

בית הספר למוסמכים במינהל עסקים ע"ש ליאון רקנאטי

1242.3273.01 – מחקר ופיתוח בעידן הסייבר והדאטה

Research and Development (R&D) in Cyber and Data Era

(דרישות קדם: אין)

סמסטר ב' תשפ"ב – מחצית ראשונה

יום בשבוע	שעה	חדר	בחינה	מרצה	דואר אלקטרוני	טלפון
א'	21:30 - 18:45	304	עבודה מסכמת + בוחר בקיאות	ד"ר יניב הראל ד"ר יעקב מנדל	yaniv.c.harel@gmail.com jacob4x4@gmail.com	

שעת קבלה – בתאום מראש

TA: ד"ר רפי הוד (PhD, MBA), rhod@tau.ac.il

היקף הלימודים

1 י"ס

1 ECTS = 4 ECTS – (European Credit Transfer and Accumulation System) ECTS, ערך הניקוד של הקורס במוסדות להשכלה גבוהה בעולם שהינם חלק מ"תהליך בולוניה".

תיאור הקורס

הקורס הינו קורס בחירה מתקדם המשלב בין המפגש עם העולם הטכנולוגי הסייברי לבין אתגר הניהול והיזמות הפרויקטלית השואפת להפוך רעיון טכנולוגי לתוצר בעל ערך יישומי ועסקי. עולם ניהול הפרויקטים, עולם המו"פ הטכנולוגי ועולם האסטרטגיה עוברים טלטלה בימים אלו בשעה שגישות מסורתיות אינן נותנות מענה מספק בעידן בו עקרונות הפעולה והמאפיינים משתנים. קצב השינויים, אי הודאות, מקורות המימון, שיתוף הידע, שמירת IP ועוד הינם מאפיינים אשר בעולם הנוכחי מתנהגים באופן שונה ומחייבים הערכות ובניית מתודולוגיות וכלים חדשים על מנת להצליח בעולם הזה.

הקורס יעסוק בסוגיית הסייבר מנקודת מבט של תפיסת ה-NIST Cybersecurity Framework הבוחנת את התועלת הסייברית מזווית האפיון, המניעה, הגילוי, התגובה וההתאוששות. לכל אחת מהתכליות קיימות טכנולוגיות מגוונות התורמות למימוש התכלית. לכל אחת מהמשימות הסייבריות תותאם צורת התארגנות ניהולית מסויימת שתנחת ותודגם באופן מפורט. הקורס מפגיש גם עם עולם ה-DATA, נוגע ב-machine Learning וכן ב-Data Sciences.

הקורס מעניק למשתתפיו חוויה מרתקת של דילוג בין העולם הטכנולוגי לבין העולם הניהולי, תוך שאיבת מקורות הידע מהעולם האקדמי והתאורטי ומנגד מהעולם המעשי ומדוגמאות קונקרטיות שהתרחשו בעולם הטכנולוגי העסקי. הסטודנטים יתנסו בביצוע עבודה קונקרטית על נושא שיבחרו בו יתרגלו את העקרונות הנלמדים בקורס.

הקורס מניח מפגשים קודמים עם רקע בסייבר ורקע בניהול פרויקטים. הקורס מעמיק במספר נושאי הסייבר הנוגעים בדוגמאות הקונקרטיות שילמדו ובוחן אותם מרמת הבנת עולם הסייבר והאתגרים הטכנולוגיים המלווים אליה. בחלק קורס אחר יוצגו עקרונות גישות ניהול פרויקטים מודרניות וגישה ביקורתית על גישות קיימות, ולאחריהן ניתוח גישות יזמיות וניתוח האקו-סיסטם של עולם ההון סיכון והשפעתו על פיתוח הטכנולוגיה. בהמשך הקורס ישלבו יחד הנושאים הטכנולוגיים עם הניהוליים וזאת במסגרת הצגת העבודות שיתמודדו עם הסוגיות הקונקרטיות. בקורס ישתתפו מספר מרצים אורחים שיביאו מעולמות הסייבר, התעשייה והיזמות. הקורס ישלב מספר שיטות הצגה ולימוד חדשניות וייחודיות כדוגמת תוכנית ה"מיזם", סימולציות דיון הנהלה, סימולציות סטארט-אפ ועוד.

תפוקות למידה

עם סיום הקורס בהצלחה יוכל הסטודנט/ית:

1. לתאר רקע על עולם הסייבר ואתגריו.
2. להבין את עולם הפיתוח ואת התמורות שחלות בו בתקופתו.
3. לעמוד על מאפייני כל שרשרת התהליכים הקשורים בפיתוח טכנולוגי סייברי ודאטאי.
4. להכיר רקע ב-Data-science וBig-data ותרומתו הפוטנציאלית לעולם הסייבר ובכלל.
5. להכיר מתודולוגיות מובילות בעולם הסייבר והדאטה ויישום שלהם בדוגמאות פרויקטים ומיקרים אמיתיים.
6. להבין מאפיינים נוספים המחיוניים היום לעולם הטכנולוגי והעסקי כדוגמת שיתופי פעולה ועוד.

