שם הקורס: Methods for detecting cyber attacks
שם הפקולטה: מדעי הטבע
שם המחלקה: מדעי המחשב
מספר הקורס:

שם המרצה: Dr. Ran Dubin
מתכונת הקורס: **הרצאה + הרצאה מעשית**

שנת לימודים: ב' **סמסטר: קיץ** **היקף שעות: 3** **נקודות זכות:3**

אתר הקורס באינטרנט:

א. מטרות הקורס (מטרות על / מטרות ספציפיות): 3 שעות
פיתוח יכולות מחקר מבוססות על מערכות למידה בתחומי הגנת הסייבר
ב. תוכן הקורס: 3 שעות

מהלך השיעורים:
הקורס מבוסס על הבנת אבני הבינין של מערכות הלמידה והמימוש שלהם בתחומי הגנת הסייבר. יעוד הקורס הוא לשפר את מיומנות המחקר של התלמידים ולאפשר להם להתנסות במחקר מוגדר במהלך הקורס ומחקר חופשי ומעמיק על מגוון נושאים במסגרת פרויקט הסיכום.
הקורס מדגיש את הקושי והאתגרים שיש בתחומי הגנת הסייבר, מבצע בקירה רחבה על איומים ודרכי הפתרון האפשריים דרך שימוש במערכות למידה.
עולם הסייבר הוא עולם קסום ומאתגר ומטרת הקורס הינו לבצע חשיפה לעולם הזה תוך כדי חיזוק יכולות המחקר האישיות של הסטודנטים. הקורס יבצע טורניר זיהוי של נוזקות (malware) ומימוש מאמרים אקדמיים כפרויקט סיכום.

תכנית הוראה מפורטת לכל השיעורים:

Lecture	Topic(s)	Date
04/03/21	הקדמה – שימוש בלמידת מכונה בעולם הסייבר סקיוריטי	04/03/21
11/03/21	מבוא למערכות למידה (הצגת פרויקטים)	11/03/21
19/03/21 08/04/21 (2 lectures)	מבוא למערכות למידה 2	19/03/21 08/04/21

		(2 lectures)
15/04/21(will change the date)	גילוי איומים בעזרת אנומליה (הצגת תרגיל תכנות ביתי גילוי אנומליה) – נקדים את השיעור	15/04/21(will change the date)
22/04/21	זיהוי נוזקות בעזרת מערכות למידה (הצגת תחרות כיתה)	22/04/21
29/04/21	שימוש במערכות למידה לניתוח מידע מוצפן	29/04/21
06/05/21	ניתוח מידע, איסוף מידע ויצירת וקטורי מאפיינים (הצגת תחרות כיתה)	06/05/21
13/05/21	תחרות כיתה והצגת ההישגים	13/05/21
20/05/21	שיטות ensemble בסייבר סקיוריטי	20/05/21
27/05/21	DLP	27/05/21
20/05/21	פרויקט מסכם	20/05/21
27/05/21	פרויקט מסכם	27/05/21

ג. חובות הקורס:

ג.1. 10% מצגת על נושאי מתקדמים בלמידת מכונה בסייבר (בהתאם לפרויקט שהסטודנטים בחרו)

ג.2. 15% תרגיל תכנות ביתי

ג.3. 35% תרגיל תכנות ותחרות כיתתית

ג.4. 40% פרויקט מסכם על מימוש מאמר ושיפור מאמר בתחום הסייבר ההגנתי

דרישות קדם: אין אך זהו קורס מעשי ומחקרי נדרש כתיבה ב python (ניתן ללמוד במהלך הקורס בצורה עצמאית אך זה הכרח).

חובות / דרישות / מטלות: בהתאם לכל חובות הקורס נדרשות.

מרכיבי הציון הסופי (ציון מספרי / ציון עובר): 56% הגשה של כל העבודות הם חובה.

ד. ביבליוגרפיה:

1. Dua S. and Du X. Data Mining and Machine Learning in Cyber Security, CRC Press, 2011
2. Maloof M.A. Machine Learning and Data Mining for Computer Security, Springer, 2006
3. Thomas Mitchell (1997), Machine Learning, McGraw-Hill.

רשימת קריאה תינתן במהלך הקורס.