Впервые в Казахстане!

Программа курсов Валерия Домарева по тематике «Система управления информационной безопасностью: от модели к практической реализации»

Руководитель курса – **Валерий Домарев** (Киев), ведущий эксперт Украины и стран СНГ по вопросам информационной безопасности, кандидат технических наук, доцент (резюме Валерия Домарева чуть ниже, подробная информация о нем - на http://www.security.ukrnet.net/modules/news/article.php?storyid=1)

Курс рассчитан на менеджеров высшего звена компаний, предприятий и организаций, руководителей подразделений и служб информационной безопасности.

В рамках курса рассматриваются вопросы организации процессов управления информационной безопасностью на основе современных требований, в том числе с учетом рекомендаций международных стандартов, таких как:

- ISO/IEC 27001:2005 "Системы менеджмента информационной безопасности. Требования" (Information technology. Security techniques. Information security management systems. Requirements);

- ISO/IEC 17799:2000 «Информационные технологии – Практическое руководство по управлению информационной безопасностью» (Information technology. Code of practice for information security management);

- ISO/IEC 15408 "Общие критерии оценки безопасности информационных технологий" (Common Criteria);

- PCI DSS «Стандарт безопасности данных индустрии платежных карт» (Payment Card Industry. Data Security Standard). И других…

В рамках курса Вы так же сможете познакомиться с программным комплексом "Матрица".
Система управления информационной безопасностью "Матрица" - это уникальный авторский проект, который является простым, универсальным и эффективным средством организации, управления и контроля процессов обеспечения информационной безопасности в любой компании. Программа легко адаптируется для решения конкретных задач обеспечения ИБ с учетом особенностей бизнес-процессов любых компаний. Прослушав курс, вы сможете самостоятельно организовать работу по созданию своей системы информационной безопасности.

Цель курса:
- Ознакомить слушателей с понятием «управление ИБ» как совокупностью принципов, методов и средств управления процессами защиты информации с целью обеспечения информационной безопасности компании;
- Сформировать системное видение вопросов обеспечения ИБ компании;

- Ознакомить с вариантом программного комплекса поддержки принятия решений (ПКР) как инструментом управления ИБ компании
- Продемонстрировать возможности ПКР для решения практических задач управления системой ИБ, формирования политики ИБ и создания нормативно-методических документов системы ИБ компании
- Рассмотреть варианты наполнения ПКР требованиями различных стандартов в области ИБ.

Тематика занятий:
- Интегральный характер проблем ИБ;
- Пути реализация системного подхода при решении задач ИБ;
- Модель представления системы ИБ (СИБ) компании;
- Теоретические и практические вопросы создания и оценки СИБ с учетом особенностей функционирования информационных технологий в конкретной компании;
- Задачи гибкого управления СИБ в зависимости от выдвигаемых требований, допустимого риска и оптимального расхода ресурсов;
- Вариант программы для поддержки решений менеджмента ИБ;
- Вариант программы оценки эффективности системы ИБ компании.

В процессе обучения слушатели получат знания, которые помогут:
- Повысить эффективность принимаемых управленческих решений по обеспечению ИБ
- Оптимизировать процессы управления системой ИБ
- Систематизировать и объединить усилия различных специалистов в области ИБ
- Оптимизировать структуру подразделений компании с учетом задач ИБ
- Определить пути создания и/или дальнейшего развития системы ИБ
- Организовать работу по созданию СИБ с учетом всего комплекса проблем ИБ
- Обеспечить возможность рационального использования финансовых средств
- Учесть индивидуальные особенности и условия функционирования ИТ с точки зрения обеспечения ИБ

Время, место, объем знаний, специфика и направленность занятий оговариваются в каждом конкретном случае индивидуально. **Тематика курса формируется заказчиком из модулей, перечисленных ниже в разделе** «Программа учебного курса» с учетом уровня базовой подготовки слушателей и длительностью курса от 40 ак.час (5 дней)

По окончанию курса слушатели будут способны самостоятельно управлять процессами создания и управления системой ИБ компании.

Плановые даты сборных (открытых) курсов Валерия Домарева в 2009 году в Алматы:

с 17 по 21 августа 2009 года*, с 12 по 16 октября 2009 года* (*) – подлежит уточнению по набору групп, при этом для групповых и корпоративных клиентов скидки на участие до 20%.

