Розділ 13. Відновлення функціонування інформаційно-комунікаційних систем (ІКС) після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження

13.1. Організаційно-технічні заходи відновлення функціонування ІКС.
13.2. Журнал аудиту подій.
13.3. Політики резервного копіювання даних.

13.1. Організаційно-технічні заходи відновлення функціонування ІКС

Можливість повної втрати даних за відсутності програми післяаварійного відновлення ставить під загрозу діяльність організацій, які не мають коштів для відновлення працездатності після катастрофічних подій. У багатьох компаніях планування надзвичайних заходів фокусується вже насамперед на IT. Програма збереження безперервності бізнес-операцій та післяаварійного відновлення може стати одним із найцінніших вкладів відділу IT у успішну діяльність організації.

Шість етапів планування

У термінології планування дій у аварійних ситуаціях фігурують два загальні поняття: **планування збереження безперервності бізнесу (Business Continuity Planning, BCP)** та **планування післяаварійного відновлення (Disaster Recovery Planning, DRP**). Ці поняття, які часто використовуються як рівноцінні, представляють різні концепції.

BCP традиційно передбачає планування заходів, що забезпечують збереження ділової активності організації у надзвичайних ситуаціях.

Сфера відповідальності DRP, за суттю, є підмножиною BCP і стосується відновлення інформації та працездатності систем у разі аварії. Наприклад, вихід з ладу жорсткого диска на сервері бази даних потенційно загрожує цілісності бізнесу, але не є результатом катастрофічних подій. Розрив водопровідної труби з затопленням серверного приміщення і зануренням сервера бази даних у воду становить загрозу цілісності бізнесу, що розглядається в рамках плану післяаварійного відновлення (DRP).

Планування заходів BCP і DRP – справа непроста, і у великих організаціях цим часто займаються спеціальні групи. Однак навіть без детального аналізу ступенів ризику та вирішення інших складних питань у рамках BCP та DRP у великих компаніях можна створити програму збереження цілісності бізнесу та післяаварійного відновлення, якщо дотримуватись наведених нижче етапів.

Етап 1. Визначення критично важливих ділових операцій

Перший крок планування рамках BCP і DRP – визначення критично важливих ділових операцій, тобто. дій, які мають виконуватися у повсякденному режимі задля збереження працездатності організації.

Наприклад, центр прийому заявок клієнтів на виконання технічного обслуговування повинен зберігати здатність приймати та фіксувати заявки.

Юридична фірма повинна мати доступ до інформації про клієнтів, надсилати та приймати електронну пошту, користуватися інтерактивними довідниками з права, а також відповідати на телефонні дзвінки.

На даному етапі планування необхідно співпрацювати з головними відповідальними особами організації у визначенні видів діяльності, важливих для збереження її працездатності. У центрі планування заходів у межах BCP знаходиться збереження ділової активності організації з допомогою відновлення цих видів діяльності.

Етап 2. Упорядкування схеми інфраструктури інформаційних систем, які забезпечують виконання критично важливих ділових операцій.

Від визначення критично важливих ділових операцій переходимо до визначення інформаційних систем, що забезпечують їхнє виконання.

Зокрема, в центрі прийому заявок клієнтів на проведення технічного обслуговування можливість перегляду зареєстрованих та фіксації нових заявок залежить від працездатності серверів бази даних, де зберігаються ці записи, та програм, що забезпечують доступ до цих серверів. Крім того, має також функціонувати певна частина центральної мережної інфраструктури, щоб ці критично важливі ділові операції могли виконуватись. Наведені вище інформаційні системи необхідно підтримувати у працездатному стані за рахунок оперативного післяаварійного відновлення.

Етап 3. Моделі загроз у вигляді передбачуваних та ймовірних подій

Практично всі катастрофи та аварії, що загрожують цілісності бізнесу, є передбачуваними з певним ступенем ймовірності. Катастрофічні події можуть бути природними (землетрус, повінь) або механічними (несправність жорсткого диска, розрив водопровідної труби тощо). Наприклад, якщо служба приймання заявок клієнтів на технічне обслуговування розташована у м. Владивосток, цілком можливо, що інформаційні системи центру рано чи пізно виявляться на шляху шторму. Так само, у будь-якій компанії, що використовує результати технічного прогресу, завжди можлива відмова апаратних засобів.

