEC 27002. Цей стандарт потрібно розглядати разом з іншими стандартами, пов'язаними з цифровими доказами та розслідуваннями інцидентів інформаційної безпеки. Цей стандарт надає настанови для специфічної діяльності з оброблення цифрових доказів, а саме: ідентифікації, збирання, здобуття та збереження цифрових доказів, що можуть мати доказове значення. Цей стандарт надає настанови для фахівців стосовно звичайних випадків, які трапляються в процесі оброблення цифрових доказів,та допомагає організаціям в їхніх дисциплінарних процедурах та забезпеченні обміну потенційними цифровими доказами між юрисдикціями. Цей стандарт надає настанови для таких пристроїв та/або функцій, використовуваних за різних обставин: Носій для зберігання цифрових даних, використовуваний у стандартних комп'ютерах, подібний жорстким дискам, гнучким дискам, оптичним і магнітооптичним дискам, цифровим пристроям з подібними функцпми; Мобільні телефони, Персональні цифрові помічники (PDAs), Персональні електронні прилади (PEDs), карти пам'яті; Мобільні навігаційні системи; Цифрові фото- та відеокамери (зокрема CCTV); Стандартний комп'ютер з мережевими з'єднаннями; Мережі, які ґрунтовані на TCP/IP та інших цифрових протоколах; Прилади з функціями, подібними наведеним вище.

- **ДСТУ ISO/IEC 27038:2018 Інформаційні технології. Методи захисту. Специфікація цифрового редагування (ISO/IEC 27038:2014, IDT) –** ISO/IEC 27038:2014 визначає характеристики методів виконання цифрового редагування цифрових документів. Він також визначає вимоги до засобів редагування програмного забезпечення та методів перевірки надійності цифрового редагування. ISO/IEC 27038:2014 не включає редагування інформації з баз даних.
- **ДСТУ ISO/IEC 27039:2017 Інформаційні технології. Методи захисту. Вибирання, розгортання та експлуатування систем виявлення та запобігання**

вторгненням (IDPS) (ISO/IEC 27039:2015, IDT) – ISO/IEC 27039:2015 надає рекомендації для допомоги організаціям у підготовці до розгортання систем виявлення та запобігання вторгненням (IDPS). Зокрема, йдеться про вибір, розгортання та роботу IDPS. Він також містить довідкову інформацію, на основі якої походять ці рекомендації.

- **ДСТУ ISO/IEC 27040:2016 Інформаційні технології. Методи захисту. Безпека зберігання (ISO/IEC 27040:2015, IDT) –** ISO/IEC 27040:2015 надає детальні технічні вказівки щодо того, як організації можуть визначити відповідний рівень зниження ризику за допомогою перевіреного та послідовного підходу до планування, проектування, документування та реалізації безпеки зберігання даних. Безпека зберігання стосується захисту (безпеки) інформації, де вона зберігається, і безпеки інформації, що передається через канали зв'язку, пов'язані зі зберіганням. Безпека зберігання включає безпеку пристроїв і носіїв, безпеку дій з управління, пов'язаних із пристроями та носіями, безпеку програм і служб, а також безпеку, актуальну для кінцевих користувачів протягом усього терміну служби пристроїв і носіїв і після завершення використання. Безпека зберігання актуальна для всіх, хто бере участь у володінні, експлуатації або використанні пристроїв зберігання даних, засобів масової інформації та мереж. Це включає керівників вищої ланки, покупців продуктів і послуг зберігання та інших нетехнічних менеджерів або користувачів, на додаток до менеджерів і адміністраторів, які мають конкретні обов'язки за інформаційну безпеку чи безпеку зберігання, роботу сховища або які відповідають за загальну безпеку організації розробка програми та політики безпеки. Це також актуально для всіх, хто бере участь у плануванні, проектуванні та реалізації архітектурних аспектів безпеки мережі зберігання. ISO/IEC 27040:2015 містить огляд концепцій безпеки зберігання та відповідних визначень. Він містить вказівки щодо загроз, дизайну та аспектів контролю, пов'язаних із типовими сценаріями зберігання та областями технологій зберігання. Крім того, він надає посилання на інші міжнародні стандарти та технічні звіти, які стосуються існуючих практик і методів, які можуть бути застосовані для безпеки зберігання.

– ДСТУ ISO/IEC 27041:2016 Інформаційні технології. Методи захисту. Посібник із забезпечення прийнятності та адекватності методів розслідування (ISO/IEC 27041:2015, IDT) – ISO/IEC 27041:2015 надає вказівки щодо механізмів забезпечення того, що методи та процеси, які використовуються під час розслідування інцидентів інформаційної безпеки, «відповідають меті». Він інкапсулює найкращі практики щодо визначення вимог, опису методів і надання доказів того, що реалізації методів можна показати, що задовольняють вимоги. Він включає в себе розгляд того, як тестування постачальників і третіх сторін можна використовувати для сприяння цьому процесу гарантії. Цей документ має на меті: надавати вказівки щодо збору й аналізу функціональних і нефункціональних вимог, пов'язаних із розслідуванням інцидентів

інформаційної безпеки (IS); давати вказівки щодо використання валідації як засобу забезпечення придатності процесів, залучених до розслідування; надати вказівки щодо оцінювання необхідних рівнів валідації та доказів, необхідних для перевірки; надати вказівки щодо того, як зовнішнє тестування та документацію можна включити в процес валідації.

- **ДСТУ ISO/IEC 27042:2016 Інформаційні технології. Методи захисту. Настанови щодо аналізу та інтерпретації цифрового доказу (ISO/IEC 27042:2015, IDT) –** ISO/IEC 27042:2015 містить настанови щодо аналізу та інтерпретації цифрових доказів у спосіб, який розглядає питання безперервності, валідності, відтворюваності та повторюваності. Він інкапсулює найкращі практики для вибору, проектування та реалізації аналітичнихпроцесів і запису достатньої інформації, щоб такі процеси могли бути піддані незалежному контролю, коли це необхідно. У ньому містяться вказівки щодо належних механізмів демонстрації кваліфікації та компетентності слідчої групи. Аналіз та інтерпретація цифрових доказів може бути складним процесом. За деяких обставин може бути застосовано кілька методів, і члени слідчої групи повинні будуть обґрунтувати свій вибір певного процесу та показати, наскільки він еквівалентний іншому процесу, який використовують інші дослідники. За інших обставин дослідникам, можливо, доведеться розробити нові методи дослідження цифрових доказів, які раніше не розглядалися, і вони повинні мати можливість показати, що отриманий метод «відповідає меті». Застосування певного методу може вплинути на

інтерпретацію цифрових доказів, оброблених цим методом. Наявні цифрові докази можуть впливати на вибір методів для подальшого аналізу цифрових доказів, які вже були отримані. ISO/IEC 27042:2015 забезпечує загальну структуру для аналітичних та інтерпретаційних елементів обробки інцидентів безпеки інформаційних систем, які можуть бути використані для допомоги у впровадженні нових методів і забезпечують мінімальний загальний стандарт для цифрових доказів, отриманих у результаті такої діяльності.

- **ДСТУ ISO/IEC 27043:2016 Інформаційні технології. Методи захисту. Принципи та процеси розслідування інцидентів (ISO/IEC 27043:2015, IDT) –** ISO/IEC 27043:2015 надає вказівки на основі ідеалізованих моделей для загальних процесів розслідування інцидентів у різних сценаріях розслідування інцидентів із використанням цифрових доказів. Це включає процеси від підготовки до інциденту до закриття розслідування, а також будь-які загальні поради та застереження щодо таких процесів. Інструкції описують процеси та принципи, застосовні до різних типів розслідувань, включаючи, але не обмежуючись, несанкціонований доступ, пошкодження даних, збої системи або корпоративні порушення інформаційної безпеки, а також будь-які інші цифрові розслідування. Підсумовуючи, цей міжнародний стандарт надає загальний огляд усіх принципів і процесів розслідування інцидентів, не вказуючи конкретних деталей у рамках кожного з принципів і процесів розслідування, охоплених цим міжнародним стандартом. Багато інших відповідних міжнародних стандартів, де є посилання в цьому міжнародному стандарті, надають більш детальний зміст конкретних принципів і процесів розслідування.

ДСТУ ISO/IEC 27050-1:2018 Інформаційні технології. Методи захисту. Електронне виявлення. – складається з 4 частин:

- ДСТУ ISO/IEC 27050-1:2018 Інформаційні технології. Методи захисту. Електронне виявлення. Частина 1. Огляд та поняття (ISO/IEC 27050-1:2016, IDT) – Електронне відкриття – це процес виявлення відповідної інформації, що зберігається в електронному вигляді (ESI) або даних, однією чи декількома сторонами, залученими до розслідування, судового розгляду чи подібного процесу. Цей документ містить огляд електронного відкриття. Крім того, у ньому даються визначення пов'язаних термінів і описуються концепції, включаючи, але не обмежуючись цим, ідентифікацію, збереження, збір, обробку, перегляд, аналіз і виробництво ESI. Цей документ також визначає інші відповідні стандарти (наприклад, ISO/IEC 27037) і те, як вони стосуються та взаємодіють із діяльністю з електронних відкриттів. Цей документ стосується як нетехнічного, так і технічного персоналу, який бере участь у деяких або всіх видах електронної техніки.
- ISO/IEC 27050-2:2018. Інформаційна технологія. Електронне відкриття. Частина 2. Керівництво з управління електронним відкриттям – У цьому документі містяться вказівки для технічного та нетехнічного персоналу на вищому рівні керівництва в організації, включно з тими, хто відповідає за дотримання законодавчих і нормативних вимог, а також галузевих стандартів. Він описує, як такий персонал може ідентифікувати ризики, пов'язані з електронним відкриттям, і взяти на себе відповідальність за них, встановити політику та досягти відповідності відповідним зовнішнім і внутрішнім вимогам. Він також пропонує, як виробити такі політики у формі, яка може інформувати процес управління. Крім того, він містить вказівки щодо того, як запроваджувати та контролювати електронні відкриття відповідно до політики.
- ДСТУ ISO/IEC 27050-3:2018 Інформаційні технології. Методи захисту. Електронне виявлення. Частина 3. Звід правил для електронного виявлення (ISO/IEC 27050-3:2017, IDT) – У цьому документі містяться вимоги та рекомендації щодо діяльності з електронного відкриття, включаючи, але не обмежуючись, ідентифікацію, збереження, збір, обробку, перегляд, аналіз і створення електронно збереженої інформації (ESI). Крім того, цей документ визначає відповідні заходи, які охоплюють життєвий цикл ESI від його початкового створення до остаточної ліквідації. Цей документ стосується як нетехнічного, так і технічного персоналу, який бере участь у деяких або всіх видах електронної техніки.

Важливо зазначити, що користувач повинен знати про будь-які застосовні вимоги юрисдикції.

- ISO/IEC 27050-4:2021. Інформаційні технології – Електронне відкриття – Частина 4: Технічна готовність – У цьому документі містяться вказівки щодо того, як організація може планувати, готуватися до та впроваджувати електронне відкриття з точки зору як технологій, так і процесів. Цей документ містить вказівки щодо профілактичних заходів, які можуть допомогти забезпечити ефективне та відповідне електронне відкриття та процеси. Цей документ стосується як нетехнічного, так і технічного персоналу, який бере участь у деяких або всіх видах електронної техніки.

– ISO/IEC 27099:2022. Інформаційні технології – Інфраструктура відкритих ключів – Практика та рамки політики – У цьому документі встановлюється система вимог до управління інформаційною безпекою для постачальників довірчих послуг інфраструктури відкритих ключів (PKI) через політику сертифікації, положення про практику сертифікації та, де це можливо, їх внутрішню підтримку системою управління інформаційною безпекою (СУІБ) (ISMS). Структура вимог включає оцінку та обробку ризиків інформаційної безпеки, адаптованих для задоволення узгоджених вимог користувачів до послуг, як зазначено в політиці сертифікатів. Цей документ також призначений для того, щоб допомогти постачальникам послуг довіри підтримувати кілька політик сертифікатів. У цьому документі розглядається життєвий цикл сертифікатів відкритих ключів, які використовуються для цифрових підписів, автентифікації або встановлення ключа для шифрування даних. У ньому не йдеться про методи автентифікації, вимоги щодо неспростування або протоколи управління ключами, засновані на використанні сертифікатів відкритих ключів. Для цілей цього документа термін «сертифікат» стосується сертифікатів відкритих ключів. Цей документ не застосовується до сертифікатів атрибутів. У цьому документі використовуються концепції та вимоги СУІБ, як визначено в сімействі стандартів ISO/IEC 27000. Він використовує кодекс практики для контролю інформаційної безпеки, як визначено в ISO/IEC 27002. Конкретні вимоги до PKI (наприклад, вміст сертифіката, перевірка ідентичності, обробка відкликання сертифіката) не розглядаються безпосередньо СУІБ, як визначено в ISO/IEC 27001. Використання ISMS або еквівалента адаптовано до застосування вимог до служби PKI, зазначених у політиці сертифікатів, як описано в цьому документі. Постачальник довірчих послуг PKI – це спеціальний клас довірчих послуг для використання сертифікатів відкритих ключів. Цей документ розрізняє системи PKI, які використовуються в закритому, відкритому та договірному середовищах. Цей документ призначений для полегшення впровадження операційного, базового контролю та практики в договірному середовищі. Хоча цей документ зосереджений на договірному середовищі, застосування цього документа до відкритих чи закритих середовищ не виключається.

ЛЕКЦІЯ 5 НАПРЯМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

5.1. Основні положення Стратегії кібербезпеки України

Стратегія кібербезпеки України (далі – Стратегія) введена в дію Указом Президента України від 15 березня 2016 року №96/2016.

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

Для досягнення цієї мети необхідними є:

– створення національної системи кібербезпеки;

– посилення спроможностей суб'єктів Сектору безпеки і 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).

Забезпечення кібербезпеки України як стану захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі, що досягається комплексним застосуванням сукупності правових, організаційних, інформаційних заходів, *має базуватися на принципах*:

– верховенства права і поваги до прав та свобод людини і громадянина;

– забезпечення національних інтересів України;

– відкритості, доступності, стабільності та захищеності кіберпростору;

– державно-приватного партнерства, широкої співпраці з громадянськимсуспільством у сфері забезпечення кібербезпеки та кіберзахисту;

– пропорційності та адекватності заходів кіберзахисту реальним та потенційним ризикам;

– пріоритетності запобіжних заходів;

– невідворотності покарання за вчинення кіберзлочинів;

– пріоритетного розвитку та підтримки вітчизняного наукового, науково- технічного та виробничого потенціалу;

– міжнародного співробітництва з метою зміцнення взаємної довіри у сфері кібербезпеки та вироблення спільних підходів у протидії кіберзагрозам,консолідації зусиль у розслідуванні та запобіганні кіберзлочинам, недопущення використання кіберпростору в протиправних та воєнних цілях;

– забезпечення демократичного цивільного контролю над утвореними відповідно до законів України військовими формуваннями та правоохоронними органами держави, що діють у сфері кібербезпеки.

Розвиток та безпека кіберпростору, запровадження електронного урядування, гарантування безпеки й сталого функціонування електронних комунікацій та державних електронних інформаційних ресурсів мають бути складовими державної політики у сфері розвитку інформаційного простору та становлення інформаційного суспільства в Україні.

Стратегія кібербезпеки України базується на положеннях Конвенції про кіберзлочинність, ратифікованої Законом України від 7 вересня 2005 року № 2824-IV, 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 № 287 "Про рішення Ради національної безпеки і оборониУкраїни" від 6 травня 2015 року "Про Стратегію національної безпекиУкраїни"."

Кіберпростір поступово перетворюється на окрему, поряд із традиційними "Земля", "Повітря", "Море" та "Космос", сферу ведення бойових дій, у якій все більш активно діють

відповідні підрозділи Збройних сил провідних держав світу. З урахуванням широкого застосування сучасних інформаційних технологій у Секторі безпеки і оборони, створення єдиної автоматизованої системи управління Збройних Сил України оборона нашої держави стає більш уразливою до кіберзагроз.

Економічна, науково-технічна, інформаційна сфера, сфера державного управління, оборонно-промисловий і транспортний комплекси, інфраструктура електронних комунікацій, Сектор безпеки і оборони України стають все більш уразливими для розвідувально-підривної діяльності іноземних спецслужб у кіберпросторі. Цьому сприяє широка, подекуди домінуюча, присутність в інформаційній інфраструктурі України організацій, груп, осіб, які прямо чиопосередковано пов'язані з Російською Федерацією.

Сучасні інформаційно-комунікаційні технології можуть використовуватися для здійснення терористичних актів, зокрема шляхом порушення штатних режимів роботи автоматизованих систем керування технологічними процесами на об'єктах критичної інфраструктури. Більшого поширення набуває політично вмотивована діяльність у кіберпросторі у виглядіатак на урядові та приватні веб-сайти в мережі Інтернет.

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. Новітні технології застосовуються не лише для скоєння традиційних видів злочинів, але і для скоєння принципово нових видів злочинів, притаманних суспільству з високим рівнем інформатизації.

Загрози кібербезпеці актуалізуються через дію таких факторів, зокрема, як:

– невідповідність інфраструктури електронних комунікацій держави, рівня її розвитку та захищеності сучасним вимогам;

– недостатній рівень захищеності критичної інформаційної інфраструктури, державних електронних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом від кіберзагроз;

– безсистемність заходів кіберзахисту критичної інформаційної інфраструктури;

– недостатній розвиток організаційно-технічної інфраструктури забезпечення кібербезпеки та кіберзахисту критичної інформаційної 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.

Національна система кібербезпеки є сукупністю суб’єктів забезпечення кібербезпеки та взаємопов’язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно- розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно- технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об’єктів критичноїінформаційної інфраструктури.

Рада національної безпеки і оборони України відповідно до Конституції України та у встановленому законом порядку має здійснювати координацію та контроль діяльності суб'єктів Сектору безпеки і оборони, які забезпечують кібербезпеку України.

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.

5.2. Сутність та завдання Національної системи забезпеченнякібербезпеки України

В прийнятій Стратегії кібербезпеки України визначені суб’єкти забезпечення кібербезпеки України та основні їх завдання відповідно до компетенцій. Більш детально Національна система забезпечення кібербезпеки України розглядається в Законі України

“Про основні засади забезпечення кібербезпеки України” від 05.10.2017 року.

Національна система кібербезпеки є сукупністю суб’єктів забезпечення кібербезпеки та взаємопов’язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно- розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно- технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об’єктів критичноїінформаційної інфраструктури.

Основними суб’єктами національної системи кібербезпеки є Державна служба спеціального зв’язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України, які відповідно до Конституції і законів України виконують в установленому порядку такі **основні завдання** (рис. 1.21):

Державна служба спеціального зв’язку та захисту інформації України:

– забезпечує формування та реалізацію державної політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту об’єктів критичної інформаційної інфраструктури, здійснює державний контроль у цих сферах;

– координує діяльність інших суб’єктів забезпечення кібербезпеки щодокіберзахисту;

– забезпечує створення та функціонування Національної телекомунікаційної мережі, впровадження організаційно-технічної моделі кіберзахисту;

– здійснює організаційно-технічні заходи із запобігання, виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків;

– інформує про кіберзагрози та відповідні методи захисту від них; забезпечує впровадження аудиту інформаційної безпеки на об’єктах критичної інфраструктури, встановлює вимоги до аудиторів інформаційної безпеки, визначає порядок їх атестації (переатестації);

– координує, організовує та проводить аудит захищеності комунікаційних і технологічних систем об’єктів критичної інфраструктури на уразливість;

– забезпечує функціонування Державного центру кіберзахисту, урядової команди реагування на комп’ютерні надзвичайні події України CERT-UA.

