התכנית לתואר שני M.Sc. בניהול טכנולוגיה

הצעה למחקר בנושא:

"סיכוני סייבר במכשור רפואי"

מוגש ע"י

שם הסטודנט: פליקס קרסניצקי צבי ששון ת.ז.: 306012865 022114730

שם מנחה/ים : ד"ר הראל מנשרי ד"ר הדס לוי

1. מבוא
   1. רציונל המחקר

מכשור רפואי ביתי דוגמת: קוצבי לב, משאבות אינסולין, מכשירי ECG ביתיים ומכשירים רפואיים אחרים, נעשים מתקדמים יותר ויותר. במקביל, שירותים רפואיים שונים עוברים טרנספורמציה דיגיטלית ולמעשה מאפשרים התגברות על פערי מרחק וזמן. מרבית המכשירים והשירותים הרפואיים מכילים תוכנה ומתבססים על חיבוריות לרשתות שונות, לרבות רשת האינטרנט. המידע הרפואי עובר על גבי רשתות בתי חולים, קופות חולים וטלפונים ניידים של המטופלים, על מנת להיות משולב בבסיסי הנתונים ולאפשר שיתוף מידע זה עם גורמי קצה (לדוג' רופאים מאבחנים).   
הטכנולוגיות החדשות עוזרות להגיע לאבחון מדויק יותר בזמן קצר, דרך איסוף כמות מידע גדולה (נתוני עתק), זיכוך וטיוב הנתונים בעזרת אלגוריתמים מתקדמים, ללא צורך בטיפול אמבולטורי. הטכנולוגיות נוחות למטופל עקב היותן משולבות בחיי היום יום שלו ומאפשרות למטפל לקבל מידע על המטופל שאין באפשרותו לקבל רק מביקור במרפאה וטיוב קבלת החלטות טיפוליות.  
לדוגמה מחשוב לביש (i.e. ECG holter) מאפשר לחולי לב להיות מנוטרים 24/7, כאשר הם ממשיכים את אורח חייהם בצורה רגילה וללא צורך באשפוז ואף ביקור במרפאות. השתלת משאבות אינסולין זעירות המבוקרות ע"י מיקרו בקר מאפשרות לחולי סכרת לקבל מינון מדויק של אינסולין, כאשר תוצאות התהליך במלואו מנותרות מרחוק ע"י רופא. שרותי אבחון המתבססים על מצלמה או על מכשור דגימה מרוחק, מאפשרות קבלת אבחון בכל שעות היום והלילה ללא יציאה מהבית. טכנולוגיות לבישות אחרות מצילות חיים יום יום ע"י אוטומציה של קריאה לעזרה רפואית כאשר מערכת חכמה מזהה נפילה או במקרי חרום אחרים.

מכלול הטכנולוגיות הללו מביא לשינוי ברפואה ובמודל הטיפולי בהפיכתו לאינטגרטיבי, רציף, נגיש בבית או בכל מקום אחר ומציב את המטופל ואורח חייו במרכז.

הטכנולוגיות הנ"ל מסתמכות על חיישנים, מזעור המחשוב ועל קישוריות רציפה או מתוזמנת, הנעשית ברובה בתווך האינטרנט, אשר פתוח לכל. בכך, טכנולוגיות אלו חשופות לאיומי סייבר, החל מאיום על פרטיות המידע, אמינותו וכלה בהשתלטות על עזרים רפואיים מרחוק, העלול להביא לסיכון ושליטה על חייהם של המשתמשים.

* 1. מטרת המחקר

עבודת מחקר זו נועדה לסייע לפיתוח הטכנולוגיות הרפואיות המרוחקות באמצעות בחינת "מודל יהלום למיפוי סיכוני סייבר במכשור רפואי מחובר". המודל מציג 4 תהליכים פונקציונליים עיקריים, המורכבים מנקודות השפעה שונות, התהליכים מתקיימים במקביל זה לזה ואינם בהכרח תלויים זה בזה. המודל מראה תלות בין נקודות ההשפעה השונות וממפה את סיכוני הסייבר העולים מתלות זו.