Визначивши критично важливі системи, можна приступати до моделювання загроз передбачуваних і ймовірних подій. Моделювання дозволяє реалізувати структурний підхід до визначення потенційних загроз, що несуть у собі максимальну небезпеку для цілісності бізнесу, та послаблення їх негативних наслідків. Складіть список можливих сценаріїв порушення працездатності критично важливих інформаційних систем, а також подій, що передують реалізації кожної загрози. Наприклад, працездатність центру прийому заявок клієнтів може бути порушена через недоступність бази заявок, що реєструються. Попередньою подією може стати відмова апаратних засобів, перебій у харчуванні або щось серйозніше, наприклад, руйнування інформаційного центру через шторм.

Етап 4. Розробка планів та процедур збереження цілісності бізнесу

Після складання списку критично важливих ділових операцій, перерахування інформаційних систем, що забезпечують їх виконання, та визначення можливих і ймовірних подій, здатних порушити працездатність зазначених інформаційних систем, можна розпочати вироблення превентивних

заходів, які мають на меті збереження цілісності бізнесу, з використанням моделей загроз.

В рамках **BCP існують чотири категорії превентивних заходів**:

– відмовостійкість та відновлення після збою;

– резервне копіювання;

– «холодне» запасне обладнання та приміщення;

– «гаряче» запасне обладнання та приміщення.

Розглянемо ці категорії більш детально:

– Відмовостійкість та відновлення після збою. Ця категорія превентивних заходів передбачає використання резервних апаратних засобів, що зберігають працездатність при відмові окремих елементів. В IT для забезпечення стійкості до відмови найбільш широко використовуються масиви жорстких дисків, технології кластеризації, акумуляторні і генераторні джерела живлення.

– Резервне копіювання. Резервне копіювання з використанням внутрішньосистемних та позасистемних засобів займає центральне місце серед превентивних заходів у рамках DRP. У разі втрати даних резервне копіювання забезпечує можливість відновлення та реконструкції інформації за останніми даними, що відповідають працездатному стану систем.

– «Холодне» запасне обладнання та приміщення. "Холодне" запасне обладнання – це автономні пристрої, які можна швидко підготувати до виконання робочих функцій. Наприклад, можна тримати набір серверів без підключення до мережі, на яких встановлені операційні системи з налаштуваннями, прийнятими в компанії. У разі аварії можна завершити налаштування конфігурації та відновити або скопіювати дані, необхідні для відновлення роботи. «Холодне» приміщення містить автономне обладнання, яке можна використовувати для відновлення роботи у разі аварії на головному устаткуванні. Часто «холодне» приміщення є просто залом, здатним вмістити робочі столи та стільці. Для більшості організацій малого та середнього бізнесу (SMB) утримання «холодних» приміщень не є економічно вигідним.

– «Гаряче» запасне обладнання та приміщення. "Гаряче" запасне обладнання – це пристрої, готові до негайної роботи у надзвичайній ситуації. Наприклад, можна безперервно дублювати критично важливу інформацію із занесенням у віддалену базу даних та забезпечити можливість перенаправлення клієнтських додатків до цих копій даних у разі потреби. "Гаряче" обладнання дозволяє дуже швидко відновлювати виконання операцій. Швидкість приведення «гарячого» устаткування працездатний стан зазвичай визначається часом, необхідним співробітникам прибуття до місця зберігання запасного устаткування. «Гаряче» обладнання має в своєму розпорядженні точні копії даних в реальному часі (або майже в реальному часі) і завжди працездатне. Утримання «гарячого» запасного обладнання та приміщень обходиться дорого, тому цей варіант використовується тільки в організаціях, які повинні зберігати працездатність у надзвичайних ситуаціях, наприклад у відомствах державної безпеки.

Етап 5. Розробка планів та процедур післяаварійного відновлення

Не всі події є передбачуваними та ймовірними. Важко знайти більш вдалий приклад непередбачуваної катастрофи, ніж атака на всесвітній торговий центр 11 вересня 2001 р. Для надзвичайних обставин такого роду, а також інших серйозних катастроф, у яких можлива повна втрата даних і працездатності головних систем, необхідна розробка планів і процедур відновлення. Оскільки післяаварійне відновлення відноситься до стресових ситуацій, дуже важливо мати під рукою добре документовані, перевірені та випробувані на практиці процедури. Переконатися у працездатності даних, які зберігаються на резервних носіях, можна як імітації роботи процедур відновлення.

