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“Управление на информационната сигурност в бизнес организациите” | |
| **Код на дисциплината: ФММ-КБИ-М-354**  **Брой кредити по учебен план: (6)** | |
| Образователно-квалификационна степен: МАГИСТЪР | Код на документа:УД/УПР-ФММ-КБИ-М-354 |
| Форма на обучение: РЕДОВНА/ЗАДОЧНА/ДИСТАНЦИОННА Език: АНГЛИЙСКИ/БЪЛГАРСКИ | Версия:v.02/2024 |

**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 | 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 | 20 | 30 | 0 |
| 2.2.2. Есета/доклади | 0 | 0 | 0 |
| 2.2.3. Казуси и делови игри | 7 | 5 | 27 |
| 2.2.4. Онлайн тестови и изпитни модули | 20 | 26 | 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% | 0% |
| 1.3. Академични задания  *(% от комплексната оценка)* | 30% | 60% | 60% |
| **2. Семестриален изпит**  *(% от комплексната оценка)*  *Форма на провеждане:*  *Тест със затворени въпроси.* | **40%** | **40%** | **40%** |
| **Общо за дисциплината** | **100%** | **100%** | **100%** |

**II. Анотация**

**2.1. Цел на курса**

Учебният курс е посветен на проблемите на информационната сигурност 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 базовите познания придобити в бакалаварския курс. Допълнително преимущество са задълбочените познания по „Информациона сигурност и защита на данните“, която дава основните понятия, принципи и постановки в тази област.

**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***

За придобиване на теоретични знания и развитие на практически умения по основните въпроси в учебния курс се използват интернет базирани информационни технологии (DL платформа, социални мрежи и сайтове за комуникиране и обучение) с прилагане на иновативни синхронни и асинхронни методи за обучение (интерактивно, инцидентно, проблемно ориентирано и казусно обучение, ролеви и игрови тип обучение) и др.

**2.4. Очаквани резултати**

Целта на курса е студентите да придобият знанията за:

• важността и обхвата на сигурността на информационните системи в бизнес организациите;

• стратегиите за управление на риска;

• модели за сигурност и защита на бизнес организациите;

• организационна структура на информационната сигурност на бизнес организацията;

• управленските политики, бизнес процедурите за защита на информационната сигурност в бизнес организацията;

**III. разпространение на дисциплината**

Курсове със сходно съдържание:

- The University of Texas at Dallas - Курс "CS 6324: Information Security"

- Georgia Tech - Курс "CS 4235 / 8803 IIS: Introduction to Information Security"

- Carnegie Mellon University - Курс "Introduction to Information Security Management"

- Икономически университет - Варна - Курс "Планиране и управление сигурността на информационните системи"