סיכון סייבר, על פי מודל CIA כולל: פגיעה בסודיות, אמינות ושלמות מידע, ותפקוד המכשיר. מודל זה פותח ע"י מערך הסייבר הלאומי, ולכך נוסיף גם את רכיבי הזמינות והשרידות

* 1. שאלות המחקר
     1. שאלות המחקר שננסה לענות עליהם הן:  
        1. האם קיימים סיכוני סייבר שלא מופו ע"י "מודל היהלום"?  
        2. מה רמת החשיפה של מכשור הרפואי ביתי והמטופל לסיכון שלא מופה ע"י מודל היהלום?  
        3. לאילו שירותים ומכשירים המודל נותן מענה מלא ולאילו פחות?
  2. משתנים תלויים ובלתי תלויים

היות ואופי המחקר הנו יותר איכותי (התאמת מודל למגוון שירותים ומוצרים) קשה לנסח מדד כמותי אמין לעבודת חקר זו.

* + 1. השערת המחקר: מודל היהלום מתאים לשימוש ככלי לזיהוי נקודות כשל אפשריות במובן של אבטחת מידע והגנה על פרטיות בפיתוח כלים ושירותים רפואיים.
    2. השערת מחקר 2: במידה ותמצא אי התאמה בין מודל היהלום ומושא הבדיקה, ניתן יהיה להתאימו בקלות יחסית עם שיכסה גם מקרה זה.
  1. חשיבות המחקר

עולם הרפואה עובר במהלך השנים האחרונות למערך של רפואה ביתית, במטרה להקל על הפעילות המתבצעת בבתי החולים ובמרכזים הרפואיים, ובעיקר על המטופלים עצמם, ולפיכך, המחקר הנו בעל חשיבות גבוהה. אירועי התקופה האחרונה ובעיקר הבידוד החברתי, בעקבות התפשטות מחלת ה COVID-19, מגביר את חשיבותו של המחקר. העולם עבר לקבלת שירותים מרוחקים, וקיימת האצה גם במתן שירותי רפואה מרחוק. עקב חוסר רגולציה ברורה לגבי שימוש במכשירים שאינם ייעודיים לעולם הרפואה ( אינטרנט, טלפון חכם) ו/או חוסר הבנה מצד חברות המפתחות מכשור לטיפול רפואי מרחוק , את נהלי הפיתוח המאובטח הרשמיים, קיים קושי בפיתוח והטמעה של מוצרים מאובטחים לשוק הרפואי.

מודל היהלום עשוי לתת מענה להגשת תהליכי פיתוח מאובטח ו/או אישור למוצרים רפואיים מרוחקים. המודל פשוט להבנה ויישומו יפשט תהליכי פיתוח וקיצור זמנים עד לקבלת מוצרים ושירותים לשוק. זאת, בהיבט אבטחת המידע ומהימנות השירותים.

1. סקר ספרות ראשונית
   1. הקדמה

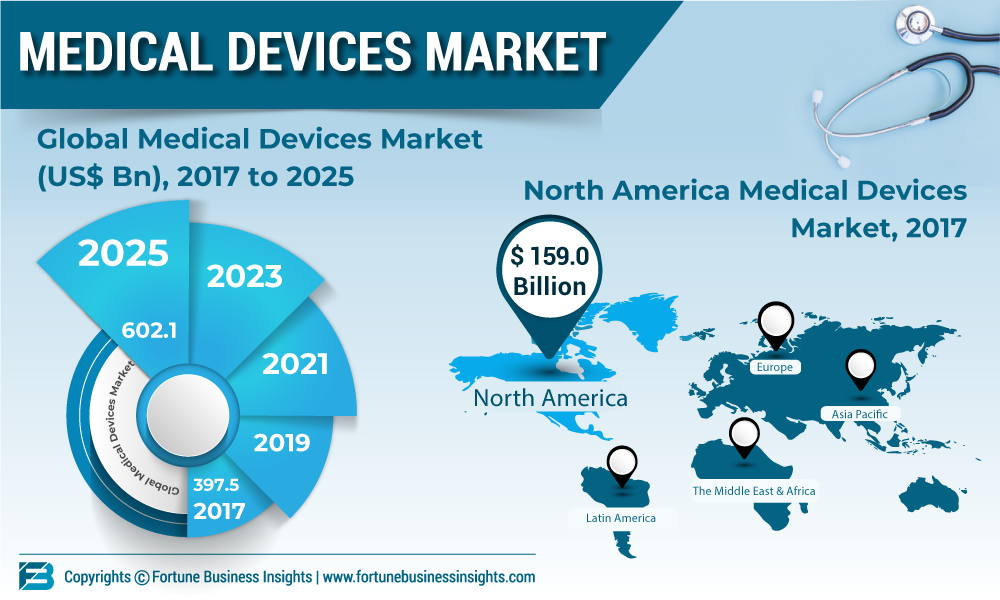
בפרק זה נסקור את המידע הזמין במקורות מקצועיים ואקדמיים בנושא:

* אבטחת מידע והגנה על פרטיות
* איומים על המידע מצד גורמים זדוניים
* טכנולוגיות רפואיות מרוחקות.

מקורות המידע הינם מקורות דיגיטליים פתוחים (מאמרים, אתרי cert לאומיים – בין היתר של מדינות OECD , ספרות מקוונת) וכן מקורות פרסונליים: מנהלי פרויקטי סייבר, יזמים בתחום הגנת מידע, מפתחים בחברות בעלות זיקה לאבטחת מידע ורפואה.

מיקוד הלמידה של התחום דואלי - מצד אחד, איומים ונהלים קיימים ומאידך פיתוח טכנולוגי רפואי.

כאמור, פיתוח טכנולוגי רפואי הנו תחום בעל קצב גדילה הולך וגובר [‏1]. זאת, במקביל להתפתחות טכנולוגיית המידע, והשימוש בה, אשר נהיה נפוץ ונגיש לרמת משתמש קצה ממוצע. כמות המידע העובר ברשתות גלויות ובין היתר מידע רפואי פרטי מהווה יעד אטרקטיבי לגורמים זדוניים על מנת ליירט ולעשות שימוש במידע כמו גם לפגוע באמינות וזמינות המידע. אבטחת המידע והגנה על הפרטיות לא הייתה נדרשת לולא האיומים על המידע מגורמים זדוניים.



איור 1 - צפי גידול שוק מדיקל [באדיבות FortuneBuisness]

* 1. סקר ספרות בנושא: אבטחה של מידע והגנה על פרטיות

<https://www.sync.co.il/ISO-27799?gclid=EAIaIQobChMIqdTTj7TZ6QIVz9vVCh3h9AiqEAAYASAAEgJzGfD_BwE>

נושא אבטחת המידע הרפואי הינו בעל חשיבות גבוהה, ומחייב את מערכת  
הבריאות הישראלית להבטיח עמידה בסטנדרטים הגבוהים ביותר.  
.1.2עם התגברות האיומים על מערכות מבוססות מחשוב, ובכלל זה הטרור הקיברנטי,  
אנו נדרשים להגן על מערכות המחשוב הקריטיות של מערכת הבריאות בכל  
הרמות, על מנת להבטיח רצף טיפולי וניהולי כנדרש.  
.1.3למערכת הבריאות קיימים איומים ייחודיים בתחום ההגנה על המידע הכוללים, בין  
השאר:  
.1.3.1מניעת שירות ( - )Denial of Serviceדבר אשר עשוי לפגוע במתן שירות  
רפואי חיוני בשגרה ובמיוחד בחירום. התלות הקיימת כיום במערכות מידע  
לצורך אספקת חלק משירותי הרפואה, הופכת איום זה למוחשי במיוחד.  
.1.3.2גניבת מידע – מידע רפואי הינו מידע אישי רגיש ולגניבתו עשויות להיות  
השלכות קשות ברמה האישית וברמת האמון במוסדות הבריאות במדינה.  
.1.3.3שיבוש מידע – הנזק אשר יכול להיגרם משינוי מידע בתיקו הקליני של  
מטופל עולה לעיתים על הנזק מגניבתו, היות ויכול להוות בסיס להחלטות  
רפואיות שגויות

