نموذج مقترح لتعزيز أمن الحواسيب ومعدات الشبكات ضد المخاطر الداخلية والخارجية

إعداد :

- أحمد محمد نور عجيل، استاذ مساعد ، جامعة السودان التقانية ، السودان

البريد الالكتروني: gehad2014.system@gmail.com

المستخلص

هذه الدراسة تقدم حلولاً لمشاكل مكونات الحاسب الآلي المادية ومعدات الشبكات وطرق حمايتها من كافة المهددات والمخاطر الداخلية والخارجية .. إهتمت الدراسة بشكل كبير بمسألة تلف أجزاء الحاسب الآلي نتيجة لعدم استقرار التيار الكهربائي بصورة ملحوظة في الآونه الأخيرة. هدفت الدراسة إلي تنبيه المؤسسات بالمخاطر والمهددات التِي تحيط بأنظمة الحاسب الآلي وضرورة توفير الميزاتيات اللازمة لتعزيز وتنفيذ نظام الأمان والحماية الفعال وتحديد نقاط الضعف في منظومة الحماية وطرقِ تقويتها وتعزيزها بما يضمن عدم حدوث الأضرار. إعتمدت الدراسة المنهج الوصفي والمنهج الاستنباطي في تحديد الأسباب التي تؤدي الي حدوث تلك المشاكل ، واستخدمت النماذج والخوارزمية في التصميم لتبسيط خطوات الحماية اللازمة . ومن أهم النتائج التي توصلت لها الدراسة: تصميم نموذج حماية له القدرة علي حماية المكونات المادية للحاسب الآلي ومعدات الشبكات والاتصالات، وتقديم طريقة أفضل وتبسيط خطوات الحماية بما يضمن من سهولة تنفيذها من قبل المؤسسات والأفراد. وقد أوصت الدراسة بضرورة إستخدام هذا النموذج الفعال لتعزيز حماية المكونات المادية والتوصية بضرورة اختيار اماكن تشغيل الحاسبات بعناية فائقة خصوصا أجهزة الخوادم الرئيسية (Servers)، وتشغيلها في أماكن أكثر حماية وتشديد الرقابة عليها ، وإستخدام أجهزة البصمة للتحكم في الدخول وتعقيد كلمات المرور و تغييرها بصورة دورية، أوصت الدراسة كذلك بإستخدام أحدث معدات الحماية والتأمين خصوصا أجهزة الحماية الكهربائية مثل (Fuse, Breaker and UPS Battery) ونظام كاميرات المراقبة الحديثة ذات الدقة العالية(CCTV).

الكلمات المفتاحية: الأمن والحماية ، حماية المكونات المادية ، تأمين الحاسوب، أجهزة الحماية الكهربائية، المهددات الداخلية والخارجية ، مراكز البيانات، معدات الشبكات.

A Proposed Model to Enhance the Security of Computers and Network Equipment against Internal and External Threats

Ahmed MohmmedNor Ejail
Assistant professor
Sudan Technological University, Sudan
Corresponding author email: gehad2014.system@gmail.com

Abstract

This study presents solutions for computer components problems and communication networks tools and the ways to preserve it from all internal and external threats and risks. The study took great care in concerning the damage of the parts of computer as results of un stability of electrical current in the last period. The study aimed to remind the institutions of the risks and threats which surround the computers system and the important of providing budget to build effective protection safety, determines the weak points in protection system and the ways of reinforce it to be secured from damage and loss of information. The study depended on descriptive and elicitation methods in determine the causes which leads to these problems using the models and Algorithm in designing simple protection steps. The study arrived to important results in designing a model has ability to protect the material components of computer, networks and communication tools and presented the best way in simple protection steps which leads to perform it easily by institutions and individuals. The study recommended of the necessary using of these effective methods in protecting materials, components and directed to choose suitable places to turn on computers carefully with great care especially the main servers to turn on them in more protected places, toughening up, using finger print devices to control the entering, complicate and change the passwords in continuity. The study recommended to use modern secure protection tools especially electrical protection devices like (Fuse, Breaker, UPS Battery) and the system of modern observation Cameras with high accuracy (CCTV), obligates the institutions to applicant these models especially in turn on the locations of Data Center.

Keywords: components protection, network, communication equipment, electrical protection devices.

المقدمة:

تعتبر عملية تأمين الحاسب الآلي ومعدات الشبكات أمرا في غاية الأهمية ، حيث تلعب مجموعة من العوامل الطبيعية واخري ذات تأثير سلبي قي إستمرار تشغيل المنظومات والتطبيقات والتسبب في توقفها عن تقديم الخدمات للمستخدمين لقترات قصيرة أو طويلة. إن تأمين وحماية مكونات الحاسب تحتاج الي خطة متكاملة لتجتنب حدوث الأعطال والبداية تكمن في تأمين المكونات المادية ومن ثم الإنتقال الي حماية البرمجيات والأنظمة لسلامة البيانات والمعلومات. إن مسألة حماية مكونات الحاسوب وتشكل هاجسا كبيرا للمؤسسات والهيئات خصوصا الأمنية والمالية منها، والتي تعتمد أعتمادا أساسيا علي منظومات الحاسوب في إنجاز الأعمال. إن الخطر الحقيقي يشمل المكونات المادية والبرمجية علي حد سواء ومعدات الشبكات والإتصالات والتي تستخدم في الربط الشبكي. وتتلخص تلك المشاكل في تذبذب التيار الكهربائي وارتفاع درجات الحرارة ودخول السوائل والأتربة والغبار، والتعرض لأشعة الشمس المباشرة ودخول الأشخاص بصورة غير قانونية علي أماكن المعدات وسرقتها أو الدخول علي الأجهزة والمعدات بغرض السرقة أو إتلاف البيانات والمعلومات.