**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 в бизнес организациите** | 4 | 0 | 2 | 0 | 4 | 0 |
| *1.1. Общи положения на концепцията за информационна сигурност 1.2. Предполагаеми заплахи за сигурността на информационните системи  1.3. Влияние на отклоненията от изискванията за информационна сигурност* |
| **Тема 2. Архитектурен модел на информационна сигурност на бизнес организация** | 5 | 1 | 2 | 1 | 5 | 1 |
| *2.1. Особености на архитектурата за информационна сигурност на бизнес организацията 2.2 Модел Sabsa за изграждане на архитектура за информационна сигурност в бизнес организацията  2.3. Връзка на архитектурата за сигурност с елементите на бизнес системата* |
| **Тема 3. Управление на риска** | 4 | 2 | 3 | 0 | 4 | 2 |
| *3.1. Идентифициране на заплахи и уязвимости 3.2. Оценка и анализ на риска 3.3. Реакция на риска. Избор и прилагане на контрамерките. 3.4. Нормативни рамки за управление на риска* |
| **Тема 4. Защита на личните данни** | 4 | 3 | 2 | 1 | 4 | 3 |
| *4.1. Основни понятния в защитата на личните данни  4.2. Законодателна рамка за защита на личните данни в България и ЕС 4.3. Права на субекта на данни 4.4. Задължения на администраторите и обработващите лични данни* |
| **Тема 5. Информационната сигурност в системите за електронна търговия** | 5 | 3 | 2 | 1 | 5 | 3 |
| *5.1. Особености на защитата на информацията и сигурността в електронната търговия 5.2. Предизвикателства пред сигурността в мобилната електронна търговия 5.3. Подходи и решения за поддържане на информационната сигурност в системите за електронна търговия 5.4. Заплахи и тенденции в развитието на заплахите за системите за електронна търговия* |
| **Тема 6. Технологии и стандарти, реализиращи защитената среда за електронна търговия** | 3 | 0 | 2 | 0 | 3 | 0 |
| *6.1. Компоненти на защитената среда за електронна търговия 6.2.Протоколи за сигурност на информацията, използвани в системите за електронна търговия 6.3. Стандарти за информационна сигурност, прилагани в електронната търговия* |
| **Тема 7. Организационна структура на информационната сигурност на бизнес организацията** | 5 | 2 | 2 | 1 | 5 | 2 |
| *7.1.Стратегия и принципи на информационната сигурност  7.2. Организационна структура на информационната сигурност на бизнес организацията 7.3. Система за физическа сигурност и защита* |
| **Тема 8. Концепция за възстановяване на информационната структура от бедствия и аварии** | 5 | 2 | 2 | 1 | 5 | 2 |
| *8.1. Видове бедствия, засягащи информационната инфраструктура на организациите 8.2. Същност и особености на възстановяването от бедствия и аварии 8.3. Показатели за определяне на способността за възстановяване от бедствия и аварии* |
| **Тема 9. Стратегия за възстановяване на информационната структура от бедствия и аварии** | 3 | 0 | 2 | 1 | 3 | 0 |
| *9.1. Използване на собствен резервен център за данни 9.2. Използване на център за колокация 9.3. Използване на облачни услуги за възстановяване* |
| **Тема 10. Технология на оценяване на разходите за информационна сигурност** | 4 | 1 | 2 | 1 | 4 | 1 |
| *10.1. Определяне ценността на информационните ресурси на бизнес организацията  10.2. Определяне на разходите за информационна сигурност 10.3. Анализ на разходите за осигуряване на информационна сигурност 10.4. Внедряване на система за отчитане на разходите за информационна сигурност* |
| **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. Шишманов, Красимир и др.. Управление на информационната сигурност в бизнес организациите / Красимир Шишманов, Юрий Кузнецов, Асен Божиков, Искрен Таиров // Свищов, Академично издателство - Ценов-, 2021, 162 с., ISBN: 978-954-23-2137-8 |
| 2. Електронна платформа за обучение. https://dl.uni-svishtov.bg/course/view.php?id=8079 |

**6.2. Допълнителна литература**

|  |
| --- |
| 1. Фети, Н., Тошкова-Николова, Д. Защита на личните данни, ИК "Труд и право", 2019, ISBN:978-954-608-263-3 |
| 2. Семерджиев, Ц., & Митев, Н. (2015). Информационна сигурност. София: Софттрейд. |
| 3. 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 |
| 4. Li, Y., Huang, G., Wang, C., & Li, Y. (2019). Analysis framework of network security situational awareness and comparison of implementation methods. EURASIP Journal on Wireless Communications and Networking volume. |
| 5. Al Hassan, L. (2017). Information Technology Disaster Recovery Plan (IT DRP) Framework – A study on IT Continuity for Smart City in Abu Dhabi Smart Government. Dubai. |
| 6. Chapple, M. Stewart, J. Gibson D. (ISC)2 CISSP Certified Information Systems Security Professional Official Study Guide 8th Edition, Wiley, 2018, ISBN: 978-1-119-47593-4 |
| 7. Blakyta, G., & Ganushchak, T. (2018). Enterprise financial security as a component of the economic security of the state. Investment Management and Financial Innovations, 15(2), 248-256 |

**6.3. Нормативни документи**

|  |
| --- |
| 1. Закон за защита на личните данни |
| 2. Закон за електронната търговия |

**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/:

|  |
| --- |
| …………………………………  (Prof. Krasimir Shishmanov, PhD) |
| …………………………………  (Head Assist.Prof. Yuriy Kuznetsov, PhD) |
| …………………………………  (Head Assist.Prof. Iskren Tairov, PhD) |
| …………………………………  (Head Assist.Prof. Asen Bozhikov, PhD) |

Ръководител катедра:

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