Заявки на участие высылайте по E-mail – pmi@nursat.kz, тел. для справок +77772106040

ПРОГРАММА УЧЕБНОГО КУРСА
(модули входящие в состав курса)

1. *Тема 001-Д-1. Законодательная, нормативно-методическая и научная база функционирования комплексных систем защиты информации*

2. Подсистема организационно-правовой защиты. Промышленный шпионаж и законодательство. Защита программного обеспечения авторским правом. Требования к содержанию нормативно-методических документов по защите информации (ЗИ).

3. *Тема 001-Д-1. Разработка нормативно-методической основы ЗИ.*

4. Некоторые нормативно-методические документы, необходимые для организации защиты информации. Научно-методологический базис защиты информации. Стратегическая направленность защиты информации. Инструментальный базис защиты информации.

5. *Тема 001-Д-1. Математические модели систем и процессов защиты информации*

6. Общая характеристика проблемы синтеза КСЗИ. Исследование предметной области с целью создания математической модели КСЗИ. Краткий анализ математических моделей КСЗИ.

7. *Тема 001-Д-1. Общая характеристика математических методов оценки и обоснования требований к КСЗИ.*

8. Основные понятия теории нечетких множеств. Методы определения важности требований, предъявляемых к КСЗИ. Методы выбора рационального варианта КСЗИ на основе экспертной информации. Методические рекомендации по проведению экспертизы при оценке КСЗИ.

9. *Тема 001-Д-1. Принципы построения систем защиты информации*

10. Понятия защиты Системность подхода Основные трудности Основные правила Защищенная ИС и система защиты информации Как обеспечить сохранность информации.

11. *Тема 002-Д-1. Структура и задачи органов, осуществляющих защиту информации*

12. Перечень задач, решаемых службой информационной безопасности Создание службы информационной безопасности. Организационно-правовой статус службы. Структура службы информационной безопасности.

13. *Тема 003-Д-1. Политика информационной безопасности (организационно-технические и режимные меры)*

14. Принципы политики безопасности. Виды политики безопасности Организация секретного делопроизводства. Политики безопасности для Internet Уровни политики безопасности. Виртуальны частные сети Роли и обязанности. Краткое содержание документов ПИБ.

15. Тема 004-Д-1. Программно-технические методы и средства защиты информации

16. Методы идентификации и аутентификации пользователей. Управление доступом. Обеспечение конфиденциальности сообщений и данных. Метод парольной защиты и его модификации. Контроль доступа пользователей к ресурсам ИС. Средства защиты от НСД. Анализаторы протоколов. Инструментальные средства тестирования системы защиты. Межсетевые экраны.

17. Тема 010-Д-1. Защита информационных и физических объектов ИС

18. Защищаемые файлы Распределенное хранение файлов Защита баз данных Защита ресурсных объектов Охранная и пожарная сигнализация Компоненты и устройства видеосистем

19. Тема 010-Д-1. Техническая защита информации на объектах ИС

20. Поиск каналов утечки информации Классификация характерных признаков радиозакладок Поиск радиозакладок с помощью средств оперативного контроля Поиск радиозакладок с помощью носимых многофункциональных поисковых приборов СРМ-700 «Акула» и ST-031 «Пиранья» Методы выявления закладных устройств, подключаемых к телефонным линиям Направленное подавление радиоэлектронных устройств

21. Тема 020-Д-1. Защита процессов и программ

22. Проблемы безопасности программного обеспечения Механизмы защиты процессов, процедур и программ обработки данных Уровни защиты процедур и программ Защита процедур управления Защита электронного документооборота Защита операционных систем Разграничение доступа пользователей к ресурсам Инструмент системного аудита Защита в сетевом информационном сервисе Ядро безопасности ОС Технологии VPN для корпоративных пользователей

23. Тема 020-Д-1. Информационная система как объект защиты.

24. Разработка и производство информационных систем. Структура ИС и принципы ее функционирования. Типовые компоненты ИС. Проблемы защиты локальных сетей. Проблемы защиты открытых систем клиент/сервер. Проблемы безопасности ИС. Проблемы интеграции систем защиты.

