РЕПУБЛИКА БЪЛГАРИЯ

**СТОПАНСКА АКАДЕМИЯ “Д. А. ЦЕНОВ” – СВИЩОВ**

|  |  |
| --- | --- |
| Факултет“МЕНИДЖМЪНТ И МАРКЕТИНГ” | Катедра  “БИЗНЕС ИНФОРМАТИКА” |
|  |  |
| **Утвърждавам:** |  |
| Декан: …...…………….............................  (проф. д-р Маргарита Богданова) | Приета от ФС, Протокол № 11 от 16.06.2021 г. Приета от КС, Протокол № 16 от 12.05.2021 г. |
| **УЧЕБНА ПРОГРАМА**  **на** | |
| Учебна дисциплина“Защита на дигиталните транзакции” | |
| **Код на дисциплината: ФММ-КБИ-М-309**  **Брой кредити по учебен план: (6)** | |
| Образователно-квалификационна степен: МАГИСТЪР | Код на документа:УД/УПР-ФММ-КБИ-М-309 |
| Форма на обучение: РЕДОВНА/ЗАДОЧНА/ДИСТАНЦИОННА Език: БЪЛГАРСКИ | Версия:v.02/2021 |

**І. ОРГАНИЗАЦИЯ НА ОБУЧЕНИЕТО**

**Часове учебна заетост (семестър с продължителност 14 седмици)**

***Таблица № 1***

|  |  |  |  |
| --- | --- | --- | --- |
| **Учебна заетост**  **/аудиторна и извънаудиторна/** | **Редовна форма на обучение** | **Задочна форма на обучение** | **Дистанционна форма на обучение** |
| **1. Аудиторна заетост (АЗ)** | **56** | **28** | **56** |
| 1.1. Лекции | 42 | 21 | 42 |
| 1.2. Семинарни занятия | 14 | 7 | 14 |
| **2. Извънаудиторна заетост (ИАЗ)** | **94** | **122** | **94** |
| 2.1.Самостоятелна работа | 47 | 61 | 47 |
| 2.2. Академични задания | 47 | 61 | 47 |
| 2.2.1. Курсови разработки и проекти | 0 | 61 | 0 |
| 2.2.2. Есета/доклади | 0 | 0 | 0 |
| 2.2.3. Казуси и делови игри | 27 | 0 | 27 |
| 2.2.4. Онлайн тестови и изпитни модули | 20 | 0 | 20 |
| **Всичко:** | **150** | **150** | **150** |

**Схема за формиране на крайната оценка по дисциплина**

***Таблица № 2***

|  |  |  |  |
| --- | --- | --- | --- |
| **Критерий** | **Тежест на критерия** | | |
| **Редовна форма на обучение** | **Задочна форма на обучение** | **Дистанционна форма на обучение** |
| **1. Изпълнение на ангажименти през семестъра, в т.ч.:** | **60%** | **60%** | **60%** |
| * 1. Посещение на учебни занятия   *(% от комплексната оценка)* | 10% | 0% | 0% |
| 1.2. Семестриални контролни  *(% от комплексната оценка)* | 20% | 0% | 20% |
| 1.3. Академични задания  *(% от комплексната оценка)* | 30% | 60% | 40% |
| **2. Семестриален изпит**  *(% от комплексната оценка)*  *Форма на провеждане:*  *тест* | **40%** | **40%** | **40%** |
| **Общо за дисциплината** | **100%** | **100%** | **100%** |

**II. Анотация**

**2.1. Цел на курса**

Учебният курс е посветен на проблемите на сигурността на дигиталните транзакции в електронния бизнес и по-специално в електронната търговия. Темите са организирани в две части. Част 1 (теми от 1 до 5) е посветена на общи проблеми на информационната сигурност като същност, управление на риска, криптография, компютърни престъпления и атаки, модели за сигурност и др., валидни за всички компютърни системи. Втората част (теми от 6 до 10) е посветена на проблемите на сигурността в електронната търговия и разглежда специфични аспекти на атаки и защита на комерсиалната електронна транзакция.

