Вступ пояснення до теми

**Керування доступом та ідентифікація**

**Виходячи з опрацьованого матеріалу, та точкових запитів до AI, а також для розширення знання у сфері оформлення внутрішніх політик безпеки, регламентів доступу та процедур реагування які впроваджуються на підприємствах, було прийнято рішення розширити зону відповідальності де існує зв’язок з інтернетом та контакт людини за рахунок віддаленого доступу.**

**Як, вірогідним до виникнення, прикладом взята мінімальна критична ситуація з перебоями зі світлом. Додані правила користування USB.**

**Правила користування Wi-Fi описані в розділі присвяченому політиці підключення до мережі Wi-Fi.**

Словник термінів наданий у кінці документу.

Опціонально додано Чек-листи які створені у кооперації з Google + EDGE + AI

Прикладом взята уявна компанія яка займається випуском дронів.

**Політика керування доступом та ідентифікацією**

**Компанія:** «Smart Drone» Incorporated

**Версія:** 1.0

**Дата затвердження:** (11.11.1111.)

**Відповідальний:** Відділ кібербезпеки / Petro Davydov

1. **МЕТА**

Політика керування доступом та ідентифікацією, надалі «Політика», встановлює правила доступу до інформаційних, фізичних та технічних ресурсів компанії відповідно до принципів конфіденційності, цілісності та доступності (CIA), з урахуванням стандарту ISO/IEC 27001, GDPR, NIS2 та Закон України «Про захист персональних даних», з метою:

* 1. Захисту конфіденційності, цілісності та доступності даних
  2. Запобігання несанкціонованому доступу
  3. Відповідності міжнародним та національним стандартам безпеки
  4. Забезпечення безперервності бізнесу

1. **Область застосування політики**

2.1 Політика застосовується до всіх співробітників, підрядників, стажерів, третіх сторін, які мають доступ до систем, даних або фізичних ресурсів компанії.

2.2 Вона охоплює всі цифрові платформи, сервери, бази даних, мережі, пристрої, а також фізичні зони доступу.

1. **Аналіз потреб(ключові процеси компанії)**

Компанія «Smart Drone» Incorporated має декілька критичних бізнес-процесів, які потребують контролю доступу та ідентифікації. Нижче наведено опис процесів(список може бути збільшений за умов розширення виробництва), із зазначенням ролей та дій відповідальних осіб у визначених ситуаціях(список може бути розширений).

**3.1 Фінансові процеси**

**3.1.1 Виплата заробітної плати**

*HR-менеджер формує список* співробітників, які мають отримати заробітну плату (на основі годин які відпрацювали чи інших документів, підтверджуючих їх право на отримання фінансової винагороди). *Бухгалтер* на основі списку готує платіжні документи. *Фінансовий директор* перевіряє правильність нарахувань і затверджує виплати. *Кібербезпека* контролює, щоб доступ до платіжних систем був обмежений, а всі дії логувалися. Дані передаються банку через інтегрований модуль.

**3.1.2 Закупівля обладнання та послуг**

*Інженери по збору дронів або розробники*, через внутрішню систему запитів або погоджувальний лист, ініціюють запит на закупівлю необхідного обладнання або сервісів. *Юрист* перевіряє правову відповідність умов закупівлі. *Бухгалтер* оцінює фінансову доцільність. *Фінансовий директо*р затверджує бюджет. *Кібербезпека* перевіряє, щоб документи закупівлі зберігалися у захищеному середовищі з обмеженим доступом.

**3.1.3 Управління фінансовими договорами**

*Юрист* готує договір з контрагентом. *Бухгалтер* перевіряє фінансові умови. *Фінансовий директор* затверджує договір. *Фінансовий аналітик* контролює терміни дії договору та відповідає за періодичний аналіз зобов’язань. *Кібербезпека* забезпечує контроль доступу до договорів та їх шифрування.