Національна поліція України:

– забезпечує захист прав і свобод людини і громадянина, інтересів суспільства і держави від злочинних посягань у кіберпросторі;

– здійснює заходи із запобігання, виявлення, припинення та розкриття кіберзлочинів, підвищення поінформованості громадян про безпеку вкіберпросторі.

Служба безпеки України:

– здійснює запобігання, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, які вчиняються у кіберпросторі;

– здійснює контррозвідувальні та оперативно-розшукові заходи, спрямовані на боротьбу з кібертероризмом та кібершпигунством, негласно перевіряє готовність об’єктів критичної інфраструктури до можливих кібератак та кіберінцидентів;

– протидіє кіберзлочинності, наслідки якої можуть створити загрозу життєво важливим інтересам держави;

– розслідує кіберінциденти та кібератаки щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури;

– забезпечує реагування на кіберінциденти у сфері державної безпеки.

Міністерство оборони України, Генеральний штаб Збройних Сил України

відповідно до компетенції:

– здійснюють заходи з підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони);

– здійснюють військову співпрацю з НАТО та іншими суб’єктами оборонної сфери щодо забезпечення безпеки кіберпростору та спільного захисту від кіберзагроз;

– впроваджують заходи із забезпечення кіберзахисту критичної інформаційної інфраструктури в умовах надзвичайного і воєнного стану.

Розвідувальні органи України:

– здійснюють розвідувальну діяльність щодо загроз національній безпеці України у кіберпросторі, інших подій і обставин, що стосуються сфери кібербезпеки.

Національний банк України:

– визначає порядок, вимоги та заходи із забезпечення кіберзахисту та інформаційної безпеки у банківській системі України та для суб'єктів переказу коштів, здійснює контроль за їх виконанням;

– створює центр кіберзахисту Національного банку України, забезпечує функціонування системи кіберзахисту у банківській системі України;забезпечує проведення оцінювання стану кіберзахисту та аудиту інформаційної безпеки на об'єктах критичної інфраструктури у банківській системі України.

Функціонування національної системи кібербезпеки забезпечується шляхом:

– вироблення й оперативної адаптації державної політики у сфері кібербезпеки, спрямованої на розвиток кіберпростору, досягнення сумісності з відповідними стандартами Європейського Союзу та НАТО;

– створення нормативно-правової та термінологічної бази у сфері кібербезпеки, гармонізації нормативних документів у сфері електронних комунікацій, захисту інформації, інформаційної безпеки та кібербезпеки відповідно до міжнародних стандартів, зокрема стандартів Європейського Союзу та НАТО;

– встановлення обов'язкових вимог інформаційної безпеки об'єктів критичної інформаційної інфраструктури, у тому числі під час їх створення, введення в експлуатацію, експлуатації та модернізації з урахуванням міжнародних стандартів та специфіки галузі, до якої належать відповідні об'єкти критичної інформаційної інфраструктури;

– формування конкурентного середовища у сфері електронних комунікацій, надання послуг із захисту інформації та кіберзахисту;

– залучення експертного потенціалу наукових установ, професійних та громадських об'єднань до підготовки проектів концептуальних документів у сфері кібербезпеки;

– проведення навчань щодо дій у разі надзвичайних ситуацій та інцидентів у кіберпросторі;

– функціонування системи аудиту інформаційної безпеки, запровадження кращих світових практик і міжнародних стандартів з питань кібербезпеки та кіберзахисту;

– розвитку мережі команд реагування на комп'ютерні надзвичайні події;

– розвитку та вдосконалення системи технічного і криптографічного захисту інформації;

– забезпечення дотримання вимог законодавства щодо захисту державних інформаційних ресурсів та інформації;

– створення та забезпечення функціонування Національної телекомунікаційної мережі;

– обміну інформацією про інциденти кібербезпеки між суб'єктами забезпечення кібербезпеки у порядку, визначеному законодавством;

– впровадження єдиної (універсальної) системи індикаторів кіберзагроз з урахуванням міжнародних стандартів з питань кібербезпеки та кіберзахисту;

– підготовки фахівців освітньо-кваліфікаційних рівнів бакалавра і магістра за державним замовленням в обсязі, необхідному для задоволення потреб державного сектору економіки, а також за небюджетні кошти, у тому числі, для підвищення кваліфікації та проведення обов'язкової періодичної атестації (переатестації) персоналу, відповідального за забезпечення кібербезпеки об'єктів критичної інфраструктури, з урахуванням міжнародних стандартів;

– впровадження організаційно-технічної моделі національної системи кібербезпеки як комплексу заходів, сил і засобів кіберзахисту, спрямованих на оперативне (кризове) реагування на кібератаки та кіберінциденти, впровадження контрзаходів, спрямованих на

мінімізацію уразливості комунікаційних систем;

– встановлення вимог (правил, настанов) щодо безпечного використання мережі Інтернет та надання електронних послуг державними органами;

– державно-приватної взаємодії у запобіганні кіберзагрозам об'єктам критичної інфраструктури, реагуванні на кібератаки та кіберінциденти, усуненні їх наслідків, зокрема в умовах кризових ситуацій, надзвичайного і воєнного стану, в особливий період;

– періодичного проведення огляду національної системи кібербезпеки, розроблення індикаторів стану кібербезпеки;

– стратегічного планування та програмно-цільового забезпечення у сфері розвитку електронних комунікацій, інформаційних технологій, захистуінформації та кіберзахисту;

– розвитку міжнародного співробітництва у сфері кібербезпеки, підтримки міжнародних ініціатив у сфері кібербезпеки, що відповідають національним інтересам України, поглиблення співпраці України з Європейським Союзом та НАТО з метою посилення спроможності України у сфері кібербезпеки, участі у заходах зі зміцнення довіри при використанні кіберпростору, що проводяться під егідою Організації з безпеки і співробітництва в Європі;

– здійснення оперативно-розшукових, розвідувальних, контррозвідуваль-них та інших заходів, спрямованих на запобігання, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, які вчиняються з використанням кіберпростору, розслідування, переслідування, оперативного реагування та протидії кіберзлочинності, розвідувально-підривній, терористичній та іншій діяльності у кіберпросторі, що завдає шкоди інтересам України, використанню мережі Інтернет у воєнних цілях;

– здійснення воєнно-політичних, військово-технічних та інших заходів для розширення можливостей Воєнної організації держави, Сектору безпеки і оборони з використанням кіберпростору, створення і розвитку сил, засобів та інструментів можливої відповіді на агресію у кіберпросторі, яка може застосовуватися як засіб стримування воєнних конфліктів та загроз з використанням кіберпростору;

– обмеження участі у заходах із забезпечення інформаційної безпеки та кібербезпеки будь-яких суб'єктів господарювання, які перебувають під контролем держави, визнаної Верховною Радою України державою-агресором, або держав та осіб, стосовно яких діють спеціальні економічні та інші обмежувальні заходи (санкції), прийняті на національному або міжнародному рівні внаслідок агресії щодо України, а також обмеження використання продукції, технологій та послуг таких суб'єктів для забезпечення технічного та криптографічного захисту державних інформаційних ресурсів, посилення державного контролю в цій сфері;

– розвитку системи контррозвідувального забезпечення кібербезпеки, призначеної для запобігання, своєчасного виявлення та протидії зовнішнім і внутрішнім загрозам безпеці України з використанням кіберпростору; усунення умов, що їм сприяють, та причин їх виникнення;

– проведення розвідувальних заходів із виявлення та протидії загрозам національній безпеці України у кіберпросторі, виявлення інших подій і обставин, що стосуються сфери кібербезпеки.

Впровадження організаційно-технічної моделі кібербезпеки як складової національної системи кібербезпеки здійснюється Державним центром кіберзахисту, який забезпечує створення та функціонування основних складових системи захищеного доступу державних органів до мережі Інтернет, системи антивірусного захисту національних інформаційних ресурсів, аудиту інформаційної безпеки та стану кіберзахисту об'єктів критичної інформаційної інфраструктури, системи виявлення уразливостей і реагування на кіберінциденти та кібератаки щодо об'єктів кіберзахисту, системи взаємодії команд реагування на комп'ютерні надзвичайні події, а також у взаємодії з іншими суб'єктами забезпечення кібербезпеки розробляє сценарії реагування на кіберзагрози, заходи щодо протидії таким загрозам, програми та методики проведення кібернавчань.

5.3. Пріоритети та напрями забезпечення кібербезпекиУкраїни згідно з чинним законодавством

Пріоритети та напрями забезпечення кібербезпеки України:

Розвиток безпечного, стабільного і надійного кіберпростору має полягати, насамперед, у:

– виробленні й оперативній адаптації державної політики у сфері кібербезпеки, спрямованої на розвиток кіберпростору, досягненні сумісності з відповідними стандартами ЄС та НАТО;

– створенні вітчизняної нормативно-правової та термінологічної бази у цій сфері, гармонізації нормативних документів у сфері електронних комунікацій, захисту інформації, інформаційної та кібербезпеки відповідно до міжнародних стандартів і стандартів ЄС та НАТО;

– формуванні конкурентного середовища у сфері електронних комунікацій, наданні послуг із захисту інформації та кіберзахисту;

– розвитку технологій кіберзахисту засобів рухомого зв'язку, забезпеченні апаратної, контентної безпеки, безпеки додатків та сервісів зв'язку;

– залученні експертного потенціалу наукових установ, професійних та громадських об'єднань до підготовки проектів концептуальних документів у сфері кібербезпеки;

– підвищенні цифрової грамотності громадян та культури безпекового поводження в кіберпросторі, комплексних знань, навичок і здібностей, необхідних для підтримки цілей кібербезпеки, впровадженні державних і громадських проектів підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту;

– проведенні навчань щодо надзвичайних ситуацій та інцидентів у кіберпросторі;

– розвитку та удосконаленні системи державного контролю за станом захисту інформації, а також системи незалежного аудиту інформаційної безпеки, запровадженні кращих світових практик і міжнародних стандартів з питань кібербезпеки та кіберзахисту;

– розвитку інфраструктури електронних комунікацій, включаючи широкосмуговий доступ до мережі Інтернет, цифрове та інтерактивне телебачення;

– розвитку мережі команд реагування на комп'ютерні надзвичайні події;

– створенні системи своєчасного виявлення, запобігання та нейтралізації кіберзагроз, у тому числі із залученням волонтерських організацій;

– розвитку та вдосконаленні системи технічного і криптографічного захисту інформації;

– розвитку міжнародного співробітництва у сфері забезпечення кібербезпеки, підтримці міжнародних ініціатив у сфері кібербезпеки, які відповідають національним інтересам України, поглибленні співпраці України з ЄС та НАТО для посилення спроможностей України у сфері кібербезпеки, участі у заходах зі зміцнення довіри у кіберпросторі, які проводяться під егідоюОБСЄ;

– створенні умов для впровадження в Україні сучасних технологій кіберзахисту.

Кіберзахист державних електронних інформаційних ресурсів та інформаційної інфраструктури, призначеної для обробки інформації, вимога щодо захисту якої встановлена законом, має полягати, насамперед, у:

– створенні та забезпеченні функціонування національної телекомунікаційної мережі – єдиної платформи захищених електронних комунікацій органів державної влади;

– упровадженні організаційно-технічної моделі національної системи кібербезпеки, оперативному реагуванні на кібератаки та кіберінциденти;

– розгортанні (відповідно до компетенції) єдиної системи ситуаційних центрів профільних органів державної влади Сектору безпеки і оборони на базі захищеної інформаційної інфраструктури;

– розбудові захищеної інтегрованої системи електронних державних реєстрів, баз даних, дата-центрів, у тому числі єдиного дата-центру резервного збереження інформації і відомостей державних електронних інформаційних ресурсів;

– удосконаленні системи зберігання, передачі та обробки даних державних реєстрів і баз даних із застосуванням сучасних інформаційно-комунікаційних технологій (включаючи технології on-line-доступу);

– розробленні нових методів запобігання кібератакам, кіберінцидентам та поширенню інформації про них;

– розробленні вимог (правил, настанов) щодо безпечного використання мережі Інтернет та надання електронних послуг державними органами;

– підвищенні обізнаності працівників державних органів у сфері інформаційної та кібербезпеки, проведенні відповідних тренінгів, навчань.

Кіберзахист критичної інфраструктури має полягати, насамперед, у:

– комплексному вдосконаленні правової основи кіберзахисту об'єктів критичної інфраструктури, визначенні критеріїв віднесення інформаційних (автоматизованих), телекомунікаційних, інформаційно-телекомунікаційних систем до критичної інформаційної інфраструктури;

– формуванні та забезпеченні функціонування державного реєстру об'єктів критичної інформаційної інфраструктури;

– регламентації вимог до кіберзахисту об'єктів критичної інфраструктури;

– створенні та забезпеченні функціонування власниками (розпорядниками) об'єктів критичної інфраструктури підрозділів кіберзахисту;

– установленні кваліфікаційних вимог для окремих категорій працівників об'єктів критичної інфраструктури з урахуванням сучасних тенденцій кібербезпеки та актуальних кіберзагроз, упровадження для таких працівників обов'язкової періодичної атестації на предмет відповідності зазначеним вимогам;

– налагодженні співробітництва між суб'єктами забезпечення кіберзахисту критичної інфраструктури, розвитку державно-приватного партнерства у запобіганні кіберзагрозам, реагуванні на кібератаки та кіберінциденти, усуненніїх наслідків, зокрема в умовах кризових ситуацій, надзвичайного і воєнного стану, в особливий період;

– розробленні та запровадженні механізму обміну інформацією між державними органами, приватним сектором і громадянами стосовно загроз критичній інформаційній інфраструктурі.

Розвиток потенціалу Сектору безпеки і оборони у сфері забезпечення кібербезпеки передбачатиме здійснення в установленому порядку, зокрема, таких заходів:

– здійснення захисту технологічних процесів на об'єктах критичної інфраструктури, в яких управління або моніторинг здійснюється за допомогою інформаційно-комунікаційних технологій, від несанкціонованого втручання у їх роботу;

– періодичне проведення огляду національної системи кібербезпеки, розроблення галузевих індикаторів стану кібербезпеки;

– розроблення та впровадження протоколів спільних дій, зокрема, інформаційного обміну у режимі реального часу, суб'єктів забезпечення кібербезпеки під час виявлення кібератак та кіберінцидентів;

– проведення навчань суб'єктів Сектору безпеки і оборони щодо реагування на кібератаки та кіберінциденти, зокрема, проведення кібернавчань Збройних Сил України, інших суб’єктів Сектору безпеки і оборони України, участь у таких навчаннях у рамках заходів колективної оборони;

– реалізація державного стратегічного планування та програмно- цільового забезпечення у сфері розвитку електронних комунікацій, інформаційних технологій, захисту інформації та кіберзахисту;

– здійснення воєнно-політичних, військово-технічних та інших заходів для розширення можливостей Воєнної організації держави, Сектору безпеки і оборони у кіберпросторі, створення, розвиток сил, засобів та інструментів можливої відповіді на агресію у кіберпросторі, яка може застосовуватись як засіб стримування військових конфліктів та загроз у кіберпросторі (активний кіберзахист);

– створення єдиного підрозділу із забезпечення кібербезпеки та кіберзахисту Збройних

Сил України на стратегічному, оперативному татактичному рівнях;

– розвиток підрозділів кібербезпеки та кіберзахисту Збройних Сил України, Державної служби спеціального зв'язку та захисту інформації України, Служби безпеки України, Національної поліції України, розвідувальних органів, досягнення сумісності із відповідними підрозділами кібербезпеки та кіберзахисту держав – членів НАТО;

– сприяння розвитку системи оперативного реагування на комп'ютерні надзвичайні події;

– удосконалення системи контррозвідувального та оперативно- розшукового забезпечення кібербезпеки держави;

– розвиток та координація проведення наукових досліджень у галузі кібербезпеки та кіберзахисту для потреб національної безпеки і оборони;

– підвищення спроможності суб'єктів боротьби з кібертероризмом щодо протидії кібератакам на державні електронні інформаційні ресурси, об'єкти критичної інфраструктури, а також розвідувально-підривної діяльності іноземних спецслужб, організацій, груп та осіб проти України у кіберпросторі;

– обмеження участі у заходах із забезпечення інформаційної та кібербезпеки будь-яких суб'єктів господарювання, які знаходяться під контролем держави-агресора, визнаної Верховною Радою України, або держав та осіб, стосовно яких діють спеціальні економічні та інші обмежувальні заходи (санкції), прийняті на національному або міжнародному рівні внаслідок агресії щодо України, а також обмеження використання продукції, технологій та послуг таких суб'єктів для забезпечення технічного та криптографічного захисту державних інформаційних ресурсів, посилення державного контролю у цій сфері;

– розмежування кримінальної відповідальності за злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, вчинені щодо державних та інших інформаційних ресурсів, щодо об'єктів критичної інформаційної інфраструктурита інших об'єктів, а також відповідне розмежування підслідності;

– розвиток системи підготовки кадрів для потреб органів Сектору безпеки і оборони України та розвиток науково-виробничого потенціалу такої системи.

Боротьба з кіберзлочинністю передбачатиме здійснення в установленому порядку, серед іншого, таких заходів:

– створення ефективного і зручного контакт-центру для повідомлень про випадки кіберзлочинів та шахрайства у кіберпросторі, підвищення оперативності реагування на кіберзлочини правоохоронних органів, зокрема їх регіональних підрозділів;

– удосконалення процесуальних механізмів щодо збирання доказів в електронній формі, що стосуються злочину, удосконалення класифікації, методів, засобів і технологій ідентифікації та фіксації кіберзлочинів, проведення експертних досліджень;

– запровадження блокування операторами та провайдерами телекомунікацій визначеного (ідентифікованого) інформаційного ресурсу (інформаційного сервісу) за рішенням суду;

– унормування порядку внесення обов'язкових до виконання операторами та провайдерами телекомунікацій приписів про термінове фіксування та подальше зберігання комп'ютерних даних, збереження даних про трафік;

– врегулювання питання можливості термінового здійснення процесуальних дій у режимі реального часу із застосуванням електронних документів та електронного цифрового підпису;

– упровадження схеми (протоколу) координації правоохоронних органів щодо боротьби з кіберзлочинністю;

– підготовка суддів (слідчих суддів), слідчих та прокурорів для роботи з доказами, що стосуються злочину, отриманими в електронній формі, з урахуванням особливостей кіберзлочинів;

– запровадження особливого порядку зняття інформації з каналів телекомунікацій у

випадку розслідування кіберзлочинів;

– підвищення кваліфікації співробітників правоохоронних органів.

5.4. НОРМАТИВНО-ПРАВОВА БАЗА УКРАЇНИ У СФЕРІ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Права людини в інформаційному суспільстві: міжнародні правові акти, що стосуються інформаційних прав особи. Принцип верховенства права в інформаційній політиці держави. Важливим аспектом інформаційної діяльності демократичної держави є ієрархія пріоритетів, серед яких на першому місці стоїть міжнародне право, на другому – національне законодавство разом з Основним Законом, і вже далі − підзаконні акти, які не повинні суперечити міжнародному та національному законодавству. Як відомо, в українському законодавстві з дотриманням цієї ієрархічності не все гаразд. Часто підзаконні акти та відомчі інструкції стоять на першому місці в діяльності окремих державних органів та посадових осіб.

Які міжнародні правові акти гарантують інформаційні права та свободи людини і громадянина, зокрема право на конфіденційність та право на вільне отримання інформації? Передусім, це «Загальна Декларація прав людини» (1948 р.). Відповідно до статті 12, «ніхто не може зазнавати безпідставного втручання у його особисте і сімейне життя“. Згідно з статтею 19 «кожна людина має право на свободу переконань і на вільне їх виявлення; це право включає свободу безперешкодно дотримуватися своїх переконань та свободу шукати і поширювати інформацію та ідеї будь-якими засобами і незалежно від державних кордонів».