**2.2. Предварителни изисквания**

От студентите се очаква да имат:

• базови знания за Microsoft Office (в т.ч. Excel и Access);

• базови знания за системи за управление на бази от данни;

• базови знания за бизнес информационни системи;

• базови знания и използване на Internet и комуникационни технологии.

**2.3. Използвани методи на преподаване**

***2.3.1 Редовна и задочна форма***

Основни методи на преподаване са лекции, консултации, демонстрации, директни инструкции, групови проекти, асинхронно и синхронно електронно обучение . Освен него се използват и съвременните методи на обучение, които осигуряват активна позиция на студента и го поставят в центъра на учебния процес, такива като дискусията, методът на проектирането, казусният метод, самостоятелни разработки на сайтове и приложения и др.

***2.3.2 Дистанционна форма***

Eлектронна платформа за дистанционно обучание, асинхронни и синхронни консултации, онлайн тестове, казуси.

**2.4. Очаквани резултати**

Целта на курса е студентите да придобият знанията за:

• важността и обхвата на сигурността на информационните системи и конкретно системите за електронна търговия;

• основните понятия и терминология на информационната сигурност;

• стратегиите за управление на риса;

• най-разпространените видовете компютърни престъпления и атаки в електронната търговия;

• популярни модели за сигурност и защита на средата за електронна търговия,

• технологичните решения за контрол на достъпа и криптиране; за защита на каналите за комуникация; на мрежите; на клиентите и сървърите;

• управленските политики, бизнес процедурите и обществените закони за защита на информационната сигурност в електронната търговия;

• фирмената стратегия за защита на информацията за защита на информационната сигурност в електронната търговия