**3.2 Технічні процеси**

**3.2.1 Розробка програмного забезпечення для дронів**

*Розробники* створюють код у захищених репозиторіях. *Тестувальники* перевіряють функціональність у тестових середовищах. *DevOps*-інженер здійснює деплой у продакшн середовище **після проходження всіх перевірок**. *Кібербезпека* контролює доступ до репозиторіїв, CI/CD та продакшн серверів.

**3.2.2 Збірка дронів**

*Інженери по збору дронів* отримують доступ до технічної документації та складу. Всі дії фіксуються. *Охорона* контролює фізичний доступ до виробничих зон. *Адміністратори баз даних* контролюють наповненість та актуальність баз даних. *Кібербезпека* контролює доступ та процеси, які проходять з базами даних та доступом до них. Всі дії логуються.

**3.2.3 Підтримка системи**

*Адміністратор БД* відповідає за резервне копіювання, оновлення та шифрування БД. *DevOps інженер* підтримує CI/CD, моніторинг та інфраструктуру, та має доступ до продакшн середовища згідно з політикою привілейованого доступу. *Кібербезпека* здійснює аудит, реагування на інциденти та контроль привілейованого доступу.

**3.3 Адміністративні процеси**

**3.3.1 Управління персоналом**

*HR-менеджер* створює облікові записи нових співробітників, призначає ролі відповідно до своїх посадових обов’язків. *Кібербезпека* перевіряє відповідність ролей принципу найменшого привілею. *При звільненні HR ініціює деактивацію доступу, а кібербезпека виконує аудит.*

**3.3.2 Юридичний супровід**

*Юрист* має доступ до правових документів, контрактів, нормативних актів. *Кібербезпека* забезпечує шифрування та контроль доступу до юридичних даних. *Директор* затверджує юридичні рішення, які мають стратегічне значення.

**3.3.3 Фінансовий аналіз**

*Фінансовий аналітик* має доступ до звітів, метаданих контрактів, KPI. Він не має права редагувати фінансові документи, лише аналізує їх. *Кібербезпека* контролює, щоб доступ був лише для перегляду, а всі дії логувалися.

1. **Рольова модель**
   1. **Принцип побудови моделей**

**4.1.1. Принцип найменшого привілею**:

Кожен користувач має доступ лише до тих ресурсів, які необхідні для виконання його посадових обов’язків.

**4.1.2 Принцип розподілу обов’язків(segregation of duties)**:

Критичні дії (фінансові операції, деплой у продакшн, юридичні затвердження) виконуються не одним користувачем, а кількома незалежними ролями.

**4.1.3 Правило двох рук**:

Для виконання дій з високим ризиком потрібне підтвердження щонайменше двох уповноважених осіб.