Необхідно подбати про засоби позасистемного зберігання копій процедур, які виконуються в рамках DRP, разом із перевіреними працездатними резервними копіями. Для більшості організацій найбільш ефективним, доступним та безпечним варіантом позасистемного зберігання перевірених резервних копій та планів DRP є депозитарні осередки та банківські сейфи.

Етап 6. Перевірка працездатності планів збереження цілісності бізнесу та випробування на практиці засобів післяаварійного відновлення

Сам характер обставин, що змушують складати плани BCP та DRP, передбачає необхідність гарантії працездатності планів, процедур та технологій, що використовуються для збереження цілісності бізнесу.

Проведіть плановані і спонтанні навчання для перевірки стану стратегій BCP і DRP. Можна щомісяця імітувати відмова кластерних вузлів, періодично виконувати відновлення «холодних» запасних серверів чи проводити повномасштабні імітації катастрофічних ситуацій із перевіркою працездатності «холодних» і «гарячих» засобів відновлення. Як мінімум, слід виконати відновлення критично важливих даних щодо резервних копій з носіїв, що зберігаються поза офісом. Носії резервних копій, що зберігаються поза офісом, – остання лінія захисту від повної втрати даних.

Шість етапів захисту від катастрофи

Виконуючи перелічені етапи, можна допомогти підприємству створити програму BCP та DRP, яка забезпечить захист від наслідків природних, механічних та обумовлених людським фактором катастроф. Коли стільниковий телефон дзвонить о другій годині ночі, найменше хочеться гарячково винаходити шляхи відновлення даних, що знаходяться на сервері та стрічках і пробули під водою протягом 30 годин, або, що ще гірше, після фізичного руйнування інформаційного центру внаслідок катастрофи.

13.2. Журнал аудиту подій

Для вирішення завдання обробки інцидентів інформаційної безпеки (ІБ) логічно міркувати, що чим більше даних (логів, подій безпеки) ми збираємо, зберігаємо та аналізуємо, тим простіше нам буде надалі не тільки оперативно зреагувати на інцидент, але й розслідувати обставини атак, що відбулися, для пошуку причин їх виникнення. При цьому велика кількість даних для обробки

має і очевидний мінус: нас може просто «засипати» повідомленнями, алеутами (попередженями), повідомленнями, тому необхідно обрати найзначніші з погляду ІБ події та налаштувати відповідні політики аудиту.

Microsoft пропонує використовувати безкоштовний набір утиліт та рекомендацій (Baselines) у своєму наборі Microsoft Security Compliance Toolkit, в якому в тому числі наведені та рекомендовані налаштування аудиту для контролерів домену, рядових серверів та робочих станцій.

Крім рекомендацій вендора можна звернутися ще до документів CIS Microsoft Windows Server Benchmark і CIS Microsoft Windows Desktop Benchmark, в яких, серед іншого, вказані рекомендовані експертами політики аудиту для серверних і десктопних версій ОС Windows.

Однак найчастіше виконання абсолютно всіх рекомендацій неефективне саме через потенційну появу великої кількості «шумлячих», малозначних з погляду ІБ подій, тому в цьому розділі наведемо список найбільш корисних і ефективних (на наш погляд) політик аудиту безпеки та відповідних типів подій безпеки Windows.

В ОС Microsoft Windows, починаючи з Microsoft Windows Server 2008 і Vista, використовується досить просунута система аудиту, яка настроюється за допомогою конфігурування розширених політик аудиту (Advanced Audit Policy Configuration). Не варто забувати про те, що як тільки на пристроях будуть включені політики розширеного аудиту, за замовчуванням старі «класичні» політики аудиту перестануть бути ефективними, хоча ця поведінка може бути перевизначена в груповій політиці. аудиту (Windows Vista або наступні версії))» (Audit: Force audit policy subcategory settings).

Політики аудиту Windows

Пройдемо послідовно за налаштуваннями, ефективними для вирішення завдань аудиту ІБ та вироблення цілісної політики аудиту безпеки.

