Тема 3. Цифрова безпека на персональному рівні

1. Публічна і персональна інформація: характеристика понять

2. Законодавство України про публічну інформацію та захист персональних даних. Стратегія формування цифрової грамотності серед населення України та цифрових компетентностей у професійній сфері

3. Найпоширеніші цифрові загрози, моделювання ризиків та основні кроки захисту персональних даних

4. Особливості документообігу та комунікації з точки зору цифрової безпеки в професійній діяльності

5. Безпекові правила роботи з організаційними соцмережами та сайтами

6. Кібератаки на громадянське суспільство та державний сектор – захист від фішингу

2. Законодавство України про публічну інформацію та захист персональних даних. Стратегія формування цифрової грамотності серед населення України та цифрових компетентностей у професійній сфері

КОНЦЕПЦІЯ
розвитку цифрових компетентностей

Із збільшенням темпів розвитку цифрових технологій, впровадженням інноваційних рішень у всіх сферах суспільного життя виникає необхідність у підвищенні якості підготовки працівників для створення можливості модернізації економіки країни відповідно до сучасних вимог.

Відсутність концептуальних засад формування державної політики у сфері розвитку цифрових навичок та цифрових компетентностей громадян не дозволяє забезпечити розвиток усіх сфер суспільного життя відповідно до сучасних вимог, процесів глобальної цифровізації економіки, сфер життєдіяльності суспільства, які відбуваються у більшості країн світу.

Таким чином, виникає необхідність забезпечення готовності суспільства до таких процесів, опанування ним ключових комбінацій знань, умінь, навичок, способів мислення, поглядів, інших особистих якостей у сфері інформаційно-комунікаційних та цифрових технологій (цифрова компетентність).

Так, цифровою компетентністю є динамічна комбінація знань, умінь, навичок, способів мислення, поглядів, інших особистих якостей у сфері інформаційно-комунікаційних та цифрових технологій, що визначає здатність особи успішно соціалізуватися, провадити професійну та/або подальшу навчальну діяльність із використанням таких технологій.

Законом України "Про освіту" визнано інформаційно-комунікаційну компетентність як одну з ключових компетентностей, необхідних кожній сучасній людині для успішної життєдіяльності.

Державною стратегією регіонального розвитку на 2021-2027 роки, затвердженою постановою Кабінету Міністрів України від 5 серпня 2020 р. № 695 (Офіційний вісник України, 2020 р., № 67, ст. 2155), серед інших загальнодержавних викликів, що стримують розвиток регіонів і держави в цілому, визначено низький рівень цифровізації регіонів і цифрової обізнаності.

Державний стандарт базової середньої освіти, затверджений постановою Кабінету Міністрів України від 30 вересня 2020 р. № 898 "Про деякі питання державних стандартів повної загальної середньої освіти" (Офіційний вісник України, 2020 р., № 81, ст. 2615), визначає інформаційно-комунікаційну компетентність такою, що передбачає впевнене, критичне і відповідальне використання цифрових технологій для власного розвитку і спілкування; здатність безпечно застосовувати інформаційно-комунікаційні засоби в навчанні та інших життєвих ситуаціях, дотримуючись принципів академічної доброчесності.

Концепцією розвитку цифрової економіки та суспільства України на 2018-2020 роки, схваленою розпорядженням Кабінету Міністрів України від 17 січня 2018 р. № 67 (Офіційний вісник України, 2018 р., № 16, ст. 560), визначено створення та виконання національної програми

навчання загальним і професійним цифровим компетенціям та знанням як одне з пріоритетних завдань на шляху до прискореного розвитку цифрової економіки.

Досвід європейських країн свідчить про суттєвий вплив здійснених заходів щодо цифрових компетентностей населення на розвиток економіки та конкурентоспроможність країн ЄС на міжнародному рівні.

Так, Європейський Парламент і Рада ЄС 22 травня 2018 р. ухвалили Рамкову програму оновлених ключових компетентностей для навчання впродовж життя (2018/С 189/01), в якій цифрова компетентність визнана однією з восьми ключових компетентностей для повноцінного життя та діяльності громадян ЄС.

Положеннями Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони, ратифікованої Законом України від 16 вересня 2014 р. № 1678-VII, передбачено сприяння її сторін розвитку співробітництва в галузі освіти, навчання та молодіжної політики.

З огляду на необхідність забезпечення реалізації стратегічного курсу держави на набуття повноправного членства України в ЄС потребує також і подальшої адаптації законодавство України із законодавством ЄС.

Проблеми, які потребують розв'язання

На сьогодні здійснюється значна кількість освітніх заходів, спрямованих на формування цифрових навичок, проте вони не мають системного характеру, забезпечують формування лише окремих навичок та не вирішують питань низького рівня володіння цифровими навичками в суспільстві та обізнаності щодо цифрових прав громадян.

Основними проблемами з питань розвитку цифрових компетентностей, які потребують розв'язання в рамках цієї Концепції, є відсутність:

правового регулювання питань розвитку цифрових компетентностей;

системи та опису цифрової компетентності (рамки цифрової компетентності), а також вимог до рівнів володіння цифровими навичками та цифровими компетентностями різних категорій працівників;

єдиних підходів до визначення цифрових компетентностей у професійних стандартах та єдиних вимог до освітніх програм з розвитку інформаційно-цифрової компетентності фахівців різних професій;

єдиних вимог до цифрових компетентностей в системі освіти;

вимог до цифрової компетентності в професійних стандартах;

системи індикаторів для моніторингу стану розвитку цифрових навичок та цифрових компетентностей;

координації дій на рівні органів виконавчої влади та органів місцевого самоврядування під час реалізації державної політики у сфері розвитку цифрових навичок та цифрових компетентностей;

системи сертифікації рівня цифрових компетентностей.

Мета і строки реалізації Концепції

Основною метою цієї Концепції є визначення пріоритетних напрямів і основних завдань з питань розвитку цифрових навичок та цифрових компетентностей, підвищення рівня цифрової грамотності населення, зокрема працездатних осіб, громадян похилого віку, малозабезпечених сімей, осіб з інвалідністю, інших вразливих груп населення, в умовах розвитку цифрової економіки та цифрового суспільства.

Реалізація цієї Концепції передбачена на період до 2025 року.

Основні завдання Концепції

Основними завданнями цієї Концепції є:

формування та розвиток цифрових навичок та цифрових компетентностей в суспільстві, що сприятимуть розвитку цифрової економіки та суспільства, а також розвитку електронної демократії і людського капіталу;

забезпечення правового регулювання з питань формування державної політики у сфері розвитку цифрових навичок та цифрових компетентностей громадян;

розроблення комплексних змін до законодавства, що забезпечить визначення цифрової освіти, цифрових навичок та цифрових компетентностей у сферах суспільного життя;

визначення системи та опису складових цифрової компетентності (рамки цифрової компетентності), а також вимог до рівня володіння цифровими навичками та цифровими компетентностями різних категорій працівників, зокрема в професійних стандартах;

забезпечення координації дій на рівні органів виконавчої влади з питань розвитку цифрових навичок та цифрових компетентностей;

створення індикаторів для моніторингу стану розвитку цифрових навичок та цифрових компетентностей;

підвищення рівня обізнаності громадян щодо небезпек в Інтернеті.

Шляхи та способи розв'язання проблем

Під час реалізації Концепції необхідно забезпечити розв'язання визначених проблем відповідно до поставлених завдань.

Формування і розвиток цифрових навичок та цифрових компетентностей в суспільстві здійснюється шляхом:

здобуття особою цифрової освіти з використанням інформаційних ресурсів, нових освітніх технологій та цифрових освітніх ресурсів, спрямованих на підвищення рівня цифрових навичок та цифрових компетентностей;

забезпечення безперервного розвитку професійних цифрових компетентностей для фахівців в системі підвищення кваліфікації різних галузей діяльності;

створення Єдиного державного веб-порталу цифрової освіти "Дія. Цифрова освіта";

розроблення заходів щодо впровадження цифрових засобів доведення інформації (телебачення, соціальні мережі, трансляція в Інтернеті тощо).