**4.2 Опис ролей та повноважень(таблиця)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Роль** | **Опис** | **Повноваження** | **Обмеження** |
| **Засновник** | Засновник компанії, стратегічний спостерігач. | Має доступ до стратегічної інформації, переглядає звіти. | Не має права редагування або затвердження операційних дій. (ISO 27001 A.9.1.1) |
| **Директор** | Вищий керівник, приймає ключові рішення. | Має повний доступ до фінансових, юридичних та операційних даних. Затверджує виплати, закупівлі, контракти | Не має прямого доступу до технічного середовища або продакшн-коду. (ISO 27001 A.9.2.3) |
| **Фінансовий директор** | Керує фінансовою політикою та бюджетами. | Перевіряє та затверджує фінансові документи, бюджети, закупівлі. | Не має доступу до продакшн-коду чи технічних середовищ. (ISO 27001 A.9.2.3) |
| **Бухгалтер** | Веде фінансовий облік та документообіг. | Формує платіжні документи, має доступ до фінансових систем. | Не має права затвердження або зміни політики. (ISO 27001 A.9.2.1) |
| **Фінансовий аналітик** | Аналізує фінансову ефективність та контракти. | Має доступ до фінансових звітів, метаданих контрактів, KPI. | Не має права редагування або затвердження. (ISO 27001 A.9.1.2) |
| **Юрист** | Забезпечує правову відповідність діяльності. | Має доступ до правових документів, контрактів, нормативних актів. Готує договори. | Не має доступу до фінансових систем або технічних середовищ. (ISO 27001 A.9.1.1) |
| **HR-менеджер** | Керує персоналом, обліковими записами та ролями. | Має доступ до персональних даних, створює облікові записи, ініціює зміну ролей. | Не має доступу до фінансових або технічних систем. (ISO 27001 A.9.2.4, GDPR Art. 5, 32) |
| **Розробники** | Створюють програмний код та функціонал. | Працюють з кодом у репозиторіях, мають доступ до дев-середовищ. | Не мають доступу до продакшн-серверів або баз даних. (ISO 27001 A.12.1.2) |
| **Тестувальники** | Перевіряють функціональність та стабільність ПЗ. | Працюють у тестових середовищах, мають доступ до логів. | Не мають права змінювати код або виконувати деплой. (ISO 27001 A.12.4.1) |
| **DevOps інженери** | Впроваджують та підтримують CI/CD, інфраструктуру. | Відповідають за деплой у продакшн, моніторинг, мають доступ до продакшн-серверів, логів, sudo. | Не мають доступу до фінансових систем або персональних даних. (ISO 27001 A.12.1.3, A.9.4.4) |
| **Адміністратор БД** | Керує базами даних, резервним копіюванням та шифруванням. | Має доступ до БД, резервного копіювання, шифрування. | Не має доступу до коду або продакшн-середовищ. (ISO 27001 A.10.1.1, A.12.3.1) |
| **Інженери по збору дронів** | Здійснюють фізичну збірку та технічне обслуговування дронів. | Мають доступ до технічної документації, складу, виробничих приміщень. | Не має доступу до ІТ-систем або цифрових даних. (ISO 27001 A.11.1.1) |
| **Охорона** | Забезпечує фізичну безпеку об’єктів та доступу. | Має доступ до камер, фізичних журналів, контролює фізичний доступ до приміщень. | Не має доступу до цифрових систем або облікових записів. (ISO 27001 A.11.2.1) |
| **Кібербезпека** | Відповідає за інформаційну безпеку, аудит, реагування на інциденти. | Має доступ до логів, SIEM, IAM, sudo, SSH, USB-контролю, політик безпеки. Контролює всі критичні точки. Має право ініціювати блокування доступом за погодженням з директором. | Не має права змінювати фінансові або юридичні документи. (ISO 27001 A.16.1.1, A.9.4.2, A.12.4.3) |

1. **Методи автентифікації**

**5.1 Загальні вимоги до автентифікації:**

5.1.1 Усі користувачі повинні проходити автентифікацію перед доступом до будь-яких систем.

5.1.2 Для привілейованих ролей (DevOps, адміністратор БД, кібербезпека) обов’язкове використання багатофакторної автентифікації (MFA).

5.1.3 Паролі повинні бути не коротші ніж 10 символів з одним спеціальним символом (!,?,$,%), змінюватися кожні 15-60 днів залежно від посади та рівня доступу (може бути змінено), не повторювати останні 3-5 паролів(залежно від посади та рівня доступу).

