Универсальная программа обучения специалистов по ИТ безопасности, основанная на опыте прикладной работы в данной области.

Андрей Александрович Владимиров, PhD, CISSP, CCNP, CCDP, CWNA, TIA Linux+
Глава по безопасности, Архонт Ltd, Бристоль, Великобритания.
http://www.arhont.com, info@arhont.com

Аннотация.
В данном докладе описывается программа подготовки специалистов в области информационной безопасности как самостоятельной дисциплины. Данная программа радикально отличается от имеющихся западных образцов и по глубине предоставляемого технического материала, и по широте охвата рассматриваемой области. В первую очередь акцент ставится на привитие обучающимся технических навыков, необходимых для выживания в агрессивной среде современного рынка разработок и услуг в сфере информационной безопасности и реалистичной защиты сетей, отдельных узлов, сервисов и приложений от мотивированных, высококвалифицированных кракеров. Для осуществления последнего, в программу включено практическое рассмотрение методологии атак на разных уровнях, направленное на развитие возможности видения информационных систем "через прицел атакующего" и понимания его образа мышления и подходов. Это также позволяет готовить аудиторов безопасности мирового класса - задача, пока неподсильная ни одному из университетов, выпускающих дипломников в этой и смежных областях. Предложенная программа основана на нашем практическом опыте как основателей и руководителей Архонт Ltd - несмотря на существующие преграды, одной из наиболее динамически развивающихся компаний в сфере оказания услуг в области сетевой безопасности в Великобритании.

Введение.
Для обеспечения логического потока представленной информации, данный доклад структурирован следующим образом: изначально мы формулируем существующую проблему в описываемой области. а затем предлагаем оптимальную методологию решения этой проблемы. Основной проблемой, которую устраняет предложенная здесь информация, безусловно является отсутствие универсальной академической системы образования и повышения квалификации специалистов по ИТ безопасности как таковой. Прямым следствием этого более чем существенного недостатка является тенденция перенаправления вопросов ИТ безопасности на специалистов в других областях. В результате образуется "пирамида перенаправления", показанная здесь сверху вниз, от более высоких занимаемых должностей к более низким:

```
Глава по безопасности                 ->        ИТ Менеджер.
        |                                              |
Консультант по безопасности           ->        программист
Консультант по безопасности
администратор по безопасности         ->        системный администратор
        |                                              |
Ассистент по безопасности             ->           техник
```

Непосредственными провалами данного подхода, которые мы наблюдаем практически ежедневно, можно считать:
1. Игнорирование различного образа мышления, мировоззрения и даже черт характера этих специалистов. Сюда же относится основное столкновение их подходов: безопасность против легкости использования сети, сервиса или приложения.
2. Игнорирование различной сферы технических знаний и умений между ИТ профессионалами общего профиля и специалистами по ИТ безопасности.
3. Перегрузку широкопрофильных специалистов несвойственными им специфическими задачами. Защита систем как сверхурочная работа и ее негативное восприятие.

Прямым результатом таких провалов можно смело считать отсутствие безопасности информационных систем несмотря на любые затраченные ресурсы, время и самые последние решения производителей в области систем по безопасности.

Рыночное мифотворчество, принижающее значение подготовки специалистов по ИТ безопасности.
Описанные провалы усугубляются двумя мифами. Первый миф - "Secure by Default"(TM). Так как ИТ инфраструктура подчиняется требованиям бизнеса и организационной работы, а не наоборот, в современных динамически развивающихся сетях дефалтные установки безопасности просто не выживают. Грубый пример - закрытие всех портов в дефалтной установке NetBSD. Система, которая в основном используется в качестве серверной, с данной установкой бессмысленна. При открытии доступа к сервисам она автоматически становится потенциально уязвимой. Пример от обратного - проактивная безопасность OpenBSD, которая в то же время ближе к концепции "Secure by Default". Тем не менее, и в ней известны прорехи, кроме того всегда возможна установка уязвимого программного обеспечения от третьих партий.

Второй миф - "автоматическая безопасность без специалиста". Примеры: концепция Cisco Self-Defending Networks и попытки заменить аудитора безопасности программным и аппаратным обеспечением (SkyBox). К недостаткам данной концепции относятся отсутствие латерального мышления, отсутствие защиты от внеканальных атак

(беспроводные, вардайалинг, социальная инженерия), уязвимость самих систем защиты, отсутствие контроля квалифицированного специалиста за системой и невозможность нахождения новых уязвимостей в процессе автоматического аудита. Установление системы автоматической защиты не устраняет необходимость в наличии администратора по безопасности, а экономит его время, одновременно повышая требования к его квалификации. Системы "аудита без аудитора" заменяют только те "проверки безопасности", которые в повседневной практике мы считаем всего лишь формой финансово направленной социальной инженерии, и защищают только от нападающих низкого уровня квалификации.