Підвищення рівня обізнаності громадян щодо небезпек в Інтернеті здійснюється шляхом:

створення соціальних ініціатив, спрямованих на підвищення рівня цифрових навичок та цифрових компетентностей для представників різних цільових груп населення;

запровадження програм, спрямованих на підвищення рівня обізнаності дітей та підлітків, цифрових компетентностей батьків та педагогічних працівників щодо небезпек дитини у цифровому середовищі, формування культури нетерпимого ставлення до порушення прав, свобод, безпеки дитини в цифровому середовищі.

Забезпечення правового регулювання з питань формування державної політики у сфері розвитку цифрових навичок та цифрових компетентностей, а також розроблення комплексних змін до законодавства, що забезпечить визначення цифрової освіти, цифрових навичок та цифрових компетентностей у сферах суспільного життя, здійснюється шляхом:

правового регулювання питань розвитку цифрових навичок та цифрових компетентностей;

удосконалення професійних стандартів з урахуванням затверджених рамок професійних цифрових компетентностей;

запровадження сертифікації цифрових навичок;

розроблення програм підготовки, перепідготовки та підвищення кваліфікації фахівців відповідно до професійних рамок цифрових компетентностей.

Визначення системи та опису складових цифрової компетентності (рамки цифрової компетентності) здійснюється шляхом:

розроблення та затвердження опису цифрової компетентності, який визначає ключові поняття, структуру цифрової компетентності за сферами, обсяг знань, умінь і практичних навичок громадян, рівні володіння цифровою компетентністю та може використовуватися з метою визнання, планування, формування, розвитку та вдосконалення цифрової компетентності громадян і працівників основних професійних груп різних сфер економічної діяльності (рамка цифрової компетентності);

запровадження вимог до рівнів володіння професійними цифровими компетентностями при наймі персоналу, під час виконання професійних та службових обов'язків, проведення сертифікації, атестації тощо;

розроблення рамок професійних цифрових компетентностей для основних професійних груп за сферами економічної діяльності та методичних рекомендацій щодо їх застосування.

Забезпечення координації дій на рівні органів виконавчої влади з питань розвитку цифрових навичок та цифрових компетентностей здійснюється шляхом залучення Міжгалузевої ради з питань цифрового розвитку, цифрових трансформацій і цифровізації, яку утворено відповідно до

постанови Кабінету Міністрів України від 8 липня 2020 р. № 595 “Про утворення Міжгалузевої ради з питань цифрового розвитку, цифрових трансформацій і цифровізації” (Офіційний вісник України, 2020 р., № 59, ст. 1855).

Створення індикаторів для моніторингу стану розвитку цифрових навичок та цифрових компетентностей здійснюється шляхом:

розроблення методології проведення досліджень з питань розвитку цифрових навичок та цифрових компетентностей;

проведення досліджень рівня цифрової грамотності різних груп населення, зокрема випускників шкіл та студентів закладів освіти, педагогічних працівників, державних службовців;

прогнозування потреб роботодавців у певних цифрових навичках працівників основних професійних груп.

Прогноз впливу на ключові інтереси заінтересованих сторін

Формування та реалізація державної політики у сфері розвитку цифрових навичок та цифрових компетентностей громадян матиме вплив на ключові інтереси громадян, суб’єктів господарської діяльності, органів виконавчої влади.

Реалізація цієї Концепції матиме позитивний вплив щодо забезпечення правового регулювання, спрямованого на розвиток цифрових навичок та цифрових компетентностей, визначення напрямів і основних завдань у зазначеній сфері, підвищення рівня цифрової грамотності населення, підвищення ефективності використання цифрових технологій та електронних послуг, підвищення рівня безпеки громадян у цифровому середовищі і прискорення процесів цифрової трансформації в економіці та суспільстві України, що сприятиме розвитку цифрової економіки та конкурентоспроможності країни в цілому.

Очікувані результати

Реалізація цієї Концепції дасть змогу:

прискорити процеси цифрової трансформації в Україні;

суттєво підвищити рівень цифрових навичок та цифрових компетентностей в суспільстві, а також рівень конкурентоспроможності держави та якість людського капіталу;

підвищити конкурентоспроможність працівників шляхом оволодіння новими цифровими навичками та цифровими компетентностями;

підвищити рівень доступності до державних послуг для громадян похилого віку, осіб з інвалідністю, малозабезпечених сімей, інших вразливих груп населення;

суттєво зменшити ризики виникнення небезпек під час користування Інтернетом;

запровадити правове регулювання з питань формування державної політики у сфері розвитку цифрових навичок та цифрових компетентностей громадян;

розробити комплексні зміни до законодавства, що забезпечить визначення цифрової освіти, цифрових навичок та цифрових компетентностей у сферах суспільного життя;

визначити систему та опис складових цифрової компетентності (рамки цифрової компетентності), а також вимог до рівня володіння цифровими навичками та цифровими компетентностями різних категорій працівників, зокрема в професійних стандартах;

забезпечити координацію дій на рівні органів виконавчої влади з питань розвитку цифрових навичок та цифрових компетентностей;

створити індикатори для моніторингу стану розвитку цифрових навичок та цифрових компетентностей.

Обсяг фінансових, матеріально-технічних, трудових ресурсів

Фінансування заходів з реалізації цієї Концепції здійснюється за рахунок та в межах коштів Державного бюджету України на відповідний рік, а також інших джерел, не заборонених законодавством.

Обсяги видатків на реалізацію заходів цієї Концепції уточнюються щороку з урахуванням можливостей державного бюджету, конкретизації заходів за підсумками їх виконання у попередні роки.

3. Найпоширеніші цифрові загрози, моделювання ризиків та основні кроки захисту персональних даних

Перш ніж перейти безпосередньо до цифрових, або ж інформаційних загроз ми розглянемо поняття інформаційна безпека.

Під **інформаційною безпекою** розуміють захищеність інформації і підтримуючої інфраструктури від випадкових або навмисних впливів природного або штучного характеру, що можуть завдати неприйнятного збитку суб'єктам інформаційних відносин, в тому числі власникам і користувачам інформації і підтримуючої інфраструктури.

Захист інформації – комплекс заходів, спрямованих на забезпечення інформаційної безпеки. Аналізуючи підходи до проблем інформаційної безпеки, необхідно починати з виявлення суб'єктів інформаційних відносин та інтересів цих суб'єктів, пов'язаних з використанням інформаційних систем (ІС). Загрози інформаційної безпеки пов'язані з використанням інформаційних технологій.

Інформаційна безпека залежить від усього комплексу заходів та сучасних технологій, керування якими відбувається із застосуванням різноманітних інформаційних систем.

Інформаційна безпека – багатогранна, багатовимірна діяльність, в якій успіх може принести тільки системний, комплексний підхід. Безпека використання інформаційних систем полягає у забезпеченні доступності, цілісності, конфіденційності та підтримці інформаційних ресурсів її інфраструктури.

До **основних складових інформаційної безпеки** належить конфіденційність, тобто захист від несанкціонованого доступу до інформації.

При аналізі проблематики, пов'язаної з інформаційною безпекою, необхідно враховувати специфіку даного аспекту безпеки, яка полягає в тому, що інформаційна безпека є складова частина інформаційних технологій – області, що розвивається безпрецедентно високими темпами. Тут важливі не стільки окремі рішення (закони, навчальні курси, програмно-технічні вироби), що знаходяться на сучасному рівні, скільки механізми генерації нових рішень, що дозволяють жити в темпі технічного прогресу.

Складність механізмів прийняття сучасних управлінських рішень щодо захисту інформації в новому інформаційному середовищі пов'язана із застосуванням стрімко розвиваючих інформаційних систем, призначених для великого обсягу обробки, обміну та використання їх в сучасному житті кожної особистості, підприємства, держави, світі, а також швидкими темпами розвитку технічних засобів.

Загрозу можна розглядати як атаку та можливість порушення інформаційної безпеки і посягання на заволодіння інформацією, а той, хто посягає на інформацію є зловмисником. Загроза проявляються через низький захист або знаходження вразливих місць у системі захисту інформаційних систем.

Основними завданнями системи інформаційної безпеки є:

- виявлення та усунення загроз безпеки нанесенню економічного, фінансового, матеріального та морального збитку;
- створення механізмів реагування на загрози розвитку і функціонуванню

підприємства та національній безпеці;

- прийняття заходів щодо забезпечення безпеки персоналу підприємства та інше.

Поняття інформаційної безпеки включає:

– надійність роботи комп'ютера;

– збереження цілісності даних;

– захист інформації від несанкціонованого доступу;

– таємниця електронного листування.