**5.2 Методи автентифікації за ролями**

|  |  |  |
| --- | --- | --- |
| **Роль** | **Метод**  **аутентифікації** | **Обґрунтування** |
| **Засновник** | VPN + MFA(Token) | Має доступ до стратегічної інформації, але не виконує операційні дії. Захист через VPN та токен забезпечує конфіденційність. (ISO 27001 A.9.4.2) |
| **Директор** | Пароль + біометрія | Має повний доступ до фінансових, юридичних та операційних даних. Біометрія забезпечує зручність і високий рівень захисту. (GDPR Art. 32) |
| **Фінансовий директор** | Пароль + OTP через SMS або додаток | Затверджує фінансові документи. OTP забезпечує додатковий рівень захисту при доступі до платіжних систем. (ISO 27001 A.9.2.4) |
| **Бухгалтер** | Пароль + OTP через SMS або додаток | Має доступ до фінансових систем, формує платіжні документи. OTP захищає від несанкціонованого доступу. (NIST SP 800-63B) |
| **Фінансовий аналітик** | Пароль + OTP | Має доступ лише до перегляду звітів. OTP достатній для захисту аналітичних даних без надмірної складності. (ISO 27001 A.9.1.2) |
| **Юрист** | Пароль + OTP | Працює з конфіденційними юридичними документами. OTP забезпечує захист без ускладнення доступу. (ISO 27001 A.9.1.1) |
| **HR менеджер** | Пароль + OTP через SMS або додаток | Має доступ до персональних даних. OTP забезпечує відповідність GDPR щодо захисту персональної інформації. (GDPR Art. 32) |
| **Розробники** | SSO + GitHub/MFA | Працюють з кодом у репозиторіях. MFA через GitHub або корпоративну SSO забезпечує безпечний доступ до dev-середовищ. (ISO 27001 A.9.4.3) |
| **Тестувальники** | Пароль + MFA | Працюють у тестових середовищах. MFA захищає доступ до логів та тестових даних. (ISO 27001 A.12.4.1) |
| **DevOps-**  **інженери** | MFA + SSH-сертифікат + апаратний токен | Відповідають за продакшн, CI/CD. SSH-сертифікати та токен забезпечують найвищий рівень захисту. (ISO 27001 A.9.4.4) |
| **Адміністратор БД** | MFA + апаратний токен (YubiKey) | Має доступ до баз даних, резервного копіювання. Апаратний токен захищає критичні дані. (ISO 27001 A.10.1.1) |
| **Інженери по збору дронів** | Пароль + RFID картка | Працюють у виробничих приміщеннях. RFID забезпечує контроль фізичного доступу. (ISO 27001 A.11.1.1) |
| **Охорона** | RFID + PIN | Контролює фізичний доступ. PIN + RFID забезпечують швидкий і безпечний доступ до камер та зон. (ISO 27001 A.11.2.1) |
| **Кібербезпека** | MFA + VPN + логування дій | Має доступ до критичних систем. VPN + MFA + повне логування забезпечують контроль та відповідність стандартам. (ISO 27001 A.12.4.3, A.16.1.1) |

1. **Перегляд політик, правил та аудит**

**6.1 Перегляд ролей та доступу:**

6.1.1. Щоквартально проводиться аудит ролей, користувачів, привілеїв та журналів активності. Ці дії забезпечують вчасне виявлення зайвих прав, видалення доступів після звільнення, відповідність змінам у структурі компанії.

6.1.2. При зміні посадових обов’язків HR-менеджер ініціює оновлення ролі, кібербезпека виконує перевірку відповідності.

6.1.3. При звільненні співробітника HR негайно повідомляє кібербезпеку, яка блокує обліковий запис та проводить аудит дій.

6.1.4. У випадку звільнення одного з керівників дії регулюються відповідно до внутрішніх процедур безпеки та затверджених регламентів управління доступом.

**6.2 Аудит доступу:**

6.2.1. Перевірка членства в AD-групах.

6.2.2 Аналіз логів входу (Windows Event ID 4624, 4625).

6.2.3 Перевірка змін у групах (Event ID 4728, 4729).

6.2.4 Логування доступу до критичних ресурсів через SIEM, Auditd, Sysmon.

**6.3 Відповідальність:**

6.3.1. Кібербезпека - виконання процесу аудиту.

6.3.2. HR - зміна ролей.

6.3.3. Директор - зміни у критичних ролях.

6.3.4. Бухгалтер - остаточне розрахування з робітником у випадку звільнення, звірка відомості

6.3.5. Фінансовий директор - перевіряє фінансові зобов’язання, погоджує остаточні виплати, контролює відповідність бюджету при звільнені.

1. **Контроль доступу до продакшн коду(для ознайомлення спеціалістів)**

**7.1 Доступ до продакшн:**

7.1.1. Має лише DevOps - інженер через CI/CD з MFA.

