ЦЕНТЪР ПО ИКОНОМИЧЕСКИ И УПРАВЛЕНСКИ НАУКИ

УЧЕБНА ПРОГРАМА

Утвърждавам:
Декан:

IT 502

ИНФОРМАЦИОННА СИГУРНОСТ В БАНКОВИЯ СЕКТОР

Приета: прот. № 15/23.06.2016 г.
Лектор: доц. д-р Веселина Жечева

АНОТАЦИЯ

Дисциплината има за цел да представи на студентите основните предизвикателства и решения, свързани с информационната сигурност в банковия сектор. Разглеждат се основните видове заплахи и уязвимости за банковите системи, както и съответните методи и средства за защита. Дисциплината завършва със защита на курсова работа и изпит.

ОСНОВНИ ЦЕЛИ И ИЗХОДНИ УЧЕБНИ РЕЗУЛТАТИ

Основна цел на дисциплината е да формира знания и умения у студентите за анализ и оценка на проблемите, свързани с информационната сигурност в банковия сектор.

След обучението си по информационна сигурност в банковия сектор, студентът ще:

- познава основните проблеми, свързани със сигурността в банковия сектор;
- анализира текущите заплахи и уязвимости на системите, работещи в съвременните банки;
- избира подходящи методи и средства за защита на банкови информационни и компютърни системи.

ПРЕДПОСТАВКИ

Дисциплината изисква базови познания в областта на информационните и комуникационни технологии, както и познаване особеностите на банковите информационни и компютърни системи.

СТАТУТ И СТРУКТУРА

специалност	статут	Кредити	редовно обучение				задочно обучение			
			л	с	у	общ	Л	с	у	Общ
Банков мениджмънт	задължителна						30	0		30

СЪДЪРЖАНИЕ НА КУРСА

Тема 1. Увод в информационната сигурност. Цел, задачи и елементи. Аспекти на сигурността на информацията.

Тема 2. Заплахи и уязвимости. Случайни и злонамерени заплахи. Видове атаки. Оценки на ценността на информацията в системата. Сигурност и цена на защитата.

Тема 3. Политика на сигурност. Същност и видове. Стъпки на определяне. Механизми за реализиране на политиката на сигурност. Основни типове.

Тема 4. Злонамерен софтуер. Същност и условия за съществуване. Автори и основни цели. Вируси. Принципи и методи на действие. Основни видове.

Тема 5. Компютърни червеи. Троянски коне. Основни типове и методи на действие. Шпионски и рекламен софтуер. Социално инженерство.

Тема 6. Основни типове атаки. Атаки, свързани с измами. Следене действията на потребителя и събиране на данни. Спам. Същност, методи и цели на разпространение.

Тема 7. Защитен софтуер. Основни типове. Антивирусни програми. Защитни стени. Демилитаризирана зона. Бастион хост. Отделена подмрежа и прокси. Избор на решения.

Тема 8. Системи за откриване на нарушения. Типове системи за откриване на пробивите. Основни компоненти и методи на действие. Одит на системата. Възстановяване и резервно копиране.

Тема 9. Криптографски защитни механизми. Типове алгоритми и области на приложение. Цифрови подписи. Инфраструктура на публични ключове и сертификати. Сигурност на транзакциите.

Тема 10. Особености на банковите системи. Основни уязвимости и заплахи. Методи за превенция.

Тема 11. Инфраструктура за информационна сигурност в банките и прилагане на цялостни решения за сигурност. Стандарти за информационна сигурност.

ПЛАНИРАНИ УЧЕБНИ ДЕЙНОСТИ И МЕТОДИ НА ОБУЧЕНИЕ

присъствени лекции, визуално обучение, интерактивно обучение, електронно обучение чрез платформа Moodle, учебни видеоматериали вкл. видеопрезентации, тестване на приложен софтуер за сигурност в симулирана среда, използване на електронни ресурси в платформа Moodle: електронен речник, с основните понятия на български и английски език; видеопрезентации, полезни връзки, тестове

МЕТОДИ ЗА ОЦЕНЯВАНЕ

Изпитът е писмен и представлява тест с отворени въпроси, който се оценява с максимално **100 т.** За оформяне на крайната оценка се провежда и събеседване в деня на изпита. Окончателната оценка се формира като точките се разпределят по скалата:

- от 54 до 60 точки - Среден (3);
- от 61 до 70 точки - Добър (4);
- от 71 до 80 точки - Много добър (5);
- от 81 до 100 точки - Отличен (6).