Важливим документом є «Європейська конвенція про захист прав людини та основних свобод» (1950 р.), яка про інформаційні права людини говорить таке: стаття 10 «Кожен має право на вираження поглядів. Це право включає свободу дотримуватися своїх поглядів, одержувати і передавати інформацію та ідеї без втручання органів державної влади і незалежно від кордонів». У цій же конвенції міститься перелік винятків, коли права громадян можуть бути обмежені на законних підставах:

«Здійснення цих свобод може бути обмежене в інтересах громадської безпеки, запобігання злочинам, охорони здоров’я, моралі, запобігання розголошенню конфіденційної інформації».

Розвиток комп’ютерних технологій призвів до масової практики автоматизованої обробки інформації в комп’ютерних мережах, в тому числі інформації персонального характеру. Виникла потреба додаткового захисту інформаційних прав людини. Цій меті має служити «Конвенція про захист осіб стосовно автоматизованої обробки даних особистого характеру» (Страсбург, 28 січня 1981 р.). У Преамбулі Конвенції зазначено, що її головною метою є гарантування свободи інформації незалежно від кордонів, безперешкодного обігу інформації між народами. Зміст Конвенції можна проілюструвати через окремі статті.

Стаття 1 гарантує право людини на недоторканність особистого життя, яке підлягає ризику під час автоматизованої обробки персональних даних. Стаття 5 визначає якість обробки даних про особу: «Дані особистого характеру, що підлягають автоматизованій обробці: а) отримуються та обробляються сумлінно та законно; б) зберігаються для визначених та законних цілей; в) мають бути адекватними, відповідними і ненадмірними з точки зору цілей, заради яких вони зберігаються; г) мають бути точними і поновлюватися (на вимогу особи); д) зберігатися не довше, ніж це потрібно цілям збереження». Стаття 6 виокремлює особливу категорію персональних даних, які одержали назву «вразливі» або «делікатні». Це «дані особистого характеру, що свідчать про расову належність, політичні або релігійні та інші переконання, а також дані особистого характеру, що стосуються здоров’я, статевого життя, не можуть піддаватися автоматизованій обробці. Це правило стосується також особистих даних, що стосуються кримінального засудження». Стаття 8 встановлює додаткові гарантії для суб’єкта даних: а*)* «особі надається можливість встановлювати існування файлу особистих даних для автоматизованої обробки, особу і місцезнаходження контролера файлу; б) отримувати без затримки чи витрат підтвердження чи спростування інформації про зберігання даних особистого характеру; в) вимагати виправлення і знищення незаконно одержаних даних; г) гарантується правовий захист персональних даних». Звісно,

європейське право передбачає чітке окреслення сфери винятків, їх обґрунтованість і зрозумілість. Обмежити інформаційні права громадян можна в кількох випадках: в інтересах захисту державної та громадської безпеки, валютно-кредитних інтересів держави, боротьби з кримінальними структурами, а також в інтересах захисту прав і свобод інших громадян (стаття 9). Крім того, особисті дані можна використовувати в статистичних підрахунках та наукових дослідженнях (як правило, в знеособленому вигляді).

Важливим міжнародним документом є також «Директива Європарламенту та Ради Європи стосовно обробки персональних даних і захисту права на невтручання в особисте життя в телекомунікаційному секторі» від 15 грудня 1997 року, метою якої є «забезпечення невтручання в особисте життя при обробці персональних даних в телекомунікаційному просторі та для забезпечення вільного переміщення таких даних». Сфера винятків будується за аналогією з попередніми європейськими актами: це громадський порядок, оборона, державна безпека (включаючи економічний добробут держави), кримінальне право.

Імплементація положень європейського права щодо захисту інформаційних прав людини та громадянина вважається необхідною умовою демократизації політико-правової системи України, її наближення до стандартів ЄС та формування громадянського суспільства.

Конституція України про інформаційні права громадян та інформаційну безпеку. Конституція (1996 р.) у статті 17 проголошує, що «захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього українського народу». Йдеться про те, що від інформаційної безпеки держави залежить доля народу, його матеріальний добробут та духовне благополуччя. Стаття 19 однозначно стверджує пріоритет Закону та Конституції перед іншими нормативними актами: «Органи державної влади та органи місцевого самоврядування, їхні посадові особи зобов’язані діяти лише в межах повноважень та у спосіб, що передбачені Конституцією та законами України». Проте громадяни мають право апелювати до Конституції як закону прямої дії, якщо посадова особа відмовляє у задоволені запиту громадянина, керуючись підзаконними актами чи внутрішніми інструкціями.

Стаття 32 гарантує, що «ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України. Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини. Кожний громадянин має право знайомитися в органах державної влади, органах місцевого самоврядування, установах і організаціях з відомостями про себе, які не є державною або іншою захищеною законом таємницею. Кожному гарантується судовий захист права спростовувати недостовірну інформацію про себе і членів своєї сім'ї та права вимагати вилучення будь-якої інформації, а також право на відшкодування матеріальної і моральної шкоди, завданої збиранням, зберіганням, використанням та поширенням такої недостовірної інформації».

Стаття 34 говорить про право «вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір», а також встановлює перелік винятків, коли право громадян може бути обмежено: «Здійснення цих прав може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя».

Як бачимо, поряд із винятками, визначеними європейськими документами, згадується кілька специфічно українських, а саме: запобігання розголошенню конфіденційної інформації та «підтримання авторитету правосуддя». При цьому найменш зрозумілим є останній виняток.

Так чи інакше, Конституція є найважливішим юридичним актом, що забезпечує інформаційні права громадян України, право на недоторканність приватного життя, та

закладає основи для розробки спеціального законодавства з охорони інформаційної безпеки держави.

Основні положення Закону України «Про національну безпеку від 21 червня 2018 року».

«Стратегія національної безпеки України від 26 травня 2015 року» про загрози в інформаційній сфері. Базовим чинним законом, що регулює інформаційну сферу, є Закон України «Про інформацію», прийнятий 2 жовтня 1992 р. Доцільно викласти основні положення закону. Під терміном «інформація» закон розуміє «документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві» (стаття 1). Основними принципами інформаційних відносин вважаються: гарантованість права на інформацію; відкритість та доступність інформації; свобода інформаційного обміну; об'єктивність та вірогідність інформації; законність її одержання, використання, поширення та збереження (стаття 5).

Статті 17 та 18 визначають галузі та види інформації: основними галузями інформації є: політична, економічна, духовна, науковотехнічна, соціальна, екологічна, міжнародна. До видів належить: статистична інформація; адміністративна інформація (дані); масова інформація; інформація про діяльність державних органів влади та органів місцевого і регіонального самоврядування; правова інформація; інформація про особу; інформація довідково-енциклопедичного характеру; соціологічна інформація.

Стаття 27 надає законодавче визначення терміну «документ»:

«Документ – це передбачена законом матеріальна форма одержання, зберігання, використання і поширення інформації шляхом фіксації її на папері, магнітній, кіно-, відео-, фотоплівці або на іншому носієві. Первинний документ – це документ, що містить в собі вихідну інформацію. Вторинний документ – це документ, що являє собою результат аналітико-синтетичної та іншої переробки одного або кількох документів».

Стаття 28 поділяє інформацію на відкриту та інформацію з обмеженим доступом (ІЗОД), а стаття 30 роз'яснює, що таке ІЗОД, встановлює режими доступу до інформації. Інформація з обмеженим доступом за своїм правовим режимом поділяється на конфіденційну і таємну.

«*Конфіденційна інформація* – це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов.

Стосовно інформації, що є власністю держави і знаходиться в користуванні органів державної влади чи органів місцевого самоврядування, підприємств, установ та організацій усіх форм власності, з метою її збереження може бути відповідно до закону встановлено обмежений доступ – надано статус конфіденційної. Порядок обліку, зберігання і використання документів та інших носіїв інформації, що містять зазначену інформацію, визначається Кабінетом Міністрів України. До конфіденційної інформації, що є власністю держави і знаходиться в користуванні органів державної влади чи органів місцевого самоврядування, підприємств, установ та організацій усіх форм власності, не можуть бути віднесені відомості:

– про стан довкілля, якість харчових продуктів і предметів побуту; про аварії, катастрофи, небезпечні природні явища та інші надзвичайні події, які сталися або можуть статися і загрожують безпеці громадян;

– про стан здоров'я населення, його життєвий рівень, включаючи харчування, одяг, житло, медичне обслуговування та соціальне забезпечення, а також про соціально-демографічні показники, стан правопорядку, освіти і культури населення;

– стосовно стану справ із правами і свободами людини і громадянина, а також фактів їх порушень;

– про незаконні дії органів державної влади, органів місцевого самоврядування, їх посадових та службових осіб;

– інша інформація, доступ до якої відповідно до законів України та міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України, не може бути

обмеженим.

Громадяни, юридичні особи, які володіють інформацією професійного, ділового, виробничого, банківського, комерційного та іншого характеру, одержаною на власні кошти, або такою, яка є предметом їх професійного, ділового, виробничого, банківського, комерційного та іншого інтересу і не порушує передбаченої законом таємниці, самостійно визначають режим доступу до неї, включаючи належність її до категорії конфіденційної, та встановлюють для неї систему (способи) захисту.

Виняток становить інформація комерційного та банківського характеру, а також інформація, правовий режим якої встановлено Верховною Радою України за поданням Кабінету Міністрів України (з питань статистики, екології, банківських операцій, податків тощо), та інформація, приховування якої являє загрозу життю і здоров'ю людей.

До таємної інформації належить інформація, що містить відомості, які становлять державну та іншу передбачену законом таємницю, розголошення якої завдає шкоди особі, суспільству і державі.

Віднесення інформації до категорії таємних відомостей, які становлять державну таємницю, і доступ до неї громадян здійснюється відповідно до закону про цю інформацію.

Порядок обігу таємної інформації та її захисту визначається відповідними державними органами за умови додержання вимог, встановлених цим Законом.

Порядок і терміни обнародування таємної інформації визначаються відповідним законом.

Інформація з обмеженим доступом може бути поширена без згоди її власника, якщо ця інформація є суспільно значимою, тобто якщо вона є предметом громадського інтересу і якщо право громадськості знати цю інформацію переважає право її власника на її захист».

Ця стаття є засадничою для роботи державних службовців з документами, що належать до категорії ІЗОД, громадян, які зацікавлені в отриманні «суспільно важливої» інформації та захисті своїх інформаційних прав, в тому числі права на конфіденційність. У наступній статті 31 якраз йдеться про право громадян на доступ до інформації, а саме: громадяни мають право «*знати у період збирання інформації, які відомості про них і з якою метою збираються, як, ким і з якою метою вони використовуються; доступу до інформації про них, заперечувати її правильність, повноту, доречність тощо.*

Державні органи та організації, органи місцевого і регіонального самоврядування, інформаційні системи яких вміщують інформацію про громадян, зобов'язані надавати її безперешкодно і безкоштовно на вимогу осіб, яких вона стосується, крім випадків, передбачених законом, а також вживати заходів щодо запобігання несанкціонованому доступу до неї. У разі порушень цих вимог Закон гарантує захист громадян від завданої їм шкоди використанням такої інформації.

Забороняється доступ сторонніх осіб до відомостей про іншу особу, зібраних відповідно до чинного законодавства державними органами, організаціями і посадовими особами.

Зберігання інформації про громадян не повинно тривати довше, ніж це необхідно для законно встановленої мети.

Всі організації, які збирають інформацію про громадян, повинні до початку роботи з нею здійснити у встановленому Кабінетом Міністрів України порядку державну реєстрацію відповідних баз даних.

Необхідна кількість даних про громадян, яку можна одержати законним шляхом, має бути максимально обмеженою і може використовуватися лише для законно встановленої мети.

Відмова в доступі до такої інформації, або приховування її, або незаконні збирання, використання, зберігання чи поширення можуть бути оскаржені до суду».

Усі ці положення відповідають європейським правовим нормам. Держава не має права безпідставно відмовляти громадянину у задоволенні його інформаційного запиту, а термін вивчення запиту не повинен перевищувати 10 днів. Задоволення ж запиту повинно відбутися упродовж 30 днів. Громадянин має право оскаржувати в суді відмову державного органу задовольнити інформаційний запит, при цьому саме держава повинна доводити в суді

законність такої відмови. Якщо суд встановив, що запитувачу відмовили незаконно, винні посадові особи притягуються до дисциплінарної та іншої, передбаченої законодавством, відповідальності.

37-ма стаття роз'яснює обмеження на доступ до тієї чи іншої інформації. Не всі інформаційні запити громадян можуть бути задоволені. До інформації, що не надається та не оприлюднюється, належать: інформація, визнана державною таємницею; конфіденційна інформація; інформація про оперативну і слідчу роботу органів прокуратури, Міністерства внутрішніх справ, Служби безпеки України, роботу органів дізнання та суду, якщо її розголошення може зашкодити оперативним заходам, розслідуванню чи дізнанню, порушити право людини на справедливий та об'єктивний судовий розгляд її справи, створити загрозу життю або здоров'ю будь-якої особи; інформація, що стосується особистого життя громадян; документи, що становлять внутрішньовідомчу службову кореспонденцію (доповідні записки, переписка між підрозділами та інше), якщо вони пов'язані з розробкою напряму діяльності установи, процесом прийняття рішень і передують їх прийняттю; інформацію, що не підлягає розголошенню згідно з іншими законодавчими або нормативними актами. Установа, до якої надано запит, може не надавати для ознайомлення документ, якщо він містить інформацію, яка не підлягає розголошенню на підставі нормативного акта іншої державної установи, а та державна установа, яка розглядає запит, не має права вирішувати питання щодо її розсекречення; інформація фінансових установ, підготовлена для контрольно-фінансових відомств.

Закон забороняє державну цензуру: «*забороняються створення будь-яких органів державної влади, установ, введення посад, на які покладаються повноваження щодо здійснення контролю за змістом інформації, що поширюється засобами масової інформації*» (стаття 45-1). Водночас інформацією та інформаційною свободою не можна зловживати: «*інформація не може бути використана для закликів до повалення конституційного ладу, порушення територіальної цілісності України, пропаганди війни, насильства, жорстокості, розпалювання расової, національної, релігійної ворожнечі, вчинення терористичних актів, посягання на права і свободи людини*» (стаття 46).

Закон гарантує рівність усіх учасників інформаційних відносин (громадяни, юридичні особи та держава), розглядає інформацію з погляду права власності. Крім того, закон визначає низку термінів, важливих у процесі інформаційних відносин: це поняття «інформація як товар», «інформаційна продукція», «інформаційна послуга».

Важливим моментом є встановлення відповідальності за розголошення інформації, яка розголошенню не підлягає (стаття 47). Однак у цій статті є важливий елемент, пов'язаний з формуванням громадянського суспільства: громадянин звільняється від відповідальності за розголошення ІЗОД, якщо він у суді зміг довести «суспільну важливість» такої інформації, тобто потреба суспільства знати цю конкретну інформацію визнана важливішою за можливі негативні наслідки її розголошення. На цьому пункті, до речі, ґрунтується легітимність роботи журналістів.

Закон «Про інформацію» 1992 р. (з доповненнями до 2005 р.) безумовно є прогресивним у плані забезпечення демократичних прав та свобод громадян, вільного обігу інформації, але до деяких його положень фахівці висловлюють зауваження. Наприклад, акцентують на відсутності у Законі концепції офіційної інформації, неконкретність положень про секретність, розмитість сфери прав та обов'язків громадян і обов'язків державних органів. До осіб, що мають право доступу до інформації, пропонують включити також жителів держави, які ще не отримали громадянства. Концепція «авторського контролю» за доступом до конфіденційної інформації вважається застарілою, принаймні, вона зникає з європейського права (йдеться про те, що власник конфіденційної інформації самостійно визначає режим доступу до неї, спосіб отримання, коло осіб, що мають доступ, захист і так далі). Також звертається увага на брак критеріїв гіпотетичної шкоди від розголошення інформації та суспільного інтересу до цієї інформації. Дослідники пропонують створити доступний реєстр усіх документів, на які поширюються положення Закону для того, щоб допомогти громадянам у пошуку потрібної їм інформації. Нарешті, найбільшій критиці підлягає положення 29-ї статті про переважне право доступу до інформації службовців під

час виконання службових обов'язків. На думку фахівців, це положення суперечить принципові рівності усіх осіб у доступі до інформації. Отже, Закон «Про інформацію» потребує істотних змін та доповнень, враховуючи демократичний поступ нашої держави та вимоги часу. Україна − суверенна держава. Тому на порядку денному – проблема захисту її інформаційного простору від негативних впливів. Це не означає запровадження цензури, мова йде лише про те, що держава, яка існує на кошти платників податків, повинна забезпечити для них належні умови для інтелектуального, фізичного, духовного розвитку.

Про захист інформаційного простору держави йдеться у Законі України «Про національну безпеку України від 21.06.2018 року (Відомості Верховної Ради (ВВР), 2018, № 31, ст.241) . У першій статті 6 пункту, загрози національній безпеці України це явища, тенденції і чинники, що унеможливлюють чи ускладнюють або можуть унеможливити чи ускладнити реалізацію національних інтересів та збереження національних цінностей України;

Державні стандарти та нормативні документи, що стосуються технічного захисту інформації (ТЗІ).

До них належать такі документи:

«Державний стандарт України. Захист інформації. Технічний захист інформації. Основні положення» (ДСТУ 3396.0-96); «Державний стандарт України. Захист інформації. Технічний захист інформації. Порядок проведення робіт» (ДСТУ 3396.1-96); «Державний стандарт України. Захист інформації. Технічний захист інформації. Терміни та визначення» (ДСТУ 3396.2-96).

Ці стандарти установлюють об'єкт, мету, основні організаційнотехнічні положення забезпечення технічного захисту інформації (ТЗІ), неправомірний доступ до якої може завдати шкоди громадянам, організаціям (юридичним особам) та державі, а також категорії нормативних документів системи ТЗІ. Вимоги стандарту обов'язкові для підприємств та установ усіх форм власності і підпорядкування, громадян – суб'єктів підприємницької діяльності, органів державної влади, органів місцевого самоврядування, військових частин усіх військових формувань, представництв України за кордоном, які володіють та користуються інформацією, що підлягає технічному захисту.

Об'єктом технічного захисту є інформація, що становить державну або іншу передбачену законодавством України таємницю, конфіденційна інформація, що є державною власністю чи передана державі у володіння, користування, розпорядження. Об'єкт, мету і завдання ТЗІ визначають і встановлюють особи, які володіють, користуються, розпоряджаються ІЗОД у межах прав і повноважень, наданих законами України, підзаконними актами та нормативними документами системи ТЗІ. Цими стандартами визначаються носії ІЗОД, середовище поширення, мета ТЗІ (див. далі), джерела загроз.

До джерел загроз належать діяльність іноземних розвідок, а також навмисні або ненавмисні дії юридичних і фізичних осіб. Далі йдеться про канали поширення загроз, розроблення і реалізацію системи захисту інформації, контроль за ТЗІ та функції нормативних документів у сфері ТЗІ. Такими функціями, зокрема, є: проведення єдиної технічної політики; створення і розвиток єдиної термінологічної системи; функціонування багаторівневих систем захисту інформації на основі взаємоузгоджених положень, правил, методик, вимог та норм; функціонування систем сертифікації, ліцензування й атестації згідно з вимогами безпеки інформації; розвиток сфери послуг у галузі ТЗІ; установлення порядку розроблення, виготовлення, експлуатації засобів забезпечення ТЗІ та спеціальної контрольно-вимірювальної апаратури; організація проектування будівельних робіт у частині забезпечення ТЗІ; підготовка та перепідготовка кадрів у системі ТЗІ. Нормативні документи системи ТЗІ поділяють на: нормативні документи із стандартизації у галузі ТЗІ; державні стандарти та прирівняні до них нормативні документи; нормативні акти міжвідомчого значення, що реєструються у Міністерстві юстиції України; нормативні документи міжвідомчого значення технічного характеру, що реєструються уповноваженим Кабінетом Міністрів України органом; нормативні документи відомчого значення органів державної влади та органів місцевого самоврядування.