"Узкий специалист широкого профиля".
Решение всех вышеперечисленных проблем заключается в полноценной подготовке и повышении квалификации специалистов в области ИТ безопасности, а также целенаправленном разъяснении их необходимости и возможностей потенциальным работодателям. Позиция специалиста по информационной безопасности среди ИТ профессионалов иллюстрируется вершиной равнобедренного треугольника, по краям основания которого находятся с одной стороны программист и инженер по сетям, с другой-ИТ менеджер и руководитель/планировщик проекта по разработке решений. Положение вершины отображает взгляд на проблемы безопасности сверху/со стороны, независимый подход. Смещение вершины в любую сторону, а также вверх или вниз, ведет к появлению уязвимостей информационных систем, разрабатываемых либо контролируемых подобным специалистом.

Проблемы образования специалистов по профилю ИТ безопасности.
Данные проблемы являются отражением более широких недостатков области как таковой и, возможно, их первоисточником. Корневой проблемой подготовки специалистов по ИТ безопасности является разрыв между теорией и практикой. Для демонстрации того, что данное утверждение не является стандартной общей фразой, приведем конкретные примеры этого разрыва с обоих сторон.

"Теория" на высоте, "практика" хромает.
Разница между алгоритмом и его имплементацией является хорошим частным примером этого случая. Эта разница прекрасно иллюстрируется симметричным алгоритмом поточного шифрования RC4, который до сих пор в достаточной мере безопасен при использовании достаточной длины ключа, и дырами в прикладной имплементации этого алгоритма. Наиболее известный, и очень хорошо нам знакомый случай - атаки на WEP от ФМС до более новых атак Корека. С одной стороны, имеем вполне надежный алгоритм проф. Рональда Ривеста. С другой стороны - AirCrack Кристофера Девина и наш рекорд по взлому WEPa за 3 минуты 40 секунд с помощью этой утилиты, запатченой заплатой акселерации, которую можно загрузить на http://www.wi-foo.com. При этом методы за пределами изначальной имплементации не устраняют проблемы - по нашим, пока ещё не опубликованным выкладкам, ротация WEP ключей с помощью стандарта 802.1x делает беспроводную сеть еще более уязвимой. На самом нижнем/последнем уровне имплементации, системный администратор способен свести на нет все усилия как теоретиков, стоящих за концепцией алгоритма или стандарта, так и разработчиков его практического воплощения. Типичные примеры подобного - использование агрессивного режима работы стандарта IPSec (уязвимость к атаке с помощью IKECrack) и CBC режима SSL/TLS (уязвимость к атаке с помощью Omen).

"Практика" на высоте, "теория" хромает.
Типичный пример - системы так называемой активной защиты, как проводной (Симбиот), так и беспроводной (Аруба). Практически, данные решения могут быть безупречными, обеспечивая почти стопроцентное отключение системы атакующего от сети. Однако разработчики явно мало представляют себе общие принципы работы сетей и катастрофические последствия установки подобных систем в Интернете. Верифицировать исходные IP и MAC адреса вне сетей IPSEC невозможно, а установка систем активной защиты на VPNax бессмысленна. Любой атакующий с минимальным уровнем знаний адресации сетей способен обернуть такие системы против их владельца либо же просто себе на пользу.

Существует ряд других недостатков, проистекающих или имеющих отношение к этой изначальной проблеме. Здесь они перечисляются без дополнительных комментариев и разъяснений, которые мы всегда готовы предоставить всем желающим:
- привязка к отдельному производителю
- привязка к отдельному уровню OSI модели
- распространенный в некоторых кругах постулат о том, что вся информационная безопасность объяснима через криптографию. В то время как значимость криптографических познаний трудно переоценить, большинство атак на современных сетях совершенно не связаны со взломом того или иного криптографического алгоритма
- подготовка менеджеров по ИТ безопасности с отсутствующим прикладным опытом
- подготовка специалистов по ИТ безопасности без знания необходимой законодательной базы
- отсутствие аудита безопасности как отдельной дисциплины

Отдельно стоящим вопросом является соответствие менталитета обучающегося данной специальности. Информационная безопасность - это образ мышления. При обучении до уровня бакалавра его необходимо воспитывать. При приеме в магистратуру по данной специальности, воспитывать уже поздно - необходимо проверять его наличие с помощью психометрического тестирования. Это абсолютно серьезное предложение и мы готовы поделиться практическими соображениями в данной области.