Інформаційні загрози можуть бути обумовлені:

– природними факторами;

– людськими факторами.

До природніх факторів відносяться такі джерел загроз, які об'єднують, обставини, що становлять непереборну силу, тобто такі обставини, що носять об'єктивний і абсолютний характер, поширюється на всіх. До непереборної сили в законодавстві і договірній практиці відносять стихійні лиха або інші обставини, що неможливо передбачити або запобігти, або можливо передбачити, але неможливо запобігти при сучасному рівні людського знання і можливостей. Такі джерела загроз абсолютно не піддаються прогнозуванню і тому заходи захисту від них повинні застосовуватися завжди.

Стихійні джерела потенційних загроз інформаційній безпеці, як правило, є зовнішніми по відношенню до тих, що захищаються і під ними розуміються насамперед природні катаклізми (пожежі, землетруси, повені, урагани, різні непередбачені обставини, незрозумілі явища та інші форс-мажорні обставини)

До людських факторів відносяться:

– загрози випадкового характеру (помилки обробки, передачі, обміну інформації);

– загрози навмисного характеру (несанкціонований доступ до інформації).

Навмисні загрози призводять до шкідливих наслідків користувачам автоматизованих інформаційних систем і можуть бути активні і пасивні.

Пасивні загрози спрямовані на несанкціоноване використання інформаційних ресурсів і не впливають на функціонування системи (прослуховування).

Активні загрози спрямовані на порушення нормального процесу функціонування системи через вплив на апаратні, програмні та інформаційні ресурси. Джерелами активних загроз можуть бути безпосередні дії зловмисників, програмні віруси і т.п.

Загрози інформаційної безпеки класифіковані за різними ознаками.

1. За аспектом інформаційної безпеки, на який спрямовані загрози.

– *Загрози конфіденційності* (неправомірний доступ до інформації).

– *Загроза порушення конфіденційності* полягає в тому, що інформація стає відомою тому, хто не має повноважень доступу до неї. Вона має місце, коли отримано доступ до деякої інформації обмеженого доступу, що зберігається в обчислювальній системі чи переданої від однієї системи до іншої. У зв'язку з загрозою порушення конфіденційності, використовується термін «витік». Подібні загрози виникають внаслідок «людського фактору» (наприклад, випадкове делегування тому чи іншому користувачеві привілеїв іншого користувача), збоїв в роботі програмних і апаратних засобів.

– *До інформації обмеженого доступу належить державна таємниця* і *конфіденційна інформація* (комерційна таємниця; персональні дані; професійні види таємниць: лікарська, адвокатська, банківська, службова, нотаріальна, таємниця страхування, слідства і судочинства, листування, телефонних переговорів, поштових відправлень, телеграфних або інших повідомлень (таємниця зв'язку); відомості про сутність винаходу, корисної моделі чи промислового зразка до офіційної публікації (ноу-хау) і ін.).

– *Загрози цілісності (неправомірна зміна даних)*. Загрози порушення цілісності – загрози, пов'язані з імовірністю модифікації тієї чи іншої інформації, що зберігається в інформаційній системі. Порушення цілісності може бути викликано різними факторами – від навмисних дій персоналу до виходу з ладу обладнання.

– *Загрози доступності* (здійснення дій, що унеможливлюють чи утруднюють доступ до ресурсів інформаційної системи). Порушення доступності є створення таких умов, при яких доступ до послуги або інформації буде або заблокований, або можливий за час, який не забезпечить виконання тих чи інших бізнес-цілей.

2. За розташуванням джерела загроз:

– внутрішні (джерела загроз розташовуються всередині системи);

– зовнішні (джерела загроз знаходяться поза системою).

Внутрішні загрози:

– виток інформації;

– неавторизований доступ.

Зовнішні загрози:

– шкідливі програми (віруси, трояни, черв'яки і т.п.);

– атаки хакерів;

– Ddos-атаки;

– таргінг атаки;

– спам;

– фішинг;

– промислові загрози (stuxnet, flame, duqu);

– шпигунське програмне забезпечення (spyware, adware);

– botnets (ботнети або зомбі-мережі).

3. За розмірами завдання шкоди:

– загальні (нанесення збитку об'єкту безпеки в цілому, заподіяння значної шкоди);

– локальні (заподіяння шкоди окремим частинам об'єкта безпеки);

– приватні (заподіяння шкоди окремим властивостям елементів об'єкта безпеки).

4. За ступенем впливу на інформаційну систему:

– пасивні (структура і зміст системи не змінюються);

– активні (структура і зміст системи піддається змінам).

5. За природою виникнення:

– *природні (об'єктивні)* – викликані впливом на інформаційне середовище об'єктивних фізичних процесів або стихійних природних явищ, що не залежать від волі людини;

– *штучні (суб'єктивні*) – викликані впливом на інформаційну сферу

людини. Серед штучних загроз в свою чергу виділяють:

– *ненавмисні (випадкові) загрози* – помилки програмного забезпечення, персоналу, збої в роботі систем, відмови обчислювальної і комунікаційної техніки;

– *навмисні (умисні) загрози* – неправомірний доступ до інформації, розробка спеціального програмного забезпечення, що використовується для здійснення незаконного втручання, розробка та поширення вірусних програм і т.і. Навмисні загрози обумовлені діями людей.

Основні проблеми інформаційної безпеки пов'язані, перш за все, з навмисними загрозами, так як вони є головною причиною злочинів і правопорушень.

Цілісність інформаційних даних означає здатність інформації зберігати початковий вигляд і структуру як в процесі зберігання, так і після неодноразової передачі. Вносити зміни, видаляти або доповнювати інформацію вправі тільки власник або користувач з легальним доступом до даних.

Конфіденційність – характеристика, що вказує на необхідність обмеження доступу до інформаційних ресурсів для певного кола осіб. У процесі дій і операцій інформація стає доступною тільки користувачам, які включені в інформаційні системи і успішно пройшли ідентифікацію.

Доступність інформаційних ресурсів означає, що інформація, яка знаходиться у вільному доступі, надається повноправним користувачам ресурсів своєчасно і безперешкодно.

Достовірність вказує на приналежність інформації довіреній особі або власнику, який одночасно виступає в ролі джерела інформації.

Забезпечення і підтримка інформаційної безпеки включають комплекс різнопланових заходів, що запобігають, відстежують і усувають несанкціонований доступ третіх осіб. Заходи інформаційної безпеки спрямовані також на захист від пошкоджень, спотворень, блокування або копіювання інформації. Принципово, щоби всі завдання вирішувалися одночасно – тільки тоді забезпечується повноцінний, надійний захист.

Класифікація вразливостей систем безпеки

Загрози інформаційної безпеки проявляються не самостійно, а через можливу взаємодію з найбільш слабкими ланками системи захисту, тобто через фактори уразливості. Загроза призводить до порушення діяльності систем на конкретному об'єкті-носії.

Основні вразливості виникають внаслідок дії наступних факторів:

– недосконаліть програмного забезпечення, апаратної платформи;

– різні характеристики будови автоматизованих систем в інформаційному потоці;

– частина процесів функціонування систем є неповноцінною;

– неточність протоколів обміну інформацією та інтерфейсу;

– складні умови експлуатації і розташування інформації.

Найчастіше джерела загрози запускаються з метою отримання незаконної вигоди внаслідок заподіяння шкоди інформації. Але можливі і випадкові загрози через недостатні міри захисту і дії масового загрозливого фактору.

Існує поділ вразливостей за класами:

– об’єктивні;
– випадкові;
– суб’єктивні.

Якщо усунути або, як мінімум, послабити вплив вразливостей, можна уникнути повноцінної загрози, спрямованої на систему зберігання інформації.

Таким чином, класифікація погроз ІБ розподіляється за характером загрози, видом впливу, джерелом та об’єктом загрози.

Дослідники виділяють три основних види погроз безпеки:
– загрози розкриття;
– загрози цілісності;
– загрози відмови в обслуговуванні.

Загроза розкриття полягає в тому, що інформація стає відомою тому, кому не варто було б її знати. У термінах комп’ютерної безпеки загроза розкриття має місце щоразу, коли отриманий доступ до певної конфіденційної інформації, що зберігається в ІС, або передається від однієї системи до іншої.