ЛЕКЦІЯ 6
РОЗРОБКА ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Політика інформаційної безпеки – набір вимог, правил, обмежень, рекомендацій, які регламентують порядок інформаційної діяльності в організації і спрямовані на досягнення і підтримку стану інформаційної безпеки організації. Політика безпеки інформації є частиною загальної політики безпеки організації і повинна успадковувати основні її принципи. Головною причиною запровадження політики безпеки зазвичай є вимога наявності такого документа від регулятора – організації, що визначає правила роботи підприємств даної галузі. У цьому випадку відсутність політики може спричинити репресивні дії щодо підприємства або навіть повне припинення його діяльності.

6.1. Організація внутрішньооб'єктного режиму і охорони приміщень

Організація внутрішньооб'єктного режиму, охорони приміщень і територій є частиною загальної роботи підприємства щодо забезпечення збереження майна та безперервності поточної діяльності. Основним завданням забезпечення внутрішньооб'єктного режиму є недопущення сторонніх осіб до інформаційних активів і запобігання загроз інформаційній безпеці.

Основою внутрішньооб'єктного режиму є пропускний режим, в рамках якого, як правило, встановлюються:

- документи, що дають право проходу на територію підприємства – як пропуску і карти доступу, видані самим підприємством, так і документи, видані сторонніми організаціями (наприклад, службові посвідчення посадових осіб деяких органів державної влади);
- категорії перепусток, які використовуються на підприємстві, відповідно до яких обмежується термін дії перепусток, час можливого проходу на територію підприємства (дні тижня, години доби) і деякі інші параметри;
- порядок видачі, обміну, продовження і вилучення перепусток, а також порядок дій співробітників і посадових осіб при втраті пропуску;
- порядок організації пропуску осіб, автотранспорту і проносу (провозу) майна: розміщення і порядок роботи контрольно-пропускних пунктів, можливість пропуску тих чи інших осіб, засобів автотранспорту і вантажів через ті чи інші КПП та ін .;
- основні положення документообігу, використовуваного при проході відвідувачів на територію підприємства - вимоги до ведення журналу реєстрації проходу відвідувачів, вимоги до документів, на основі яких видаються разові перепустки, порядок видачі разових перепусток і т.п.;
- порядок огляду транспортних засобів, що допускаються на територію підприємства.

Крім того, в рамках організації внутрішньооб'єктного режиму може бути передбачено поділ приміщень і територій на окремі зони з обмеженням доступу (в тому числі на основі поділу приміщень і територій на різні категорії), а також розмежування доступу окремих співробітників (категорій персоналу) і відвідувачів в різні зони; також можуть бути визначені основні вимоги до технічних засобів розмежування доступу і організації їх використання.

З технічної точки зору заходи щодо забезпечення пропускного та внутрішньооб'єктного режимів можуть бути реалізовані тими ж засобами, які використовуються для забезпечення безпеки в інших сферах, крім інформаційної (захист майна та персоналу, забезпечення безперервності виробничого процесу), – засобами контролю доступу, відеоспостереження, сигналізації і фізичного захисту.

В основі засобів контролю доступу лежать механізми розпізнавання особистості і порівняння з встановленими параметрами. Політика підприємства може встановлювати як спрощені підходи до розпізнання, коли охоронці підприємства перевіряють документи (підтвердження особи, підтвердження можливості проходу на територію в даний час через даний КПП), так і використання автоматизованих засобів, коли впізнання відвідувача і підтвердження (або заборона) можливості проходу на територію (виходу з території, з будівлі) проводиться автоматизованою системою контролю доступу на основі наявних у

відвідувача машинозчитних засобів персональної ідентифікації (пластикових карт, жетонів тощо) або на основі зчитування і аналізу його фізичних особливостей (геометрії особи, відбитків пальців, малюнка райдужної оболонки ока, голосу і т.п.).

При виборі конкретних засобів біометричної ідентифікації фахівцям і керівникам підприємства слід пам'ятати, що різні технології мають різну ступінь надійності, а також можуть бути більш-менш зручними в повсякденному використанні великою кількістю людей. Так, наприклад, вважається, що одна з передових технологій біометричної ідентифікації – ідентифікація по кровоносним судинам пальця (коли інфрачервоний промінь просвічує палець і створює тривимірне зображення унікальної для кожної людини структури кровоносних судин).

6.2. Фізичний захист

Фізичний захист об'єктів, як правило, передбачає посилення конструкцій огорож, елементів будівель, споруд і окремих приміщень. До таких засобів відносяться захист віконних прорізів металевими гратами і віконницями, спеціальне скління вікон, використання броньованих дверей, запірних пристроїв, сейфів для зберігання коштів обчислювальної техніки і носіїв інформації. Відповідно до особливостей використовуваних приміщень і територій політика безпеки підприємства також може передбачати розташування місць зберігання і обробки інформації (наприклад, архівів або серверних кімнат) в приміщеннях, найменш доступних для проникнення, найбільш віддалених від місць зберігання вибухонебезпечних і легкозаймистих речовин, найменш схильних до затоплення (для об'єктів розташованих в долинах річок і на узбережжі), найбільш захищених від ударів блискавки і т.п.

З фізичним захистом безпосередньо пов'язано використання засобів сигналізації та відеоспостереження. Залежно від характеру об'єкту, що охороняється (територія, будівля, прохід, приміщення, окремий шафа або сейф) в засобах сигналізації можуть застосовуватися датчики, що працюють на різних фізичних принципах (фотоелектричні датчики, датчики обсягу, акустичні датчики і т.п.), що мають різні настройки і використовують різні канали зв'язку.

На відміну від засобів сигналізації засоби відеоспостереження дозволяють не тільки встановити факт порушення, а й в деталях відстежувати його, контролювати ситуацію, а також вести відеозапис, який можна буде використовувати для прийняття подальших заходів (пошук порушників, кримінальне переслідування і т.п.).

Окремим завданням є забезпечення інформаційної безпеки при процесі транспортування носіїв інформації та інших об'єктів, що вимагає використання як спеціальних організаційних прийомів, так і спеціальних технічних засобів. До організаційних методів відноситься залучення спеціально підготовлених кур'єрів, а також поділ носіїв інформації (об'єктів) на частини і їх роздільне транспортування з метою мінімізації можливостей витоку інформації. До технічних засобів, що застосовуються при транспортуванні об'єктів, відносяться захищені контейнери, спеціальні пакувальні матеріали, а також тонкоплівкові матеріали і голографічні мітки, що дозволяють ідентифікувати справжність об'єктів і контролювати несанкціонований доступ до них.

6.3. Організація режиму секретності в установах і на підприємствах

Організація режиму секретності в установах і на підприємствах ґрунтується на вимогах законодавства, що стосується питань державної таємниці, і відповідних підзаконних актів. Відповідно до діючих норм до державної таємниці може бути віднесена інформація, що стосується обороноздатності країни, її економіки, міжнародних відносин, державної безпеки та охорони правопорядку (в тому числі відомості про методи та засоби захисту секретної інформації, а також про державні програми і заходи в області захисту державної таємниці); в законодавстві також спеціально уточнюються області діяльності, інформація про які не може бути віднесена до державної таємниці. Віднесення конкретної інформації до державної таємниці здійснюється рішенням спеціально призначених посадових осіб, а загальний Перелік відомостей, віднесених до державної таємниці, затверджується

Президентом і підлягає обов'язковому опублікуванню. Для відомостей, що становлять державну таємницю, встановлюються три ступені секретності: "особливої важливості", "цілком таємно" та "таємно", а носії таких відомостей (документи) повинні мати відповідні реквізити.

Основним елементом організації режиму секретності є допуск посадових осіб і громадян до відомостей, що становлять державну таємницю. Він передбачає виконання керівництвом підприємства і підрозділів із захисту державної таємниці (у взаємодії з уповноваженими правоохоронними органами) наступних основних заходів.

- Ознайомлення посадових осіб і громадян з нормами законодавства, які передбачають відповідальність за порушення вимог.
- Отримання згоди на тимчасові обмеження їх прав відповідно до законодавства.
- Отримання згоди на проведення щодо них перевірочних заходів.
- Прийняття рішення про допуск до відомостей, що становлять державну таємницю.
- Висновок щодо осіб, які отримали допуск, що відображає взаємні зобов'язання таких осіб і адміністрації підприємства (в т.ч. зобов'язання таких осіб перед державою з нерозповсюдження довірених їм відомостей, що становлять державну таємницю).

Крім віднесення відомостей до державної таємниці та допуску посадових осіб і громадян до засекречених відомостей, важливим елементом системи забезпечення режиму секретності є організація інформаційного обміну між підприємствами при спільному виконанні робіт. Зокрема, передача засекречених відомостей від одного підприємства до іншого повинна проводитися з дозволу уповноваженого державного органу, договір на виконання робіт повинен передбачати зобов'язання сторін щодо забезпечення схоронності відомостей, а замовник робіт повинен контролювати виконання нормативних вимог контрагентами за такими договорами (наявність ліцензій, оформлення допуску співробітників і т.п.) і вживати необхідних заходів у разі виявлення порушень. Також важливим елементом забезпечення режиму секретності є організація передачі відомостей, що становлять державну таємницю, іншим державам (в тому числі ознайомлення з такими відомостями і надання можливості доступу до них).

Політика опублікування матеріалів у відкритих джерелах (таких як газети, журнали, виставки, мережа Інтернет, радіо- і телепередачі, конференції, музейні експозиції і т.п.) повинна забезпечувати запобігання випадкових і організованих витоків конфіденційної інформації при взаємодії підприємства із засобами масової інформації, громадськими і державними органами, науковими, академічним і бізнес-спільнотою. Для того щоб уникнути шкоди інтересам підприємства, така політика повинна містити основні правила і процедури підготовки інформаційних матеріалів до відкритої публікації. Зокрема, в політиці безпеки слід передбачати створення спеціальної експертної ради, відповідальної за розгляд всіх інформаційних матеріалів, які передбачається опублікувати у відкритих джерелах (політика безпеки повинна містити конкретні обмеження на опублікування інформаційних матеріалів без їх розгляду експертною радою). Основним завданням такої ради є підготовка висновків про можливість або неможливість опублікування певних інформаційних матеріалів, а також підготовка конкретних пропозицій щодо вилучення певних відомостей з матеріалів, підготовлених до публікації. При відсутності єдиної думки у членів експертної комісії рішення про можливість опублікування може бути прийнято керівником підприємства з урахуванням рекомендацій експертів. Для ефективного вирішення завдань члени експертної ради повинні детально знати всі існуючі обмеження (зокрема, встановлені законодавством) і володіти ситуацією в тій сфері, в якій функціонує підприємство. При цьому, як правило, сам автор підготовлених до публікації матеріалів не може входити до експертної ради, а редактор або керівник, який відповідає за підготовку матеріалів, не може бути головою експертної ради.

Політика управління паролями (або, в більш загальному вигляді, політика ідентифікації і аутентифікації) може визначати періодичність заміни паролів, дії, які необхідно здійснити при компрометації паролів, основні вимоги до їх якості, процедур їх генерації, розподілу основних обов'язків, пов'язаних з генерацією паролів, їх зміною і доведенням до користувачів, а також основні заходи відповідальності за порушення встановлених правил і

вимог. Політика на цьому рівні також може встановлювати заборону зберігання записаних паролів, заборона повідомляти будь-кому свій пароль (в тому числі керівникам і адміністраторам інформаційних систем) та інші аналогічні обмеження.

Політика встановлення та оновлення версій програмного забезпечення може включати в себе деякі обмеження на самостійне придбання і установку програмного забезпечення окремими підрозділами та користувачами, а також певні вимоги до кваліфікації фахівців, які здійснюють їх установку, настройку і підтримку.

Політика придбання інформаційних систем і їх елементів (програмних і апаратних засобів) може включати в себе вимоги до ліцензування та сертифікації використовуваного програмного забезпечення і устаткування, а також певні вимоги до фірм, які здійснюють їх поставку та впровадження.

Політика доступу сторонніх користувачів (організацій) в інформаційні системи підприємства може містити перелік основних ситуацій, коли такий доступ можливий, а також основні критерії і процедури, відповідно до яких здійснюється доступ. Також політика може передбачати розподіл відповідальності співробітників самого підприємства за дії зовнішніх користувачів, які отримують такий доступ.

Політика щодо розробки ПЗ може містити вимоги як до питань безпеки і надійності програмних засобів, самостійно розроблених підприємством, так і щодо передачі розробки програмних засобів (модулів інформаційних систем, окремих програмних бібліотек і т.п.) стороннім спеціалізованим організаціям (т.зв. "аутсорсинг"), а також щодо придбання та використання тиражованих програмних бібліотек (модулів), які розповсюджуються компаніями-виробниками. Зокрема, політика може містити вимоги до тестування самостійно розробленого ПЗ, аналізу його вихідних кодів, описувати основні критерії надійності і т.п.

Політики використання окремих універсальних інформаційних технологій в масштабі всього підприємства можуть включати в себе:

- політику використання електронної пошти (e-mail);
- політику використання засобів шифрування даних;
- політику захисту від комп'ютерних вірусів і інших шкідливих програм;
- політику використання модемів і інших аналогічних комунікаційних засобів;
- політику використання інфраструктури публічних ключів;
- політику використання технології віртуальних приватних мереж (Virtual Private Network - VPN).

Політика використання електронної пошти може включати в себе як загальні обмеження на її використання певними категоріями співробітників, так і вимоги до управління доступом і збереження конфіденційності повідомлень, а також до адміністрування поштової системи і зберігання електронних повідомлень. Крім того, політика може передбачати:

- заборону на використання електронної пошти в особистих цілях;
- спеціальні вимоги до відправлення та одержання приєднаних файлів, які потенційно можуть містити шкідливі програми;
- заборону на використання електронної пошти тимчасовими співробітниками;
- вимоги шифрування переданих повідомлень;
- спостереження за всіма переданими і одержуваними повідомленнями;
- обмеження на передачу конфіденційної інформації за допомогою електронної пошти та інші положення.

Політика використання комунікаційних засобів може визначати межі використання технологій, що дозволяють підключити комп'ютери та інформаційні системи підприємства до інформаційних систем і комунікаційних каналів за його межами.

Зокрема, така політика може вводити певні обмеження на використання модемів для телефонних ліній, пристроїв, що використовують сучасні бездротові технології, такі, як GSM (GPRS), Wi-Fi, передача даних в мережах стандарту CDMA і т.п.

Політика використання мобільних апаратних засобів може ставитися до різних пристроїв, таким як мобільні ПК, КПК (PDA), переносні пристрої зберігання інформації

(дискети, USB-flash, карти пам'яті, що підключаються жорсткі диски і т.п.). Вона може відображати загальне ставлення підприємства до використання співробітниками таких пристроїв, визначати вимоги і встановлювати конкретні області, в яких їх використання допустимо. Також можуть встановлюватися додаткові загальні вимоги до стаціонарного обладнання з метою обмеження підключення до них мобільних комп'ютерів і засобів передачі даних.

6.4. Інформаційна безпека: робота з персоналом

В лекції описується робота департаменту інформаційної безпеки як основної структурної одиниці, що відповідає за комплексний захист інформації на підприємстві. Розкривається внутрішня структура департаменту, основні завдання та напрями його діяльності, методи роботи. Також розкриваються основні аспекти роботи з персоналом підприємства, спрямованої на захист інформаційних активів (як в частині підбору і розстановки співробітників, пов'язаних з обробкою інформації, так і в частині поточної роботи з персоналом).

Ключові слова: управління інформаційної безпекою, CISO, джерело загрози, інформаційні системи, державна таємниця, державна стратегія, аналіз, контроль поведінки, розподіл функцій, доступ, зловмисник.

6.4.1. Департамент інформаційної безпеки

Департамент інформаційної безпеки (далі – департамент) підприємства є самостійним структурним підрозділом підприємства, безпосередньо виконує ключові функції захисту інформаційних ресурсів.

Його основними завданнями, як правило, є:

- організація та координація робіт із забезпечення комплексного захисту інформації на підприємстві;
- контроль за виконанням встановлених вимог та оцінка ефективності роботи підрозділів і персоналу підприємства щодо забезпечення інформаційної безпеки;
- виконання окремих адміністративних і технічних функцій щодо забезпечення інформаційної безпеки;
- формування, підтримка та документальне забезпечення політики інформаційної безпеки на всіх рівнях;
- впровадження різних засобів захисту інформації;
- адміністрування окремих інформаційних систем.

Склад завдань департаменту і його внутрішня організаційна структура в кожному конкретному випадку визначається такими особливостями функціонування підприємства, як:

- значимість інформаційних ресурсів у роботі підприємства і характер існуючих загроз;
- ставлення керівництва і власників підприємства до питань інформаційної безпеки та їх управлінська кваліфікація;
- функціональність і характер використовуваних інформаційних систем, їх роль у бізнес-процесах;
- організація роботи та структура IT-служби;
- фінансовий стан підприємства.

Таким чином, рішення про склад і структуру департаменту в кожному випадку має бути індивідуальним і враховує всі основні умови.

Функції, пов'язані **з формуванням, підтримкою і документальним забезпеченням політики інформаційної безпеки підприємства,** можуть включати в себе:

- консультування керівників і власників підприємства з питань розробки та вдосконалення політики інформаційної безпеки;
- самостійну розробку політики безпеки, її узгодження і подання її керівництву підприємства для затвердження, а також внесення необхідних змін у міру зміни умов роботи

підприємства;

- самостійну розробку політик безпеки, що стосуються окремих питань захисту інформації (правил застосування телекомунікаційних технологій, вимог, обов'язкових для всіх персональних комп'ютерів, що використовуються на підприємстві, тощо);
- формування вимог і регламенту процедур перегляду політики безпеки, окремих правил, типових форм та інших документів;
- аналіз окремих договорів і угод зі сторонніми організаціями (постачальниками, покупцями, партнерами по проведенню науково-дослідних робіт тощо) на предмет відповідності вимогам політики інформаційної безпеки;
- аналіз та узагальнення передового досвіду та сучасних теорій у сфері управління інформаційною безпекою з метою їх практичного застосування на підприємстві;
- залучення сторонніх фахівців, дослідників, консультантів (консалтингових компаній) для розробки та вдосконалення політики безпеки підприємства та впровадження розвинених методів управління в цій сфері;
- управління навчанням персоналу компанії (контроль за повнотою та правильністю матеріалів навчальних програм, пов'язаних з інформаційною безпекою, забезпечення своєчасності проходження навчання тощо);
- консультування фахівців та керівників підрозділів підприємства з питань відповідності розроблюваних внутрішніх документів окремих підрозділів вимогам політики безпеки підприємства;
- контроль відповідності внутрішніх організаційних документів підприємства (правил внутрішнього розпорядку, посадових інструкцій, інструкцій з використання інформаційних систем, типових форм договорів тощо) вимогам політики інформаційної безпеки, а також узгодження таких документів при їх затвердженні.