**III. разпространение на дисциплината**

Upsala University, Sweden

Electronic Commerce and Security

RMIT University, Australia

Secure Electronic Commerce

University of Pittsburgh, USA

Security in E-Business

**IV. Учебно съдържание**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **ТемИ** | **Редовна форма на обучение** | | **Задочна форма на обучение** | | **Дистанционна форма на обучение** | |
| **Л** | **У** | **Л** | **У** | **Л** | **У** |
| **${temi#1}Глава 1. Информационна сигурност** | 3 | 1 | 1.5 | 0.5 | 3 | 1 |
| *1.1. Въведения и основни понятия  1.2. Основни рискове за информационната сигурност 1.3. Заплахи за сигурността на информационните системи 1.4. Източници на проблеми за информационната сигурност в електронната търговия* |
| **${temi#2}Глава 2. Управление на риска** | 3 | 0 | 1.5 | 0 | 3 | 0 |
| *2.1. Въведение 2.2. Определяне на риска 2.3. Начини за справяне с риска* |
| **${temi#3}Глава 3. Криптография** | 3 | 0 | 1.5 | 0 | 3 | 0 |
| *3.1. Въведение 3.2. Криптиране със симетричен ключ 3.3. Криптиране с публичен ключ 3.4. Криптиране с публичен ключ, използвайки цифров подпис и хеш функция 3.5. Криптиране с публичен ключ и цифрови пликове 3.6. Цифрови сертификати и инфраструктура с публичен ключ* |
| **${temi#4}Глава 4. Компютърни престъпления и атаки** | 3 | 0 | 1.5 | 0 | 3 | 0 |
| *4.1. Въведение 4.2 Видове компютърни престъпления 4.2.1. Използване на вредителски софтуер 4.2.2. Кражба на информация 4.2.3. Унищожаване и/или модифициране на данни 4.2.4. Отказ от услуга и разпределен отказ от услуга (DoS и DDоS атаки) 4.2.5. Използване на root kits 4.2.6. Криптографски атаки  4.2.7. Социален инженеринг 4.2.8. Хакери и кибер вандализъм* |
| **${temi#5}Глава 5. Модели за сигурност** | 4 | 1 | 2 | 1 | 4 | 1 |
| *5.1. Въведение 5.2. Слоеве за сигурност 5.3. Разделяне на задълженията 5.4. Етично хакерство 5.5. Възстановяване* |
| **${temi#6}Глава 6. Защитена среда за електронна търговия** | 4 | 1 | 2 | 1 | 4 | 1 |
| *6.1. Въведение 6.2. Основни аспекти на защитата в електронната търговия 6.3. Противоречия* |
| **${temi#7}Глава 7. Заплахи за сигурността в средата за електронна търговия** | 4 | 0 | 2 | 0 | 4 | 0 |
| *7.1. Основни точки на уязвимост в електронната търговска транзакция 7.2. Основни форми на заплаха за сигурността на потребителите и на сайтовете за ЕТ 7.2.1 Вредителски код 7.2.2. Потенциално нежелана програма 7.2.3. Фишинг и кражба на самоличност 7.2.4. Кражби/измами с кредитни карти 7.2.6. Отказ от обслужване и разпределен отказ от обслужване 7.2.7. Подслушване 7.2.8. Вътрешни атаки 7.2.9. Лошо проектиран сървърен или клиентски софтуер* |
| **${temi#8}Глава 8. Технологични решения за защита на транзакциите в електронната търговия** | 5 | 2 | 2.5 | 1 | 5 | 2 |
| *8.1. Въведение 8.2. Защита на интернет комуникациите 8.3. Защита на комуникационните канали 8.4. Защита на мрежите 8.4.1. Защитна стена (Firewall) 8.4.2. Прокси сървъри 8.4.3. Системи за откриване и противодействие на проникване в системата (Intrusion Detection and Prevention Systems) 8.5. Защита на сървърите и клиентите 8.5.1. Антивирусен софтуер 8.5.2. Средства за защита на информацията в операционната система Windows* |
| **${temi#9}Глава 9. Управленски политики, бизнес процедури и обществени закони** | 4 | 2 | 2 | 1 | 4 | 2 |
| *9.1. Въведение 9.2. Планиране на защитата 9.3. Роля на закона и обществената политика за защита на електронната търговия 9.4. Правни основи на електронната търговия в България* |
| **${temi#10}Глава 10. Фирмена стратегия за защита на информацията** | 5 | 5 | 2.5 | 2.5 | 5 | 5 |
| *10.1. Въведение 10.2. Фактори за развитие на стратегиите за сигурност 10.3. Компоненти на корпоративния план за защита 10.4. Стратегия за защита на транзакциите в електронната търговия* |
| **${temi#11}Тема 11. Стандарти за информационна сигурност, прилагани в електронната търговия** | 2 | 1 | 1 | 0 | 2 | 1 |
| *11.1. Въведение 11.2. Необходимост от стандартите за информационна сигурност 11.3. Основни стандарти за информационна сигурност 11.4. Сравнителен анализ на стандартите за информационна сигурност, използвани в електронната търговия* |
| **${temi#12}Тема 12. Мерки за създаване на рамка за информационна сигурност в системите за електронна търговия** | 2 | 1 | 1 | 0 | 2 | 1 |
| *12.1. Елементи на рамката за информационна сигурност в системите за електронна търговия 12.2. Формиране на подход към създаване на политика за информационна сигурност 12.3. Методология за създаване на политика за сигурност 12.4. Архитектурен модел на решение за информационна сигурност в системите за електронна търговия* |
| **${temi\_sum#1}Общо:** | **42** | **14** | **21** | **7** | **42** | **14** |

**V. ИЗПОЛЗВАНИ УЧЕБНО-ТЕХНИЧЕСКИ СРЕДСТВА**

|  |  |  |
| --- | --- | --- |
| **Наименование на**  **Учебно-техническото средство** | **Използвани учебно-технически средства по вид на занятията** | |
| **Лекции** | **Семинарни**  **занятия** |
| 1. Мултимедийни системи за презентиране | X | X |
| 2. Интернет | X | X |
| 3. Специализирани програмни продукти: |  |  |
| 3.1 | X | X |