25. Тема 020-Д-1. Проблемы, связанные с безопасностью в Internet

26. Internet в структуре информационно-аналитического обеспечения органов государственной власти. Использование электронной почты. Хосты в

Internete Стек протоколов TCP/IP Слабая аутентификация Легкость наблюдения за передаваемыми данными Потенциальные проблемы с электронной почтой Сложность конфигурирования и мер защиты Проблемы, возникающие из-за брандмауэров

27. Тема 020-Д-1. Технологии брандмауэров

28. Понятие брандмауэра Виртуальные сети Политика брандмауэра Политика сетевого доступа Гибкость политики Политика усиленной аутентификации удаленных пользователей Политика доступа через модемы Компоненты брандмауэра Принципы функционирования брандмауэра Межсетевые экраны Защита Web-серверов

29. Тема 030-Д-1. Защита каналов связи

30. Криптографические методы и средства защиты информации. Основные сведения о криптографии. Подсистема криптографической защиты. Аутентичность сообщений. Анализ существующих методов криптографических преобразований. Алгоритмы шифрования DES и RSA. Защита данных при передаче по каналам связи ИС. Защита целостности сообщений. Использование функций подтверждения подлинности. Защита телефонных линий от прослушивания.

31. Тема 040-Д-1. Подавление побочных электромагнитных излучений

32. Источники утечки информации по каналам ПЭМИН Организация защиты информации в ИС от утечки по каналам ПЭМИН Рекомендации по защите информации от перехвата излучений технических средств объектов ИС Оценка защищенности информации от утечки по каналам ПЭМИН

33. Тема 050-Д-1. Управление системой защиты

34. Управление защитой Принципы организации и контроля системы защиты Реализация политики безопасности Оптимизация хранения и обработки информации Контроль за наиболее ценной информацией Административная группа управления защитой Опасные события и их предупреждение Идентификация, аутентификация и авторизация Методы разработки защищенных ИС Модели управления доступом Управление механизмами КСЗИ Проблемы внедрения систем управления доступом Ограничения обработки Функции контроля и управление КСЗИ Контроль за состоянием технической защиты информации Интеграция механизмов защиты ИС Управление ключами защиты

35. Тема 100-Д-1. Определение информации, подлежащей защите

36. Порядок отнесения информации к государственной тайне Распоряжение сведениями, составляющими государственную тайну Защита государственной тайны Допуск должностных лиц и граждан к государственной тайне Сведения, составляющие коммерческую тайну Определение степени секретности информации

37. Тема 200-Д-1. Выявление потенциальных каналов утечки и угроз

38. Угрозы информационной безопасности в сферах деятельности государства Анализ характеристик угроз и уязвимых мест для информации в ИС Угрозы для объектов ИС Угрозы для процессов, процедур и программ обработки информации Угрозы для информации в каналах связи Угрозы информации, возникающие за счет побочных электромагнитных излучений и наводок Угрозы для механизмов управления системой защиты Как проводить анализ угроз и каналов утечки информации

39. Тема 300-Д-1. Оценка уязвимостей и рисков

40. Анализ рисков Разработка методологии оценки риска Оценка ущерба, связанная с реализацией угроз Анализ стоимость/эффективность Группа оценки риска Элементы управления риском

41. Тема 400-Д-1. Требования к системам защиты информации

42. Общие требования Организационные требования. Требования к подсистемам защиты информации. Требования к техническому обеспечению. Требования к программному обеспечению. Требования по применению способов, методов и средств защиты. Требования к документированию. Требования к составу проектной и эксплуатационной документации. Перечень основных функциональных задач, которые должна решать КСЗИ. Технические требования по защите информации от утечки по каналам ПЭМИН. Требования по защите от перехвата ПЭМИН. Требования по защите системы заземления объекта ИС. Требования по защите систем электроснабжения объекта ИС.

43. Тема 500-Д-1. Осуществление выбора средств защиты

44. Услуги и механизмы обеспечения безопасности сетей на основе модели ВОС Базовые сервисы для обеспечения безопасности компьютерных систем Механизмы обеспечения безопасности Использование услуг безопасности Обзор средств защиты информации в ИС Средства защиты от НСД Анализаторы протоколов Инструментальные средства тестирования системы защиты Приобретение брандмауэра.