Функції, пов'язані з **впровадженням засобів захисту інформації,** можуть включати в себе:

- аналіз сучасних програмних і апаратних засобів захисту інформації та пов'язаних з ними методик захисту, а також ринку доступних засобів захисту інформації, що застосовуються для різних цілей, і підготовка обгрунтованих пропозицій щодо придбання певних продуктів у певних постачальників;
- аналіз закуповуваних інформаційних систем (операційних систем, прикладних програм, телекомунікаційного устаткування, обчислювальної техніки тощо) на предмет їхньої потенційної надійності і наявності вразливостей;
- залучення сторонніх експертів і консультантів для аналізу закуповуваних і використовуваних засобів захисту інформації з точки зору їх надійності, а також з точки зору доцільності їх застосування (впровадження);
- формулювання вимог (пов'язаних із забезпеченням інформаційної безпеки) до самостійно розроблюваних програмних продуктів або програмного забезпечення, що створюється на замовлення сторонніх розробників;
- участь у проектуванні нових інформаційних систем, а також тестуванні знову розроблених і впроваджуваних програмних продуктів;
- розробку техніко-економічного обґрунтування для проектів впровадження засобів захисту інформації, а також залучення для цих цілей сторонніх аналітиків і консультантів, що спеціалізуються на питаннях аналізу засобів захисту інформації;
- підготовку обгрунтованих рішень про вибір між самостійною розробкою засобів захисту інформації (наприклад, програмних модулів, що здійснюють шифрування даних) і передачею їх розробки стороннім компаніям.

Функції, пов'язані з адмініструванням **інформаційних систем і систем захисту інформації** можуть включати в себе:

- виконання деяких функцій з адміністрування окремих інформаційних систем (баз даних, систем колективної роботи з документами, поштових систем тощо), а також адміністрування та конфігурування систем захисту інформації (міжмережевих екранів, систем виявлення вторгнень тощо);

- визначення необхідних типових налаштувань і конфігурацій робочих станцій (персональних комп'ютерів), що мають відношення до інформаційних систем підприємства (зокрема, підключених до його локальної мережі);
- залучення сторонніх організацій для здійснення поточного адміністрування інформаційних систем і систем захисту інформації, а також для консультаційної та технічної підтримки при виникненні інцидентів, пов'язаних з інформаційною безпекою (зокрема, при здійсненні нападів на інформаційні системи підприємства);
- установку (в тому числі і спільно з фахівцями IT-підрозділу) програмних і апаратних засобів захисту інформації на робочі місця користувачів і в інші елементи інформаційних систем;
- консультування користувачів з питань, пов'язаних з інформаційною безпекою, і оперативне вирішення проблем;
- реагування на різні інциденти, пов'язані з порушенням інформаційної безпеки;
- прийняття активних зустрічних заходів при виявленні вторгнень в інформаційну систему (інформування правоохоронних органів, самостійний пошук нападників тощо);
- генерування паролів користувачів інформаційних систем та забезпечення їх збереження;
- участь у відновленні працездатності інформаційних систем після збоїв та порушень у роботі.

Функції, пов'язані з **контролем виконання вимог політики інформаційної безпеки та проведення аудитів** можуть включати в себе:

- збір та аналіз відомостей про порушення різних вимог політики безпеки, що надходять з різних джерел (у тому числі і від адміністраторів інформаційних систем) і визначення пріоритетних напрямів контрольної роботи;
- перевірку організаційної документації окремих підрозділів підприємства на предмет відповідності вимогам політики інформаційної безпеки (у тому числі і своєчасності внесення всіх необхідних змін до чинних внутрішніх документів організації);
- перевірку стану (правильності ведення) поточної господарської та кадрової документації окремих підрозділів підприємства, пов'язаної із забезпеченням інформаційної безпеки (правильності і своєчасності заповнення журналів, своєчасність оформлення зобов'язань про нерозголошення відомостей співробітниками тощо);
- проведення комплексних аудитів інформаційної безпеки на підприємстві;
- організацію контрольних перевірок захищеності окремих елементів інформаційних систем (серверів, сегментів мережі тощо);
- залучення сторонніх організацій для проведення аудитів інформаційної безпеки на підприємстві, перевірок надійності інформаційних систем.

Крім перерахованих функцій, безпосередньо пов'язаних із захистом інформаційних ресурсів, також велике значення має виконання функцій, пов'язаних з охороною майна підприємства і вирішенням завдань, які пов'язані з забезпеченням безпеки підприємства у більш широкому сенсі. Зокрема, для забезпечення інформаційної безпеки має значення виконання таких функцій як:

- охорона території та майна підприємства, а також охорона персоналу;
- забезпечення дотримання пропускного режиму;
- спостереження за територією і приміщеннями (у тому числі за допомогою відеокамер);
- контроль за ввезенням на територію підприємства та вивезенням готової продукції, матеріалів, документів та іншого майна;
- організацію внутрішніх службових перевірок та розслідувань, а також взаємодію з правоохоронними органами;
- контроль за дотриманням тимчасового режиму роботи, а також за дотриманням правил внутрішнього розпорядку.

6.4.2. Організаційна структура та персонал департаменту інформаційної безпеки

На практиці департамент є підрозділом, або безпосередньо підпорядковується першій особі підприємства, або входить, як структурна одиниця, в службу безпеки підприємства. Співробітники департаменту знаходяться в адміністративному та функціональному підпорядкуванні у керівника департаменту, який несе відповідальність за забезпечення інформаційної безпеки на підприємстві. Висновок департаментів інформаційної безпеки зі структури IT-служб на підприємствах є однією з важливих сучасних тенденцій в управлінні бізнесом, інформаційними технологіями та інформаційною безпекою, тому, на думку деяких фахівців, у цих підрозділів є деякі частково взаємосуперечні інтереси і тому деякі завдання не можуть бути ефективно вирішені в рамках одного структурного підрозділу.

У складі департаменту для підвищення ефективності роботи можуть бути виділені самостійні групи (відділи), що спеціалізуються на виконанні певних функцій (рисунок 5.1):

- відділ (група, бюро) нормативної (організаційної) документації;
- відділ (група, бюро) адміністрування інформаційних систем;
- відділ (група, бюро) аудиту інформаційної безпеки;
- відділ (група, бюро) впровадження інформаційних систем і систем захисту інформації.

Рисунок 5.1 – Приклад організаційної схеми Департаменту інформаційної безпеки підприємства

Відділ нормативної документації вирішує завдання, пов'язані з формуванням, підтримкою і документальним забезпеченням політики інформаційної безпеки підприємства, і повинен, головним чином, включати в себе фахівців з менеджменту та бізнес-аналізу, що пройшли додаткову підготовку у сфері управління інформаційною безпекою. Також до складу такого відділу можуть входити юристи. Аналогічний кадровий склад може бути і у **Відділу внутрішнього аудиту інформаційної безпеки.** При цьому до кваліфікації співробітників Відділу нормативної документації, як правило, повинні пред'являтися набагато більш високі професійні вимоги.

Відділ адміністрування інформаційних систем, а також **Відділ впровадження інформаційних систем і захисту систем інформації,** як правило, повинні включати в себе фахівців з інформаційних технологій та засобів захисту інформації, що мають значний досвід впровадження та експлуатації корпоративних інформаційних систем.

6.4.3. Робота з персоналом підприємства

Практична реалізація всіх положень сформованої політики інформаційної безпеки потребують від підприємства тривалих практичних зусиль. Одним з основних і найбільш складних напрямків роботи є робота з персоналом, цілі якої:

- відбір і попередня перевірка персоналу, прийнятого на роботу (на службу);
- навчання співробітників;
- досягнення взаєморозуміння керівників і співробітників в питаннях забезпечення інформаційної безпеки;
- психологічна підготовка з метою протистояння методам т.зв. "соціальної інженерії".

Основною причиною, що визначає значущість людського фактора в загальній системі захисту інформації, є те, що при всій розвиненості сучасних засобів автоматизації інформаційні системи як і раніше представляють собою людино-машинні комплекси і їх

функціонування багато в чому залежить від роботи окремих людей. Саме з цієї причини неадекватне поводження службовців підприємства з компонентами інформаційної системи може завдати серйозної шкоди інформаційній безпеці навіть при наявності детально опрацьованих політик безпеки і високоефективних програмних і апаратних засобів захисту інформації.

Початкова стадія роботи - підбір і розстановка кадрів - може мати кілька аспектів. У першу чергу, основним критерієм для призначення на певні посади, пов'язані з роботою з відомостями, які становлять державну таємницю, є отримання відповідної форми допуску. Відповідно до вимог чинних нормативно-правових актів Перелік посад, при призначенні на які необхідно оформляти спеціальний допуск, встановлюється керівником підприємства і може періодично переглядатися. Ця вимога пов'язана, з одного боку, з тим, що керівник підприємства несе відповідальність за забезпечення режиму секретності, а з іншого – з тим, що для виконання функціональних обов'язків співробітникам підприємства необхідно працювати з певними відомостями і, відповідно, мати певний рівень допуску.

Також при підборі і розстановці кадрів можуть застосовуватися і менш формалізовані методи. Це можуть бути різні методики психологічної оцінки, що включають в себе:

- аналіз мотиваційних аспектів особистості;
- оцінку психологічної стійкості особистості;
- оцінку рівня пізнавальних здібностей особистості (успішність придбання нових знань і навичок і здатність до їх практичного застосування);
- оцінку активності особистості в досягненні поставленої мети, уміння об'єктивно оцінювати ситуацію і людей, вміння виробляти оптимальну стратегію поведінки.

Такого роду аналіз може бути необхідний як щодо фахівців і керівників, які працюють з інформацією, що підлягає захисту, у зв'язку з виконанням своїх посадових обов'язків за основним профілем роботи підприємства, так і фахівців і керівників, чиїм основним завданням є забезпечення інформаційної безпеки підприємства (аудиторів ІБ, проектувальників і адміністраторів інформаційних систем і систем захисту інформації тощо).

Крім ретельного підбору, однією з важливих основ роботи з персоналом є його навчання способам забезпечення інформаційної безпеки і безпечній роботі з інформаційними системами. Навчання і наступний контроль отриманих (наявних) знань може бути як первинним, так і повторним. У загальному випадку співробітник підприємства не може бути допущений до виконання своїх посадових обов'язків і роботі з інформаційними системами доти, поки він не пройде навчання з питань інформаційної безпеки і не буде:

- детально ознайомлений з усіма діючими на підприємстві вимогами і загальними правилами;
- повністю навчений методам і прийомам забезпечення інформаційної безпеки, необхідним для виконання його посадових обов'язків;
- ознайомлений з усіма можливими заходами відповідальності (дисциплінарної, адміністративної, кримінальної), які можуть бути до нього застосовані в разі порушення вимог, а також у випадку нанесення шкоди за його вини.

У завершенні всієї попередньої роботи співробітник повинен дати всі необхідні зобов'язання про нерозголошення конфіденційних відомостей, а також письмово засвідчити, що він повністю ознайомлений з основними положеннями політики безпеки. У процесі роботи підприємство також може проводити періодичний контроль знань і навичок, пов'язаний із забезпеченням інформаційної безпеки з тією метою, щоб засвідчити компетентність працівників у цій сфері. Також одним з інструментів навчання може бути періодичне ознайомлення персоналу з реальними прикладами інцидентів, що недавно відбулися, пов'язаних з інформаційною безпекою. Крім того, додаткове навчання персоналу підприємства може проводитись у випадках:

- впровадження нових автоматизованих інформаційних систем;
- зміни бізнес-процесів підприємства;
- зміни вимог політик безпеки (наприклад, у зв'язку зі зміною вимог законодавства).

Необхідність додаткового навчання при впровадженні нових інформаційних систем і, зокрема, інтегрованих систем управління підприємством, як правило, може бути обумовлене появою нових функціональних можливостей програмного забезпечення і зміною процедур обробки інформації. Також доступ до інтегрованих інформаційних систем потенційно може дати доступ до раніше недоступної інформації та надати раніше відсутні можливості впливати на різні інформаційні потоки. У зв'язку з цим може виникнути потреба в тому, щоб співробітники мали додаткові зобов'язання про дотримання заходів інформаційної безпеки. Аналогічні організаційні заходи щодо забезпечення захисту інформації можуть бути необхідні і під час зміни бізнес-процесів підприємства, коли змінюється його структура, розподіл функцій між підрозділами і обов'язків співробітників, і відповідно, вносяться зміни в організаційні схеми, штатні розписи і посадові інструкції персоналу. Зміни вимог політики безпеки можуть бути пов'язані з появою нових загроз, зміною законодавчих вимог, розширенням ринків, зміною ставлення керівництва і власників підприємства до питань інформаційної безпеки та іншими факторами, - всі ці уточнення і зміни також повинні своєчасно і в повному обсязі доводитися до персоналу.

У процесі навчання певну значимість може мати роз'яснення раціональних причин, з яких підприємство застосовує саме таку політику безпеки. Це може служити як для кращого розуміння та засвоєння положень політики безпеки, так і для певної розрядки психологічної напруженості.

Окремим напрямом навчання та підвищення кваліфікації може бути розвиток у персоналу компанії навичок протидії методам т.зв. соціальної інженерії. Використання для незаконного проникнення в інформаційні системи методів соціальної інженерії пов'язано з т.зв. "людським фактором", який являє собою сукупність певних психологічних схильностей і особливостей мислення і поведінки, які властиві практично всім людям. До числа таких схильностей і особливостей можна віднести:

- нездатність адекватно оцінити небезпеку в деяких ситуаціях;
- специфічне ставлення до подій, що відбуваються рідко (притуплення уваги);
- зайва довіра і покладання на засоби автоматизації;
- схильність до маніпулювання, що ґрунтується, наприклад, на бажанні допомогти людям (у тому числі і незнайомим) або на зайвій довірі людям, одягненим в спеціальну уніформу, тощо

Саме з використанням деяких психологічних особливостей такого роду здійснюється багато найбільш успішних (для нападників) проникненнь в корпоративні інформаційні системи. Прикладами таких проникнень є ситуації, коли зловмисник:

- здійснює телефонний дзвінок, представляється адміністратором і, пославшись на певні обставини (такі як збій в системі), просить повідомити йому пароль;
- приходить в офіс в спеціальній уніформі (наприклад, у формі співробітника компанії, займається обслуговуванням і ремонтом комп'ютерів) і просить надати йому доступ до інформаційної системи;
- надсилає повідомлення електронною поштою від імені адміністратора інформаційної системи або керівництва підприємства і просить повідомити пароль або вчинити певні дії.

Велику значимість у системі заходів з подолання впливу людського фактора має повсякденна робота з персоналом. Крім навчання персоналу і застосування дисциплінарних заходів впливу, одним з основних завдань такої роботи є постійне нагадування всім співробітникам про необхідність дотримання правил інформаційної безпеки. Конкретні способи, за допомогою яких такі нагадування можуть бути зроблені, будуть залежати від уподобань керівників підприємства, сформованої корпоративної культури, специфіки бізнес-процесів та інших обставин. Характерними способами того, як підприємство може постійно нагадувати своїм співробітникам про необхідність дотримуватися обережності, є:

- розміщення та періодична зміна (оновлення дизайну та змісту) нагадувань про необхідність дотримуватися вимог політики інформаційної безпеки на предметах, які постійно перебувають у полі зору співробітників протягом робочого дня: настінних і

настільних календарях, кавових чашках, обкладинках блокнотів, настільних експонатах, ручках, олівцях та іншому канцелярському приладді;

- періодична розсилка відповідних брошур, бюлетенів і буклетів, а також повідомлень по електронній пошті;
- використання скрінсейверів, що містять відповідні нагадування;
- використання голосової пошти і гучного зв'язку для періодичної передачі повідомлень про необхідність дотримання правил інформаційної безпеки тощо

Таким чином, комплекс всіх організаційних заходів по роботі з персоналом підприємства, що включає в себе систему навчання персоналу, систему притягнення порушників до відповідальності, і постійне підтримання атмосфери відповідального ставлення до питань безпеки, повинен в певній мірі зменшити негативний вплив людського фактора на захищеність інформаційних систем і стан інформаційної безпеки.

6.5. Реагування на надзвичайні ситуації

Реагування на виникаючі надзвичайні ситуації (інциденти), пов'язані з порушенням інформаційної безпеки, є таким же важливим напрямком роботи, як і побудова системи захисту та запобігання порушень. Під інцидентом, як правило, розуміється будь-яке відхилення від нормального процесу використання інформаційних ресурсів і функціонування інформаційних систем, що спричинило збитки для певних інформаційних активів підприємства або безпосередньо створює загрозу завдання такої шкоди. В лекції описуються основні розділи регламентів реагування на інциденти (надзвичайні ситуації) у сфері інформаційної безпеки. Детально розкриваються типові дії, які повинні виконуватися персоналом підприємства при виникненні таких ситуацій.

6.5.1. Вступ

Реагування на виникаючі надзвичайні ситуації (інциденти), пов'язані з порушенням інформаційної безпеки, є таким же важливим напрямком роботи, як і побудова системи захисту та запобігання порушень. Під інцидентом, як правило, розуміється будь-яке відхилення від нормального процесу використання інформаційних ресурсів і функціонування інформаційних систем, що спричинило збитки для певних інформаційних активів підприємства або безпосередньо створює загрозу завдання такої шкоди.

Надзвичайна ситуація (інцидент), пов'язана з порушенням інформаційної безпеки, може бути обумовлена:

- руйнівним впливом на весь майновий комплекс підприємства при виникненні стихійних факторів (повінь, пожежа, землетрус тощо) або цілеспрямованим нападом (підрив, підпал, руйнування будівель та приміщень тощо);
- негативним впливом виключно на інформаційні ресурси підприємства (як правило, здійснюваним віддалено, з використанням телекомунікаційних каналів).

У загальному випадку організаційні процедури (регламенти) реагування на надзвичайні ситуації повинні включати в себе:

- регламенти альтернативних процесів обробки інформації (у тому числі, можливо, і без використання засобів автоматизації) на період виходу з ладу основних інформаційних ресурсів;
- визначення груп персоналу, відповідальних за виконання тих чи інших функцій у разі виникнення надзвичайної ситуації, а також визначення процедур взаємодії між групами і окремих груп з керівництвом підприємства;
- технічну та організаційну документацію, необхідну для відновлення інформаційних систем і даних після надзвичайної ситуації;
- порядок зберігання архівних (резервних) копій даних і програмних додатків обробки даних в місцях, захищених від механічних впливів, крадіжок, повеней, пожеж;
- угоди з постачальниками програмних і апаратних засобів, що входять в інформаційну інфраструктуру підприємства, про термінову поставку компонент, що вийшли з ладу і вимагають заміни в випадку надзвичайної ситуації.

Далі в даному розділі найбільш докладно розглядаються інциденти, причиною яких є навмисно здійснювані напади на інформаційні ресурси підприємства.

Процес реагування на такого роду інциденти включає в себе чотири основні етапи:

- виявлення нападу;
- локалізація нападу;
- ідентифікація нападників;
- оцінка і подальший аналіз процесу нападу і його обставин.

6.5.2. Виявлення атак і розпізнавання вторгнень

Виявлення атак і розпізнавання вторгнень, як правило, є інженерно-технічним завданням, що вирішується за допомогою спеціальних програмних і іноді апаратних засобів. Зокрема, виявлення може здійснюватися на основі аналізу мережевого трафіку і журналів (лог-файлів), в яких фіксуються різні дії. Виявлення може здійснюватися на основі сигнатур – формалізованих наборів ознак певних вірусів, типів атак тощо Також, очевидно, джерелом інформації про порушення є повідомлення користувачів про відхилення в роботі інформаційних систем і поява явних негативних наслідків порушень, що сталися.

Для забезпечення своєчасного виявлення порушень підприємство повинно організувати постійну (при необхідності – цілодобову) роботу фахівців, що відповідають за вирішення інцидентів. Для цього може бути вибраний один з можливих підходів.

Організація власної чергової служби, що складається з компетентних фахівців, що несуть позмінне чергування і оснащені засобами мобільного зв'язку.

Залучення сторонньої організації, що спеціалізується на наданні подібних послуг.

При цьому співробітники підприємства повинні знати номери телефонів та інші способи зв'язку, за допомогою яких вони могли б оперативно повідомляти черговим фахівцям про всі події.

