РЕПУБЛИКА БЪЛГАРИЯ

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

|  |  |
| --- | --- |
| Факултет“МЕНИДЖМЪНТ И МАРКЕТИНГ” | Катедра “БИЗНЕС ИНФОРМАТИКА” |
|  |  |
| **Утвърждавам:** |  |
|  Декан: …...…………….............................(доц. д-р Ваня Григорова) | Приета от ФС, Протокол № 4 от 17.12.2024 г.Приета от КС, Протокол № 7 от 10.12.2024 г. |
| **УЧЕБНА ПРОГРАМА****на** |
| Учебна дисциплина“Защита на дигиталните транзакции” |
| **Код на дисциплината: ФММ-КБИ-М-329****Брой кредити по учебен план: (6)** |
| Образователно-квалификационна степен: МАГИСТЪР | Код на документа:УД/УПР-ФММ-КБИ-М-329 |
| Форма на обучение: РЕДОВНА/ЗАДОЧНА/ДИСТАНЦИОННАЕзик: БЪЛГАРСКИ | Версия:v.03/2024 |

**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 | 28 | 14 | 28 |
| 1.2. Семинарни занятия | 28 | 14 | 28 |
| **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 | 27 | 41 | 27 |
| 2.2.2. Есета/доклади |  0  |  0  |  0  |
| 2.2.3. Казуси и делови игри |  0  |  0  |  0  |
| 2.2.4. Онлайн тестови и изпитни модули | 20 | 20 | 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***

Използва се платформата за дистанционно и електронно обучение за лекции, консултации, демонстрации, директни инструкции, групови проекти, асинхронно и синхронно електронно обучение.

**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** |
| **Тема 1. Информационна сигурност** | 2 | 1 | 1 | 0.5 | 2 | 2 |
| *1.1. Въведения и основни понятия1.2. Основни рискове за информационната сигурност1.3. Заплахи за сигурността на информационните системи1.4. Източници на проблеми за информационната сигурност в електронната търговия* |
| **Тема 2. Управление на риска** | 2 | 1 | 1 | 0.5 | 2 | 2 |
| *2.1. Въведение2.2. Определяне на риска2.3. Начини за справяне с риска* |
| **Тема 3. Криптография** | 2 | 2 | 1 | 1 | 2 | 2 |
| *3.1. Въведение3.2. Криптиране със симетричен ключ3.3. Криптиране с публичен ключ3.4. Криптиране с публичен ключ, използвайки цифров подпис и хеш функция3.5. Криптиране с публичен ключ и цифрови пликове3.6. Цифрови сертификати и инфраструктура с публичен ключ* |
| **Тема 4. Компютърни престъпления и атаки** | 2 | 2 | 1 | 1 | 2 | 2 |
| *4.1. Въведение4.2 Видове компютърни престъпления4.2.1. Използване на вредителски софтуер4.2.2. Кражба на информация4.2.3. Унищожаване и/или модифициране на данни4.2.4. Отказ от услуга и разпределен отказ от услуга (DoS и DDоS атаки)4.2.5. Използване на root kits4.2.6. Криптографски атаки 4.2.7. Социален инженеринг4.2.8. Хакери и кибер вандализъм* |
| **Тема 5. Модели за сигурност** | 3 | 2 | 1.5 | 1 | 3 | 3 |
| *5.1. Въведение5.2. Слоеве за сигурност5.3. Разделяне на задълженията5.4. Етично хакерство5.5. Възстановяване* |
| **Тема 6. Защитена среда за електронна търговия** | 2 | 2 | 1 | 1 | 2 | 2 |
| *6.1. Въведение6.2. Основни аспекти на защитата в електронната търговия6.3. Противоречия* |
| **Тема 7. Заплахи за сигурността в средата за електронна търговия** | 3 | 4 | 1.5 | 2 | 3 | 3 |
| *7.1. Основни точки на уязвимост в електронната търговска транзакция7.2. Основни форми на заплаха за сигурността на потребителите и на сайтовете за ЕТ7.2.1 Вредителски код7.2.2. Потенциално нежелана програма7.2.3. Фишинг и кражба на самоличност7.2.4. Кражби/измами с кредитни карти7.2.6. Отказ от обслужване и разпределен отказ от обслужване7.2.7. Подслушване7.2.8. Вътрешни атаки7.2.9. Лошо проектиран сървърен или клиентски софтуер* |
| **Тема 8. Технологични решения за защита на транзакциите в електронната търговия7** | 4 | 4 | 2 | 2 | 4 | 4 |
| *8.1. Въведение8.2. Защита на интернет комуникациите8.3. Защита на комуникационните канали8.4. Защита на мрежите8.4.1. Защитна стена (Firewall)8.4.2. Прокси сървъри8.4.3. Системи за откриване и противодействие на проникване в системата (Intrusion Detection and Prevention Systems)8.5. Защита на сървърите и клиентите8.5.1. Антивирусен софтуер8.5.2. Средства за защита на информацията в операционната система Windows* |
| **Тема 9. Управленски политики, бизнес процедури и обществени закони** | 3 | 4 | 1.5 | 2 | 3 | 3 |
| *9.1. Въведение9.2. Планиране на защитата9.3. Роля на закона и обществената политика за защита на електронната търговия9.4. Правни основи на електронната търговия в България* |
| **Тема 10. Фирмена стратегия за защита на информацията** | 5 | 6 | 2.5 | 3 | 5 | 5 |
| *10.1. Въведение10.2. Фактори за развитие на стратегиите за сигурност10.3. Компоненти на корпоративния план за защита10.4. Стратегия за защита на транзакциите в електронната търговия10.5. Добри практики на защитни политики. Дефиниране на стратегия и провеждане на политика по сигурността, която да защитава ИТ активите на различни типове конкретни организации.* |
| **Общо:** | **28** | **28** | **14** | **14** | **28** | **28** |

**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. Учебен курс в Платформата за дистанционно и електронно обучение на СА “Д. А. Ценов“, https://dl.uni-svishtov.bg/course/view.php?id=4507 |
|  2. Емолова, П. Защита на дигиталните транзакции. Свищов, Академично издателство “Ценов”, 2017 |

 **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. 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 |
|  4. Remove CryptoLocker virus (Files Encrypted Ransomware), https://malwaretips.com/blogs/remove-cryptolocker-virus |
|  5. Securing WordPress Against Hackers and DDoS Attacks, http://www.sitepoint.com/securing-wordpress-hackers-ddos-attacks |
|  6. McDowell, Mindi. Security Tip (ST04-015). Understanding Denial-of-Service Attacks,  https://www.us-cert.gov/ncas/tips/ST04-015 |
|  7. Cannel, J. “Cryptolocker Ransomware: What You Need to Know.” October 8, 2013. blog.malwarebytes.org/intelligence/2013/10/cryptolocker-ransom |

 **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/:

|  |
| --- |
|  …………………………………(доц. д-р Петя Емилова) |
|  …………………………………(гл. ас. д-р Юрий Кузнецов) |

Ръководител катедра:

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