7.1.2. Розробники не мають прямого доступу до продакшн-серверів.

**7.2 Процедура деплою:**

7.2.1. Зміни проходять через Pull Request - Code Review - Automated tests - Approval - Deployment.

7.2.2. Деплой(Deployment) дозволено лише з main (або master) гілки.

**7.3 Логування:**

7.3.1. Всі дії деплою логуються: користувач, час, змінені файли, статус (та додаткові дані які будуть визначені за потреби кібербезпекою)

7.3.2. Логи зберігаються в CI/CD системі та SIEM.

**7.4 Відповідальність:**

7.4.1. DevOps - технічне виконання.

7.4.2. Кібербезпека - аудит змін.

7.4.3. Директор - затвердження політик.

1. **Контроль Wi-Fi доступу**

**8.1.** Доступ до корпоративного Wi-Fi *дозволено лише зареєстрованим пристроям.*

**8.2 Реєстрація. Обов’язкова процедура:**

* MAC-адреса або IMEI реєструється кібербезпекою.
* Дані зберігаються у білому списку на контролері Wi-Fi.

**8.3 Захист:**

* Незареєстровані пристрої блокуються автоматично.
* Спроби підключення логуються.

**8.4 Відповідальність:**

* Кібербезпека - реєстрація, моніторинг, аудит.
* Охорона - фізичний контроль доступу до зони покриття.

1. **sudo доступ (для ознайомлення спеціалістів)**

**9.1 Доступ до команди sudo дозволено лише наступним ролям:**

* Кібербезпека
* Розробники
* Адміністратор БД.
* DevOps-інженери

**9.2 Реалізація:**

* Файл /etc/sudoers налаштовується через visudo
* Усі sudo-команди логуються в /var/log/auth.log (або іншу директорію та файл який визначено відділом кібербезпеки)

**9.3 Аудит:**

* Щотижнева перевірка логів sudo.
* При виявленні несанкціонованих команд, службове розслідування вважається розпочатим автоматично

1. **Контроль USB носіїв на території та в приміщені підприємства**

**10.1** Підключення дозволено лише зареєстрованим USB-носіям.

**10.2 Реєстрація:**

* Серійний номер, ім’я користувача, дата(мета використання за вимогою)
* Реєстрація здійснюється кібербезпекою.

**10.3 Технічна реалізація:**

* У Windows - через GPO.
* У Linux - через udev правила.

**10.4 Логування:**

* Користувач, час, серійний номер, дії (читання та запис), та інші дані у випадку необхідності, які визначить відділ кібербезпеки
* Щотижневий звіт кібербезпеки.
* У випадку фіксування використання пристрою не за призначенням, службове розслідування вважається відкритим автоматично.

1. **Віддалений доступ(для ознайомлення спеціалістів)**

**11.1 Умови доступу:**

* Віддалений доступ дозволено лише співробітникам, які мають відповідні ролі (визначається за погодженням з кібербезпекою)
* Доступ здійснюється виключно через захищене з’єднання SSH з використанням сертифікатів та багатофакторної автентифікації (MFA).
* Всі підключення мають бути здійснені *з попередньо зареєстрованих IP-адрес, внесених до білого списку*.

**11.2 Обмеження:**

* Максимальна тривалість віддаленої сесії - 3 (три) години на день.
* У разі трьох поспіль невдалих спроб автентифікації - IP-адреса блокується (час блокування визначається кібербезпекою відповідно до характеру інциденту)
* Віддалений доступ до продакшн-середовища дозволено лише DevOps-інженерам, з зареєстрованих пристроїв.

**11.3 Логування:**

* Логуються: сертифікат користувача, IP адреса, час підключення, тривалість сесії, виконані команди.
* Логи зберігаються у SIEM системі та аналізуються щотижнево або щоденно (визначається кібербезпекою)

**11.4 Відповідальність:**

* Кібербезпека - моніторинг, аудит, блокування IP, та інші дії відповідно ситуації для запобігання витоку будь-якої інформації за межі підприємства.
* DevOps - технічна підтримка віддаленого доступу.
* Директор - затвердження політики доступу.