Крім описаних у таблиці 13.1 налаштувань, має сенс контролювати появу в журналі безпеки події з EventID=1102, яке формується відразу після очищення журналу безпеки, що може говорити про шкідливу активність. Більше того, розумно буде включити в каталозі «Конфігурація комп'ютера – Конфігурація Windows – Параметри безпеки – Локальні політики – Параметри безпеки» політику «Мережева безпека: обмеження NTLM: вихідний трафік NTLM до віддалених серверів» у значення «Аудит всього». Після цього EventID=8001 у журналі Microsoft-Windows-NTLM/Operational міститиме інформацію про автоматичну автентифікацію на веб-ресурсах з обліковим записом користувача. Наступним кроком стане allow list із переліком веб-ресурсів, які легітимно можуть вимагати облікові записи, а вказану політику можна буде перевести в режим блокування. Це не дозволить шкідливим ресурсам отримувати NTLM-ґеші користувачів, які натиснули на посилання з фішингового листа.

Звернімо увагу і на те, що підсистема журналювання Windows дуже гнучка і дозволяє налаштувати аудит довільних папок і гілок реєстру – слід вибрати критичні для ІТ-інфраструктури об'єкти аудиту і включити дані опції.

Таблиця 13.1 – Політики аудиту Windows

Категорія аудиту	**Підкатегорія аудиту**	**Події аудиту**	**EventID**	**Коментарі**
Вхід облікового запису	Аудит перевірки облікових даних	Успіх, Відмова	4776	Доцільно контролювати на домен-контролерах під час використання NTLM-автентифікації.
	Аудит служби автентифікації Kerberos	Успіх, Відмова	4771	Неуспішна автентифікація облікового запису на контролері домену за допомогою Kerberos-автентифікації.
			4768	Запит квитка Kerberos, слід аналізувати коди відповіді сервера.
	Примітка: Даний тип аудиту слід включати на контролерах домену, при цьому для детального вивчення спроб підключення та отримання IP-адреси пристрою, що підключається на контролері домену, слід виконати команду nltest /dbflag:2080ffff і проводити аудит текстового лог-файлу %windir%\debug\netlogon. log			
Управління обліковими записами	Аудит керування обліковими записами комп'ютерів	Успіх	4741	Заведення пристрою до домену Active Directory; може використовуватися зловмисниками, оскільки будь-який користувач домену за замовчуванням може завести домен 10 пристроїв, на яких може бути встановлено неконтрольоване компанією ПЗ, у тому числі шкідливе.
	Аудит управління групами безпеки	Успіх, Відмова	4728	Додавання члена глобальної групи.
			4732	Додавання члена локальної групи.
			4756	Додавання члена універсальної групи.

	Аудит керування обліковими записами користувачів	Успіх, Відмова	4720	Створення облікового запису.
			4725	Вимкнення облікового запису.
			4740	Блокування облікового запису.
			4723	Зміна пароля.
			4724	Скидання пароля.
Детальне відстеження	Аудит створення процесів	Успіх	4688	Під час створення процесу.
			4689	Після завершення процесу.
	Примітка: Щоб для командного інтерпретатора вівся запис введених команд, слід включити політику «Конфігурація комп'ютера – Конфігурація Windows – Адміністративні шаблони – Система – Аудит створення процесів –> Включати командний рядок у події створення процесів». Примітка: Щоб вести запис виконуваних PowerShell-команд і завантажених PowerShell-модулів, слід увімкнути в каталозі «Конфігурація комп'ютера – Конфігурація Windows – Адміністративні шаблони – Компоненти Windows – Windows PowerShell» політики «Увімкнути ведення журналу модулів» (у налаштуваннях політики вказати всі модулі символом «* ») та «Включити реєстрацію блоків сценаріїв PowerShell» (у налаштуваннях політики відзначити check-box «Реєстрація початку або зупинення виклику блоків сценаріїв»). Робота скриптів PowerShell реєструється з EventID=4104,4105,4106 у журналі Microsoft-Windows-PowerShell/Operational, а завантаження PowerShell-модулів реєструється з EventID=800 у журналі Windows PowerShell.			
Вхід вихід	Аудит виходу із системи	Успіх	4634	Для неінтерактивних сесій.
			4647	Для інтерактивних сесій та RDP-підключень.
	Примітка: При цьому слід звертати увагу на код Logon Type, який показує тип підключення (інтерактивне, мережне, із закешованими обліковими даними, з наданням облікових даних у відкритому вигляді тощо).			