45. Тема 600-Д-1. Внедрение и использование выбранных мер защиты

46. Выбор основных решений по обеспечению ЗИ .Обеспечение ЗИ на стадиях проектирования ИС. Рабочая документация, относящаяся к КСЗИ. Обеспечение ЗИ в процессе подготовки ИС к эксплуатации. Содержание работ предпроектной стадии. Организация работы персонала. Установка и внедрение средств защиты. Содержание и последовательность работ по защите информации. Этапы выполнения работ по созданию КСЗИ. Процесс создания механизмов защиты ИС. Построение системы защиты информации. Порядок проведения работ по ЗИ. Реализация организационных мер защиты. Реализация технических мер защиты. Приемка, определение полноты и качества работ.

47. Тема 700-Д-1. Контроль целостности и управление КСЗИ

48. Контроль за работой пользователей Управление доступом к рабочим местам в ИС Использование паролей Пользовательское оборудование, оставленное без присмотра Отслеживание времени простоя терминалов Ограничение периода подключения Ограничение доступа к сервисам Управление доступом к сервисам Защита целостности данных и программ от вредоносного программного обеспечения. Контроль за состоянием безопасности ИС Системы обнаружение атак Как работает сканер безопасности? Консалтинг в информационной безопасности

49. Тема 700-Д-1. Модель комплексной оценки КСЗИ

50. Блок показателей ОСНОВЫ (Oi). Блок показателей НАПРАВЛЕНИЯ (Hj). Блок показателей ЭТАПЫ (Mk). Структура модели оценки КСЗИ. Методика оценки качества КСЗИ на основе матрицы знаний. Шкала соответсвия. Лингвистическая переменная. Оценка качества КСЗИ на основе анализа профиля безопасности.

51. Тема 720-Д-1. Сертификация ИС и ее компонентов по требованиям информационной безопасности

52. Основные функции органа сертификации. Что такое сертификат безопасности. Сертификат и экономические аспекты безопасности. Риски применения средств защиты без сертификатов. Корректность. Эффективность. Критерии безопасности. Функции защиты. Качество защиты. Уровни корректности. Сертификация продукции. Процесс сертификации. Порядок подготовки и проведения сертификации. Сертификация программного обеспечения (ПО) на соответствие требованиям безопасности.

Базовый теоретический курс:

«Построение комплексной системы защиты информации предприятия. Подходы и решения»

Курс предназначен для повышения квалификации и профессиональной переподготовки специалистов подразделений технической защиты информации и ориентирован на:

- *руководителей подразделений технической защиты информации (ТЗИ),* непосредственно отвечающих за состояние информационной безопасности и организацию работ по созданию комплексных систем защиты информации в информационных системах (ИС);
- *аналитиков по вопросам компьютерной безопасности,* отвечающих за анализ состояния информационной безопасности, определение требований к защищенности различных подсистем информационных систем и путей обеспечения их защиты, а также за разработку необходимых нормативно-методических и организационно-распорядительных документов по вопросам защиты информации;
- *администраторов средств защиты, контроля и управления,* отвечающих за сопровождение и администрирование средств защиты

информации и средств анализа защищенности подсистем информационных систем.

Содержание курса

В рамках курса рассматриваются:

- Законодательная, нормативно-методическая и научная база
- Структура и задачи органов (подразделений), осуществляющих комплексную защиту информации
- Организационно-технические и режимные меры
- Программно-технические методы и средства защиты информации
- Техническая защита информации на объектах ИС
- Защита информационных и физических объектов информационных систем
- Защита процессов, процедур и программ обработки информации
- Защита каналов связи;
- Подавление побочных электромагнитных излучений
- Управление системой защиты
- Определение информационных и технических ресурсов, а также объектов ИС подлежащих защите;
- Выявление потенциально возможных угроз и каналов утечки информации;
- Проведение оценки уязвимости и рисков информации (ресурсов ИС);
- Определение требований к системе защиты информации;
- Осуществление выбора средств защиты информации и их характеристик;
- Внедрение и организация использования выбранных мер, способов и средств защиты;
- Осуществление контроля целостности и управление системой защиты.
- Теоретические и правовые основы защиты информации и обеспечения безопасности информационных систем;
- Современные технологии и средства защиты информации;
- Принципы построения комплексных систем защиты;
- Основные направления деятельности служб информационной безопасности (ИБ) в действующих и проектируемых информационных системах;
- Способы рационального распределения функций и задач сотрудников служб информационной безопасности;
- Организация эффективного взаимодействия по вопросам защиты информации всех подразделений и сотрудников, использующих и обеспечивающих функционирование информационных систем;
- Вопросы разработки нормативно-методических и организационно-распорядительных документов, необходимых для реализации КСЗИ:
- Способы применения конкретных систем разграничения доступа и средств обеспечения безопасности в информационных системах (ИС).