ПРЕПОРЪЧИТЕЛНА ЛИТЕРАТУРА

1. Макмилън Т., Cisco: Компютърни мрежи – основи, АлексСофт, 2016.
2. Малхотра С., Microsoft .NET Framework сигурност, Дуодизайн, 2013.
3. Семерджиев Ц., Сигурност и защита на информацията, Софтрейд, 2012.
4. Lars Klander, Hacker Proof: The Ultimate Guide to Network Security, Jamsa Press, 1999, (английско издание).
5. Майк Шима, Брадли Джонсън, Анти-хакер, СофтПрес ООД, 2005, ISBN 954-685-324-0, (българско издание).
6. Mike Shema, Bradley Johnson, Anti-Hacker Tool Kit, McGraw-Hill Companies, 2004, (английско издание).
7. Пол Улфе, Чарли Скот, Майк Ъруин, Анти-спам, СофтПрес ООД, 2005, ISBN 954-685-328-3, (българско издание).
8. Швета Базин, Основи на мрежовата сигурност, Дуо дизайн ООД, 2004, ISBN 954-8396-21-1, (българско издание).
9. Shweta Bhasin, Web Security Basics, Premier Press, 2004, (английско издание).
10. Ашок Апу, Администриране и защита на Apache Server, Дуо дизайн ООД, 2004, ISBN 954-8396-19-X, (българско издание).
11. Ashok Appu, Administering and Securing the Apache Server, Premier Press, 2004, (английско издание).
12. Харприт Гангули, JAVA сигурност, Дуо дизайн ООД, 2004, ISBN 954-8396-24-6, (българско издание).
13. Harpreet Sethi, Java ™ Security, Premier Press, 2005, (английско издание).
14. Сурби Малхотра, Microsoft .NET Framework сигурност, Дуо дизайн ООД, 2005, ISBN 954-8396-25-4, (българско издание).
15. Surbhi Malhotra, Microsoft .NET Framework Security, Premier Press, 2005, (английско издание).
16. http://securityfocus.com
17. Информационен сайт на Касперски Лаб, https://securelist.com/
18. Национална лаборатория по компютърна вирусология, http://nlcv.bas.bg
19. Сайт за борба с компютърни престъпления на НСБОП http://www.cybercrime.bg/bg
20. http://www.sans.org/reading-room/
21. http://www.cert.org/
22. Information Security Magazine http://www.infosecuritymag.com/

ИЗПИТЕН ВЪПРОСНИК

:

IT 502

ИНФОРМАЦИОННА СИГУРНОСТ В БАНКОВИЯ СЕКТОР

Лектор: доц. д-р Веселина Жечева

1. Увод в информационната сигурност. Цел, задачи и елементи. Аспекти на сигурността на информацията.
2. Заплахи и уязвимости. Случайни и злонамерени заплахи. Видове атаки. Оценки на ценността на информацията в системата. Сигурност и цена на защитата.
3. Политика на сигурност. Същност и видове. Стъпки на определяне. Механизми за реализиране на политиката на сигурност. Основни типове.
4. Злонамерен софтуер. Същност и условия за съществуване. Автори и основни цели. Вируси. Принципи и методи на действие. Основни видове.
5. Компютърни червеи. Троянски коне. Основни типове и методи на действие. Шпионски и рекламен софтуер. Социално инженерство.
6. Основни типове атаки. Атаки, свързани с измами. Следене действията на потребителя и събиране на данни. Спам. Същност, методи и цели на разпространение.
7. Защитен софтуер. Основни типове. Антивирусни програми. Защитни стени. Демилитаризирана зона. Бастион хост. Отделена подмрежа и прокси. Избор на решения.
8. Системи за откриване на нарушения. Типове системи за откриване на пробивите. Основни компоненти и методи на действие. Одит на системата. Възстановяване и резервно копиране.
9. Криптографски защитни механизми. Типове алгоритми и области на приложение. Цифрови подписи. Инфраструктура на публични ключове и сертификати. Сигурност на транзакциите.
10. Особености на банковите системи. Основни уязвимости и заплахи. Методи за превенция.
11. Инфраструктура за информационна сигурност в банките и прилагане на цялостни решения за сигурност. Стандарти за информационна сигурност.

ПРЕПОРЪЧИТЕЛНА ЛИТЕРАТУРА

1. Макмилън Т., Cisco: Компютърни мрежи – основи, АлексСофт, 2016.
2. Малхотра С., Microsoft .NET Framework сигурност, Дуодизайн, 2013.
3. Семерджиев Ц., Сигурност и защита на информацията, Софтрейд, 2012.
4. Lars Klander, Hacker Proof: The Ultimate Guide to Network Security, Jamsa Press, 1999, (английско издание).
5. Майк Шима, Брадли Джонсън, Анти-хакер, СофтПрес ООД, 2005, ISBN 954-685-324-0, (българско издание).
6. Mike Shema, Bradley Johnson, Anti-Hacker Tool Kit, McGraw-Hill Companies, 2004, (английско издание).

7. Пол Улфе, Чарли Скот, Майк Ъруин, Анти-спам, СофтПрес ООД, 2005, ISBN 954-685-328-3, (българско издание).
8. Швета Базин, Основи на мрежовата сигурност, Дуо дизайн ООД, 2004, ISBN 954-8396-21-1, (българско издание).
9. Shweta Bhasin, Web Security Basics, Premier Press, 2004, (английско издание).
10. Ашок Апу, Администриране и защита на Apache Server, Дуо дизайн ООД, 2004, ISBN 954-8396-19-X, (българско издание).
11. Ashok Appu, Administering and Securing the Apache Server, Premier Press, 2004, (английско издание).
12. Харприт Гангули, JAVA сигурност, Дуо дизайн ООД, 2004, ISBN 954-8396-24-6, (българско издание).
13. Harpreet Sethi, Java ™ Security, Premier Press, 2005, (английско издание).
14. Сурби Малхотра, Microsoft .NET Framework сигурност, Дуо дизайн ООД, 2005, ISBN 954-8396-25-4, (българско издание).
15. Surbhi Malhotra, Microsoft .NET Framework Security, Premier Press, 2005, (английско издание).
16. http://securityfocus.com
17. Информационен сайт на Касперски Лаб, https://securelist.com/
18. Национална лаборатория по компютърна вирусология, http://nlcv.bas.bg
19. Сайт за борба с компютърни престъпления на НСБОП http://www.cybercrime.bg/bg
20. http://www.sans.org/reading-room/
21. http://www.cert.org/
22. Information Security Magazine http://www.infosecuritymag.com/