1. **Контроль встановлення нового обладнання**

**12.1 Ініціація:**

* Директор або CTO ініціює закупівлю нового обладнання.
* HR, бухгалтер, фінансовий директор та кібербезпека погоджують потребу, бюджет та безпекові вимоги.

**12.2 Доставка та приймання:**

* Охорона приймає обладнання, перевіряє упаковку та серійні номери.
* Кібербезпека реєструє пристрої в інвентаризаційній системі, присвоює унікальний ID.

**12.3 Встановлення:**

* DevOps-інженер з представниками технічного персоналу або підрядниками відповідальними за монтаж - встановлюють обладнання.
* Підключення до живлення, мережі, UPS.
* Встановлення базової ОС, BIOS - паролів, шифрування дисків.
* *DevOps - контролює та несе відповідальність за остаточні дії з обладнанням*

**12.4 Конфігурація та безпека:**

* Кібербезпека налаштовує доступи, SSH, sudo, MFA, та інші налаштування пов’язані з зоною її відповідальності визначених затвердженою на підприємстві та у законний спосіб документацією
* Встановлюються антивірусні засоби, SIEM-агенти, моніторинг.

**12.5 Документування:**

* Журнал встановлення включає: дату, серійний номер, MAC-адресу, відповідальних осіб, призначення пристрою.
* Документація зберігається у внутрішньому репозиторії політик.

**12.6 Відповідальність:**

* DevOps - технічне встановлення.
* Кібербезпека - аудит, безпека, логування.
* Охорона - фізичний контроль доступу.

1. **Дії при аварійному вимкненні електроенергії**

**13.1 Автоматичні дії:**

* Активація UPS.
* Автоматичне завершення роботи серверів.
* Камери переходять у автономний режим (налаштування є обов’язковим).

**13.2 Дії персоналу:**

|  |  |
| --- | --- |
| **Роль** | **Дії** |
| *Кібербезпека* | Перевірка журналів UPS, SIEM, стану шифрування, контроль доступу. |
| *DevOps-інженер* | Перевірка CI/CD, продакшн-сервісів, підготовка до перезапуску. |
| *Адміністратор БД* | Перевірка цілісності баз даних, запуск скриптів перевірки логів. |
| *Охорона* | Контроль фізичного доступу, перевірка камер, фіксація часу інциденту. |
| *Директор / CTO* | Оцінка впливу на бізнес, рішення про запуск резервного живлення. |

**13.3 Відновлення:**

* Перевірка логів, цілісності даних.
* Перезапуск сервісів.
* Верифікація резервних копій.

**13.4 Документування:**

* Журнал аварійних подій включає: дату, причину, дії, вплив, рекомендації.
* Звіт передається директору та зберігається у внутрішній системі.

1. **Відповідність стандартам**

**14.1. ISO/IEC 27001:**

* A.9 - Контроль доступу.
* A.12.1.2 - Управління змінами.
* A.8.3 - Управління носіями.
* A.17.1.2 - Процедури безперервності бізнесу.

**14.2. GDPR:**

* Стаття 5 - Принципи обробки персональних даних.
* Стаття 32 - Безпека обробки.

**14.3. NIS2:**

* Захист критичної інфраструктури, управління ризиками, реагування на інциденти.

**14.4. Законодавство України:**

* ЗУ «Про захист персональних даних».
* ЗУ «Про електронні комунікації».
* ЗУ «Про захист інформації в інформаційно-телекомунікаційних системах».

1. **Відповідальність**

**15.1. Загальні положення:**

* Кожен співробітник несе *персональну відповідальність* за дотримання політики доступу та ідентифікації.
* Заборонено передавати облікові дані третім особам.
* У разі виявлення порушень - негайне повідомлення кібербезпеки.
* Повідомлення кібербезпеки автоматично вважається підставою для відкриття службового розслідування.