Виявлення порушень може бути здійснено не тільки за явними ознаками, такими як повідомлення користувачів про припинення функціонування окремих елементів інформаційних систем, одночасне використання одного облікового запису на кількох робочих станціях або явне виявлення вірусів в даних, переданих локальною мережею, але й за деякими непрямими ознаками (аномальними явищами), які в окремих випадках можуть свідчити (а можуть і не свідчити) про порушення. Прикладами таких непрямих свідчень можуть бути:

- використання інформаційних систем і певних облікових записів в нехарактерний час (рано вранці, пізно ввечері тощо);
- різке нехарактерне підвищення навантаження на інформаційні системи або їх окремі елементи (сегменти мережі, сховища даних і т.п.);
- зміна характеру поведінки користувачів (наприклад, послідовності певних дій при використанні інформаційної системи)
- та інші.

Для більш ефективного аналізу таких непрямих ознак та інтерпретації різних фактів фахівцям з реагування на інциденти може знадобитися аналіз функціональності інформаційних систем і взаємодія аналітиків департаменту інформаційної безпеки з користувачами (вивчення особливостей їх роботи). Також для автоматизації такого аналізу можуть бути використані спеціальні програмні засоби, які автоматично здійснюють статистичний аналіз мережевого трафіку і інших елементів інформаційної інфраструктури та сигналізують при виявленні аномальної активності, для того щоб адміністратори могли провести подальший якісний аналіз виявлених відхилень і при необхідності зробити активні дії у відповідь. В цілому, розробка та вдосконалення таких засобів аналізу в складі комплексних систем виявлення вторгнень є одним з перспективних напрямків розвитку засобів захисту інформації.

Таким чином, основним завданням на початковому етапі реагування є визначення характеру порушень і достовірне встановлення того, що виявлені аномальні події, дії і

характеристики є дійсно порушеннями, а, наприклад, не проявом особливостей роботи програмного забезпечення.

Одним з найважливіших організаційних аспектів реагування на інциденти (і, зокрема, на окремі сигнали про деякі події) є та обставина, що може відбуватися більш-менш часте надходження помилкових сигналів (помилкових чи спеціально спровокованих) про деякі події, і реакція персоналу департаменту інформаційної безпеки з часом може поступово слабшати (так само як, наприклад, може притупитися увага при частих помилкових спрацьовуваннях охоронної сигналізації). Зокрема, за оцінкою деяких фахівців, в середньому в 90% випадків, коли користувачі повідомляють про те, що, на їхню думку, комп'ютер заражений вірусом, вони помиляються. У зв'язку з цим при організації реагування на інциденти необхідно приділити особливу увагу психологічній підготовці персоналу, що відповідає за реагування, а також по можливості аналізувати причини появи таких хибних сигналів і запобігати їм надалі.

Також значущим питанням організації роботи з користувачами в ситуаціях реагування на інциденти є те, що взаємодія між користувачами і групами реагування, а також різних груп реагування між собою по можливості необхідно здійснювати спеціальними захищеними каналами зв'язку.

6.5.3. Локалізація та усунення наслідків

Локалізація та усунення наслідків є основним етапом, в рамках якого, власне, здійснюється реагування на інцидент. На цьому етапі відбувається:

- визначення конкретних параметрів порушення (нападу), його характеру (конкретних сегментів мережі, серверів, груп робочих станцій, додатків, порушених нападом);
- попередній аналіз дій порушника і сценарію події (що відбувається) нападу, алгоритму роботи вірусу, що з'явився тощо.;
- блокування дій порушника (якщо порушення триває);
- блокування (повне або часткове) роботи інформаційної системи (сервера, баз даних, сегмента мережі тощо) з метою недопущення подальших руйнівних дій, поширення шкідливих програм або витоку конфіденційної інформації.

Припинення нападу і відновлення нормальної роботи інформаційних систем може зажадати скоординованих дій не тільки самих співробітників департаменту інформаційної безпеки, але й:

- спеціалістів IT-підрозділів, відповідальних за інформаційні сервіси, що атакуються;
- користувачів атакованих інформаційних систем;
- підприємств-партнерів, які мають відношення до атакованих інформаційних ресурсів;
- розробників і постачальників атакованих інформаційних систем;
- постачальників телекомунікаційних послуг, через яких здійснюється атака;
- сторонніх консультантів, що спеціалізуються на відповідних проблемах інформаційної безпеки.

Одним з найбільш важливих обставин роботи на даному етапі є те, якими повноваженнями володіє спеціаліст (черговий), відповідальний за реагування на інциденти. Зокрема, необхідно заздалегідь передбачити можливість оперативного самостійного відключення тих чи інших інформаційних сервісів фахівцями з реагування на інциденти (самостійно, або через відповідний IT-підрозділ). Особливу важливість має здатність відповідальних фахівців оперативно оцінити ситуацію, провести її аналіз (в більшості практичних ситуацій це необхідно буде робити за неповними даними про сторону, що нападає) і прийняти рішення про припинення роботи тих чи інших інформаційних сервісів, до виявлення і усунення загроз і/або введення в дію додаткових коштів протидії вторгненням. При прийнятті такого рішення необхідно враховувати (як правило, на основі експертних оцінок) як можливий збиток, який може бути викликаний виявленим порушенням, так і можливі збитки від зупинки інформаційних сервісів, як (зупинення) може бути здійснена з метою запобігання збитку від дій сторони, що нападає. Характерним прикладом такої ситуації є напад на систему електронної торгівлі, коли сторона, що нападає,

може завдати серйозної шкоди (викрасти конфіденційну інформацію учасників торговельних угод, самостійно вчинити незаконні угоди від імені учасників торгової системи тощо), а зупинка сервісу з метою запобігання такої шкоди може призвести до втрат, пов'язаних з упущеною вигодою від невиконаних угод і шкодою для ділової репутації. Іншим прикладом такої ситуації є реагування на розподілені атаки типу "відмова в обслуговуванні" (Distributed Deny of Service, DDoS), часто здійснювані на сервери в мережі Інтернет, коли може бути необхідно на деякий час повністю відключити сервер як на шкоду користувачам, так і в збиток власникам інформаційних ресурсів, розташованих на сервері.

Основою для прийняття рішень може бути заздалегідь сформований перелік (довідник) можливих основних інцидентів і ознак порушень (проникнень), в якому може бути приведена оцінка ризиків сумарних втрат і рекомендовані дії для кожного типу порушень (у тому числі і перелік ситуацій, коли необхідно здійснити відключення сервісів, щоб уникнути витоку або порушення цілісності інформації, що є найбільш критичною для всієї діяльності підприємства).

6.5.4. Ідентифікація нападника (або джерела розповсюдження шкідливих програм)

Ідентифікація нападника (або джерела розповсюдження шкідливих програм) є важливим кроком у процесі реагування, наступним безпосередньо за локалізацією нападу. У разі якщо напад здійснювався з локальної мережі підприємства, при належному дотриманні внутрішніх режимних правил ця задача може виявитися досить легкою. У разі якщо напад було скоєно ззовні, завдання ідентифікації нападників принципово ускладнюється і в деяких ситуаціях проблема стає практично нерозв'язною.

Як правило, для виявлення джерела нападу необхідно:

- детально вивчити всі технічні аспекти нападу;
- провести якісний аналіз процесу нападу в контексті функціонування системи захисту інформації, що атакується;
- організувати взаємодію зі сторонніми організаціями, які можуть сприяти в ідентифікації нападника.

Одним з найбільш важливих завдань аналізу процесу нападу є встановлення тієї інформації, яка була відома нападникам до початку нападу і якою вони скористалися для здійснення цього нападу. Зокрема, в процесі такого аналізу з певним ступенем впевненості можна встановити, що до початку нападу зловмисникам були відомі:

- інформація про структуру і склад інформаційної системи, що атакується, (використовувані програмні і апаратні засоби, їх архітектура і використовувані налаштування);
- відомості про режим роботи організації та функціонування окремих елементів інформаційної системи. Відомості про регламент деяких бізнес-процесів підприємства;
- конкретні ідентифікаційні дані (імена користувачів, паролі), необхідні для проникнення в інформаційну систему та/або правила (алгоритми) їх генерації.

Узагальнення всіх цих відомостей може допомогти встановити, які контакти були у нападників з атакованою компанією (а яких не було), і, зіставляючи факти, а також користуючись методом виключення, постаратися обмежити коло осіб, які потенційно могли бути причетні до організації даного інциденту.

У свою чергу, проведення такого аналізу буде можливим тільки в тому випадку, якщо всі інформаційні системи та системи захисту інформації налаштовані належним чином (зокрема, в них ведуться всі необхідні системні журнали) і системні дані не були пошкоджені в процесі нападу.

Другим важливим напрямком організаційної та аналітичної роботи при встановленні (ідентифікації) нападників, які вчинили напад ззовні, є взаємодія з адміністраторами систем (телекомунікаційних мереж, комп'ютерів, що використовувалися в якості проксі-серверів, тощо), з використанням яких було здійснено напад. Підходи до такої взаємодії в кожному конкретному випадку, швидше за все, будуть індивідуальними і можуть залежати від політики розкриття інформації адміністрації тієї мережі або вузла, через який здійснювалася

атака. Також можуть бути зроблені дії для того, щоб у судовому порядку або із залученням правоохоронних органів зобов'язати адміністрації таких мереж і вузлів надати необхідну інформацію, пов'язану з подією нападу.

Процес ідентифікації повинен по можливості проводитися з урахуванням того, що згодом необхідно буде використовувати інформацію про нападників як доказ у кримінальному процесі. Зокрема, при знятті (копіюванні) необхідних лог-файлів з атакованих комп'ютерів представниками правоохоронних органів, що проводять слідство у даній справі, повинні бути дотримані всі процесуальні формальності, передбачені кримінально-процесуальним законодавством. Однією з особливостей процедури вилучення доказів у потерпілої сторони в цьому випадку є те, що поняті, присутні при вилученні, повинні по можливості мати хоча б загальне уявлення про сенс проведеної процедури. Також на цьому етапі при необхідності може бути проведена техніко-криміналістична експертиза комп'ютерних систем.

6.5.5. Оцінка і подальший аналіз процесу нападу

Одним із заключних кроків процесу реагування на інцидент є **оцінка та аналіз процесу нападу і його обставин.** Цей аналіз необхідно проводити в контексті цілей і завдань функціонування всього підприємства, з урахуванням результатів роботи з ідентифікації осіб, які вчинили напад. Основні завдання аналітичної роботи на даному етапі:

- аналіз цілей і мотивів нападників;
- аналіз фундаментальних (організаційних і технічних) причин, які зробили напад можливим і успішним (якщо він був успішним);
- аналіз наслідків (у тому числі і довгострокових) нападу для всієї діяльності підприємства;
- аналіз і оцінка роботи персоналу та взаємовідносин з підприємствами-партнерами (у тому числі і з постачальниками інформаційних систем і засобів захисту інформації).

Результатом аналізу повинні бути висновки, які можуть послужити основою для організаційної роботи в різних напрямках:

- коригування та уточнення політики інформаційної безпеки підприємства;
- проведення додаткової роботи з персоналом підприємства (покарання, заохочення, додаткове навчання тощо);
- проведення додаткової роботи з персоналом департаменту інформаційної безпеки підприємства, а також персоналом IT-служб;
- перегляд взаємовідносин з контрагентами підприємства (покупцями, постачальниками тощо), що мають доступ до його інформації, що захищається, або до інформаційних систем;
- залучення сторонніх консультантів з інформаційної безпеки та фахівців із засобів захисту інформації;
- ініціювання технічного переоснащення окремих ділянок інформаційної інфраструктури підприємства.

Таким чином, аналіз і всебічна оцінка інцидентів є відправною точкою для реалізації комплексу заходів щодо вдосконалення системи забезпечення інформаційної безпеки на підприємстві. Всі ці заходи повинні в майбутньому знизити ймовірність аналогічних інцидентів, а також зменшити ймовірність нанесення істотного збитку в разі їх повторення.

Важливою складовою аналізу нападу також є *оцінка збитку від події порушення інформаційної безпеки.* Збиток може бути оцінений одночасно з декількох точок зору і залежить від характеру позаштатної ситуації, що виникла. Найбільш простим для кількісної економічної оцінки є прямий збиток: витрати на відновлення втраченої інформації (можуть бути розраховані на основі трудомісткості робіт з відновлення інформації та даних про середню вартість робочого часу відповідних фахівців), витрати на заміну скомпрометованих паролів, кодів і ключів, вартість пошкодженого обладнання, штрафні санкції за розголошення конфіденційної інформації (якщо такі санкції, наприклад, були передбачені договорами з підрядниками, постачальниками або замовниками) і т.п. Також оцінки потребує упущена вигода, яка може бути пов'язана як з безпосереднім припиненням (зупиненням,

уповільненням) поточних операцій підприємства, так і з довгостроковим (перспективним) негативним впливом виниклої позаштатної ситуації - втратою довіри до підприємства, що призводить до відтоку замовників, формуванням негативного іміджу підприємства тощо. Окремо також може бути оцінене падіння ринкової вартості підприємства - його акцій (якщо мова йде про підприємство, акції якого котируються на біржовому ринку).

Найбільш складним для оцінки є моральний збиток і наслідки від розголошення інформації особистого характеру (наприклад, відомостей, що становлять лікарську таємницю). Конкретні суми моральної шкоди, як правило, можуть бути встановлені за результатами судових розглядів з окремими особами, яким такий збиток був нанесений, або процедур досудового врегулювання конфліктів (на основі вимог постраждалих осіб).

Заключним етапом процесу реагування також є усунення негативних наслідків нападу - локалізація шкоди, заподіяної подією порушенням. Ця робота може включати в себе:

- зміну скомпрометованих паролів окремих користувачів;
- перевстановлення пошкоджених операційних систем, а також пошкодженого програмного забезпечення;
- відновлення порушеної конфігурації (налаштувань) програмного забезпечення та операційних систем;
- відновлення пошкодженої інформації (баз даних, файлів), як з раніше створених резервних копій, так і іншими способами.

В процесі відновлення працездатності інформаційних систем на деякий час можуть бути задіяні резервні (альтернативні) апаратні і програмні платформи.

Крім того, необхідним завершальним кроком може бути додаткова інформаційна робота, яка може в себе включати:

- розсилку користувачам інформації про інциденти, що відбулися (у вигляді спеціальних листів і бюлетенів);
- передачу деяких відомостей про напад в засоби масової інформації;
- передачу відомостей про напад великим групам реагування на інциденти, пов'язаних з інформаційною безпекою, а також у науково-дослідні центри, що займаються проблемами захисту інформації;
- додаткову інформаційну роботу з постачальниками інформаційних систем та підрядниками, які здійснювали їх поставку, впровадження та налагодження.

З точки зору розподілу обов'язків щодо виконання окремих функцій у рамках процесу реагування на інциденти, одним з ефективних і досить широко використовуваних підходів до організації реагування на інциденти є побудова централізованої системи реагування на інциденти, коли одна група реагування обслуговує декілька підрозділів або підприємств.

6.6. Аудит стану інформаційної безпеки

Аудит стану інформаційної безпеки на підприємстві являє собою експертне обстеження основних аспектів інформаційної безпеки, їх перевірку на відповідність певним вимогам. У деяких випадках під аудитом інформаційної безпеки мається на увазі перевірка захищеності окремих елементів інформаційної інфраструктури підприємства і надійності засобів захисту інформації. Однак ми виходимо з того, що аудит інформаційної безпеки є комплексним дослідженням всіх аспектів інформаційної безпеки (як технічних, так і організаційних) в контексті всієї господарської діяльності підприємства з урахуванням діючої політики інформаційної безпеки, об'єктивних потреб підприємства і вимог, що пред'являються третіми особами (державою, контрагентами тощо). В лекції описуються цілі аудитів інформаційної безпеки, їх класифікації за типами, передбачувані результати роботи, а також детально розкривається процес проведення аудиту всіх основних етапів.

6.6.1. Аудит, види аудиту

Аудит стану інформаційної безпеки на підприємстві являє собою експертне обстеження основних аспектів інформаційної безпеки, їх перевірку на відповідність певним вимогам. *У деяких випадках під аудитом інформаційної безпеки мається на увазі перевірка захищеності*

окремих елементів інформаційної інфраструктури підприємства (сегментів його мережі, окремих серверів, баз даних, Інтернет-сайтів тощо.) і надійності засобів захисту інформації (міжмережевих екранів, систем виявлення вторгнень тощо Однак ми надалі виходимо з того, що аудит інформаційної безпеки є комплексним (по можливості, вичерпним) дослідженням всіх аспектів інформаційної безпеки (як технічних, так і організаційних) в контексті всієї господарської діяльності підприємства з урахуванням діючої політики інформаційної безпеки, об'єктивних потреб підприємства і вимог, що пред'являються третіми особами (державою, контрагентами тощо).

Розрізняють два основних види аудиту: внутрішній (проводиться виключно силами співробітників підприємства) і зовнішній (здійснюваний сторонніми організаціями).

Цілями аудиту можуть бути:

- встановлення ступеня захищеності інформаційних ресурсів підприємства, виявлення недоліків і визначення напрямів подальшого розвитку системи захисту інформації;
- перевірка керівництвом підприємства та іншими зацікавленими особами досягнення поставлених цілей у сфері інформаційної безпеки, виконання вимог політики безпеки;
- контроль ефективності вкладень в придбання засобів захисту інформації та реалізацію заходів щодо забезпечення інформаційної безпеки;
- сертифікація на відповідність загальновизнаним нормам і вимогам у сфері інформаційної безпеки (зокрема, на відповідність національним і міжнародним стандартам).

Одним із стратегічних завдань, що вирішуються при проведенні аудиту інформаційної безпеки та отриманні відповідного сертифіката, є демонстрація надійності підприємства, його здатності виступати в якості стійкого партнера, здатного забезпечити комплексний захист інформаційних ресурсів, що може бути особливо важливо при здійсненні угод, що передбачають обмін конфіденційною інформацією, яка має велику вартість (фінансовими відомостями, конструкторсько-технологічною документацією, результатами НДДКР тощо).

У тому випадку, якщо аудит є внутрішнім, групу аудиторів необхідно сформувати з числа таких фахівців, які самі не є розробниками і адміністраторами використовуваних інформаційних систем і засобів захисту інформації та не мали відношення до їх впровадження на даному підприємстві.

Як правило, підприємство може вдаватися до допомоги зовнішніх аудиторів з метою:

- підвищення об'єктивності, незалежності та професійного рівня перевірки;
- отримання висновків про стан інформаційної безпеки та відповідності міжнародним стандартам від незалежних аудиторів.

Компанії, що спеціалізуються на проведенні аудитів, можуть здійснювати перевірки стану інформаційної безпеки на відповідність таким загальновизнаним стандартам і вимогам, як:

- ISO 15408: Common Criteria for Information Technology Security Evaluation (Загальні критерії оцінки безпеки інформаційних технологій);
- BSI\IT: Baseline Protection Manual (Настанова базового рівня із захисту інформаційних технологій Агентства інформаційної безпеки Німеччини);
- COBIT: Control Objectives for Information and related Technology (Основні цілі для інформаційних і пов'язаних з ними технологій);
- та інших документів (таких як SAC, COSO, SAS 55/78).

При цьому організація, що здійснює зовнішній аудит, повинна відповідати певним вимогам:

- мати право (ліцензію) на видачу висновків про відповідність певним вимогам (наприклад, акредитацію UKAS - United Kingdom Accreditation Service);
- співробітники повинні мати право доступу до інформації, що становить державну і військову таємницю (якщо така інформація є на підприємстві, що перевіряється);
- володіти необхідними програмними та апаратними засобами для вичерпної перевірки наявного у підприємства програмного і апаратного забезпечення.