הערכת הסטודנט בקורס והרכב הציין

משקל	מטלה	תאריך	גודל קבוצה/ הערות
60%	פרויקט מסכם	בשיעור האחרון	קבוצות של 2-3 משתתפים
15%	הצגת הפרויקט בכיתה	במהלך הקורס	נוכחות חובה
15%	בוחן מסכם על חומר נלמד	TBD	מבוסס על כל החומרים שילמדו בכיתה, יפורסמו במודל, ועל הרצאות האורחים (אם יהיו)
10%	השתתפות פעילה בכיתה**	שוטף	

* עפ"י תקנון האוניברסיטה תלמיד חייב להיות נוכח בכל השיעורים (סעיף 5). תלמיד, הנעדר משיעור המחייב השתתפות פעילה או שלא השתתף באורח פעיל, רשאי המורה להודיע למזכירות כי יש למחוק את שמו מרשימת המשתתפים. (התלמיד יחויב בתשלום בגין קורס זה)

** תלמידים המשתתפים במפגש בכיתה חייבים לחתום על דף נוכחות על מנת שזה יחשב להם כנוכחות פעילה. באותם מקרים (אם יהיו) בהם תלמידים ישתתפו במפגש באמצעות הזום, חובה עליהם להגיש דו"ח קצר בן 5 נקודות, עד סוף יום המפגש: מה הם למדו במפגש ומה הם לוקחים ממנו לעתיד, על מנת שזה יחשב להם כנוכחות פעילה.

פירוט המטלות בקורס

נוכחות בשיעורים
השתתפות פעילה בשיעורים
בחירת נושא וכתובת עבודה בקבוצה המיישמת את אחד מסוגי המקרים הנלמדים ומנותחים בקורס
הצגת העבודה הקבוצתית
בוחן מסכם על החומר הנלמד

כל אי עמידה במי ממטלות הקורס מחיבת הודעה מראש (במייל) לעוזר ההוראה (TA)

מדיניות שמירה על טווח ציונים

החל משנה"ל תשס"ט מונהגת בפקולטה מדיניות שמירה על טווח ציונים בקורסי התואר השני. עקרונות השיטה חלים על כל קורסי התואר השני, ומדיניות השמירה על טווח הציונים תיושם לגבי הציין הסופי בקורס זה. מידע נוסף בנושא זה מתפרסם בהרחבה באתר הפקולטה.

<https://coller.tau.ac.il/MBA-students/programs/2021-22/MBA/regulations/exams>

הערכת הקורס ע"י הסטודנטים

בסיומו של הקורס הסטודנטים ישתתפו בסקר הוראה על מנת להסיק מסקנות לטובת צרכי הסטודנטים והאוניברסיטה.

אתר הקורס

אתר הקורס יהווה המקום המרכזי בו ימסרו הודעות לסטודנטים, לפיכך מומלץ להתעדכן בו מדי שבוע, לפני השיעור, ובכלל – גם בתום הסמסטר. **כמו-כן, כל התקשורת בנושאי הקורס תעשה דרך תיבת מסרים אישית שתפתח עבור זה במודל.**

שקפי הקורס יהיו באתר הקורס באתר.

לתשומת לבכם - בכיתה ידונו גם נושאים (ובפרט דוגמאות) שאינם מופיעים בשקפים או מופיעים בכותרת בלבד. כל אלו גם הם חלק בלתי נפרד מחומר הקורס.