* 1. סקר ספרות בנושא: איומים על מערכות מידע מגורמים זדוניים
  2. סקר ספרות בנושא: תשתיות, שיטות ודוגמאות לשירותים ומוצרים רפואיים
  3. סיכום סקר הספרות

1. מתודולוגיה ראשונית
   1. מערך המחקר, אוכלוסיית המחקר (אם רלבנטי – הארגונים שיכללו במחקר).
   2. הפרדיגמה המחקרית – מחקר כמותי או איכותי או משולב. לנמק!
   3. תכנון מחקר גישוש (אם קיים).
   4. המדגם – (במחקר כמותי בו מתוכנן מדגם): מה יהיה גודל המדגם ומדוע? איך ייבחרו הנבדקים? במחקר איכותי: מי יהיו הנבדקים וכיצד ייבחרו?
   5. שיטת המחקר – במחקר כמותי, מה תהיה שיטת המחקר (ניסוי, סקר, מחקר קורלטיבי וכד')?
   6. כלי איסוף הנתונים – מדידות: היכן ואיך? שאלונים: כמה? איזה? מסמכים? סוג הראיונות (למשל, חצי מובנים) וסוג התצפיות (למשל, הצופה המשתתף) עם נימוקים להצדקתם.
   7. כלי מחקר נוספים (מה שרלבנטי) – סימולציות, מודלים, פיתוחים מתימטיים, תוכנות, כלי קבלת החלטות ובחירת חלופות, אלגוריתמים וכד'.
   8. בסקר – תכנון שלבי בניית השאלון (או השאלונים).
   9. תוקף ומהימנות (אם יש כבר מה לכתוב – לא הכרחי)
   10. ניתוח הנתונים - מה תהיה שיטת ניתוח ועיבוד הנתונים? בכמותי: כלים סטטיסטיים. באיכותי: ניתוח תוכן.
   11. אתיקה – דילמות אתיות ודרכי התמודדות.

כמו בכל עבודה הקשורה לדיון בפגיעויות ואפשרויות דלף של מידע אישי, עלול החוקר לגלות פרצה שמאפשרת פגיעה/שליפה של מידע אישי. במצבים אלו בעולם חקר האבטחת מידע, נהוג לדווח לחברה האחראית בדיסקרטיות, לאפשר פרק זמן לתיקון ורק אז לפרסם כי נמצאה הבעיה. הליך זה אינו אחיד ולכל חברה מדיניות משלה (Disclosure Policy). אם במהלך עבודה זו תתגלה פגיעות קריטית, נאמץ במסגרת עבודה זו את המדיניות של גוגל ונחכה במשך 90 [‏4] יום מדיווח הבעיה לחברה האחראית.

* 1. תכנון לוחות זמנים ושלבי העבודה – הסבר ותרשים גאנט
  2. הערה: כמובן שלא כל תתי הסעיפים רלוונטים לכל העבודות.

1. רשימת מקורות References ראשונית

1. [סקר חיזוי גודל שוק מכשור רפואי](1.%09https:/www.medgadget.com/2020/01/medical-devices-market-regional-analysis-2020-2025-global-market-size-research-report-trends-growth.html)
2. [הרשות להגנת הפרטיות – מדריך לתקנות להגנה על פרטיות](https://foi.gov.il/sites/default/files/%D7%94%D7%9E%D7%93%D7%A8%D7%99%D7%9A%20%D7%94%D7%9E%D7%9C%D7%90%20%D7%9C%D7%99%D7%99%D7%A9%D7%95%D7%9D%20%D7%AA%D7%A7%D7%A0%D7%95%D7%AA%20%D7%90%D7%91%D7%98%D7%97%D7%AA%20%D7%9E%D7%99%D7%93%D7%A2%20-%20PDF%20%D7%9C%D7%94%D7%93%D7%A4%D7%A1%D7%94.pdf)
3. [מדריך תורת הגנה ארגונית](https://www.gov.il/he/departments/topics/11)
4. [Google project zero Disclosure Policy](https://googleprojectzero.blogspot.com/)

את רשימת המקורות References יש לערוך לפי תקן APA. ראו למשל:

1. [http://owl.english.purdue.edu/owl/resource/560/01](http://owl.english.purdue.edu/owl/resource/560/01/)