Необходимая базовая подготовка

Для лучшего усвоения материала курса слушателям желательно иметь представление о современных информационных технологиях и

информационных системах, о правовых, организационных и технических аспектах проблемы обеспечения информационной безопасности.

Приобретаемые знания и навыки

В процессе изучения курса слушатели приобретают знания по:

- основам обеспечения безопасности информационных технологий, современным концепциям построения и эффективного применения комплексных систем защиты информации в информационных системах;
- современным методам и средствам технической защиты информации, подходам к выбору необходимых программно-аппаратных средств защиты информации в информационных системах и сетях;
- планированию защиты, рациональному распределению функций по ТЗИ между подразделениями и сотрудниками предприятия, по организации их взаимодействия на различных этапах жизненного цикла подсистем информационных систем;
- основам проведения информационных обследований и анализа подсистем информационных систем как объектов защиты;
- разработке организационно-распорядительных документов по вопросам защиты информации;
- порядку применения средств защиты информации от несанкционированного доступа (СрЗИ НСД) в информационных системах;
- проблемам информационной безопасности в сетях Internet/Intranet, уязвимостям сетевых протоколов и служб, атакам в IP-сетях;
- основам поиска и использования оперативной информации о новых уязвимостях в системном и прикладном программном обеспечении, о средствах защиты и другой актуальной информации по ИБ.

Дополнительная информация

Каждый слушатель получает CD-ROM, содержащий справочную информацию, а также демонстрационные версии основных рассматриваемых в курсе средств защиты. По завершении обучения слушателям предоставляется возможность в течение месяца получать бесплатные консультации специалистов учебного центра в рамках пройденного курса.

Резюме руководителя курса - **Домарев Валерий Валентинович**, полковник ВС Украины в отставке, эксперт по вопросам информационной безопасности, кандидат технических наук, доцент. Диссертационные исследования посвящены проблемам создания комплексных систем защиты информации. Автор популярных книг: "Защита информации и безопасность компьютерных систем", "Безопасность информационных технологий. Методология создания систем защиты", а также "Безопасность информационных технологий. Системный подход". **Автор более 40 научных статей и публикаций**. Создатель одного из первых в СНГ сайтов по технической защите информации "Protect Box" в 1996 году. Образование высшее: Киевское высшее зенитное ракетное училище (1979 г.) Военная академия ПВО сухопутных войск (1988 г.) Национальная академия обороны

Украины (2000 г.) **Основные этапы прохождения службы**: Киевское высшее зенитное ракетное училище (инженер по радиоэлектронике и средствам радиолокационной разведки), Зенитно-ракетная бригада (инженер по АСУ), Командный пункт войск ПВО страны (направление ЗРВ), Военная академия ПВО сухопутных войск (преподаватель), Генеральный штаб ВС Украины (старший офицер Управления режима секретности и шифрованной связи), Государственный комитет Украины по вопросам государственных секретов и технической защиты информации (начальник информационно-аналитического отдела), Центральный научно-исследовательский институт вооружения и военной техники ВС Украины (начальник отдела развития средств связи и АСУ), Аппарат совета национальной безопасности и обороны Украины (государственный эксперт по вопросам информационной безопасности).

По роду своей деятельности занимался внедрением современных информационных технологий, а также поиском путей обеспечения безопасности информации при создании и эксплуатации компьютерных систем. В течение последних 15 лет работал над решением вопросов организации защиты информации в государственных, банковских и коммерческих информационных системах. Осуществлял руководство рядом научно-исследовательских работ по проблемам обеспечения безопасности современных информационных технологий. Участник ликвидации аварии на Чернобыльской АЭС.

Сфера интересов:
- методология создания комплексных систем информационной безопасности;
- аудит систем информационной безопасности;
- менеджмент информационной безопасности;
- безопасность информационных технологий;
- техническая защита информации;
- безопасность информационного общества;
- информационные войны;
- информационно-психологическое воздействие.