مشكلة الدراسة:

1- إحتراق بعض مكونات الحاسب الآلي المادية واجزاء من معدات الشبكات والاتصالات نتيجة لتذبذب التيار الكهربائي، وتوقف بعض المعدات عن العمل نتيجة لتراكم الغبار والأتربة ودخول السوائل، وإختراق المتطفلين لأنظمة الحاسب الآلي والشبكات.

2 – عدم إتباع معظم المؤسسات سياسة الخصوصية الآمنة والحماية اللازمة للمحافظة علي الأجهزة والمعدات، وإزدياد المخاطر في مراكز البيانات(Data Center) للمؤسسات والهيئات والمراكز البحثية.

3- التوقف المفاجئ لأنظمة الحاسب الآلي نتيجة لحدوث أضرار في المكونات المادية أو البرمجية، وارتفاع تكاليف الصيانة خصوصا الأضار في وحدات المعالجة والتخزين والمراِقبة والاتصالات.

4- عدم المراقبة الكافية لأماكن تشغيل الحاسبات تجعلها عرضة للسرقة وفقدان بعض المعدات الهامة.

أهداف الدراسة:

- تكمن أهداف الدراسة في إتباع سياسة تأمين وحماية للحاسب الآلي ومعدات الشبكات والاتصالات ، ضد تذبذب التيار الكهربائي. تقديم طريقة أفضل للتشغيل الآمن باستخدام خوارزمية توضح أفضل السبل التي يجب إتباعها في الأمن والحماية(Security & Protection).

- تقديم افضل السبل لتأمين وحماية مكونات الحاسب المادية وملحقاته بما يضمن من إستمرارية في العمل وتفادي المشاكل والاعطال، ورفع درجة الوعي لدي المستخدمين بضرورة التشديد علي تنفيذ أقصي ما يمكن لتطبيق خطط التأمين والحماية.
- تنبيه المؤسسات والأفراد بالمخاطر والمهددات التي تحيط بأنظمة الحاسب الآلي، وضرورة توفير الميزاتيات اللازمة، وتبني مبدأ الوقاية من البرمجات الضارة وأهمية إقتناء البرمجيات الاصلية للدفاع لصد هجمات الفيروسات والإختراق.

أهمية الدراسة:

تكمن أهمية هذه الدراسة في تقديم وتعزيز طريقة أمثل في تأمين الحاسبات والمعدات بوسائل حماية ذات درجات حماية أعلي من حيث مبدأ العمل ونظرية التشغيل، وتشكل جملة التهديدات خطرا يهدد من استمرارية العمل علي الانظمة خصوصا خطر عدم الاستقرار الكهربائي وتأثيره علي تلف بعض المكونات والمعدات وتكون سببا للأعطال وتوقف الانظمة عن العمل مع ملاحظة ارتفاع تكاليف الصيانة والزيادات العشوائية في قطع الغيار في الاسواق. تكمن اهمية الدراسة ايضا للتقليل من المهددات الطبيعية ووضع سياسات تشغيل تساعد في خفض درجات الحرارة وزيادة درجة المراقبة للاجهزة والمعدات من السرقة والتطفل وتوفير حماية قصوي للأنظمة التي تحتوي البيانات والمعلومات ، وضرورة توفير أعلي معايير الدخول المصرح به للأماكن الحساسة في المؤسسات مثل: مراكز البيانات، أماكن معالجة البيانات الحساسة، مراكز المراقبة الأمنية، غرف إتصالات الشبكة و سجلات المراقبة لنظام الكاميرات الرقمية الحديثة (CCTV).

منهجية الدراسة:

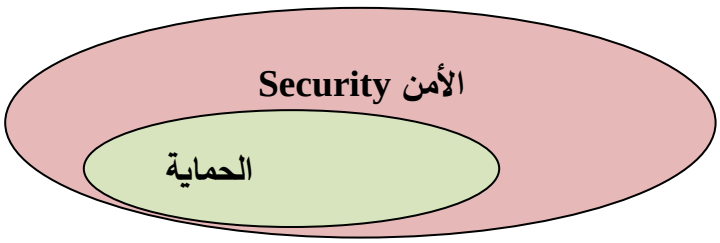
استخدمت الدراسة المنهج الوصفي والاستنباطي لفهم طبيعة المشاكل والمهددات والمخاطر التي تهدد الحاسب الآلي وملحقاته ومعدات الشبكات والاتصالات الضرورية لتشغيل الأنظمة التي تخدم المستخدمين، وتم استنتاج واستخلاص جملة من المعايير القياسية الموصي بها لضمان سلامة البيانات والمعلومات وتأمين المعدات الخاصة والعمل علي تنفيذها بيما يضمن استمرارية العمل وضمان استمرار الأنظمة في تقديم الخدمات للمستخدمين وطرق تأمين وحماية ووضع الخطوات الضرورية تلك في صورة نموذج يضمن التشغيل الآمن للحاسب الآلي وتم استخدام الخوارزميات في التصميم ووضع الحلول اللازمة لحل تلك المشاكل والمهددات وتطبيق مجموعة المعايير الضرورية لضمان الأمن والحماية القصوي.