	Аудит входу до системи	Успіх, Відмова	4624	При успішній спробі автентифікації створюється на локальному ПК і на домен-контролері при використанні NTLM і Kerberos-автентифікації.
			4625	При неуспішній спробі автентифікації створюється на локальному ПК і на домен-контролері при використанні NTLM автентифікації; при Kerberos-автентифікації на контролері домену створюється EventID=4771.
			4648	При спробі входу з явною вказівкою облікових даних, наприклад, при виконанні команди runas, а також при роботі хакерської утиліти Mimikatz.
	Примітка: При цьому слід звертати увагу на код входу (Logon Type), який показує тип підключення (інтерактивне, мережне, із закешованими обліковими даними, з наданням облікових даних у відкритому вигляді тощо). Доцільно також звертати увагу на код помилки (Status/SubStatus), який також зберігається у події аудиту та характеризує причину неуспішного входу – неіснуюче ім'я облікового запису, недійсний пароль, спроба входу із заблокованим обліковим записом тощо.			
	Аудит інших подій входу та виходу	Успіх, Відмова	4778	RDP підключення було встановлено.
			4779	RDP-підключення було розірвано.
	Аудит спеціального входу	Успіх	4672	На вході з адміністративними повноваженнями.

Доступ до об'єктів	Аудит відомостей про загальний файловий ресурс	Успіх, Відмова	5145	При доступі до системних мережних ресурсів, таких як \C$\. Ця подія буде створюватися під час роботи ransomware, націленого на горизонтальне переміщення по мережі.
	Аудит інших подій доступу до об'єктів	Успіх, Відмова	4698	Під час створення завдання у «Планувальнику завдань», що часто використовується зловмисниками як метод закріплення та приховування активності в атакованій системі.
Зміна політики	Аудит зміни політики аудиту	Успіх	4719	Зміна політики аудиту.
			4906	Зміна налаштування CrashOnAuditFail.
	Примітка: Змінити реакцію ОС на неможливість вести журнал аудиту безпеки (налаштування CrashOnAuditFail) можна в каталозі «Конфігурація комп'ютера – Конфігурація Windows – Параметри безпеки – Локальні політики – Параметри безпеки» у політиці «Аудит: негайне відключення системи, якщо неможливо внести в журнал запису про аудит безпеки ».			
Система	Аудит розширення системи безпеки	Успіх	4610 4614 4622	З появою у системі нових пакетів автентифікації, що має відбуватися несанкціоновано.
			4697	При створенні нового сервісу, який часто використовується зловмисниками як метод закріплення та приховування активності в атакованій системі.

Утиліта Sysmon

Окрім залучення штатного функціоналу підсистеми журналювання, можна скористатися і офіційною безкоштовною утилітою Sysmon із пакета Microsoft

Windows Sysinternals, яка суттєво розширює та доповнює можливості моніторингу ОС. Дана утиліта дає можливість проводити аудит створення файлів, ключів реєстру, процесів та потоків, а також здійснювати моніторинг завантаження драйверів та бібліотек, мережевих підключень, WMI-подій та іменованих каналів. З особливо корисних функцій відзначимо можливість утиліти показувати батьківський процес та командний рядок процесу, відображати значення ґеш-сум при подіях створення процесу та завантаження драйверів та бібліотек із зазначенням наявності та дійсності цифрового підпису. Нескладним шляхом можна автоматизувати порівняння отриманих ґеш-сум з індикаторами компрометації (IoCs, Indicator of Compromise) з даних фідів CyberThreat Intelligence, а також використовувати додаток QVTI для IBM QRadar, за допомогою якого ґеші файлів, що запускаються, автоматично перевіряються через сервіс VirusTotal. Ще однією приємною опцією є можливість створення XML-конфігурацій, в яких можна чітко вказати об'єкти контролю та налаштування роботи Sysmon. Одними з найбільш розвинених і детальних варіантів XML-конфігурацій, на наш погляд, є конфіги https://github.com/ion-storm/sysmon-config і https://github.com/SwiftOnSecurity/sysmon-config.