Загроза цілісності включає будь-яку навмисну зміну (модифікацію або навіть видалення) даних, що зберігаються в ІС, або передаються з однієї системи до іншої. Зазвичай вважається, що загрозі розкриття піддаються більшою мірою державні структури, а загрозі цілісності – ділові або комерційні структури.

Загроза відмови в обслуговуванні виникає щоразу, коли в результаті деяких дій блокується доступ до певного ресурсу ІС. Реальне блокування може бути постійним, так щоб запитуваний ресурс ніколи не був отриманий, або блокування може викликати тільки затримку запитуваного ресурсу, досить тривалу для того, щоб він став непридатним. У таких випадках кажуть, що ресурс вичерпаний.

Крім того, пропонується наступна класифікація погроз ІБ. Хоча єдиної й загальноприйнятої класифікації погроз ІБ не існує й, швидше за усе, не буде взагалі, тому що згодом з’являються нові загрози, які все складніше ідентифікувати.

Найпоширеніші dos атаки (відмова в обслуговуванні).

1. Ping-of-Death.

Посилає ICMP-пакет, розміром більше 64 Кб, що може призвести до переповнення буфера операційної системи і виведення системи, що атакується, з ладу.

2. SYN Flood .

Дуже швидко посилає велику кількість TCP SYN-пакетів (які ініціюють з’єднання), залишаючи жертву чекати величезну кількість з’єднань і викликаючи таким чином посилене завантаження ресурсів і відмову від санкціонованих з’єднань.

3. Land/Latierra.

Посилає підроблений SYN-пакет з ідентичними вихідною адресою та кінцевим портом так, що система рухається по нескінченній петлі, намагаючись виконати TCP-з’єднання.

4. WinNuke.

Посилає OOB/URG-дані для TCP-з’єднання із портом 139 (NetBIOS Session/SMB), що призводить до зависання ОС Windows. Найбільшому впливу піддається ОС Windows 95, пізніші версії ОС Windows мають проти цієї атаки

відповідний захист.

Найпоширеніші процеси сканування

1. Ping sweeps.

Протягом цього простого процесу сканування діапазон IP-адрес аналізується утилітою ping (так зване пінгування) з метою визначення активних комп'ютерів. Слід зауважити, що більшість складних сканерів буде використовувати інші протоколи (такі, як SNMP sweep), щоб виконувати ту ж саму дію.

2. TCP-сканування.

Зондування відкритих TCP-портів у пошуках сервісів, які може використовувати порушник. Сеанси сканування можуть використовувати звичайні TCP-з'єднання або приховані (stealth) сеанси сканування, що використовують наполовину відкриті з'єднання (для того, щоби захистити їх від реєстрації в журналах) або FIN-сеанси сканування (ніколи не відкривають порт, але тестують, якщо щось прослуховується). Сеанси сканування можуть бути послідовними або випадковими, або зконфігуровані за переліком портів.

3. UDP-сканування.

Ці сеанси сканування є складнішими, тому що (User Datagram Protocol) UDP- працює без встановлення віртуального з'єднання. Метод полягає в тому, щоби послати «сміттєвий» UDP-пакет до наміченого порту. Більшість машин будуть реагувати за допомогою ICMP-повідомлення «destination port unreachable», яке вказує, що на даному порту немає сервісу, який прослуховується. Однак багато комп'ютерів «поглинають» ICMP повідомлення, тому ви не зможете здійснювати швидке UDP-сканування.

4. Ідентифікація ОС.

Шляхом посилання неприпустимих (або дивних) ICMP або TCP-пакетів порушник може ідентифікувати ОС. Стандарти зазвичай встановлюють, яким чином комп'ютери повинні реагувати на легальні пакети, тому машини мають тенденцію бути однаковими у своїй реакції на припустимі вхідні дані. Однак стандарти упускають (як правило навмисно) реакцію на неприпустимі вхідні дані. Таким чином, унікальні реакції кожної ОС на неприпустимі вхідні дані формують сигнатуру, яку хакери можуть використовувати для того, щоби зрозуміти, під чиїм управлінням функціонує обраний комп'ютер. Цей тип діяльності має місце на нижньому рівні (начебто прихованих сеансів TCPсканування), на якому аналізовані системи не реєструють події.

Сучасні загрози

Носіями загроз інформаційній безпеці є джерела загроз, якими виступають як суб'єктивні (особистості), так і об'єктивні обставини (конкуренти, злочинці, корупціонери, адміністративно-управлінські органи, інше). Джерела загроз переслідують при цьому наступні цілі: ознайомлення з відомостями які охороняють, їх модифікація в корисливих цілях і знищення для нанесення прямих матеріальних збитків.

Всі джерела загроз інформаційній безпеці можна розділити на три основні групи.

Обумовлені діями суб'єкта (антропогенні джерела) – суб'єкти, дії яких призводять до порушення безпеки інформації, кваліфікуються як умисні або випадкові злочини.

Джерела, дії яких можуть призвести до порушення безпеки інформації можуть бути як зовнішніми так і внутрішніми. Дані джерела можна зпрогнозувати, і вжити адекватних заходів.

Обумовлені технічними засобами (техногенні джерела) – ці джерела загроз менш прогнозовані, безпосередньо залежать від властивостей техніки і тому вимагають особливої уваги. Дані джерела загроз інформаційній безпеці, також можуть бути як внутрішніми, так і зовнішніми.

Стихійні джерела – дана група об'єднує обставини, що становлять непереборну силу (стихійні лиха або інші обставини, що неможливо передбачити або запобігти, або можливо передбачити, але неможливо запобігти). Ці обставини, що носять об'єктивний і абсолютний характер, поширюється на всіх. Такі джерела загроз абсолютно не піддаються прогнозуванню і, тому заходи проти них повинні застосовуватися завжди. Стихійні джерела, як правило, є зовнішніми по відношенню до інформаційних джерел що захищаються і під ними, як правило, розуміються природні катаклізми.

Загроза безпеці комп'ютерної системи – це потенційно можлива подія, незалежно від того, навмисна чи ні, що може здійснити небажаний вплив на саму систему, а також на інформацію, що зберігається в ній.

Вразливість комп'ютерної системи – це якась її невдала характеристика, що уможливлює виникнення загрози. Інакше кажучи, саме через наявність вразливостей у системі відбуваються небажані події.

Атака на комп'ютерну систему – це дія, що вчиняється зловмисником і полягає в пошуку й використанні загрози або іншої вразливості. Таким чином, атака – це реалізація загрози. Слід зауважити, що таке тлумачення атаки (за участю людини, яка має злий намір), виключає присутній у визначенні загрози елемент випадковості. Але, як показує досвід, часто буває неможливо розрізнити навмисні й випадкові дії, і надійна система захисту повинна адекватно реагувати на кожне з них.

Більш детально розглянемо особливості зовнішніх загроз.

1. Хакерські атаки.

Отримавши доступ до системи, вони направлені на крадіжку конфіденційних даних або встановлюють шкідливі програми та використовують "взламані" комп'ютери для розсилки спаму. В програми закрадаються помилки, що робить їх уразливими для атаки. Хакерам ці лазівки дозволяють проникнути в систему, а ті, хто пише віруси, використовують помилки в коді додатків, щоб забезпечити автоматичний запуск на комп'ютері шкідливих програм.

Хакери – це електронні "взламники", які проникають в комп'ютерну систему, використовуючи особливі уразливі лазівки у програмному забезпеченні. Захиститися від них можна за допомогою особливого додатку – мережевого екрану з пакетною фільтрацією, що входить до складу антивірусних програм і робить комп'ютер невидимим для хакерів.

Для захисту від шкідливого коду і хакерських атак:

– встановлюється антивірусна програма;

– встановлюється оновлення ОС Windows (Update), що відповідає за безпеку;

– увага при роботі зі спамом в електронній пошті і системах миттєвих повідомлень;

– збереження резервної копії (BackUp) даних.

2. Технологія інфраструктури відкритих ключів.

Технологія інфраструктури відкритих ключів дозволяє перевіряти і засвідчувати справжність користувача. Інфраструктура відкритих ключів або PKI забезпечує єдину ідентифікацію, аутентифікацію і авторизацію користувачів системи, додатків і процесів і разом з цим гарантує доступність, цілісність і конфіденційність інформації. Інфраструктура PKI являє собою систему цифрових сертифікатів, носіями яких є USB-ключі або смарт-карти.