الدراسات السابقة(مقارنة وتعقيب)

ركزت الدراسات السابقة بصورة رئيسية علي أمن المعلومات ووضع سياسات وضوابط التعامل معها وكيفية المحافظة عليها مثل دراسة (عبدالباري،2020) والتي إهتمت بدراسة أمن وشفافية المعلومات في بيئة تكنولوجيا المعلومات ، وهنالك دراسة (عبدالحميد،2012) والتي ركزت علي أهمية أمن شبكات المعلومات وما هي المخاطر التي تهددها؟ وكيفية مناهضة هذه المخاطر والحماية منها. وهنالك منشورات الهيئة الوطنية للأمن السيراني(2018) ، والتي إهتمت ووضعت ضوابط للأمن السيبراني للأنظمة التشغيلية وكيفية تأمين الأنظمة التي تخدم المؤسسات والمراكز البحثية. بينما تناولت الدراسة جملة المهددات الداخلية والخارجية وركزت بصورة كبيرة علي المهددات المادية ، والتي تتمثل في إحتراق بعض مكونات الحاسب الآلي المادية واجزاء من معدات الشبكات والاتصالات نتيجة لتذبذب التيار الكهربائي، وتوقف بعض المعدات عن العمل نتيجة لتراكم الغبار والأتربة ودخول السوائل، وإختراق المتطفلين لأنظمة الحاسب الآلي والشبكات. التوقف المفاجئ لأنظمة الحاسب الآلي نتيجة لحدوث أضرار في المكونات المادية أو البرمجية، وارتفاع تكاليف الصيانة خصوصا الأضار في وحدات المعالجة والتخزين والمراقبة والاتصالات. عدم إتباع معظم المؤسسات لسياسة الخصوصية الآمنة والحماية اللازمة للمحافظة علي الأجهزة والمعدات، وإزدياد المخاطر في مراكز البيانات(Data Center).

الأمن والحماية (Security and Protection):

هنالك اختلاف كبير جدا ما بين الامن والحماية الخاصة بالحاسب الالي ومعداته من شبكات واتصالات والتي تتمثل في التالي:



شكل (1): الاختلاف بين الأمن والحماية

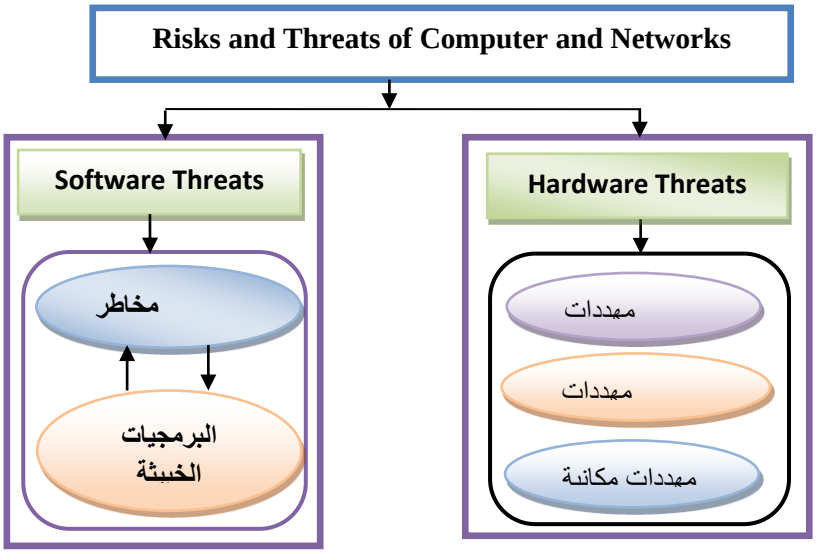
المصدر: تصميم الباحث 2026م

من خلال الشكل أعلاه يتضح أن الأمن(Security) مسألة خارجية تتضمن توفير أقصي درجات الحماية للمعدات والمكونات من المهددات الخارجية للأجهزة وتأمين الغرف التي تستخدم كغرف للخوادم (Servers) ، وحمايتها عن طريق التحصين الجيد للمباني واستخدام نظام كاميرات المراقبة(CCTV)، والبوابات الالكترونية وانظمة البصمة للدخول، واستخدام كلمات المرور للعمل علي الحاسبات ومعدات الاتصالات والربط الشبكي،

حيث تعتبر مسألة تامين المعدات الفيزيائية والاهتمام بها ذات أثر كبير وذلك لضمان السلامة الداخلية لنظم المعلومات. أما الحماية (Protection) فهي مسألة داخلية ترتبط ارتباطا وثيقا بحماية الأنظمة والملفات والبيانات والمعلومات بصورة أساسية وضرورة توفير اقصي درجات الحماية لها من المهددات الخارجية والداخلية وضرورة اتباع سياسات الخصوصية للتعامل مع الملفات في الحاسب الالي وتوزيع الصلاحيات للمستخدمين بما يضمن المسائلة القانونية في حال حدوث خرق للأنظمة وتجاوز الصلاحيات.