13.3. Політики резервного копіювання даних

13.3.1 Політика резервного копіювання даних

Резервне копіювання або бекап – створення копій всіх файлів, наявних на пристрої, жорсткого диска на інших пристроях або передача їх для зберігання в хмарі на випадок втрати або пошкодження комп'ютера.

Виділяють два види резервного копіювання:

1. Повне, при якому копіюються всі важливі файли, що зберігаються на комп'ютері або знаходяться на корпоративному сервері або в хмарі.
2. Диференціальне, коли спочатку на носій копіюються всі файли, а потім згідно з встановленим заздалегідь графіком копіюються дані, які були змінені.

Другий варіант вважається найбільш продуктивним. Але, тим не менш, не всі програми на даний момент підтримують резервне копіювання даних.

Причини втрати даних

До найбільш частих причин, через які відбувається втрата даних, можна віднести:

– Помилки власника, коли потрібні і важливі документи і файли видаляються через неуважність або помилок.

– Збій системи. В такому випадку файл може бути, як видалений, так і пошкоджений, що унеможливлює роботу з цим файлом.

– Вірус. Занесений в систему вірус або шкідлива програма може стати як причиною пошкодження або видалення файлів з жорсткого диска, так і зміни даних в ньому.

– Шифрувальник. Останнім часом в компаніях дуже гостро постала проблема з вірусами шифрувальниками, вони повністю зашифровують

диск, а якщо комп'ютер включений в локальну мережу, то і всі комп'ютери в локальній мережі і сервери компанії. Після такого шифрування ви не зможете користуватися комп'ютерами і серверами до тих пір, поки ви не сплатите хакерам їх вимогу за розшифровку даних. Але навіть якщо ви оплатили, з великою ймовірності вам все одно нічого не розшифрують і дані будуть назавжди загублені, а гроші витрачені.

– Хакерська атака може пошкодити файли, що зберігаються на сервері компанії або бухгалтерські бази даних.

– Вихід з ладу жорсткого диска або комп'ютера в цілому.

Періодичність виконання резервного копіювання

Резервне копіювання даних необхідно виконувати з тією частотою, з якою відбувається оновлення документів. Наприклад, якщо компанія щодня вносить зміни в свої файли, формує звіти – то виконувати резервну копію необхідно щодня, в кінці робочого дня. Якщо фірма невелика, і файли зі звітністю оновлюються раз на тиждень – то дані необхідно копіювати щотижня.

Копіювання обов'язково необхідно виконувати і перед перевстановленням операційної системи або при оновленні програмного забезпечення.

Для того щоб не забувати вчасно робити бекап, слід встановити спеціальну програму для резервного копіювання даних. Як налаштувати резервне копіювання для тієї чи іншої програми, можна дізнатися з інструкції до неї або звернеться до обслуговуючого системного адміністратора.

Програмне забезпечення буде або нагадувати власнику про необхідність чергового бекапа, або ж виконувати його самостійно, якщо мова йде про копіювання документів в хмарне сховище.

Вибір програми для створення резервної копії

При виборі програми необхідно звернути увагу на кілька основних параметрів:

– Можливість налаштування розкладу копіювання даних. Важливо, щоб програма заздалегідь нагадувала вам про необхідність виконати резервне копіювання.

– Управління розміщенням і копіями даних. Програма повинна підтримувати можливість резервного копіювання даних на кілька носіїв. Більш того, аналізувати всі файли і вибирати для копіювання ті, в які були внесені зміни з дати останнього резервного копіювання.

– Програма повинна підходити співробітникам і бути проста в управлінні. Чим простіше інтерфейс і чим швидше ваші співробітники навчаться користуватися програмою, тим краще.

Носії для зберігання резервних копій

Серед найбільш популярних фізичних носіїв для зберігання інформації виділимо:

1. SSD і HDD диски. Це жорсткі диски з великим об'ємом вбудованої пам'яті. Незважаючи на високу вартість, вважаються одними з найбільш надійних. Проте, їх необхідно берегти від ударів і падінь, в іншому випадку, накопичувач може вийти з ладу.

2. USB-накопичувачі з великим об'ємом пам'яті. З переваг можна виділити порівняно невелику вартість пристрою, компактність і зручність підключення до будь-якого пристрою. З мінусів-обмежена кількість записів і менший обсяг пам'яті.