К сожалению, как университетская, так и прикладная подготовка специалистов в области информационной безопасности на рабочем месте не является сбалансированной. В первом случае, часто хромают внедрение и обслуживание систем безопасности на практике. Во втором - идет мощная и, в большинстве случаев, неоправданная привязка к отдельному производителю и отсутствие целостного видения архитектур безопасности и потенциальных угроз этим архитектурам. В конечном счете получается "узкий специалист узкого профиля", неспособный справиться со своей задачей.

Проект программы по универсальной подготовке специалистов в области информационной безопасности.
Мы предлагаем эскиз полной программы подготовки специалистов по информационной безопасности с учетом всех перечисленных недостатков подготовки. Данная программа может использоваться на трех уровнях:
- университетский: Балакавр по Информационной Безопасности и Сетевой Защите
- университетский: Магистр по Информационной Безопасности и Сетевой Защите (оригинальный курс или конверсия из других ИТ специальностей)
- курсы повышения квалификации для работающих специалистов

Безусловно, максимальная реализация программы возможна только в университетской среде, так как ограничения по времени и физиологическим возможностям человеческого мозга не позволят освоить подобный пласт информации за кратковременный курс. Тем не менее, отдельные фрагменты программы можно использовать как элементы курсов повышения квалификации, в том числе для подготовки к стандартным сертификатам по безопасности, таким как CISSP с последующими расширениями.

Оптимальным было-бы готовить специалистов начиная со степени Бакалавра. В этом случае, первые два курса следует посвятить изучению основ программирования (i386 ассемблер,C и один из языков высокого уровня по выбору, Перл предпочтителен) и системной/сетевой администрации (Windows, UNIX, Cisco) с частичным акцентом на безопасности, и только затем переходить к изложенной программе. Степень Магистра при окончании такого курса будет являться надстройкой над ним с внедрением большего количества технических деталей и практическим проектом. Альтернативно, должна существовать конверсионная программа Магистра по Информационной Безопасности для дипломников в других ИТ областях, а также системных администраторов и программистов без диплома, но со значительным рабочим стажем, подкрепленным промышленными сертификатами. Сертификаты, имеющие отношение к безопасности (e.g. TIA Security+, сертификаты от производителей решений по безопасности (Checkpoint, Cisco CCSP etc.)) должны служить плюсом при поступлении. Покрытие областей в программе по обучению специалистов по информационной безопасности должно происходить от общего к частному, как изложено в по-модульном описании, следующем далее.

Модуль 1. Введение в информационную безопасность. Содержание модуля:
Отграничение области информационной безопасности: цели, задачи, подход, менталитет, направления. Триада информационной безопасности. Теория режимов и архитектур безопасности. Виды и методы ограничения доступа. Международные и отечественные организации и комитеты по информационной безопасности и их деятельность. Промышленные стандарты безопасности и оценка аппаратного и программного обеспечения согласно этим стандартам. Международные сертификаты квалификации экспертов по информационной безопасности, их значение и как их получить. Карьера в области информационной безопасности и защиты сетей. Общий обзор угроз информационной безопасности: разновидности атак и атакующих, цели и мотивации кракеров разных типов, статистика атак. *Реферат на одну из рассмотренных тем.*

Модуль 2. Сетевая безопасность. Содержание модуля:
Иерархический дизайн и зоны безопасности сетей. Безопасность и уязвимости протоколов второго уровня. Виртуальные локальные сети, STP, частные протоколы второго уровня, атаки на коммутаторы, защита коммутаторов, атаки, связанные с ARP и защита от них. *Лабораторные работы: атака второго уровня, защита коммутатора на примере Циско Каталиста, атака с помощью ARP и защита от нее.*

Безопасность и уязвимости протоколов третьего уровня. Подделка IP адресов, IP фрагментация и безопасность, атаки, связанные с ICMP, атаки на протоколы маршрутизации, глобальные атаки на Интернет через BGP, фильтрация пакетов на третьем уровне, защита протоколов маршрутизации и автономных систем. *Лабораторные работы: фильтрация пакетов на третьем уровне, атака и защита избранного протокола маршрутизации.*

Безопасность и уязвимости протоколов четвертого уровня. Типы межсетевых экранов. Безопасность TCP vs UDP. Фильтрация пакетов на четвертом уровне - простая и статическая. Методы преодоления фильтрации кракерами. Удаленное определение типов и версий операционных систем. *Лабораторные работы: Nmap и xprobe от А до Я, фильтрация пакетов на четвертом уровне.*