مهددات الحاسب الآلي

هنالك مجموعة من المخاطر والمهددات التي تعمل علي الحاق أضرار كبيرة تتمثل في التخريب والعبث بالبيانات والمعومات أو التسبب في ايقاف الأنظمة عن العمل وتعطيل بعض الخدمات ، مما يتسبب في أضرار وخسائر كبيرة مع الأخذ في الاعتبار إرتفاع تكاليف الصيانة(القياس،2010). أخطر المهددات علي الاطلاق هو تذبذب التيار الكهربائي وارتفاع درجات الحرارة و البرمجيات الضارة (Male ware) ، مثل فايرويس حصان طروادة (Trojans) بعض من هذه الفيروسات من هذا النوع تصيب وتعطل عمل الدوائر المتكاملة التي تم تصنيعها باستخدام الشرائح ذات التقنية عالية(VLSI) وتحاول أن تعطل طريقة عملها المنطقي(Logic) حتي تخرجها من طور عملها الصحيح(He,2022). تعمل هذه المهددات علي الحاق الضرر الكبير بأنظمة الحاسب الآلي والتلاعب بالبيانات والمعلومات والتحكم في تشغيل الانظمة وتطبيقاتها، تلك المهددات والمخاطر تعمل لعدة أسباب منها اسباب اقتصادية ومالية أو سياسية وأخري بغرض التخريب فقط، وتقع مسؤلية تلك المهددات والمخاطر علي عاتق المهندسين ومدراء مراكز البيانات في المؤسسات وضرورة إتباعهم أعلي درجات الحزر والمحافظة علي تلك الأنظمة وجعلها تعمل بصورة مستمرة.



شكل (2): مهددات ومخاطر الحاسوب

المصدر: تصميم الباحث 2026م

❖ **المهددات الطبيعية:** جملة من العوامل الطبيعية تمثل خطرا علي الحاسب الالي وملحقاته منها:

I. **الغبار:** يحتوي الغبار علي ذرات دقيقة من الرمل ومواد عضوية تعمل تعمل علي سد مراوح التهوية الداخلية وتكون طبقة عازلة مما يتسبب في توقفها عن العمل وبالتالي ارتفاع درجات الحرارة، ايضا يسد الغبار والاتربة رؤس القراءة والعين الليزرية في المشغلات (Drivers).

II. ارتفاع درجات الحرارة: إرتفاع درجات الحرارة من أخطر المهددات للحاسب الآلي وملحقاته ، ولابد من توفير التهوية المناسبة واستخدام مكيفات الفريون في غرفة الخادم(Server) حتي نضمن البرودة العالية وهي الافضل للتشغيل ظويل الأمد للحاسبات ومعدات الشبكات والاتصالات. من المعلوم ان ان العناصر الالكترونية تحتاج الي تبريد مستمر خصوصا تلك التي تعمل بصورة دائمة بدون توقف مثل الحواسيب الرئيسية(Main Frame) وتطلق علي الحاسبات الكبيرة جدا very large computer ، والتي يتم استخدامها في تشغيل التطبيقات التجارية مثل البنوك وشركات التأمين، ولها القدرة علي معالجة كمية هائلة من بيانات(المهدي،2009).

III. **عوامل التآكل :** يعتبر دخول الماء والاملاح مواد خطرة علي الحاسب الالي وملحقاته وبالتالي الالتزام بتجنب انسكاب الماء او اي سوائل اخري والمحافظة من الرطوبة. تتسبب السوائل (والغازات) في سرعة تآكل أجهزة الكمبيوتر ومكوناتها وتكمن المشكلة الحقيقية في تأكسد الموصلات بالدوائر مما يسبب في تآكل المكونات الداخلية(عبدالكريم،1999)

مخاطرومهددات الطاقة الكهربائية(Power Risks):