При використанні індивідуального секретного пароля і засобів криптографічного захисту, цифрові сертифікати отримують роль електронних паспортів. Використання в корпоративній мережі технології інфраструктури відкритих ключів значно підвищує безпеку всієї мережі в цілому, так як дозволяє відмовитися від використання парольної аутентифікації користувачів всередині, а також забезпечує безпечний доступ віддалених користувачів в систему. Основними носіями інформації є USB-ключі та смарт-карти.

Користувачам не треба запам'ятовувати складні паролі і періодично їх міняти – досить підключити електронний ключ або смарт-карту і ввести PIN-код.

3. Системи одноразових паролів.

Системи багатофакторної аутентифікації засновані на технології одноразових паролів (one time password) OTP призначені для аутентифікації мобільних користувачів, які відрізняється простотою у використанні, установці і адмініструванні.

Дана технологія заснована на тому, що пароль користувача не постійний і змінюється з плином часу спеціальним пристроєм (апаратним або програмним) – токеном. Дане рішення широко використовується в системах віддаленого доступу, в тому числі системах клієнт-банк, для аутентифікації користувачів при доступі з недовірених середовища (Інтернет-кафе, бізнес-центри, і т.д.).

OTP-токен – мобільний персональний пристрій, що належить певному користувачеві і генерує одноразові паролі, які використовуються для аутентифікації даного користувача. OTP-токени мають невеликий розмір і випускаються у вигляді: кишенькового калькулятора; брелока; смарт-карти; пристрою, комбінованого з USB-ключем; спеціального програмного забезпечення для кишенькових комп'ютерів. Як приклад рішень OTP, можна привести лінійку RSA SecurID, ActivCard Token, комбінований USB-ключ Aladdin eToken NG-OTP.

Структура системи:

– сервер аутентифікації (баз даних акаунтів, прив'язаних до пристроїв, синхронізація за часом);

– канал передачі;

– форма для введення аутентифікаційних даних (зазвичай три поля (Login, OTP, PIN));

– клієнтська частина (OTP брелок і ін.).

4. Біометричні системи.

Біометричні системи – це вимірні фізіологічні або поведінкові дані людини. Біометричні дані унікальні для кожної людини і їх можна використовувати для встановлення особи або перевірки декларованих особистих даних:

– для ідентифікації користувача (замість введення імені користувача);

– для однофакторної аутентифікації користувача;

– спільно з паролем або аутентифікаційї токеном (таким, як смарткарта) для забезпечення двофакторної аутентифікації.

Біометричні дані діляться на групи:

1. Фізіологічні біометричні характеристики – засновані на даних, отриманих шляхом вимірювання анатомічних характеристик людини, таких, як відбиток пальця, форма обличчя або кисті, сітківка ока.

2. Поведінкові біометричні характеристики (динамічні) – засновані на даних, отриманих шляхом вимірювання дій людини. Характерною рисою для поведінкових характеристик є їх протяжність в часі – вимірюється дією, що має початок, середину і кінець. Наприклад, голос, підпис.

5. Криптографічний захист даних.

Криптографія – область знань, що вивчає тайнопис (криптографія) і методи його розкриття (криптоаналіз). Криптографія вважається розділом математики.

Мета криптографічної системи полягає в тому, щоби зашифрувати вихідний текст (шифртекст, криптограма).

Одержувач, якому він призначений, повинен бути здатний розшифрувати («дешифрувати») цей шифртекст, відновивши, таким чином, відповідний йому відкритий текст. При цьому зловмисник повинен бути нездатний розкрити вихідний текст.

Існує відмінність між розшифрування (дешифрованием) і розкриттям шифртексту. Широко відомим історичним прикладом криптосистеми є так званий шифр Цезаря, що представляє з себе просту заміну кожної букви відкритого тексту третьої наступної за нею буквою алфавіту (з циклічним перенесенням, коли це необхідно). Наприклад, «A» замінювалося на «D», «B» на «E», «Z» на «C».

Всі методи шифрування поділяються на дві групи:

– шифри з секретним ключем (симетрична схема);

– шифри з відкритим ключем (асиметрична схема).

Перший тип шифрів має на увазі наявність інформації (ключа), володіння якою дозволяє як зашифрувати, так і розшифрувати повідомлення. Шифри з відкритим ключем – відкритого і закритого типу; один використовується для шифрування, інший для розшифровки повідомлень.

Основні напрямки шифрування:

– шифрування даних на локальних дискових системах (клієнтське шифрування);

– криптографічний алгоритм (шифр) – математичний спосіб обробки інформації для приховування її змісту.

Основні тенденції застосування шифрування:

– шифрування окремих файлів;

– шифрування окремих розділів на жорсткому диску, віртуальних дисків;

– шифрування жорстких дисків цілком.

6. Електронний підпис (ЕП).

Електронний підпис – послідовність символів, отримана в результаті криптографічного перетворення вихідної інформації з використанням закритого ключа ЕЦП, яка дозволяє підтверджувати цілісність і незмінність цієї інформації, а також її авторство за умови використання відкритого ключа ЕП і його

сертифіката.

Цифровий підпис забезпечує:

– вихідні джерела документа. Залежно від деталей визначення «документа» можуть бути підписані такі поля як автор, внесені зміни, мітка часу т.і.;

– захист від змін документа. При будь-якому випадковому або навмисному зміні документа (або підпису) зміниться хеш (хеш-функція або геш-функція – функція, що перетворює вхідні дані будь-якого розміру в дані фіксованого розміру), отже підпис стане недійсним;

– неможливість відмови від авторства. Так як створити коректний підпис можна лише знаючи закритий ключ, а він відомий тільки власнику, то власник не може відмовитися від свого підпису під документом.

Для підпису документа з початку обчислюється значення хеш-функції для документа, а потім це значення за спеціальним криптоалгоритмом підписується секретним ключем автора документа.

Для перевірки справжності документа необхідно за допомогою відкритого ключа перевірити підпис, потім обчислити його хеш-значення і порівняти з підписаним контрольним підписом. Якщо обидва значення збігаються, то підпис вірний, інакше документ недійсний.

Інформаційні ризики

Сучасні системи спеціального призначення характеризуються наявністю в своєму складі інформаційних систем (ІС). Реалії часу диктують необхідність в умовах обмеженої можливості фінансування розробки ІС отримати оцінку розумної достатності захищеності таких ІС від ризиків. Класичне визначення ризику визначає його як комбінацію ймовірності події та її наслідків [ISO Guide 73: 2002]. Серед різновидів ризиків українські та зарубіжні автори виділяють операційний ризик відповідно до Базель III (Базель III - документ Базельського комітету з банківського нагляду, що містить методичні рекомендації в області банківського регулювання), що визначається ризиком прямих або непрямих втрат, джерелами яких можуть бути невідповідні або неправильно організовані внутрішні процеси, людські ресурси і системи або зовнішні події. Наслідком виникнення таких подій є зниження вірогідності, повноти та актуальності створюваної і інформації, що обробляється.

Отже, інформаційний ризик може бути визначений як різновид операційного ризику, що відбувається в результаті неадекватних і помилкових внутрішніх процесів, дій працівників або зовнішніх подій. Стандарт ISO27000: 2018 вказує: інформаційний ризик – це потенційна можливість того, що загроза буде використовувати уразливість активу або групи активів, завдаючи шкоди організації.

Ризик викликає інцидент інформаційної безпеки – одне або серія небажаних або несподіваних подій інформаційної безпеки, що мають значну ймовірність порушення бізнес-операцій або становлять загрозу для інформаційної безпеки [SO / IEC TR 15446: 2017]. Таким чином, приступаючи до аналізу інформаційних ризиків, необхідно визначити перелік об’єктів і їх вразливостей, на які спрямовані атаки, реалізуючи загрози. Інформаційні ризики спрямовані на наступні види активів: інформація, мережеве, системне і

прикладне програмне забезпечення, персональні комп’ютери,

накопичувальні і друкувальні пристрої, мережеві сервера, шлюзи, інтерфейси, сервіси.

Витік інформації

Сьогодні більшість підприємств використовують багаторівневі системи обробки інформації – комп'ютери, хмарні сховища, корпоративні мережі і т. п.

