РЕЗЮМЕ

на научните трудове, публикации и разработки

на подполковник инж. Зарко Иванов Здравков, д-р

представени за участие в конкурса за научното звание "ДОЦЕНТ" в научна секция „Доктрини, концепции и поуки от практиката" в Института „Перспективни изследвания за отбраната" на Военна академия „Георги С. Раковски"
т. 2.12, раздел II на МЗ No ОХ-460/ 16.05.2019 г.

1. **Монография „Проектиране на защитени автоматизирани информационни системи"**

Монографията предлага цялостен и систематизиран подход за създаване на защитени АИС. Разгледани са въпросите, свързани с управлението на рисковете за организациите и технологията за формулиране на политики за сигурност, и е направен обзор на функциите и архитектурите на средствата за обезпечаване на сигурността. Като резултат е предложна методика за проектиране на защитена АИС. Методиката е верифицирана чрез разработен пример за проектиране на защитена АИС на организация. В примера е показано как анализът започва с обща информация за АИС и средата, в която функционира, преминава през етапите на методиката и завършва с конкретни архитектури на аргументирано подбрани технологии и средства за защита. Този подход създава необходимата увереност за ефективна защита.

2. **Доклад „Контрол на действията на длъжностните лица от щаба при работа със щабна автоматизирана информационна система"**

В доклада се определя мястото на контролът на действията на длъжностните лица от щаба при работа със щабни АИС в общата система на информационна сигурност и се предлага инвариантна технология за създаване на средства за контрол на действията със специализираните услуги на щабните АИС.

3. **Доклад „Анализ на модели за контрол на достъп"**

Докладът разглежда възможността моделите за достъп до ресурси да се прилагат за контрол на достъп до АИС. Извършеният анализ определя условията, при които тези модели са приложими.

4. **Доклад „Методика на тест за проникване в автоматизираните информационни системи“**

Докладът е посветен на теста за проникване в автоматизираните информационни системи като начин за проверка на сигурността. Предложена е Методика на тест за проникване.

5. **Статия „Архитектура на информационната система за предоставяне на публичен достъп до пространствените данни и услуги на МО“**

В статията се анализира архитектурата на разработената Информационна система за публичен достъп до пространствени данни и услуги на МО. Чрез програмните приложения и разработки, внедрени в Информационната система, са удовлетворени нуждите на институциите, гражданите и хората от онлайн достъп до пространствени данни. Информационната система допринася за хармонизирането на крайните електронни услуги за пространствени данни съгласно Директива 2007l2lEO INSPIRE

6. **Доклад „Разпределен релационен модел за групов отчет на набора“**

В доклада са разгледани теоретични модели на релационни бази от данни, използвани при управлението на данните при групов отчет на подлежащия на мобилизация набор. Данните се обменят и обработват на различни нива по различен начин.

7. **Доклад „Проектиране на релационна БД ORACLE 7.3, съдържаща йерархичната структура на списъка на тиловите материални средства“**

Докладът изследва възможностите на програмния пакет Designer 2000 на релационна БД ORACLE 7.3 да трансформира логически модел на БД във физически. Извършен е анализ на четирите възможности при трансформирането на понятията супертип и подтип. Проектантът трябва да използва вариант, съобразявайки се с особеностите на данните. Избран е най-ефикасния вариант за създаване на БД, съдържаща йерархичната структура на списъка на тиловите материални средства.

8. **Доклад „Софтуерни средства за защита на данните в системи за управление на бази данни“**

В доклада са анализирани софтуерните средства за защита на базите данни, които са резултат от опита на авторите и изследвания, проведени в Изследователския и демонстрационен център на Института за перспективни изследвания за отбраната. Описани са предимствата и недостатъците на изследваните програмни приложения.

9. **Доклад „Защита на данните в база данни ORACLE“**

В доклада се разглежда програмното приложение Secure Network Services. То се използва за преодоляване на рисковете и заплахите за данните, съществуващи при използването на стандартните средства за защита, но не е включено в стандартния инсталационен пакет на СУБД ORACLE. Предложени и аргументирани са добри практики при употребата на този софтуер.

10. **Доклад „Стратегия за информационна сигурност в C4I системите на българската армия“**

В доклада са отразени опитът на авторите при разработване и внедряване на нормативни документи и системи за защита на информацията в Автоматизираните Системи за Управление на Българската Армия, участието им при създаването на Стратегията за развитие на Информационното Общество в Република България и изводите и препоръките от съвместното Българо-Американско изследване на C4I системите на Българската Армия.

11. **Доклад „Е-мрежов модел за защита на сесия в разпределени релационни бази от данни“**

В доклада са представени два Е-мрежови модела на сесията в РРБД. Първият е модел на сесията без средства за защита, а вторият е със средства за защита. Моделите могат да се използват за симулация, анализ и оценка на сигурността на конкретни реализации.