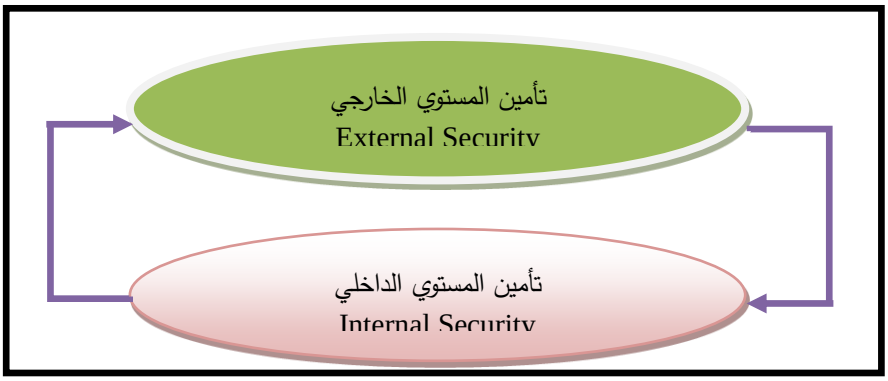
- **تذبذب التيار الكهربائي:** من الملاحظ والشائع جدا في الآونة الاخيرة عدم الاستقرار في التيار الكهربائي، وجملة المشاكل الناتجة عن ازدياد الجهد وانخفاضه ويسمي تذبذبا في التيار الكهربائي، ومن المعروف ان انخفاض الجهد يؤدي الي زيادة التيار الكهربائي المستهلك وبالتالي يؤدي ارتفاع درجات الحرارة في وحدة مزود الطاقة(Power Supply) وبالتالي التسبب في احتراق الفيوز(Fuse) او احد مكوناته الداخلية مثل المكثفات(جيلاني،2006).
- **الكهرباء الساكنة(static electricity):** مصدرها جسم الانسان وتصدر نتيجة للاحتكاكات، وتظل في جسم الانسان الي حين ملامسة شحنة معاكسة لها حينها تنشط وتتحول الي كهرباء لها تأثير علي المكونات الالكترونية(Michael,2017). ولتجنبها يجب لبس أساور تفريغ الشحنات وهي عبارة عن أداة جاهزة تستخدم بكثرة لدي الفنيين أو بملامسة أي جسم معدني لتفريغ الشحنات خصوصا عند الشروع في صيانة

الحاسب الآلي. تكون الكهرباء الساكنة خطرة عندما تقترب نسبة الرطوبة من 100% وإزدياد مستوي الفولتية عندها تكون خطرا علي الشرائح اللالكترونية وتتأثر بها الحاسبات(عبدالكريم،1999).

المخاطر والمهددات المكانية

هنالك مجموعة من المهددات تنشأ من عدم تهيئة المكان بصورة جيدة وعدم اختيار المكان المناسب لتشغيل أجهزة الحاسوب ومعدات الشبكات والاتصالات تكون هذه المعدات عرضة لخطر السرقة وبالتالي لابد من وضعها في أماكن محصنة وتشديد الرقابة علي الوصل الي تلك الأماكن وذلك باستخدام بوابات متينة واستخدام نظام البصمة و انظمة المراقبة الالكترونية بتثبيت الكاميرات الرقمية الحديثة ذات الدقة العالية والمراقبة من علي البعد. يجب تركيب مجسات الحرائق وتوصيلها بمنظومة إطفاء الحريق في المبني. تتضمن مجموعة من الاحتياطات اللازمة للحفاظ علي المعدات والاجهزة من خطر المهددات التي تحيط بها وهي توفير طفايات حريق ومجسات تعمل كشف الدخان والحريق والتاكد من عملها وتجربتها مسبقا.

مستويات الحماية للحاسب الآلي(Levels of Protection):

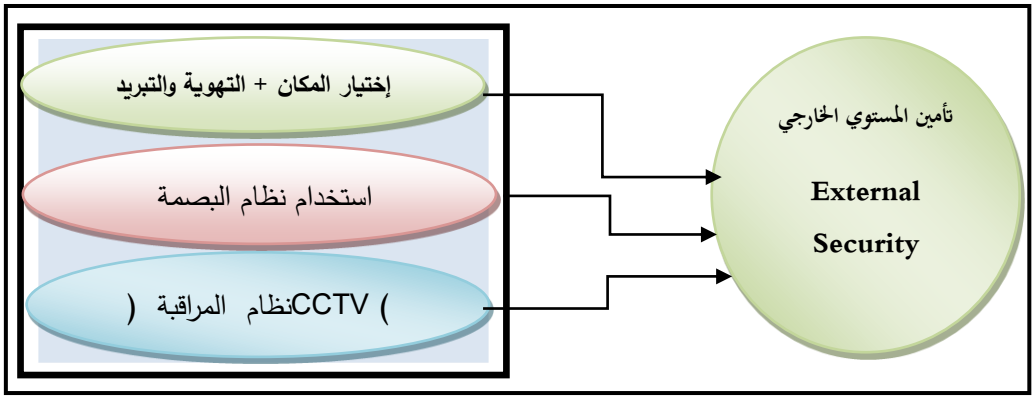


شكل(3): بنية مستويات الحماية

المصدر: تصميم الباحث 2026م

1. **مستوي الحماية الخارجي (External Level):** يقصد به المحيط الخارجي لأماكن تشغيل الحاسبات ومعدات الشبكات والاتصالات والبيئة المحيطة بها من الخارج والمراقبة الدقيقة والإختيار الصحيح للمكان وضرورة توفير أصي حماية، وضع سياسات وضوابط التامين الخارجي.
2. **مستوي الحماية الداخلي (Internal Level):** يقصد به توفير تيار آمن لتشغيل معدات الحاسوب ولحقاته ومعدات الشبكات والاتصالات، وضبط صلاحية الدخول لتلك الأجهزة والمعدات والعمل عليها باستخدام كلمات المرور.