6.6.2. Етапи проведення аудиту

Основними етапами проведення аудиту є:

- ініціювання проведення аудиту;
- безпосереднє здійснення збору інформації та проведення обстеження аудиторами;
- аналіз зібраних даних і вироблення рекомендацій;
- підготовка аудиторського звіту та атестаційного висновку.

Аудит повинен бути ініційований керівництвом підприємства з досить чітко сформульованою метою на певному етапі розвитку інформаційної системи або системи забезпечення інформаційної безпеки підприємства (наприклад, після завершення одного з етапів впровадження). У разі якщо аудит не є комплексним, на початковому етапі необхідно визначити його безпосередні межі:

- перелік обстежуваних інформаційних ресурсів та інформаційних систем (підсистем);
- перелік будівель, приміщень і територій, в межах яких проводитиметься аудит;
- елементи системи забезпечення інформаційної безпеки, які необхідно включити в процес перевірки (організаційне, правове, програмно-технічне, апаратне забезпечення);

Основна стадія – **проведення аудиторського обстеження та збір інформації** – як правило, має включати в себе:

- аналіз наявної політики інформаційної безпеки та іншої документації організації;
- проведення нарад, опитувань, довірчих бесід та інтерв'ю зі співробітниками підприємства;
- перевірку стану фізичної безпеки інформаційної інфраструктури підприємства;
- технічне обстеження інформаційних систем – програмних і апаратних засобів (інструментальна перевірка захищеності).

Перш ніж приступити власне до аудиту інформаційної безпеки, аудиторам (зокрема, якщо проводиться зовнішній аудит) необхідно ознайомитися зі структурою підприємства, його функціями, завданнями та основними бізнес-процесами, а також з наявними інформаційними системами (їх складом, функціональністю, процедурами використання і роллю на підприємстві). На початковому етапі аудитори приймають рішення про те, наскільки глибоко і детально будуть досліджені окремі елементи інформаційної системи та системи захисту інформації. Також необхідно заздалегідь скоординувати з користувачами інформаційних систем процедури перевірки та тестування, що вимагають обмеження доступу користувачів (такі процедури по можливості повинні проводитися в неробочий час або в періоди найменшого завантаження інформаційної системи).

Якісний **аналіз діючої на підприємстві політики безпеки** є відправною точкою для проведення аудиту. Одне з перших завдань комплексного аудиту – встановлення того, якою мірою діюча політика відповідає об'єктивним потребам даного підприємства в безпеці, чи можуть дії в рамках даної політики забезпечити необхідний рівень захищеності інформації і засобів її обробки, зберігання та передачі. Це, в свою чергу, може вимагати проведення додаткової оцінки значущості основних інформаційних активів підприємства, їх вразливості, а також існуючих ризиків і загроз. Аналіз політики також може включати оцінку таких її характеристик, як:

- повнота і глибина охоплення всіх питань, а також відповідність змісту політик нижнього рівня цілям і завданням, встановленим у політиках верхнього рівня;
- зрозумілість тексту політики для людей, які не є технічними фахівцями, а також чіткість формулювань і неможливість їх подвійного тлумачення;
- актуальність всіх положень і вимог політики, своєчасність обліку всіх змін, що відбуваються в інформаційних системах і бізнес-процесах.

Після перевірки основних положень політики безпеки в процесі аудиту можуть бути вивчені (перевірені) діючі класифікації інформаційних ресурсів за ступенем критичності і конфіденційності, а також інші документи, що мають відношення до забезпечення інформаційної безпеки:

- організаційні документи підрозділів підприємства (положення про відділи, посадові інструкції);
- інструкції (положення, методики), що стосуються окремих бізнес-процесів

підприємства;

- кадрова документація, зобов'язання про нерозголошення відомостей, дані співробітників, свідоцтва про проходження навчання, професійної сертифікації, атестації та ознайомленні з діючими правилами;
- технічна документація та користувацькі інструкції для різних використовуваних програмних і апаратних засобів (як розроблених самим підприємством, так і придбаних у сторонніх постачальників): міжмережевих екранів, маршрутизаторів, операційних систем, антивірусних засобів, систем управління підприємством тощо.

Основна робота аудиторів у процесі збору інформації полягає у вивченні фактично застосованих заходів щодо забезпечення захисту інформаційних активів підприємства, таких як:

- організація процесу навчання користувачів прийомам і правилам безпечного використання інформаційних систем;
- організація роботи адміністраторів інформаційних і телекомунікаційних систем і систем захисту інформації (правильність використання програмних і апаратних засобів адміністрування, своєчасність створення і видалення облікових записів користувачів, а також налаштування їх прав в інформаційних системах, своєчасність заміни паролів і забезпечення їх відповідності вимогам безпеки, здійснення резервного копіювання даних, ведення протоколів усіх вироблених у процесі адміністрування операцій, вжиття заходів при виявленні несправностей тощо);
- організація процесів підвищення кваліфікації адміністраторів інформаційних систем і систем захисту інформації;
- забезпечення відповідності необхідних (відповідно з політикою безпеки та посадовими обов'язками) прав користувачів інформаційних систем і фактично наявних;
- організація призначення і використання спеціальних ("суперкористувацьких") прав в інформаційних системах підприємства;
- організація робіт і координації дій при виявленні порушень інформаційної безпеки та відновленні роботи інформаційних систем після збоїв і нападів (практичне виконання "аварійного плану");
- вживаються заходи антивірусного захисту (належне використання антивірусних програм, облік всіх випадків зараження, організація роботи з усунення наслідків заражень тощо);
- забезпечення безпеки придбаних програмних і апаратних засобів (наявність сертифікатів і гарантійних зобов'язань, підтримка з боку постачальника при усуненні виявлених недоліків тощо);
- забезпечення безпеки самостійно розроблюваного програмного забезпечення (наявність необхідних вимог у проектній документації інформаційних систем, якість програмної реалізації механізмів захисту тощо);
- організація робіт з встановлення та оновлення програмного забезпечення, а також контролю за цілісністю встановленого ПЗ;
- вживаються заходи щодо забезпечення обліку і схоронності носіїв інформації (дисків, дискет, магнітних стрічок тощо.), а також з їх безпечного знищення після закінчення використання;
- ефективність організації взаємодії співробітників підприємства – користувачів інформаційних систем – зі службою інформаційної безпеки (зокрема, з питань реагування на інциденти та усунення їх наслідків).

Одним з важливих напрямків аудиторської перевірки є контроль того, наскільки своєчасно і повно положення та вимоги політики безпеки та інших організаційних документів доводяться до персоналу підприємства. В тому числі, необхідно оцінити, наскільки систематично і цілеспрямовано здійснюється навчання персоналу (як при занятті посад, так і в процесі роботи), і, відповідно, дати оцінку тому, якою мірою персонал розуміє всі пропоновані до нього вимоги, усвідомлює свої обов'язки, пов'язані із забезпеченням

безпеки, а також можливу відповідальність, яка може настати при порушенні встановлених вимог.

У процес проведення інтерв'ю, нарад і бесід з персоналом необхідно включити якомога більше співробітників підприємства, які мають хоча б якесь відношення до інформаційних систем і процедур обробки інформації : адміністраторів і розробників інформаційних систем, операторів та інших користувачів, допоміжний персонал тощо При безпосередній роботі з персоналом аудиторам необхідно з'ясувати особливості перебігу окремих бізнес-процесів, ролі окремих співробітників в цих процесах і їх потенційні можливості впливати на інформаційну безпеку. Також необхідно оцінити, якою мірою співробітники фактично виконують свої обов'язки щодо забезпечення інформаційної безпеки.

Одним із важливих завдань аудиту може бути встановлення того, наскільки підприємство здатне протидіяти внутрішнім загрозам в особі співробітників, цілеспрямовано діючих, щоб завдати той чи інший збиток підприємству і мають для цього різні можливості. Зокрема, для цього можуть бути досліджені:

- процедури відбору та прийняття нових співробітників на роботу, а також їх попередньої перевірки;
- процедури контролю за діяльністю співробітників (відстеження їх дій);
- процедури реєстрації користувачів і призначення їм прав в інформаційних системах;
- розподіл функцій між різними співробітниками і мінімізація їхніх привілеїв, а також можливу наявність надлишкових прав у деяких користувачів та адміністраторів.

Перевірка стану фізичної безпеки інформаційної інфраструктури, як правило, включає в себе:

- перевірку того, щоб найбільш важливі об'єкти інформаційної інфраструктури та системи захисту інформації розташовувалися в зонах (частинах будинків, приміщеннях), що мають пропускний режим, а також обладнаних камерами відеоспостереження та іншими засобами контролю (електронними замками, засобами біометричної ідентифікації тощо);
- перевірку наявності та працездатності технічних засобів, що забезпечують стійку роботу комп'ютерного та телекомунікаційного обладнання: джерел безперебійного енергопостачання, кондиціонерів (там, де це необхідно) тощо;
- перевірку наявності та працездатності засобів пожежної сигналізації та пожежогасіння;
- перевірку розподілу відповідальності за фізичний (технічний) стан об'єктів інформаційної інфраструктури підприємства.

Інструментальна перевірка захищеності є в основному технічним завданням і здійснюється з використанням спеціалізованого програмного забезпечення, яке підключається до інформаційної системи підприємства і автоматично проводить збір всіляких відомостей: версій встановлених операційних систем і програмного забезпечення, даних про мережеві протоколи, що використовуються, номерів відкритих портів, даних про версії встановлених оновлень тощо. До інших напрямків інструментального та технічного контролю також відносяться такі роботи, як:

- безпосереднє вивчення роботи окремих серверів, робочих станцій і мережевого устаткування відповідними технічними фахівцями, які можуть перевірити різні аспекти їх функціонування (процедури завантаження, виконувані процеси, вміст конфігураційних файлів тощо);
- збір і подальший аналіз даних про те, як виконуються процедури резервного копіювання, а також інші необхідні технічні процедури, передбачені регламентом;
- перевірка якості програмного забезпечення, самостійно розробленого підприємством (у тому числі і шляхом аналізу вихідних кодів і проектної документації до нього), виявлення помилок, які можуть стати причиною збоїв, несанкціонованих проникнень, руйнування і витоку інформації та інших інцидентів;
- вивчення роботи мережі (мережевого трафіку, завантаження різних сегментів мережі

тощо);

- проведення з метою тестування пробних, контрольованих "порушень" інформаційної безпеки (по можливості без нанесення реальної шкоди і у позаробочий час), таких як атаки типу "відмова в обслуговуванні" (DoS) або проникнення в певні бази даних і на певні сервери, а також використання різних відомих вразливостей з метою з'ясування конкретних параметрів безпеки, стабільності та надійності інформаційної системи, яка перевіряється.

Також в процесі аудиту може бути перевірено ведення журналів (лог-файлів) інформаційних систем і застосування інших інструментів збору та аналізу інформації, необхідних для забезпечення поточного контролю за дотриманням вимог інформаційної безпеки та своєчасного реагування на інциденти (засобів виявлення вторгнень, аналізаторів роботи локальних мереж тощо). Інформація, накопичена в лог-файлах за час використання інформаційних систем, є одним з важливих об'єктів аналізу в процесі аудиту. На основі цих даних можуть бути зроблені оцінки та висновки щодо дотримання встановлених правил використання інформаційних систем, ефективності використовуваних засобів захисту інформації, поведінки користувачів, а також про потенційно можливі проблеми.

Аналіз всієї інформації, отриманої в процесі ознайомлення з документацією, контролю фактичного виконання всіх встановлених вимог, отримання відомостей від співробітників, вивчення роботи апаратних засобів і програмного забезпечення, перевірки фізичної захищеності та проведення інструментальних перевірок повинен бути проведений з урахуванням виявлених ризиків та потреб підприємства в інформаційній безпеці. Зокрема, такий аналіз передбачає виявлення конкретних особливостей програмних і апаратних засобів, бізнес-процедур, організаційних правил і розподілів функціональних обов'язків та повноважень, які можуть негативно вплинути на забезпечення інформаційної безпеки, а також опис причинно-наслідкових взаємозв'язків між виявленими особливостями функціонування підприємства і збільшенням ризиків порушення інформаційної безпеки. Всі досліджені обставини, виявлені недоліки та особливості повинні бути узагальнені, і таким чином має бути сформоване загальне уявлення про стан інформаційної безпеки на підприємстві, відображені основні переваги і недоліки діючої системи захисту інформаційних ресурсів, а також позначені основні пріоритети та напрями її подальшого розвитку та вдосконалення.

Результати аналізу можуть бути представлені як у вигляді узагальнених коротких формулювань, що характеризують захищеність інформації підприємства (адресованих керівництву та власникам підприємства), так і у вигляді переліку конкретних зауважень і пропозицій, що відносяться до окремих ділянок роботи (адресованих керівнику департаменту інформаційної безпеки, керівнику служби безпеки, функціональним директорам та керівникам структурних підрозділів підприємства).

Заключним результатом аналізу та узагальнення даних, отриманих в процесі аудиту, є звіт (висновок), який може включати в себе:

- оцінку стану (рівня) захищеності інформаційних ресурсів та інформаційних систем;
- висновки про практичне виконання вимог, передбачених політикою інформаційної безпеки підприємства та іншими вимогами та документами;
- висновок про ступінь відповідності фактичного рівня інформаційної безпеки вимогам певних стандартів і нормативних документів;
- пропозиції щодо удосконалення політики інформаційної безпеки та реалізації додаткових практичних заходів у цій сфері (як організаційних, так і технічних), а також про ті заходи, які необхідно реалізувати для проходження сертифікації на відповідність певному стандарту (якщо за результатами проведеного аудиту зроблено висновок про те, що поточний рівень захищеності інформаційних ресурсів підприємства не відповідає таким вимогам);
- висновок про ступінь відповідності політики безпеки підприємства та всього комплексу заходів щодо захисту інформації вимогам чинного законодавства та відомчих нормативних актів;

- оцінки економічної ефективності вкладень у ті чи інші засоби захисту інформації, а також організаційні заходи (віддачі від них);
- кількісна (грошова) оцінка можливих втрат від тих чи інших порушень, які можуть статися при існуючому рівні забезпечення інформаційної безпеки, а також розрахунок необхідних вкладень, які необхідно здійснити для досягнення певного рівня захищеності.

Також за результатами аудиту можуть бути сформульовані додаткові рекомендації, що стосуються:

- перегляду окремих бізнес-процесів і процедур;
- вдосконалення роботи з персоналом підприємства;
- впровадження і використання сучасних технічних (програмних і апаратних) засобів обробки і захисту інформації;
- організації роботи із захисту інформації;
- вибору пріоритетів в процесі усунення існуючих недоліків.

ЛЕКЦІЯ 7.
НЕСАНКЦІОНОВАНИЙ ДОСТУП. ПОРУШНИКИ БЕЗПЕКИ
7.1 Поняття несанкціонованого доступу

Спосіб несанкціонованого доступу (НСД) - це сукупність прийомів і порядок дій з метою одержання (добування) інформації, що охороняється, незаконним протиправним шляхом і забезпечення можливості впливати на цю інформацію (наприклад: підмінити, знищити і т.п.).

При здійсненні несанкціонованого доступу, зловмисник переслідує три мети:

- одержати необхідну інформацію для конкурентної боротьби;
- мати можливість вносити зміни в інформаційні потоки конкурента у відповідності зі своїми інтересами;
- завдати шкоди конкурентові шляхом знищення матеріалу інформаційних цінностей.

Спроба одержати несанкціонований доступ до комп'ютерної мережі з метою ознайомитися з нею, залишити інформацію, виконати, знищити, змінити або викрасти програму або іншу інформацію кваліфікується як «**комп'ютерне піратство**».

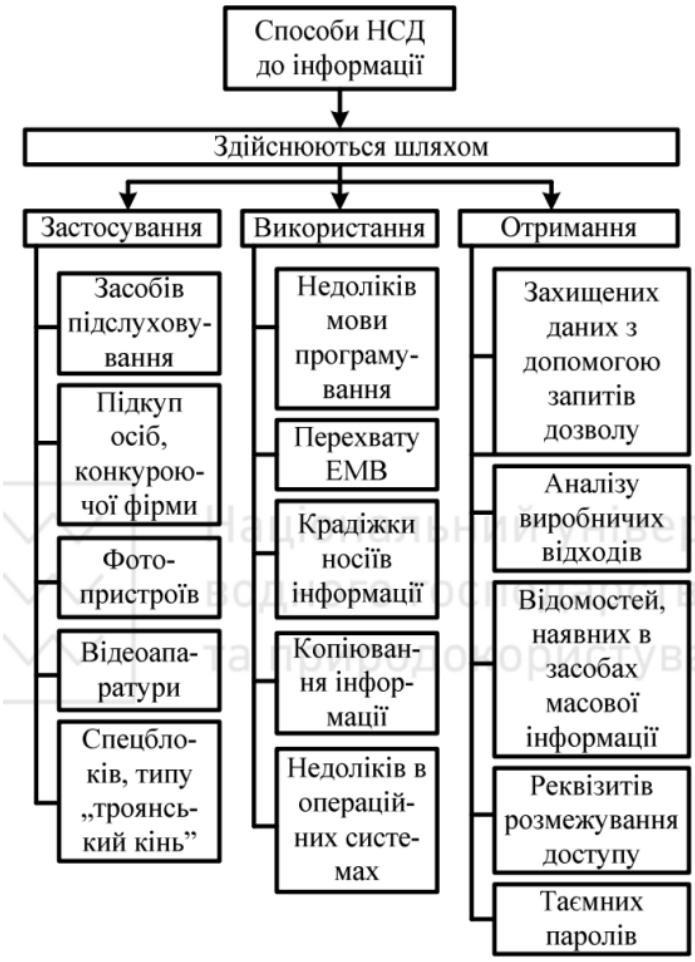


Рис. 7.1. Способи НСД до конфіденційної інформації

Для запобігання можливих загроз, фірми повинні не тільки забезпечити захист операційних систем, програмного забезпечення і контроль доступу, але і спробувати виявити категорії порушників і ті методи, які вони використовують.

Залежно від мотивів, мети та методів, дії порушників безпеки інформації можна поділити на чотири категорії:

- шукачі пригод;
- ідейні «хакери»;
- «хакери»-професіонали;
- ненадійні (неблагополучні) співробітники.

Шукач пригод, - рідко є продуманий план атаки. Він вибирає мету випадковим чином і звичайно відступає, зіштовхнувшись із ускладненнями. Знайшовши діру в системі безпеки, він намагається зібрати закриту інформацію, але практично ніколи не намагається її таємно змінити. Своїми перемогами такий шукач пригод ділиться тільки зі своїми близькими друзями-колегами.

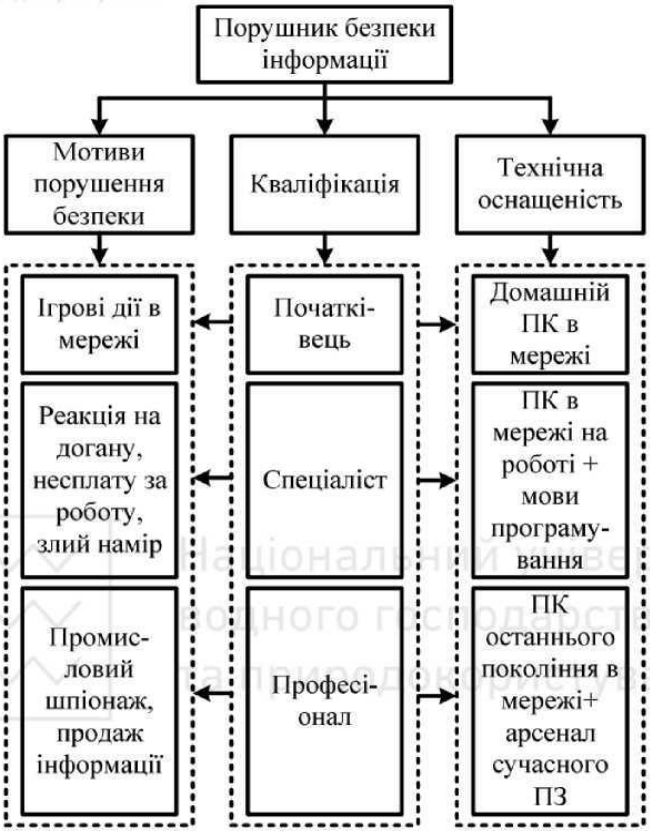
Ідейний «хакер» - це той же шукач пригод, але більш майстерний. Він уже вибирає собі конкретні цілі (хости і ресурси) на підставі своїх переконань. Його улюбленим видом атаки є зміна інформаційного наповнення Webсервера або, рідше, блокування роботи ресурсу, що атакується. У порівнянні із шукачем пригод, ідейний «хакер» розповідає про успішні атаки набагато більшій аудиторії, звичайно розміщаючи інформацію на хакерському Webвузлі.