Всі ці системи не тільки передають дані, але і є середовищем їх можливого витоку. Витік секретної інформації – процес неконтрольованого розголошення ключових даних.

Комерційна таємниця – інформація про організацію діяльності підприємства, технології розробки продукції, дані про грошові потоки, інтелектуальна власність та інші відомості, володіючи якими отримуються фінансові вигоди.

Причина 1 – Персонал

Кожен співробітник підприємства є потенційною загрозою для безпеки інформації. Часто люди забирають роботу додому – переміщують робочі файли на свої флеш-носії, передають їх по незахищеним каналам з'єднання, обговорюють інформацію зі співробітниками конкуруючих компаній.

Дії персоналу бувають навмисними і ненавмисними. Ненавмисні дії – це наслідок незнання регламенту роботи з комерційною інформацією.

Ризик витоку інформації від персоналу є завжди, і його не можна виключити повністю. Служба безпеки може вжити заходів, щодо обмежень взаємодії працівників з конфіденційною інформацією та впровадити правила розмежування доступу.

Правила – перелік чітких прав і обмежень, що повинні дотримуватися кожним співробітником. Їх основний принцип – кожен працівник взаємодіє тільки з тими даними, які потрібні для його роботи. Таким чином, простий менеджер не зможе дізнатися технологію розробки продукції та інші важливі дані, що бажає знати зловмисник.

Питаннями контролю роботи персоналу з секретними матеріалами повинен займатися уповноважений співробітник або відділ безпеки. Їхнє завдання це стежити за діяльністю працівників протягом усього робочого дня і оперативно виявляти всі випадки витоку інформації.

На практиці виявити людину, що зливає комерційну таємницю, можна за такими ознаками:

– *Співробітник без попередження затримується після роботи на своєму робочому місці.*

В такому випадку є ймовірність того, що він намагається отримати доступ до секретної інформації в момент, коли поруч нікого немає.

На такого працівника потрібно звернути увагу і простежити, чи не є його метою дізнатися таємні відомості. Контролювати час перебування персоналу на робочому місці допомагають спеціальні системи обліку доступу. Починати розслідування потрібно лише в тому випадку, якщо стали відомі конкретні факти витоку інформації, що захищається.

– *Співробітник зберігає на свій персональний комп'ютер або смартфон занадто багато електронних документів компанії.*

Такий варіант витоку можна відстежити в компаніях, що використовують системи захисту файлової системи. Суть їх роботи полягає в створенні

загального сервера, що діє в рамках однієї корпоративної або Wi-Fi-мережі. Під час кожного відкриття, копіювання та переміщення даних на службовому комп'ютері вся інформація про процеси надходить на сервер. Таким чином, адміністратор безпеки може виявити, з якого комп'ютера і в якій кількості була переміщена секретна інформація.

– Співробітник без необхідності копіює паперовий документообіг електронним (сканує документи або фотографує).

Згідно з нормами документування, всі фізичні папки і файли з комерційною таємницею повинні зберігатися в захищеній частині архіву.

Доступ до документів можливий тільки для уповноважених працівників. Всі дані про отримання документа з таємницею для користування повинні документуватися (із зазначенням імені працівника і точного часу видачі документа).

Якщо ж секретний документ потрапив в руки недобросовісного співробітника, відстежити його несанкціоноване копіювання можна на сканері або ксероксі, що зберігає звіт щодо діяльності за останній час. Також існують факсимільні апарати, доступ до яких можливий тільки після правильного введення пари «ідентифікатор користувача-пароль».

– Працівник регулярно порушує загальні вимоги безпеки при роботі з комерційною таємницею.

Якщо персонал регулярно намагається обійти систему заборони, переглядаючи заборонені ресурси, або використовує особисту техніку для обробки секретних даних, необхідно впровадити додаткові системи контролю користувачів. Наприклад, DLP-системи. Їх завдання полягає в моніторингу всіх листувань користувачів з комерційної пошти та інших електронних скриньок, які зареєстровані в системі. Також модуль захисту забороняє установку стороннього ПЗ, а всі дії співробітника за комп'ютером видно адміністратору безпеки.

– Співробітник був викритий в контактах із службовцями конкуруючих компаній.

У великих компаніях працівники часто спілкуються поза робочим часом.

Таким чином, вони отримують більше інформації один про одного і можуть дізнатися про зв'язки колеги і працівника конкуруючої організації. Ймовірність звичайних дружніх відносин між людьми теж можлива, але краще оповістити керівництво компанії про це, щоб уникнути непотрібних підозр.

Причина 2 – Проблеми підбору кадрів

Часта зміна персоналу, масштабні зміни в організації роботи компанії, зниження заробітних плат, скорочення співробітників – все це є частиною «плинності» кадрів. Таке явище часто стає причиною витоку секретної інформації.

Криза, нестача коштів для видачі зарплат змушують керівництво погіршувати умови роботи персоналу. В результаті підвищується невдоволення працівників, які можуть звільнитися або ж просто почати поширювати секретні дані конкурентам. Проблема зміни персоналу особливо важлива для керівних посад, адже всі керуючі повинні мати доступ до секретної документації.

Загрозу поширення таємниці можуть нести не тільки ті співробітники, які звільнилися, але і поточні працівники, рівень мотивації яких знижений.

Для запобігання проблеми слід створити для працівників максимально

комфортні умови роботи. У разі серйозної кризи рекомендується зібрати персонал для обговорення можливих шляхів виходу зі складної ситуації.

Важливо повідомляти співробітників про всі зміни в нарахуванні заробітних плат заздалегідь, а не за фактом виплати окладу.

Часом несприятливу атмосферу в колективі створює один співробітник. Встановлення систем автоматизованого профайлингу які аналізують листування працівників в електронній пошті і месенджерах та створюють їх психологічні портрети. Система визначає позитивні і негативні сторони характеру людини, що дозволяє приймати вірні управлінські рішення.

Для усунення «плинності» працівників важливо виконувати наступні рекомендації:

– Налагодити систему найму кадрів.

Всі передові організації мають спеціальний відділ, що займається питаннями найму, звільнення і підтримки співробітників. Не слід шукати працівника на вакансію, що звільнилася або з'явилась якомога швидше.

Хороший HR (фахівець з підбору кадрів Human resources) зобов’язаний прослухати кілька претендентів на посаду, поширити інформацію про вільну вакансію на популярних Інтернет-майданчиках, провести підсумковий конкурс, результати якого визначать кандидатуру, яка найбільше підходить.

– Впровадження системи винагород.

За успіхи в роботі, перевиконання планів і укладення вигідних контрактів співробітників потрібно заохочувати. Прикладами заохочення можуть бути підвищення заробітної плати, покращення умов роботи, просування по кар’єрним сходах.

– Надання всім співробітникам можливості професійного зростання, підвищення кваліфікації.

Хороші компанії завжди відправляють своїх співробітників на курси підвищення кваліфікація або ж закуповують онлайн-тренінги для більш зручного проходження навчання. Також рекомендується організовувати тренінги від провідних професіоналів галузі.

Причина 3 – Відрядження

Робочий процес фірми включає ділові зустрічі, поїздки в інші філії компанії, країни. Співробітники, які часто виїжджають у відрядження, можуть ненавмисно стати основною причиною витоку секретної інформації підприємства.

У поїздці такий працівник завжди має при собі особистий або корпоративний ноутбук/смартфон, що обробляє захищені документи. Техніка може бути залишена в громадському місці, зламана або викрадена. Якщо за співробітником ведеться стеження або ж він зустрічається з керівниками конкуруючої компанії, загублений ноутбук може стати головним джерелом розголошення службової інформації.

Для запобігання подібних випадків важливо використовувати системи шифрування жорсткого диска тих ПК, що видаються співробітникам на час ділових зустрічей. Навіть в результаті крадіжки і несанкціонованого доступу інформація буде надійно захищена, і зламати її, без знання ключа, буде неможливо.

Причина 4 – Співпраця з іншими компаніями

Більшість автоматизованих систем захисту здатні обмежити доступ до

службової інформації тільки в рамках однієї будівлі або одного підприємства (якщо кілька філій використовують загальний сервер зберігання даних).

У процесі спільного виконання проєкту декількома фірмами, служби безпеки не можуть в повній мірі простежити за тим, як реалізується доступ до службової таємниці кожного з підприємств.