نموذج الحماية للمستوي الخارجي(External Level Model):



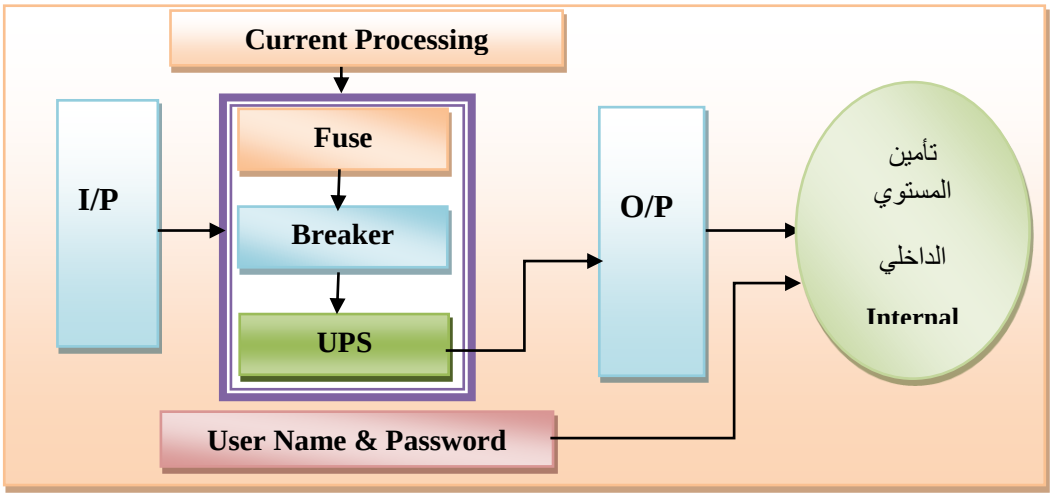
شكل(4): بنية النموذج المقترح لحماية المستوي الخارجي

المصدر: تصميم الباحث 2026م

طريقة عمل النموذج :

في النموذج اعلاه في البداية يتم اختيار المكان الانسب وبعيدا من الواجهات الرئيسية، خصوصا الأجهزة الرئيسية وخوادم البيانات (Servers) وضرورة توفير التهوية المناسبة واضافة عناصر التبريد مثل مكيفات الفريون، وتأمين عملية الدخول باستخدام أجهزة أدخال البيانات الحيوية(بصمة العين –– بصمة الوجه وبصمة اليد) وانشاء قاعدة بيانات لحفظ سجلات الاشخاص المصرح لهم بالدخول واستخدام تلك الاجهزة والمعدات خصوصا اذا كانت الغرفة مستخدمة كمركز بيانات للمؤسسة(Data Center) ، وتحفظ بداخلها الأجهزة الرئيسية مثل(Server, Fiber Switch, Routers)، مراقبة المكان باستخدام نظام كاميرات المراقبة الحديثة(CCTV) ذات الجودة والدقة العالية.

نموذج الحماية للمستوي الداخلي(Internal Level Model)