3. Оптичні диски CD, DVD або Blu-ray. Бюджетний варіант, у якого є маса недоліків. В першу чергу, невеликий обсяг вільної пам'яті. По-друге, це нетривалий час служби. Диски необхідно оберігати від перепадів температури, впливу ультрафіолету, механічних пошкоджень.

4. Мережеві сховища NAS. Це спеціальні пристрої невеликого розміру, в яких встановлені жорсткі диски. Мережеве сховище підключається в локальну мережу організації після чого всі комп'ютери і сервери компанії можуть централізовано здійснювати резервне копіювання даних на цей тип носія інформації. Це найбільш дорогий спосіб організації резервного копіювання даних, але і найефективніший і не вимагають будь-яких дій від користувача. Система резервного копіювання на мережеве сховище налаштовується системним адміністратором один раз і потім працює довгий час без збоїв.

Хмарні сервіси зі створення та зберігання резервних копій

Створення резервної копії в хмарі на iCloud або Google Drive є одним з популярних варіантів. Більшість сервісів надають клієнтам можливість самостійно вибирати необхідний обсяг сховища і оплачувати тільки використовуване місце. Крім того, деякі фірми і зовсім надають своїм користувачам кілька гігабайт в хмарі безкоштовно, що ідеально підходить для невеликих фірм і компаній.

Незважаючи на свою простоту і порівняно невисоку вартість, використання хмарного сервісу для зберігання інформації має і свої недоліки.

В першу чергу, це передача корпоративної інформації на чужий сервер. При неналежному рівні захисту, вона в будь-який момент може стати надбанням громадськості.

Крім того, провайдери, що надають хмарні технології та їх розробники не несуть відповідальності за збої в мережі і тим більше не відповідають за видалення даних. Тобто, при збої в роботі сервера, зникнення важливої інформації компанія може зазнати збитків, які їй ніхто не відшкодує.

Крім того після закінчення підписки дані клієнтів і їх файли видаляються з хмарного сервісу. Звичайно, цей процес не буде запущений відразу після закінчення терміну підписки, але як мінімум протягом місяця ваші дані будуть видалені. Хорошим варіантом є наявність власного сервера або мережевого сховища для резервного копіювання даних.

Дані, які підлягають резервуванню

І все ж, які документи потребують резервного копіювання?

– В першу чергу, це робочі документи: бланки договорів, статутні документи підприємства, анкети співробітників та інша документація, яка не особливо бере участь в роботі підприємства, але в той же час повинна завжди бути під рукою на випадок перевірки.

– Звіт. Наприклад, резервне копіювання бухгалтерських програм і всіх створених в програмі звітів.

– База даних. Бухгалтерська база та інші важливі бази даних обов'язково повинні резервуватися.

– Закладки браузера. Чи не найнеобхідніше, але в деяких ситуаціях не буде зайвим мати копії адрес відвідуваних вами і корисних для компанії сайтів.

– Файли налаштувань програм, які часто використовуються на підприємстві.

– Контакти. Всі важливі контакти, зокрема, дані Ваших партерів, їх номери телефонів, адреси електронної пошти повинні бути продубльовані.

Бажано робити не одну, а кілька резервних копій, щоб уникнути неприємних ситуацій, коли інформація втрачена, а флешка або диск з резервною копією був загублений. Найкраще зробити кілька резервних копій на різних носіях і зберігати їх в різних місцях.

Порядок створення резервної копії

Резервне копіювання серверів або даних комп'ютера повинно проходити в кілька основних етапів.

1. На першому етапі підключається зовнішній накопичувач або ж відбувається підключення до хмари або мережевого сховища.
2. На другому етапі відбувається безпосередньо копіювання всіх необхідних даних.
3. На третьому етапі важливо перевірити дані, поміщені в резервне сховище: чи всі вони були передані, коректно відкриваються, чи не пошкоджені архіви.
4. Останній етап – відключення накопичувача.

Попередньо можна використовувати програми-архіватори, щоб файли займали менше місця.

Резервне копіювання даних – це не модна тенденція, а необхідність. Вчасно збережені дані не потрібно відновлювати, витрачаючи час і гроші. Незважаючи на те, що дані можна відновити навіть після того, як вони були видалені з кошика, все ж резервне копіювання залишається єдиним надійним варіантом зберігання даних. Це пов'язано з тим, що для відновлення видалених файлів знадобитися установка спеціальних програм, а в деяких випадках, допомогти зможе тільки фахівець з сервісного центру.