תכנית הקורס *

שבוע	תאריך	נושאים	קריאת חובה	הגשות
1	13.2.22	מבוא לקורס – התחום המקצועי והמוטיבציה לקורס, מבוא לתופעת הסייבר, רקע על הטכנולוגיות ועל התופעה הסייברית העולמית, מהפכות טכנולוגיות והתקדמויות טכנולוגיות קודמות. הסתכלות רחבה על Cyber Security, על שימושים, אתגרים וטכנולוגיות.	Tabansky L. & I. Ben Israel. 2015. The National Innovation Ecosystem of Israel. <i>Cybersecurity in Israel</i> . Springer International Publishing.	
2	20.2	נושאים מתקדמים בסייבר – זירת הסייבר המתפתחת, מודיעין סייבר, לוחמת סייבר, הזיקה בין סייבר לשדות לחימה קונבנציונליים והשפעתו האפשרית עליהם, תשתיות קריטיות, מאפייני תשתיות קריטיות, פשיעת סייבר, התמודדות המדינות עם אתגר ה-cyber crime. מבוא לעולם ה-Data. השוני מעולם הנתונים הוותיק. טכנולוגיות Big Data ו-Data Science מובילות. הגישה לסוגיות טכנולוגיות ותפעוליות מזוית תפיסות הדאטה.	Karaman M., Catalkaya H., Gerehan A. Z. & K. Goztepe. 2016. Cyber operation planning and operational design. <i>International Journal of Cyber-Security and Digital Forensics</i> . 5(1): 21-29. Dhar V. 2013. Data science and prediction. <i>Communications of the ACM</i> , 56(12): 64-73.	הגשת נושא לעבודה
3	27.2	מחקר ופיתוח – מתודולוגיות ניהול פרויקטים, גישות קלסיות לניהול פרויקטים, גישת המשולש, PMBOK, תכנון פרויקט, מרכיבי הצלחת פרויקט, תכונות מנהל הפרויקט, גישות מתקדמות לניהול פרויקטים, AGILE, מחקרים SPL, COMPREHENSIVE, מובילים בניהול פרויקטים. הצגות הסטודנטים את נושאי עבודותיהם.	לעיין: PMBOK. 2013. <i>PMBOK: A Guide to the Project Management Body of Knowledge</i> . Newtown Square, PA: Project Management Institute Inc.	הצגת נושאי עבודת הקבוצות

שבוע	תאריך	נושאים	קריאת חובה	הגשות
4	6.3	זיהוי – detection – ניתוח נושא זיהוי ארועי סייבר, גישות לזיהוי, טכנולוגיות ותאוריות מובילות, ההבדל בין ארוע תפעולי לסייברי והדרכים להבחין. מה בין התבססות על שיטות מקומיות לבין פתרונות מבוססי ענן. דיון בהקמת חברת סטארט-אפ כשיטת פיתוח לפתרונות זיהוי. היתרונות בסטארט-אפ כיישנות פיתוח, הקשיים וצווארי הבקבוק, מחזור חיי סטארט-אפ, האתגר המשאבי הרצוף. ניתוח מקרה סטארט-אפ העוסק בטכנולוגית זיהוי. הרצאת אורח.	Pritam M. 2017. A brief study of intrusion detection techniques to overcome cyber attacks. <i>Industrial Automation and Electromechanical Engineering Conference (IEMECON)</i> , 2017 8th Annual	
5	13.3	מניעה – prevention – העמקה בתפיסות שונות למניעת תקיפת סייבר. מגישות נקודתיות לתפיסה רחבה. עיסוק בהזדהות, ניטור ובקרה, חיסון, רמת עדכונים, שיקולי הטמעה, מודיעין, ועוד. דיון בניהול פרויקט גדול בחברה קיימת. יתרונות וחסרונות של חברה קיימת, הבדלים בין סוגי חברות. מאפייני פרויקט פיתוח סייברי. ההבדלים בין פרויקט פיתוח סייברי לאחרים. ניתוח מקרה דוגמא של פרויקט סייבר בחברה גדולה. הרצאת אורח.	Shay R. et al. 2016. Designing password policies for strength and usability. <i>ACM Transactions on Information and system security</i> . 18(4): Article 13: 1-34.	
6	20.3	תגובה – respond – מהי הדרך להתמודד עם ארוע סייבר או חשש לארוע סייבר. ההבדל בין הצעדים האינטואיטיביים לנכונים. ניתוח פונקציית המטרה במיקרה תקיפה ארגונית, אמצעי ושיטות התמודדות קיימות. מהו שירות? דרכים להקמת שירות, מודל עיסקי של גוף שירות ותנאים הכרחיים להצלחה. ניתוח מספר דוגמאות של חברות שירות בסייבר.	Denning D. E. 2014. Framework and principles for active cyber defense. <i>Computers & Security</i> , 40: 108-113.	
7	27.3.22	שיתופי פעולה – מרכיב מרכזי בהצלחה בתחום הסייבר. מהם שיתופי פעולה, ומהם הדרכים להצליח בהם. מרכיב התקשורת בשיתופי פעולה. אתגר התקשורת והבנת תפיסות והנחות עבודה בשת"פ בין תרבויות. הצגות סיכום של הסטודנטים מבוססי ארועים שנתחו במסגרת העבודות. סיכום הקורס.	Zrahia A. 2014. A Multidisciplinary Analysis of Cyber Information Sharing. <i>Military and Strategic Affairs</i> . 6(3): 59-77.	הגשת עבודות סיכום. הצגת מצגות של אחרונת הקבוצות.

*התכנית הינה בסיס לשינויים.