شكل (5): بنية النموذج المقترح لحماية المستوي الداخلي

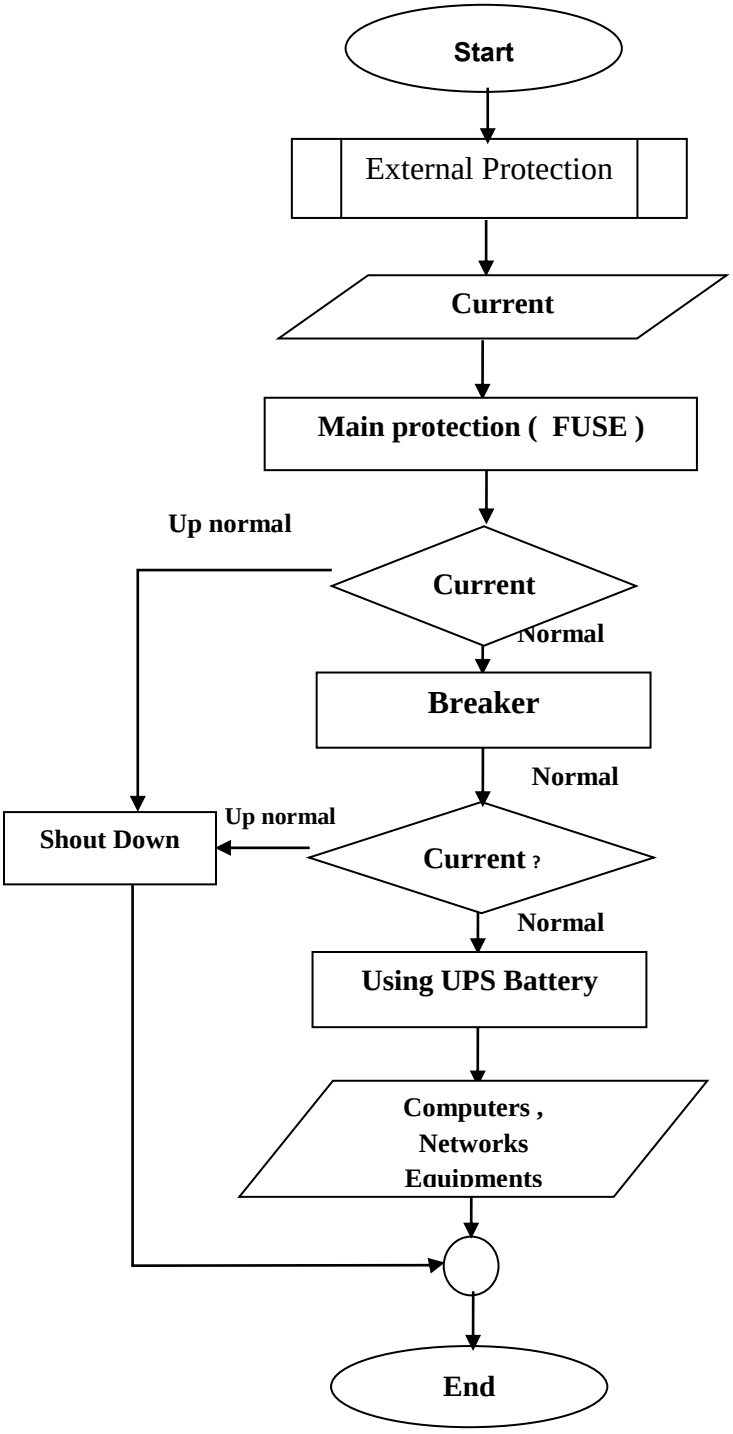
المصدر: تصميم الباحث 2026م

طريقة عمل النموذج :

يعتمد تنفيذ النموذج أعلاه علي مجموعة مكونات كهربائية واخري الكترونية وبرمجية، في البدية لابد من اختيار المكان المناسب لتشغيل الحاسب الالي واختيار الابواب ذات الاقفال الجيدة وادخال انظمة البصمة لفتحها وضرورة تركيب الكاميرات الرقمية عالية الدقة مع اضافة خاصية التسجيل وذات الحساسة بالنسبة للضوء لتعمل ليل نهار بدون توقف لمراقبة المكان، واخيرا استخدام كلمات المرور القوية وتعقيدا والعمل علي تغييرها بصورة دورية للدخول علي الحاسبات وأجهزة الشبكات.

علي المستوي الثاني لابد من استخدام المنصهر(Fuse) عند مدخل التيار الكهربائي لتحسس مقدار الجهد الداخل والاحتراق في حال الجهد العالي ومن ثم تمريره علي قاطع الدائرة والحماية(Circuit breaker) للحماية وفصل التيار الكهربائي في حال حدوث مشكلة في احد المعدات(العسلي،2024). بعده يمرر الجهد علي المنظم الرقمي ذات التقنية العالية((uninterrupted power system(**UPS**) حيث يعمل هذا النوع من المنظمات علي استلام الجهد والتحقق من قيمته (220 v) ودرجة ملائمته لتشغيل لأجهزة الحاسب الالي. أيضا هذا النوع من المنظمات الرقمية له القدرة علي تخزين الطاقة الكهربائية بقدر يسمح بتشغيل المعدات واجهزة الحواسيب عمد الانقطاع المفاجئ لمصدر الطاقة الأساسي وإاليحين تأمين مصدر طاقة بديل، وهذا يضمن من استمرارية التشغيل للمعدات والحواسيب بدون إنقطاع للخدمات التي تقدم للمستخدمين.

الخوارزمية العامة:



شكل(6): الخوارزمية العامة

المصدر: تصميم الباحث 2026م

الخلاصة

من خلال تتبع تصميم النموذج المقترح والخوارزمية التي توضح الخطوات والاجراءات فإن الإلتزام بتنفيذها تضمن الدراسة الي الوصول الي أقصي درجات الحماية والتي تتمثل في الآتي:

1- ضمان أقصي درجات الحماية للحاسبات والمعدات من المهددات والمخاطر ومخاطر تذبذب التيار والكهربائي مما يضمن استمرارية التشغيل وعدم توقف الانظمة التي تعمل علي تشغيل التطبيقات التي تخدم المستخدمين.

2- تضمين هذا النموذج للمراقبة الحديثة لأماكن تشغيل أجهزة الحواسيب وملحقاتها يضمن مراقبتها من علي البعد عبر غرف المراقبة المركزية أو المراقبة عبر استخدام الإنترنت في حال التجوال، ويحقق أقصي ضمان لمراقبة المكان وتوثيق عمليات الدخول والخروج.

3- تطبيق نماذج الحماية المقترحة في الدراسة يحقق أفضل طريقة لإدارة المخاطر بصورة تضمن من تخفيض تكاليف الصيانه والسيطرة عليها وتوفير المال والجهد وضمان التشغيل المستمر للأنظمة والتطبيقات.

4- إتباع سياسات الحماية المتبعة في التصميم والتمتع بكافة الخدمات وضمان استمراريتها من قبل الشبكات الموزعة والتي تخدم مجموعة أجهزة الحواسيب الطرفية.