**VI. ПреПОРЪЧИТЕЛНИ МАТЕРИАЛИ И НОРМАТИВНИ ИЗТОЧНИЦИ**

**6.1. Основна литература**

|  |
| --- |
| 1. Емолова, П. Защита на дигиталните транзакции. Свищов, Академично издателство “Д. А. Ценов”, 2017 |
| 2. Loudon, K, Traver, C. E-commerce: business. technology. society. 2016. 12th edition. PEARSON |
| 3. Blakyta, G., & Ganushchak, T. Enterprise financial security as a component of the economic security of the state. Investment Management and Financial Innovations, 15(2), 248-256 |
| 4. Turban, E., Volonino, L. & Wood, G., Information Technology for Management (Advancing Sustainable, Profitable Business Growth. Ninth Edition. 2013, Wiley |
| 5. Laan, S. IT Infrastructure Architecture: Infrastructure building blocks and concepts. Lulu Press Inc., Second edition, 2013 |
| 6. Turban, E., King, D., Lee, J.K., Liang, T.-P., Turban, D.C. Electronic Commerce a Managerial and Social Networks Perspective 2015, Springer |

**6.2. Допълнителна литература**

|  |
| --- |
| 1. Gareth J., Banking security in 2020: what to expect. [Online] Published: 30 january 2020, Avialable at: https://www.techradar.com/news/banking-security-in-2020-what-to-expect |
| 2. Suby, M. “The 2013 (ISC) 2 Global Information Security Workforce Study.” Mountain View, CA: Frost andSullivan, 2013, https://www.rsaconference.com/writable/presentations/file\_upload/prof-m01-2013\_global\_information\_security\_workforce\_study\_-\_final.pdf |
| 3. Lawinski, J. “Companies Spend on Security Amid Mobile and Social Threats.” Baseline, September 14, 2011 |
| 4. IBM Corporation. “IBM X-Force 2012 Mid-year Trend and Risk Report.” IBM Security Systems , White Paper# WGE03019-USEN-00, September 2012. public.dhe.ibm.com/common/ssi/ecm/en/wgl03014usen/WGL03014USEN.PDF |
| 5. Finkle, J. “‘Pony’ Botnet Steals Bitcoins, Digital Currencies: Trustwave.” Reuters.com US Edition , February 24, 2014, http://www.reuters.com/article/us-bitcoin-security-idUSBREA1N1JO20140224 |
| 6. Remove CryptoLocker virus (Files Encrypted Ransomware), https://malwaretips.com/blogs/remove-cryptolocker-virus |
| 7. Securing WordPress Against Hackers and DDoS Attacks, http://www.sitepoint.com/securing-wordpress-hackers-ddos-attacks |
| 8. McDowell, Mindi. Security Tip (ST04-015). Understanding Denial-of-Service Attacks,  https://www.us-cert.gov/ncas/tips/ST04-015 |
| 9. Cannel, J. “Cryptolocker Ransomware: What You Need to Know.” October 8, 2013. blog.malwarebytes.org/intelligence/2013/10/cryptolocker-ransom |
| 10. Възстановяване на ИТ инфраструктурата при бедствия. Networkworld България, бр 1, 2002 г., http://netw |

**6.3. Нормативни документи**

|  |
| --- |
| 1. Закон за защита на личните данни. (2002). http://econ.bg/ЗАКОН-ЗА-ЗАЩИТА-НА-ЛИЧНИТЕ-ДАННИ\_l. |

**6.4. Интернет ресурси**

|  |
| --- |
| 1. National Institute of Standards and Technology. https://www.nist.gov |
| 2. E-commerce securities. http://www.uky.edu/~dsianita/390/390wk4.html |

Съставил/и/:

|  |
| --- |
| …………………………………  ${authors#1}(доц. д-р Петя Емилова) |
| …………………………………  ${authors#2}(гл. ас. д-р Искрен Таиров) |

Ръководител катедра:

|  |  |
| --- | --- |
| …………………………………  (проф. д-р Красимир Шишманов) |  |