Як і в попередньому випадку, використання криптоконтейнера (систем шифрування жорсткого диска) дозволить захистити таємну інформацію від злому.

Причина 5 – Використання складних IT-інфраструктур

Великі корпорації використовують комплексні системи захисту службових відомостей. Автоматизовані системи мають на увазі наявність декількох відділів безпеки і роботу понад п’яти системних адміністраторів, завдання яких полягає тільки в підтримці збереження комерційної таємниці.

Складність системи теж є ризиком витоку, адже одночасна робота кількох людей може бути незлагодженою. Наприклад, один адміністратор може впровадити або видалити правила розмежування доступу, а інший – забути внести дані прав доступу до серверів.

При використанні складних систем захисту інформації важливо грамотно розподіляти всі обов’язки і контролювати їх своєчасне виконання. В іншому випадку – створена система може нашкодити компанії.

Наприклад, можна розмежувати доступ співробітників служби безпеки до певних звітів і операцій в системі. Максимальне число повноважень надійніше довірити керівнику ІБ-служби.

Причина 6 – Поломки техніки

Помилки в роботі ПЗ

Всілякі збої в роботі програмного забезпечення виникають постійно. В момент появи уразливості захищені файли ризикують стати перехопленими хакером. Важливо вчасно виявляти всі неполадки в роботі встановлених програмних і апаратних компонентів. За працездатність і взаємодію всіх модулів захисту відповідальний адміністратор безпеки.

В результаті збою в базі даних втрачається значна кількість важливої документації. Відновлення жорстких дисків – це складне завдання, що не дає гарантії повернення втрачених відомостей.

Збої в роботі серверного обладнання

Безпечніше зберігати всю інформацію з використанням хмарних сховищ. Cloud-платформи підвищують швидкість обробки інформації. З їх допомогою кожен співробітник зможе отримати доступ до потрібних файлів з будь-якого пристрою. Система шифрування використовується віддаленим сервером, тому немає необхідності захищати канали передачі.

Збої на серверах постачальника послуг можуть траплятися через природні катаклізми або через масивні хакерські атаки. Як правило, власники хмарних платформ завжди зберігають архівовані резервні копії вмісту акантів користувачів, тому збої швидко вилучаються без втрати важливих документів.

Поломка технічних засобів захисту

Для збереження комерційної таємниці рекомендується захищати не тільки операційні системи і гаджети, але і весь периметр офісного приміщення, а також зону контролю вуличних комунікацій. Для цих цілей використовуються

заглушки на вікна, ущільнювачі архітектурних конструкцій (для запобігання прослуховувань), пристрої для екранування і зашумлення (для неможливості перехоплення радіохвиль), інші гаджети.

Через поломку одного з таких пристроїв виникає канал витоку інформації, що стає доступним зловмисникові для перехоплення секретних даних.

У разі поломки комп'ютерів і інших засобів обробки даних, їх необхідно відремонтувати в сервісному центрі. Винос гаджета за межі приміщення і передача його сторонній людині (навіть якщо він не зацікавлений в отриманні службової таємниці) є можливою причиною витоку. Департамент безпеки компанії не може контролювати гаджети, поки вони знаходяться за межами фірми.

Причина 7 – Витік з технічних каналів передачі даних

Канал витоку даних – це фізичне середовище, всередині якого не контролюється поширення таємної інформації. На будь якому підприємстві, що використовує комп'ютери, серверні стійки, мережі, є канали витоку. З їх допомогою зловмисник може отримати доступ до комерційної таємниці.

Існують наступні канали витоку:

Мовний. Конкуренти часто використовують прослуховувачі та інші закладки, за допомогою яких відбувається крадіжка таємниці.

Віброакустичний. Цей канал витоку виникає в процесі зіткнення звуку з архітектурними конструкціями (стінами, підлогою, вікнами). Вібраційні хвилі можна зчитати і перевести в мовної текст. За допомогою спрямованих мікрофонів на відстані до 200 метрів від приміщення зловмисник може зчитати розмову, в якій фігурує службова інформація.

Електромагнітний. В результаті роботи всіх технічних засобів виникає магнітне поле. Між апаратними елементами передаються сигнали, що можна вважати спеціальним обладнанням на великих відстанях і отримати секретні дані.

Візуальний. Приклад появи візуального каналу крадіжки – це проведення нарад і конференцій з неприкритими вікнами. З сусіднього будинку зловмисник може легко переглянути всю інформацію. Також можливі варіанти використання відеозакладок, які передають картинку того, що відбувається конкурентам.

Для захисту технічних каналів витоку рекомендується використовувати:

– *Тепловізор*. За допомогою такого девайса можна просканувати всі стіни і частини інтер'єру на наявність закладних пристроїв (жучків, відеокамер).

– *Пристрої, що заглушають подачу сигналу радіочастот.*

– *Засоби захисту архітектурних конструкцій* – ущільнювачі для вікон, дверей, підлоги і стелі. Вони ізолюють звук і унеможливлюють зчитування вібраційних хвиль з поверхні будівлі.

– *Пристрої для екранування і зашумлення*. Вони використовуються для захисту електромагнітного каналу витоку.

Також слід заземлити всі комунікації, що виходять за межі приміщення і контрольованої зони (труби, кабелі, лінії зв'язку).

Існує кілька дієвих способів, що допоможуть знизити ризик витоку і розголошення інформації. Підприємство може використовувати всі методи

захисту або тільки кілька з них, адже система безпеки повинна бути економічно вигідною. Збитки від втрати секретної інформації не можуть бути менше вартості впровадження та підтримки системи безпеки.

Шифрування. *Шифрування* – це простий і дієвий метод захисту комерційної таємниці. Сучасні алгоритми шифрування використовують світові стандарти в області криптографії (шифри AES, ГОСТ), двосторонній обмін ключами (з його допомогою хакер не зможе зламати шифр навіть після отримання доступу до каналу передачі), еліптичні криві для генерації захисту.

Такий підхід робить злом шифрованого повідомлення неможливим для стандартних комп'ютерів.

Переваги використання шифрування з метою запобігання витоку комерційної інформації:

Простота застосування. Реалізація шифрування проводиться спеціальним ПЗ. Програма повинна бути встановлена на всі комп'ютери і мобільні пристрої, в яких циркулює секретна інформація. Роботу додатка налаштовує системний адміністратор або адміністратор безпеки. Таким чином, звичайному користувачеві автоматизованих систем не потрібно вчитися використовувати систему захисту. Всі файли шифруються і дешифруються автоматично в рамках корпоративної мережі.

У разі необхідності передачі важливих електронних документів за межі комерційної мережі вони будуть зберігатися на флеш-носії, хмарному носії або в клієнтській пошті виключно в зашифрованому вигляді. Недолік – без спеціального ПЗ працівник не зможе переглянути вміст файлу.

Високий ступінь надійності. З використанням потужних обчислювальних алгоритмів криптографії зловмисникові складно перехопити секретні повідомлення або трафік фірми, а розшифровка, без знання відкритого і закритого ключа, неможлива.

Відзначимо, що шифрування є не єдиним варіантом захисту таємниці від всіх можливих атак. Працівники здатні без проблем прочитати вміст електронних документів в рамках комерційної мережі, тому ризик несанкціонованого розголошення третім особам залишається. Використання криптографії є невід'ємною частиною функціоналу кожної комплексної системи безпеки.

Контроль персоналу

Якщо технічні засоби легко контролювати, то персонал є одним з найнебезпечніших джерел витоку. Людський фактор присутній завжди, і навіть співробітники відділу безпеки не завжди можуть встановити, від якого працівника може виходити загроза.

Як правило, пошук зловмисника серед персоналу виконується вже тоді, коли стали відомі перші випадки передачі даних конкурентам. Адміністратори безпеки перевіряють можливість перехоплення інформації технічними каналами витоку, і, якщо всі канали надійно захищені, підозра падає на працівників.

Діяльність співробітників організації контролюється за допомогою систем обліку робочого часу. Це комплексне апаратне і програмне забезпечення, що документує точний час прибуття на роботу, час догляду, діяльність персоналу за комп'ютером, записує листування корпоративної пошти, проводить відеоспостереження і передає всі ці дані керівництву фірми або керівнику відділу

безпеки. Далі вся отримана інформації аналізується і виявляється число працівників, які могли поширювати комерційну таємницю.