**15.2 Порушення політики:**

* Порушення є підставою для дисциплінарного впливу.
* Може включати: блокування доступу, службове розслідування, повідомлення керівництву.

**15.3 Відповідальні особи:**

*Кібербезпека* - аудит, моніторинг, реагування, оновлення політики, звітування директору та ініціювання блокування у азі порушень.

*HR-менеджер* - управління обліковими записами, ініціація змін ролей, деактивація доступу.

*Директор* - затвердження політики, стратегічне управління доступом.

*DevOps-інженер* - технічна реалізація доступу, підтримка інфраструктури.

**Словник**

**Терміни поняття які використовуються в документі**

**Міжнародні стандарти**

**ISO/IEC 27001**

Міжнародний стандарт, який визначає вимоги до системи управління інформаційною безпекою (*ISMS*). Його мета - забезпечити конфіденційність, цілісність і доступність інформації шляхом управління ризиками. Стандарт охоплює політики, процедури, технічні та організаційні заходи. (Джерело: ISO/IEC 27001:2022)

**GDPR (General Data Protection Regulation)**

Загальний регламент ЄС про захист персональних даних. Встановлює правила обробки персональних даних фізичних осіб у межах ЄС. Основні принципи - законність, справедливість, прозорість, мінімізація даних, точність, обмеження зберігання, цілісність і конфіденційність. (Стаття 5, Стаття 32)

**NIS2 (Network and Information Security Directive)**

Оновлена директива ЄС щодо кібербезпеки критичних секторів. Вимагає від організацій впровадження заходів управління ризиками, реагування на інциденти, безперервності бізнесу та звітності. Застосовується до постачальників цифрових послуг, енергетики, транспорту, охорони здоров’я тощо.

**Бізнес-терміни**

**KPI (Key Performance Indicator)**

Ключовий показник ефективності - це кількісна метрика, яка використовується для оцінки успішності організації або окремого процесу. Наприклад: прибуток, рентабельність, виконання бюджету, терміни виконання. KPI допомагають фінансовому аналітику оцінити продуктивність і приймати обґрунтовані рішення.

**Витяги зі стандарту ISO/IEC 27001**

**A.9.1.1** - «Доступ до інформації має надаватися на основі бізнесових вимог, з урахуванням політики безпеки.»

**A.9.2.3** - «Привілеї доступу до інформаційних систем мають бути обмежені відповідно до ролі користувача.»

**A.9.4.1** - «Системи доступу мають забезпечувати унікальну ідентифікацію користувача.»

**A.9.2.1** - «Процедури реєстрації та деактивації користувачів мають бути формалізовані.»

**A.9.1.2** - «Доступ до мереж і сервісів має бути обмежений лише авторизованим користувачам.»

**A.9.2.4** - «Привілеї доступу мають переглядатися регулярно.»

**A.12.1.2** - «Зміни в інформаційних системах мають проходити контрольований процес управління змінами.»

**A.12.4.1** - «Журнали подій мають бути створені, збережені та регулярно переглядатися.»

**A.12.1.3** - «Захист від шкідливого ПЗ має бути реалізований у всіх системах.»

**A.9.4.4** - «Використання привілейованих утиліт має бути контрольованим.»

**A.10.1.1** - «Криптографічні засоби мають використовуватися для захисту конфіденційності, цілісності та автентичності.»

**A.12.3.1** - «Резервне копіювання інформації має здійснюватися регулярно.»

**A.11.1.1** - «Фізичний доступ до критичних зон має бути обмежений.»

**A.11.2.1** - «Обладнання має бути захищене від фізичних загроз та несанкціонованого доступу.»

**A.16.1.1** - «Інциденти безпеки мають бути зареєстровані та розслідувані.»

**A.9.4.2** - «Процедури входу до систем мають бути захищені.»

**A.12.4.3** - «Журнали доступу мають бути захищені від несанкціонованого доступу»

**Технології автентифікації**

**YubiKey** - апаратний токен, який забезпечує двофакторну автентифікацію через USB/NFC. Підтримує OTP, FIDO2, PIV, OpenPGP.