«Хакер»-професіонал має чіткий план дій і спрямовує його на визначені ресурси. Його атаки добре продумані і, звичайно, здійснюються у кілька етапів. Спочатку він збирає попередню інформацію (тип ОС, надані сервіси і міри захисту). Потім він складає план атаки з урахуванням зібраних даних і підбирає (або навіть розробляє) відповідні інструменти. Далі, провівши атаку, він одержує закриту інформацію і, нарешті, знищує всі сліди своїх дій. Такий професіонал звичайно добре фінансується і може працювати один або у складі команди професіоналів.

Ненадійний (неблагополучний) співробітник своїми діями може спричинити стільки ж проблем (буває і більше), скільки промисловий шпигун, до того ж, його присутність звичайно складніше знайти. Крім того, йому доводиться долати не зовнішній захист мережі, а тільки, як правило, менш жорсткіший, внутрішній. Він не такий витончений у способах атаки, як промисловий шпигун, і тому частіше допускає помилки, і тим самим може видати свою присутність.

Модель порушника визначає:

- категорії осіб, у числі яких може виявитися порушник;
- можливі цілі порушника і їх градації за ступенем важливості та небезпеки;
- припущення про його кваліфікації;
- оцінка його технічної озброєності;
- обмеження і припущення про характер його дій.



Сьогодні, зі стрімким розвитком Internet, «хакери» стають справжньою загрозою для державних і корпоративних комп'ютерних мереж. Так, за оцінками експертів США, напади «хакерів» на комп'ютери і мережі федеральних державних систем відбуваються в цій країні не рідше 50-ти раз на день. Багато великих компаній і організації піддаються атакам кілька разів у тиждень, а деякі навіть щодня. Виходять такі атаки не завжди ззовні, 70% спроб зловмисного проникнення в комп'ютерні системи мають джерело всередині самої організації.

7.2. Шляхи забезпечення безпеки інформації

Концепція захисту інформації

Вразливість інформації в автоматизованих комплексах обумовлена великою концентрацією обчислювальних ресурсів, їх територіальною розподіленністю, довгостроковим збереженням великого об'єму даних на магнітних та оптичних носіях, одночасним доступом до ресурсів багатьох користувачів.

Вживання заходів захисту мають певні труднощі:

1. немає єдиної теорії захисту систем;
2. виробники засобів захисту, в основному, пропонують окремі компоненти для рішення приватних задач, залишаючи питання формування системи захисту і сумісності цих засобів на розсуд споживачів;
3. для забезпечення надійного захисту необхідно розв'язати цілий комплекс технічних і організаційних проблем і розробити відповідну документацію.

Концепція захисту інформації - офіційно прийнята система поглядів на проблему інформаційної безпеки і шляхи її рішення з урахуванням сучасних тенденцій. Вона є методологічною основою політики розробки практичних заходів для її реалізації. На базі сформульованих у концепції цілей, задач і можливих шляхів їх рішення формуються конкретні плани забезпечення інформаційної безпеки.

Стратегія та архітектура захисту інформації.

В основі комплексу заходів щодо інформаційної безпеки повинна бути **стратегія захисту інформації**. У ній визначаються мета, критерії, принцип і процедури, необхідні для побудови надійної системи захисту. Найважливішою особливістю загальної стратегії інформаційного захисту є дослідження системи безпеки.

Можна виділити два основних напрямки:

- аналіз засобів захисту;
- визначення факту вторгнення.

На основі концепції безпеки інформації розробляються стратегія безпеки інформації та архітектура системи захисту інформації, а далі - політика безпеки інформації (рис.7.3).

Рис. 7.3 Ієрархічний підхід до забезпечення безпеки інформації

Розробку концепції захисту рекомендується проводити в три етапи (рис. 7.4).

Рис. 7.4 Етапи розробки концепції захисту інформації

На першому етапі повинна бути чітко визначена цільова установка захисту, тобто які реальні цінності, виробничі процеси, програми, масиви даних необхідно захищати. На цьому етапі доцільно диференціювати за значимістю окремі об'єкти, що вимагають захисту.

На другому етапі повинен бути проведений аналіз злочинних дій, що потенційно можуть бути зроблені стосовно об'єкта, що захищається. Важливо визначити ступінь реальної небезпеки таких найбільш широко розповсюджених злочинів, як економічне шпигунство, саботаж, крадіжки зі зломом. Потім потрібно проаналізувати найбільш ймовірні дії зловмисників стосовно основних об'єктів, що потребують захисту.

Головною метою **третього етапу** є аналіз обставин, у тому числі місцевих специфічних умов, виробничих процесів, уже встановлених технічних засобів захисту.

Концепція захисту повинна містити перелік організаційних, технічних і інших заходів, що забезпечують максимальну безпеку при заданому залишковому ризику і мінімальні витрати на їх реалізацію.

Політика захисту - це загальний документ, де перераховуються правила доступу, визначаються шляхи реалізації політики та описується базова архітектура середовища захисту.

Власне документ складається із декількох сторінок тексту. Він формує основу фізичної архітектури мережі, а інформація, що знаходиться в ньому, визначає вибір продуктів захисту. При цьому, документ може і не включати список необхідних закупок, але вибір конкретних компонентів після його складання повинен бути очевидним.

Політика захисту повинна обов'язково включати наступне:

1. контроль доступу (заборона на доступ користувача до матеріалів, якими йому не дозволено користуватися);
2. ідентифікацію та аутентифікацію (використання паролів або інших механізмів для перевірки статусу користувача);
3. облік (запис усіх дій користувача в мережі);
4. контрольний журнал (журнал дозволяє визначити, коли і де відбулося порушення захисту);
5. акуратність (захист від будь-яких випадкових порушень);
6. надійність (запобігання монополізації ресурсів системи одним користувачем);
7. обмін даними (захист усіх комунікацій).

Види забезпечення безпеки інформації.

В даний час комп'ютерні злочини надзвичайно різноманітні. Це несанкціонований доступ до інформації, що зберігається в комп'ютері, введення в програмне забезпечення логічних бомб, розробка і поширення комп'ютерних вірусів, розкрадання комп'ютерної інформації, недбалість у розробці, виготовленні та експлуатації програмно-обчислювальних комплексів, підробка комп'ютерної інформації.

Всі заходи протидії комп'ютерним злочинам, що безпосередньо забезпечують безпеку інформації, можна підрозділити на:

- правові;
- організаційно-адміністративні;
- інженерно-технічні.

До правових заходів варто віднести розробку норм, що встановлюють відповідальність за комп'ютерні злочини, захист авторських прав програмістів, удосконалювання карного і цивільного законодавства, а також судочинства.

До організаційно-адміністративних заходів відносяться: охорона комп'ютерних систем, підбір персоналу, виключення випадків ведення особливо важливих робіт тільки однією людиною, наявність плану відновлення працездатності центру після виходу його з ладу, обслуговування обчислювального центру сторонньою організацією або особами, незацікавленими в приховуванні фактів порушення роботи центру, універсальність засобів захисту від усіх користувачів (включаючи вище керівництво), покладання відповідальності на осіб, що повинні забезпечити безпеку центру, вибір місця розташування центру і т.п.

До інженерно-технічних заходів можна віднести:

1. захист від несанкціонованого доступу до комп'ютерної системи,
2. резервування важливих комп'ютерних систем,
3. забезпечення захисту від розкрадань і диверсій,
4. резервне електроживлення, розробку і реалізацію спеціальних програмних і апаратних комплексів безпеки тощо.

Фізичні засоби містять у собі різні інженерні засоби, що перешкоджають фізичному проникненню зловмисників на об'єкти захисту, що захищають персонал (особисті засоби безпеки), матеріальні засоби і фінанси, інформацію від протиправних дій.

До **апаратних** засобів відносяться прилади, пристрої, пристосування та інші технічні рішення, які використовуються в інтересах забезпечення безпеки. У практиці діяльності будь-якої організації знаходить широке застосування різна апаратура: від телефонного апарату до розроблених автоматизованих інформаційних систем, що забезпечують її виробничу діяльність. Основна задача апаратних засобів - стійка безпека комерційної діяльності.

Програмні засоби - це спеціальні програми, програмні комплекси і системи захисту інформації в інформаційних системах різного призначення і засобах обробки даних.

Криптографічні засоби - ця спеціальні математичні та алгоритмічні засоби захисту інформації, переданої по мережах зв'язку, збереженої та обробленої на комп'ютерах з використанням методів шифрування.

Визначається деяка однозначна функція *с*(*X*) (тобто відображення {*с*: *O^L*}), яка дозволяє для будь-яких об’єктів *X* і *Y* сказати, що коли *Y* більш цінний об’єкт, ніж *X*, то *с*(*Y*)>*с*(*X*).

Означення. Політика МПБ вважає інформаційний потік *X*-^ *Y* дозволеним тоді і тільки тоді, коли *с*(*Y*)>*с*(*X*) в решітці *L*.

Означення. В системі з двома доступами *г* і *м* політика МПБ визначається наступними правилами доступу

X-^ У &c(X^c(У),

X^^У ^c(X}$c(ї}.

МПБ в сучасних системах захисту на практиці реалізується мандатним контролем. Він реалізується на найнижчому апаратно-програмному рівні, що дозволяє досить ефективно будувати захищене середовище для механизма мандатного контроля. Пристрій мандатного контролю називають монітором звернень.

Мандатний контроль ще називають обов’язковим, так як його має проходити кожне звернення суб’єкта до об’єкта, якщо вони знаходяться під захистом СЗІ. Організується він так: кожний об’єкт О має мітку з інформацєю про свій рівень секретності с(О); кожний суб’єкт 8 також має мітку з інформацією про те, до яких об’єктів він має право доступу с(8). Мандатний контроль порівнює мітки і задовольняє запит суб’єкта 8 до об’єкта О на читання, якщо с(8)>с(О) і задовольняє запит на запис, якщо с(8)<с(О). Таким чином, мандатний контроль реалізує МПБ.

Наведемо ряд переваг МПБ порівняно з ДПБ.

1. Для систем, де реалізовано МПБ, є характерним більш високий ступінь надійності. Це пов’язано з тим, що за правилами МПБ відстежуються не тільки правила доступу суб’єктів системи до об’єктів, але і стан самої АС. Таким чином, канали витоку в системах

такого типу не закладені первісно (що є в положеннях ДПБ), а можуть виникнути тільки за практичної реалізації систем внаслідок помилок розробника.

2. Правила МПБ більш ясні і прості для розуміння розробниками і користувачами ІТС, що також є фактором, що позитивно впливає на рівень безпеки системи.

3. МПБ стійка до атак типу «Троянський кінь».

4. МПБ допускає можливість точного математичного доказу, що дана система в заданих умовах підтримує ПБ.

Однак МПБ має дуже серьйозні вади - вона є винятково складною для практичної реалізації і вимагає значних ресурсів обчислювальної системи. Це пов'язано з тим, що інформацйних потоків в системі величезна кількість і їх не завжди можна ідентифікувати.

Рольова політика безпеки.

Рольову політику безпеки (Role Base Access Control - RBAC) не можна віднести ані до дискреційної, ані до мандатної, тому що керування доступом в ній здійснюється як на основі матриці прав доступу для ролей, так і за допомогою правил, які регламентують призначення ролей користувачам та їх активацію під час сеансів.

РПБ базується на наступних властивостях:

1. всі суб'єкти і об'єкти повинні бути однозначно ідентифіковані;
2. визначено набір ролей в системі;
3. кожній ролі встановлено певний обсяг повноважень;
4. доступ суб'єктів до об'єктів здійснюється за допомогою певних правил в рамках певної ролі.

В РПБ класичне поняття **суб'єкт** заміщується поняттями **користувач** і **роль.** Користувач - це людина, яка працює з системою і виконує певні службові обов'язки. Роль - це активно діюча в системі абстрактна суттєвість, з якою пов'язаний обмежений, логично зв'язаний набір повноважень, які необхідні для здійснення певної діяльності.

В моделі РПБ визначаються наступні множини:

- *U* - множина користувачів;
- *R* - множина ролей;
- *P* - множина повноважень на доступ до об'єктів, що представляється, наприклад, у вигляді матриці прав доступу;
- *S* - множина сеансів роботи користувачів з системою.

Для перелічених множин визначаються наступні відношення:

PA Ç *P* x *R* - відображає множину повноважень на множину ролей, встановлюючи для кожної ролі набір наданих їй повноважень;

UA Ç *U* x *R* - відображає множину користувачів на множину ролей, визначаючи для кожного користувача набір доступних йому ролей.

Правила керування доступом рольової політики безпеки визначаються наступними функціями:

user : *S*^ *U* - для кожного сеанса *s* ця функція визначає користувача *u*, який здійснює цей сеанс роботи з системою: *user*(*s*)=*u*;

roles : *S*^ *R* - для кожного сеанса *s* ця функція визначає набір ролей з множини R, що можуть бути одночасно доступні користувачу *u* в цьому сеансі: *roles* (*s*)={ *r* |(*user*(*s*), *r*)Є *UA* };

permissions : *S*^*P* - для кожного сеанса *s* ця функція задає набір доступних в ньому повноважень, який визначається як сукупність повноважень всіх ролей, що приймають участь в цьому сеансі: *permissions* (*s*)={*p* |(*p, r*)Є *PA* }.

В якості критерію безпеки рольової моделі використовується наступне правило: **система вважається безпечною, якщо будь-який користувач системи *u*, що працює в сеансі *s*, може здійснити дії, які вимагають повноважень *p* тільки в тому випадку, коли *p*Є*permissions*(*s*).**

Монітор безпеки

Для здійснення операцій з об'єктами в захищеній ІТС необхідна додаткова інформація (і наявність відповідного об'єкта, що її містить) про дозволені та заборонені операції. Такою компонентою є **монітор безпеки** - компонента КС, яка активізується при виникнення будь-якого потоку від одного об'єкта до іншого і дозволяє реалізуватися потокам, що належать тільки множині легального доступу *L*.

МБ повністю приймає участь у потоці від об'єкта до об'єкта і основна його цільова функція - фільтрація інформаційних потоків для забезпечення безпеки КС, тобто фактично - це механізм реалізації ПБ в КС. Множина об'єктів, що входять до складу МБ як компоненти КС, повинна містити підмножину процесів, з якими повинні бути асоційовані всі інші об'єкти КС, і, звичайно, хоча б одного користувача. Всі об'єкти КС повинні бути асоційованими з цим користувачем (якого зазвичай називають адміністратором безпеки).

Вибір методів і механізмів залишається за розробником і єдиною вимогою є реалізація функції захисту, причому для МБ повинні виконуватися наступні загальні вимоги:

- МБ повинен забезпечувати неперервний і повний захист;
- бути достовірним (захищеним від модифікацій);
- мати невеликі (відносно) розміри.

Точно сформулювати і формально описати необхідні умови реалізації МБ дуже важко. Проте можна описати деякі важливі властивості МБ, якими він завідомо повинен володіти незалежно від конкретної ПБ. Серед цих властивостей зазначимо наступні:

- при реалізації будь-якої ПБ найважливішим кроком є ідентифікація всіх об'єктів КС. При цьому повинна мати місце унікальність імен об'єктів, що дозволяє реалізувати механізм ідентифікації і автентифікації (ІА);
- неможливість доступу до об'єктів без участі МБ: якщо в для об'єкт *0'Є.О,* отримав в момент *t* доступ O_i-£-*О:, *0^0/,* то

З *к>0, k&N0* таке, що в момент *t-k, t-k&N0* відбувся запит на доступ, який позначатимемо O_i -(відсутність обхідних шляхів). Запит на доступ можна також вважати одним з видів доступу від об'єкта O_i до інших об'єктів. Очевидно, що в якості об'єктів-огримувачів доступу до O_i повинні виступати лише активні об'єкти *V. (E.u,i'* = і Ру ЄР, у - 1,...,^;

- обов'язкова наявність механізму ІА: якщо для УлЕЛУ $^o_i,o_i \epsilon o_1$ має місце o_i^^*o.*, то МБ однозначно визначає належність O_i і *О.* до відповідних множин *(У, Р* або О;
- обов'язкова присутність в МБ дозвільного механізму, тобто при запиті $O_I.O_I \epsilon O_!$ в залежності від належності потоку до иідмножин *Ь* або *Р* приймається відповідне рішення, і доступ від O_i до *О* ■ здійснюється або ні. Належність визначається на основі правил, що декларуються конкретною ПБ (наприклад, для дискреційної ПБ - це матриця доступу, для мандатної ПБ - міточннй контроль)

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Cyber Security. Simply. Make it Happen. : Monograph / edit. Abolhassan. – SpringerInternational Publishing, 2017. – ISBN 978- 3-319-46528-9 (print) ; 978-3-319-46529-6(online). 127 p.
2. Cyber-Physical Security : Monograph / edit. Clark. – Springer International Publishing, 2017. – ISBN 978-3-319-32822-5 (print) ; 978-3-319-32824-9 (online). 299 p.
3. Enterprise Security : Monograph / edit. Chang. – Springer International Publishing, 2017. – ISBN 978-3-319-54379-6 (print) ; 978-3-319-54380-2 (online). 277 p.
4. Бурячок В.Л., Грищук Р.В., Хорошко В.О. Політика інформаційної безпеки, підручник, - К.; ПВП «Задруга», 2014. - 222 с
5. Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу : НД ТЗІ 2.5-010-03.
6. Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи. НД ТЗІ 3.1-001-07
7. Інформаційна безпека / Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв,С. С. Войтусік, А. Я. Горпенюк, О. А. Нємкова, І. М. Журавель, Б. М. Березюк, Є. І.Яковенко, В. І. Отенко, І. Я. Тишик. Львів : Видавництво Львівської політехніки, 2019.580 с.
8. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу: НД ТЗІ 2.5-004-99
9. Методичні вказівки з виконання зіставлення результатів оцінювання засобів захисту інформації від несанкціонованого доступу на відповідність вимогам ISO/IEC 15408 з вимогами НД ТЗІ 2.5-004-99 : НД ТЗІ 2.7-013-2016.
10. Організація комп’ютерних мереж [Електронний ресурс] : підручник: для студ.спеціальності 121 «Інженерія програмного забезпечення» та 122 «Комп’ютерні науки» /КПІ ім. Ігоря Сікорського ; Ю. А. Тарнавський, І. М. Кузьменко. – Електронні текстовідані (1 файл: 45,7 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2018. – 259 с.
11. Порядок зіставлення компонентів довіри до безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99 : НД ТЗІ 2.6-003-2015.
12. Порядок зіставлення функціональних компонентів безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99 : НД ТЗІ 2.6-002-2015.
13. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі : НД ТЗІ 3.7-003-05.
14. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР. – URL: https://zakon.rada.gov.ua/laws/show/80/94-вр
15. Технічний захист інформації. Комп’ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу : НД ТЗІ 3.6-001-2000.