13.3.2 Політика резервного копіювання сайту

Резервні копії потрібні, коли основні файли сайту втрачені або пошкоджені. Статися це може в різних ситуаціях, ось розповсюдженіші з них:

– **Несвоєчасна оплата послуг**. По завершенні сплаченого періоду хостингу доступ до нього блокується. Зазвичай провайдери залишають клієнту можливість продовжити термін послуги ще якийсь час. Наприклад, ми зберігаємо клієнтські файли ще 95 днів.

– **Зараження сайту вірусом**. Для створення сайту багато хто використовує відкриті системи управління контентом на зразок Joomla або WordPress. Це зручно, швидко й безкоштовно. При цьому в таких систем є мінус – відкритий код, що дозволяє зловмисникам знаходити «дірки» і зламувати проекти. Резервне копіювання допоможе відновити сайт таким, яким він був до

зламу. Але тут важливо розуміти, що резервна копія не закриє «дірок» у сайті, їх повинні виправляти розробники.

– **Помилкове видалення файлів**. Усі ми робимо помилки. Іноді такі помилки можуть коштувати дуже дорого. Наприклад, якщо ви випадково видалите файли власного сайту, то без наявності резервної копії відновити їх не зможете.

– **Зникнення розробника або системного адміністратора**. Наймані фахівці не завжди якісно виконують роботу, а іноді й зовсім зникають безслідно. Особливо це актуально для людей, найнятих на біржах фрилансу. Наприклад, ви замовили розробку сайту, оплатили роботу, зробили сайт, але в якийсь момент розробник зник. Не бере слухавку і не відповідає на повідомлення. Що робити? Діставати резервну копію, звичайно! Якщо вона є. Рекомендую всім реєструвати хостинг і домен одразу на свої особисті дані. У такому випадку ви зможете відновити послуги, звернувшись до провайдера.

– **Переїзд з одного хостингу на інший.** Якщо поточний хостинг-провайдер вас не влаштовує, його потрібно змінювати. Суть переїзду в тому, щоб взяти копію сайту і завантажити її на новий сервер. Створюючи копію перед переїздом, перевірте, щоб вона містила всі файли та бази даних.

Як створювати резервні копії та де зберігати бекап

Щоб мати можливість у будь-який час дня і ночі розгорнути бекап, потрібно перш за все зробити копію і вибрати правильне місце для її зберігання.

Якщо ми говоримо про стандартну послугу з розміщення сайту – хостинг, то зазвичай провайдери самі роблять копії файлів раз на якийсь період. Знайти таку копію можна в панелі керування послугою.

Існує так звана «ротація» копій, коли старіша копія змінюється новою. Купуючи простий віртуальний хостинг для свого сайту, ви можете як зберігати копії на сервері провайдера, так і завантажувати їх на особистий комп’ютер або сторонній сервіс.

Резервне копіювання можна зробити й примусово, наприклад, перед внесенням глобальних змін у сайт. Якщо щось піде не так, ви зможете «відкотитися» до попередньої версії, просто розгорнувши резервну копію.

Якщо ж мова йде про віртуальні та виділені сервери, то найчастіше резервне копіювання – це завдання розробників, системних адміністраторів або тих, хто підтримує проект. Оскільки подібні послуги вимагають передачу клієнту сервера в повне керування, провайдер просто не має доступу до налаштувань і файлів.

Для створення резервних копій необхідно розробити і правильно налаштувати систему. Для цього можна використовувати вже готові скрипти і програмне забезпечення або створити їх самостійно. Також важливо вибрати й місце для зберігання створених копій.

В ідеалі це має бути ще один сервер, розташований в іншому дата-центрі (центрі зберігання й обробки даних), щоб мінімізувати ризики.

Ось три конкретні рекомендації, як не втратити сайт:

– Перевірте, чи налаштована функція створення резервних копій на вашому хостингу, віртуальному або виділеному сервері.

– Дізнайтеся, де зберігаються резервні копії.

– Зберігайте копію раз на певний час (залежить від частоти внесення змін на сайті) в альтернативному сховищі.