1. Ananth A. & T. Frederick. 2017. Security management of cyber physical control systems using NIST SP 800-82r2
2. Bonnal P., Gourc D. & G. Lacoste. 2002. The life cycle of technical projects. *Project Management Journal*, 33(1): 8-19.
3. Denning D. E. 2014. Framework and principles for active cyber defense. *Computers & Security*, 40: 108-113.
4. Dhar V. 2013. Data science and prediction. *Communications of the ACM*, 56(12): 64-73.
5. Elisa B. & H. Nathan. 2015. Cybersecurity for product lifecycle management a research roadmap. *International Conference on Intelligence and Security Informatics (ISI)*, IEEE.
6. Harel, Y. C. & A. Tishler. 2008. Should we Use a Long R&D Program or a Sequence of Short Ones? *12th Annual Conference on Economics and Security*, Ankara, Turkey.
7. Harel, Y., I. Ben Gal & Y. Elovici. 2017. Cyber Security and the Role of Intelligent Systems in Addressing its Challenges. *ACM Transactions on Intelligent Systems and Technology (TIST)*, 8(4): 49:1-49:12.
8. Karaman M., Catalkaya H., Gerehan A. Z. & K. Goztepe. 2016. Cyber operation planning and operational design. *International Journal of Cyber-Security and Digital Forensics*. 5(1): 21-29.
9. Kerzner, H. 2009. *Project Management - A Systems Approach to Planning, Scheduling and Controlling*. New York, NY: John Wiley & Sons .
10. Mehdi K. 2014. Cyber-Attack Attributes. *Technology Innovation Management Review*. 4(11): 22-27.
11. PMBOK. 2013. *PMBOK: A Guide to the Project Management Body of Knowledge*. Newtown Square, PA: Project Management Institute Inc.
12. Pritam M. 2017. A brief study of intrusion detection techniques to overcome cyber attacks. *Industrial Automation and Electromechanical Engineering Conference (IEMECON)*, 2017 8th Annual
13. Shay R. et al. 2016. Designing password policies for strength and usability. *ACM Transactions on Information and system security*. 18(4): Article 13: 1-34.
14. Shabtai A. et al. 2016. Behavioral Study of Users When Interacting with Active Honeytokens. *ACM Transactions on Information and System Security (TISSEC)*, 18(3): Article 9: 1-17.
15. Tabansky L. & I. Ben Israel. 2015. The National Innovation Ecosystem of Israel. *Cybersecurity in Israel*. Springer International Publishing.
16. Zrahia A. 2014. A Multidisciplinary Analysis of Cyber Information Sharing. *Military and Strategic Affairs*. 6(3): 59-77.

1. Anna L. & G. Erhan. 2017. A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. *IEEE Communications Surveys & Tutorials*, 18(2): 1153-1176.
2. Albanese M. et al. 2011. Scalable analysis of attack scenarios. *Computer Security—ESORICS 2011*. Springer Berlin Heidelberg. 416-433.
3. Bass T. 2000. Intrusion detection systems and multisensor data fusion. *Communications of the ACM*, 43(4): 99-105.
4. Cleland D. I. & L. R. Ireland. 2006. *Project Management: Strategic Design and Implementation*, 5th ed. New York, NY: McGraw-Hill.
5. Dvir D. & T. Lechler. 2004. Plans are nothing, changing plans is everything: The impact of changes on project success. *Research Policy*, 33(1): 1-15.
6. Filipe P. & F. Marcelo. 2016. Project management best practices for cyber-physical system development
7. Green I., Raz T. & M. Zviran. 2007. Analysis of active intrusion prevention data for predicting hostile activity in computer networks. *Communications of the ACM*, 50(4): 63-68.
8. Miller W. L. & L. Morris. 1999. *Fourth Generation R&D: Managing Knowledge, Technology and Innovation*. New York, NY: John Wiley & Sons.
9. Pasqualetti F., Dorfler F. & F. Bullo. 2013. Attack Detection and Identification in Cyber-Physical Systems. *IEEE Transactions on Automatic Control*, 58(11): 2715 – 2729.
10. Provost F. & T. Fawcett. 2013. Data science and its relationship to big data and data-driven decision making. *Big Data* 1.1 : 51-59.
11. Pywtranker K. 2015. An Umbrella in a Hurricane: Cyber Technology and the December 2013 Amendment to the Wassenaar Arrangement. *Northwestern Journal of Technology and Intellectual Property*. 13: 153-180.
12. Rajkumar R. R., Lee I., Sha L. & J. Stankovic. 2010. Cyber-physical systems: the next computing revolution. In *Proceedings of the 47th Design Automation Conference* (pp. 731-736). ACM.
13. Schneier B. 2009. Architecture of privacy. *IEEE Security & Privacy*, January/February.
14. Siaterlis C & B. Genge. 2014. Cyber Physical Testbeds. *Communications of ACM*. 57(6): 64-73.
15. Wang W. & Z. Lu. 2013. Cyber security in the Smart Grid: Survey and challenges. *Computer Networks*, 57(5): 1344-1371.