12. **Доклад „Формален модел на система за информационна сигурност на база данни“**

В доклада е предложен модел на система за информационна сигурност на БД, който подходящо описва информационната и физическа структура от гледна точка на информационната сигурност. Позволява да се опишат връзките между тях и средствата за защита. Удобен е за спецификация от

описанието на БД. Намира приложение основно при създаването на разпределени бази от данни в етапите: проектиране (за създаване на политики за сигурност) и експлоатация (за анализ и проверка).

13. **Доклад „Сигурността в разпределени релационни бази данни“**

Докладът разглежда защитата в разпределена релационна база данни. Специфична част от тази защита е контролът на достъпа до / между физическите единица на базата данни и защитата при обмена на данни.

14. **Доклад „Контрол на достъпа в база данни ORACLE“**

В доклада са разгледани три възможности за организиране на контрола на достъпа до БД Oracle. Разгледани са положителните им и отрицателни страни и са направени предложения за употребата им.

15. **Доклад „Модел на релационни бази данни за планиране на учебния процес във военна академия “Г. С. Раковски”**

В доклада е представена възможност за формализиране на учебния план на Военна академия “Г. С. Раковски” . На базата на предложения формален модел е създаден модел на релационна база данни.

16. **Доклад „Провеждане на разделна двустепенна щабна тренировка на свързочно съединение със средствата за дистанционно обучение“**

В доклада е представена възможността за провеждане на разделна двустепенна щабна тренировка на свързочно съединение със средствата за дистанционно обучение.

17. **Доклад „Модел на релационни бази данни за контрол на работата с класифицирани документи в корпоративна организация“**

В доклада са предложени информационни структури на информационната система за контрол на класифицирани документи, изградени на базата на РБД. Информационните структури са организирани в модел на РБД.

18. **Доклад „Модел за регистриране на действията с класифицирани документи в корпоративна организация“**

В доклада са дефинирани понятия информационна единица “класифициран документ” и “жизнен цикъл на информационна единица “класифициран документ” и е предложен конструктивен и инвариантен Формален модел на класифицирани документи.

19. **Доклад „Програмни средства за пасивно разузнаване на мрежовата среда на автоматизираните информационни системи“**

В доклада е направен обзор на съществуващи програмни инструменти, позволяващи легално да се събира информация от частни сървъри, които споделят различни данни с публичното пространство. Тези данни могат да се използват за организиране на атаки.

20. **Доклад „Програмни средства за активно разузнаване на мрежовата среда на автоматизираните информационни системи“**

В доклада е направен обзор на средства за активно проучване на мрежи. Активното проучване е етап от провеждането на атака. Представени са и атаки, използващи информация, получена при активно проучване.

21. **Доклад „Тестване на сигурността на автоматизираните информационни системи“**

В доклада е представен начин за проверка на сигурността на информационната система. Разгледан е процесът на тестване на сигурността и анализа на риска.

22. **Доклад „Структура на стандартни оперативни процедури за противодействие на атаки срещу автоматизираните информационни системи на министерството на отбраната и българската армия**

Докладът предлага начин за разработване на стандартни оперативни процедури (СОП) и предлага структурата на СОП.

23. Доклад „Технологични възможности за провеждане на кибер операции“

Докладът представя обобщена информация за технологии за провеждане на кибер-операции. Технологиите са класифицирани като средства за кибер-оръжие и кибер-отбрана.

24. Доклад „Изследване на зависимостта на критичните задачи на НАТО от национални информационни системи“

В доклада е представена методика за изследване на зависимостта на критичните задачи на НАТО от национални информационни системи.

25. Доклад „Предизвикателства по управление на проект за „изграждане на информационна система за редоставяне на публичен достъп до пространствените данни и услуги на министерство на отбраната“

В доклада са разгледани някои от съществените предизвикателства при цялостното управление на първия проект на Министерството на отбраната, финансиран по оперативна програма „Административен капацитет“. Споделя се натрупания опит и проблемите, с които са възникнали в процесите по разработването на проектното предложение и изпълнението му. Изложените предизвикателства са групирани по функционалните области, известни от теорията за управление на проекти. Част от тези предизвикателства са били предвидими и характерни за такъв тип проекти, други са възникнали неочаквано, а при някои ефектът е с натрупване. В допълнение е представен анализ на рисковите, застрашаващи качественото и навременно изпълнение на проекта.

26. Доклад „Определяне на последиците за обект от критичната информационна инфраструктура при оценка на риска“

В доклада е представен подход за определяне на последиците за обект от критична информационна инфраструктура при сбъдване на рисково събитие. Подходът е подходящ за употреба при анализ на риска.

27. Методика „Методика за оценка на риска за установените критични инфраструктури и обектите им в сектор „Отбрана“ в Република България“

Методиката за оценка на риска за установените критични инфраструктури и обектите им в сектор „Отбрана“ в Република България покрива дефицитите в областта като предлага единен и систематизиран подход за управление на риска. За прилагането на предложения математически апарат за оценка на риска са определени последователните етапи за управление на риска, рисковите събития за обектите от КИ и са определени най-значимите уязвимости на обектите, асоциирани към всяко рисково събитие. Представени са шаблони на документи за улесняване работата на експертите и е разработено софтуерно приложение.

10.07.2019 г.

…….. /Зарко Здравков/