**Апаратний токен** - фізичний пристрій, який генерує одноразові паролі або зберігає криптографічні ключі.

**OTP (One-Time Password)** - одноразовий пароль, який дійсний лише для однієї сесії або транзакції.

**SSO (Single Sign-On)** - механізм, який дозволяє користувачеві автентифікуватися один раз і отримати доступ до кількох систем.

**SSH-сертифікат** - цифровий сертифікат, який використовується для автентифікації користувача при підключенні через SSH.

**RFID-картка** - безконтактна картка, яка використовується для фізичного доступу до приміщень або пристроїв.

**Моніторинг подій та систем**

**Event ID 4728** - додавання користувача до групи безпеки.

**Event ID 4729** - видалення користувача з групи безпеки.

**SIEM (Security Information and Event Management)** - система централізованого збору, аналізу та кореляції логів безпеки.

**Auditd** - демон Linux, який записує події безпеки в системний журнал згідно з політикою аудиту.

**Sysmon** - служба Windows, яка логує створення процесів, мережеві з’єднання, зміни файлів. Використовується для виявлення аномалій.

**visudo** - команда Linux для безпечного редагування файлу sudoers. Перевіряє синтаксис перед збереженням, запобігає помилкам.

**GPO (Group Policy Object)** - набір політик у Windows, які централізовано керують налаштуваннями користувачів і комп’ютерів у домені.

**udev-правила** - правила в Linux, які визначають поведінку системи при підключенні або зміні пристроїв. Дозволяють автоматичні дії на основі атрибутів пристрою.

**Опціонально до домашньої роботи**

Можливо існують подібні чек листи, для контролю роботи, я спробував відтворити, пошукавши в інтернеті. Але всі підприємства та організації орієнтуючись на певні вимого і законодавства створюють свої чек листи, принаймні я так зрозумів.

Тому у зв’язці з Google + EDGE + AI + конспект = приблизно ось так:

№ 1 Чек лист для облікового запису

|  |  |  |
| --- | --- | --- |
| Крок | Дія | Відповідальний |
| 1 | Отримати запит на створення облікового запису | HR |
| 2 | Визначити роль згідно посадових обов’язків | HR + CS |
| 3 | Створити обліковий запис у AD / IAM | DevOps + AdminDB |
| 4 | Призначити групи доступу | CS |
| 5 | Налаштувати автентифікацію (пароль, MFA) | CS |
| 6 | Задокументувати створення | CS +HR |

№2 Чек лист для АУДИТУ

\* тут все просто для контролю за своїми діями для CS(я думаю є і більш розширені, але поки як є)

|  |  |  |
| --- | --- | --- |
| Крок | Дія | Відповідальний |
| 1 | Перевірити актуальність ролей | CS |
| 2 | Перевірити членство в групах | CS |
| 3 | Перевірити логування входів | CS |
| 4 | Перевірити sudo / SSH / USB активність | CS |
| 5 | Сформувати звіт | CS |
| 6 | Надати рекомендації директору | CS |

№3 Чек лист для Реакції на аварійне вимкнення світла

|  |  |  |
| --- | --- | --- |
| Крок | Дія | Відповідальний |
| 1 | Перевірити UPS та завершення роботи серверів | DevOps |
| 2 | Перевірити фізичний доступ | Охорона |
| 3 | Перевірити цілісність БД | AdminDB |
| 4 | Перевірити логи та шифрування | CS |
| 5 | Прийняти рішення щодо запуску резервного живлення | Директор |
| 6 | Задокументувати інцидент | CS |

№4 Чеклист для встановлення нового обладнання

|  |  |  |
| --- | --- | --- |
| Крок | Дія | Відповідальний |
| 1 | Ініціація закупівлі | Директор /CTO |
| 2 | Перевірка доставки | Охорона |
| 3 | Реєстрація пристрою | CS |
| 4 | Фізичне встановлення | DevOps + відповідальні |
| 5 | Налаштування безпеки | CS |
| 6 | Документування | CS |