التوصيات:

1- ضرورة تطبيق المعايير الموصي بها بما يضمن التشغيل الآمن وتحقيق أعلي درجات الحماية القصوي لجميع معدات الحاسب الآلي وأجهزة الربط الشبكي والإتصالات، ووضع الميزانيات المطلوبة لتنفيذ وتطبيق ما جاء في النموذج والبروتوكول الموصي به وتنفيذه في كافة مواقع تشغيل الحاسبات ومعدات الشبكات والاتصالات.

2- ضرورة تنفيذ هذا النموذج الفعال في المؤسسات والهيئات خصوصا في مواقع تشغيل الحاسبات المركزية(Servers) ومراكز البيانات الرئيسية(Data Center).

3- إستخدام أحدث معدات الحماية والتأمين خصوصا أجهزة الحماية الكهربائية مثل (Fuse, Breaker and UPS Battery) وكاميرات المراقبة الحديثة ذات الدقة العالية(CCTV).

4- عدم مشاركة الحاسوب لأي جهاز كهربائي آخر علي نفس مصدر الطاقة وعدم تشغيل المحركات الحثية ثلاثية الطور علي نفس المصدر.

5- التأكد من عدم وجود أي مصدر للإهتزازات علي نفس الطاولة التي يعمل عليها الحاسب الآلي مع عدم إشتراك الحاسب الالي مع جهاز كهربائي في مصدر الطاقة(Voltage Source).

6- تشغيل الحاسب الرئيسية في أماكن أكثر حماية وتأمينا وتشديد الرقابة عليها وإستخدام أجهزة البصمة للتحكم في الدخول وتعقيد كلمات المرور وضرورة تغييرها بصورة مستمرة.

7- ضرورة الالتزام بإجراء النسخ الاحتياطي(Backup) للبيانات والمعلومات بصورة دورية والاحتفاظ بها بعيدا عن أماكن تشغيل الحاسبات والخوادم الرئيسية(Servers).

8- عدم تشغيل أجهزة كهربائية تولد طاقة حرارية اثناء التشغيل مثل الثلاجات والافران الكهربائية ، ولابد من تركيب مجسات للحرارة لكي تطلق انذارا في حال ارتفاع درجات الحرارة خارج النطاق المسموح به.

9- إبعاد الحاسوب من مصادر الضجيج العالية وعدم تعرضه لأشعة الشمس المباشرة والمحافظة علي مستوي معتدل لدرجات الحرارة وضروة تأمين التبريد لغرف تشغيل الخوادم الرئيسية(Servers).

قائمةالمراجع والمصادر:

1- محمد علي محمد المهدي / فايد كرم علي (2009)، أساسيات الحاسب الآلي، جامعة قناة السويس ، ص 21.

2- حسنين، رجب عبد الحميد(2012) ، " أمن شبكات المعلومات الإلكترونية: المخاطر والحلول" Cybrarians Journal ، العدد(30) ، الصفحات : 74 – 101 .

3- شركة القياس لمهارات الحاسوب(2010)، أمن تكنولوجيا المعلومات، سلسلة منشورات الرخصة الدولية لقيادة الحاسب الآلي(ICDL Approved Courseware 2010) ، الاصدار السادس ، ص17.

4- عبدالباري منير عبدالفتاح(2020) ، " أمن وشفافية المعلومات في البيئة الرقمية : إعتبارات وأبعاد وتوجهات أمن المعلومات " ، المركز الرئيسي - الجامعة الاسلامية بمنيسوتا .

5- المؤسسة العامة للتدريب التقني والمهني(-)، مهارات صيانة الحاسب الالي، الادارة العامة لتصميم وتطوير المناهج ، المملكة العربية السعودية، ص19.

6- العقيل عبدالكريم (1999)، الكمبيوتر المرجع الكامل ، مكتبة جرير ، الطبعة الاولي ، ص64.

7- جيلاني محمود(2006)، نظم الحماية الكهربائية ، جامعة القاهرة ، الطبعة الاولي.ص35.

8- العسلي فراس / النائلي نصر / المرادات عوني(2024)، الشبكة الكهربائية الذكية ومدي مرونتها انظمة الحماية الكهربائية في التهديدات السيبرانية ، الجامعة الهاشمية ، المجلة العربية للبحث العلمي،.ص1-12.

9- الهيئة الوطنية للأمن السيبراني(2018)، الضوابط الاساسية للأمن السيبراني Essential Cyber security Control (ECC-1: 2018) ، وزارة الاتصالات ، المملكة العربية السعودية. ص25.

مصادر باللغة الإنجليزية:

1- Hansen Stive, Jordan Byron, Lang Mike and Walsh Peter (2016) "System Protection Note 1: Fuses versus circuit breaker s for low voltage applications", Expertise, our Source of Energy EP.MERSEN.com – page 3.

2- Michael and Herbert (2017) "Principal of information security", Congage Learning, Sixth edition Kennesaw state University, Page 505.

3- He Yang(2022), " study on Hardware Security and its Defense Measures " , SHS web Conference 144,02011(2022) ,[STEHF 2022]. Page 3.