Норми документування та передачі комерційної таємниці

Захищати треба не тільки електронні документи, а й всю друковану документацію, що містить секретні відомості. Відповідно до Закону "Про зберігання і обробку відомостей, що містять комерційну таємницю", слід виконувати такі вимоги:

– Зберігати всі документи з комерційною таємницею виключно в окремих закритих приміщеннях, що охороняються цілодобово системами відеоспостереження або охоронцями.

– Доступ до службової таємниці можуть мати тільки співробітники, яким вона потрібна в процесі роботи.

– Запис про вилучення документа з архіву вноситься до реєстраційного журналу. Вказується точна дата, гриф документа та ініціали особи, яка здобула копію файлу. Аналогічні дії проводяться при поверненні об’єкта.

– Документ, що містить комерційну таємницю, не можна виносити за межі офісу без повідомлення про це керівника департаменту безпеки.

– Для передачі таємних документів між філіями підприємства використовується фельд’єгерська пошта – захищена кур’єрська передача документів особливої важливості.

Відповідальність роботодавців

Забезпечення захисту персональних даних співробітників — це не лише юридичне зобов’язання, але й важлива складова корпоративної етики. Роботодавці мають створити безпечне середовище для зберігання та обробки інформації, що включає в себе наступні аспекти:

- розробка детальної політики конфіденційності та процедур захисту даних, які відповідають законодавчим вимогам та високим стандартам безпеки;
- просвітницька робота серед співробітників щодо впроваджених процедур, а також їх оновлення з урахуванням змін в технологіях та законодавстві;
- впровадження технічних заходів для захисту даних, таких як шифрування, аутентифікація та контроль доступу;
- створення структурної організації обробки даних, визначення відповідальних осіб та навчання персоналу.

Практичні кроки

Ефективний захист персональних даних вимагає від роботодавців впровадження конкретних організаційних так технічних заходів.

Розробка політик конфіденційності

Політика конфіденційності має чітко описувати, як компанія збирає, використовує, розкриває та захищає персональні дані. Важливо, щоб ця політика була доступна та зрозуміла для всіх співробітників, а також для осіб, чиї дані обробляються.

Внутрішні стандарти безпеки

Встановлення внутрішніх стандартів безпеки допомагає визначити технічні та організаційні заходи, які компанія повинна вжити для захисту персональних даних. Ці стандарти можуть включати в себе процедури шифрування, аудиту безпеки, моніторингу доступу до даних та їх видалення після завершення терміну зберігання.

Аудит безпеки та моніторинг

Регулярний аудит безпеки та моніторинг систем обробки даних дозволяють виявляти потенційні вразливості та несанкціоновані дії. Впровадження системи безперервного моніторингу, яка фіксує всі операції з даними, є ключовим для забезпечення прозорості обробки та можливості швидкого реагування на інциденти.

Шифрування даних

Шифрування є критично важливим для захисту конфіденційності. Використання сучасних алгоритмів шифрування для захисту даних, які зберігаються на серверах компанії або передаються через мережу, допомагає запобігти несанкціонованому доступу до інформації. Це може бути здійснено за допомогою шифрування на рівні диска, баз даних, а також використання зашифрованих каналів передачі, таких як SSL/TLS для веб-трафіку.

Аутентифікація та контроль доступу

Міцна система аутентифікації забезпечує те, що доступ до персональних даних мають лише авторизовані особи. Багатофакторна аутентифікація (MFA), що вимагає від користувачів пред'явити два або більше доказів своєї ідентичності (наприклад, пароль та одноразовий код, отриманий на мобільний телефон), значно підвищує безпеку. Контроль доступу має бути гнучким, дозволяючи встановлювати різні рівні доступу залежно від ролі користувача в компанії.

Створення структурної організації обробки даних

Цей крок передбачає визначення процесів та відповідальність за обробку персональних даних в організації. Важливо чітко розподілити обов'язки між співробітниками, які займаються збором, обробкою, зберіганням та видаленням персональних даних, а також забезпечити їх належним навчанням.

Визначення відповідальних осіб

Призначення відповідальних осіб, таких як уповноважений з захисту даних (Data Protection Officer, DPO), які координують заходи з захисту та забезпечують дотримання вимог законодавства. Вони також слугують точкою контакту для співробітників та регуляторних органів у питаннях, пов'язаних із персональними даними.

Навчання персоналу

Освітні програми та тренінги для співробітників допомагають підвищити обізнаність про важливість захисту персональних даних та про основні принципи їх безпечної обробки. Регулярні навчальні сесії, вебінари, інформаційні бюлетені та інші заходи сприяють підтримці високого рівня культури конфіденційності в організації.

Підготовка до інцидентів та план дій

Попри всі заходи безпеки, повний захист від потенційних загроз неможливий. Тому важливо мати розроблений та відпрацьований план дій на випадок інцидентів з безпекою даних. Такий план повинен включати процедури виявлення, оцінки, реагування на інциденти, а також сповіщення відповідальних органів і суб'єктів даних про порушення їхніх прав.

Впровадження цих технічних і організаційних заходів дозволить створити ефективну систему захисту персональних даних, знизити ризики їх витоку або

несанкціонованого доступу та забезпечити високий рівень довіри співробітників та клієнтів до компанії.

Реагування на інциденти

Ризики витоку або порушення безпеки завжди актуальні. Роботодавці повинні бути готові до ефективного реагування. Відповідь на інциденти безпеки є важливою складовою стратегії захисту персональних даних у будь-якій організації. Підготовка до можливих інцидентів та здатність ефективно на них реагувати може значно знизити потенційні збитки та відновити нормальну роботу. Розробка плану реагування на такі випадки включає:

1. **Чітке визначення інцидентів безпеки.** План повинен чітко визначати, що вважається інцидентом безпеки, включаючи втрату даних, несанкціонований доступ, зловмисне програмне забезпечення, фішингові атаки тощо.
2. **Процедура реагування.** Встановлення кроків реагування на інцидент, які можуть включати ідентифікацію інциденту, його оцінку, ізоляцію для запобігання подальшому розповсюдженню, ліквідацію причин інциденту, відновлення послуг та звітність.
3. **Ролі та відповідальності.** План має чітко визначати ролі та відповідальності команди реагування на інциденти, включаючи уповноваженого з захисту даних, IT-персонал, юридичний відділ та керівництво.
4. **Тренування та відпрацювання.** Проведення регулярних тренувань та відпрацювання плану реагування на інциденти допомагає забезпечити, що всі учасники процесу знають свої обов’язки та можуть ефективно діяти в кризовій ситуації.
5. **Сповіщення внутрішніх структур.** Швидке інформування внутрішніх структур організації про інцидент дозволяє залучити необхідних спеціалістів для своєчасного реагування на інцидент.
6. **Повідомлення суб’єктів даних.** У випадку, коли інцидент безпеки може мати негативний вплив на права та свободи суб’єктів, необхідно своєчасно повідомити їх про інцидент, описати можливі ризики та запропонувати рекомендації щодо захисту їхніх даних.
7. **Повідомлення регулятора.** Згідно з законодавством багатьох країн, включаючи GDPR в Європейському Союзі, організації зобов’язані повідомляти про значні інциденти безпеки даних відповідним регуляторним органам протягом певного терміну після їх виявлення.
8. **Документування інцидентів.** Ведення детальної документації по кожному інциденту, включаючи опис інциденту, час виявлення, вжиті заходи, результати розслідування та висновки, є важливим для аналізу причин і планування заходів щодо запобігання подібним інцидентам у майбутньому.

Ефективна підготовка та реагування на інциденти безпеки даних не лише допомагає зменшити негативний вплив на організацію та суб’єкти даних, але й підвищує довіру до компанії з боку клієнтів, партнерів та регуляторних органів.

У сучасному бізнес-середовищі, де цифровізація глибоко інтегрована у всі аспекти діяльності, важливість захисту персональних даних не може бути недооцінена. Цей крок вимагає від роботодавців не лише дотримання законодавчих вимог, але й активної участі у створенні безпечного інформаційного середовища. Реалізація рекомендованих практичних кроків та

впровадження ефективної системи управління інформаційною безпекою допоможе знизити ризики та забезпечити захист персональних даних співробітників. Відповідальне ставлення до персональної інформації та її захист є ключовим для побудови довіри та забезпечення успіху в будь-якому бізнесі.