Безопасность и уязвимости уровней с 5-го по 7-ой. Межсетевые экраны на высоких уровнях, фильтрация по содержимому пакетов на этих уровнях, "Хищник", COPM-2 и "Великий Китайский Межсетевой Экран". Безопасность и узязвимости DNS. Безопасность и уязвимости сетевой почты, SPAM. Безопасность и уязвимости распределенных ресурсов. Безопасность и уязвимости FTP. Общая безопасность и уязвимости вебсерверов. Безопасность и уязвимости SNMP. *Лабораторные работы: подделка DNS, фильтрация спама, установка веб-*

прокси и конфигурация прокси-брандмауэра. Фильтрация по содержимому поля данных пакетов. Атаки и защита SNMP, установка защищенного SNMPv3.

Модуль 3. Безопасность отдельного узла. Содержание модуля:
Безопасность, уязвимости и защита систем Windows. *Лабораторная работа: установка защищенного Windows сервера.*

Безопасность, уязвимости и защита систем UNIX. *Лабораторная работа: установка защищенного Linux сервера.*

Безопасность, уязвимости и защита систем сетевого аппаратного обеспечения (маршрутизаторы, коммутаторы, межсетевые экраны и так далее). *Лабораторная работа: защита маршрутизатора Циско.*

Модуль 4. Общая безопасность кода. Содержание модуля:
Принципы написания безопасного кода на языках низкого и высокого уровней. Переполнение стека и динамических областей. Защита от него. Прорехи проверки вводимых данных. Защита от них. Race conditions, утечка информации и другие проблемы безопасности кода. Аудит безопасности открытого кода: методология, доступные утилиты, облегчающие эту задачу. Методы устранения обнаруженных в программе уязвимостей. Написание отчета о проделанном аудите кода. *Лабораторная работа: аудит безопасности предложенного кода и устранение обнаруженных проблем. Написание краткого формального отчета о проделанной работе. Проекты на выбор: написание любой программы связанной с пройденным материалом: небольшой безопасный сервер, шеллкод, эксплойт.*

Модуль 5. Безопасность кода - критические приложения. Содержание модуля:
Безопасность веб-приложений. Безопасность CGI, ASP.NET, ActiveX, PHP, Java и JSP. Безопасность шоппинг-карт и финансово-мотивированные атаки. Безопасность веб-служб. Кросс-сайт скриптование и похищение файлов cookie. Атаки "человек в середине" на веб приложения с помощью прокси. Атаки на браузеры и конфигурация безопасности браузеров. *Лабораторная работа: написание небольшого безопасного веб приложения на языке по выбору, работа с Paros, Spike, Peach.*

Безопасность баз данных. Ограничение доступа к базам данных. Авторизация. SQL и SQL иньекции. Защита от них. *Лабораторная работа: конфигурация безопасности MySQL. Практическая SQL инъекция.*

Модуль 6. Беспроводная безопасность. Содержание модуля:
Общая безопасность микроволновой, лазерной и инфракрасной передачи данных. Основные принципы микроволнового радио: характеристики и принципы работы антенн, зона распространения сигнала, радиоисчисления и юридические регуляции по выходной мощности. Безопасность на первом сетевом уровне, пиратские устройства, глушение и глушилки.

Безопасность стандарта 802.11. Диапазоны частот ISM и UNII, различные стандарты 802.11, сетевых архитектуры 802.11, CSMA/CA vs. CSMA/CD, структура и типы 802.11 фреймов. Разнообразные атаки против 802.11. Введение в структуру протокола 802.11i, индустриальный и SOHO 802.11i. WPAv1, WPAv2, TKIP и CCMP. Другие методы защиты сетей 802.11. Безопасность стандарта 802.15. Типы Bluetooth и архитектура сетей 802.15. Уровни безопасности 802.15. Варнибблинг и известные прорехи мобильных устройств. Безопасность стандарта 802.16 и частных каналов беспроводной передачи данных на высоких частотах. Безопасность спутниковой передачи данных от перехвата и несанкционированного доступа. Защита спутниковых провайдеров.

Лабораторные работы: установка 802.11 сетей, защищенных согласно индустриальному и SOHO стандартам WPAv1 или WPAv2. Создание гибких защищенных беспроводных шлюзов на базе платформ Линукс и BSD. "Боевые выезды" и варнибблинг на практике. Атаки "человек в середине" против защищенных 802.11 сетей. Иньекция данных в сети, защищенные с помощью WEP, используя WepWedgie и AirCrack. Взлом WEP с помощью атак Корека.

Модуль 7. Физические аспекты информационной безопасности. Содержание модуля:
Безопасность электромагнитных эманаций. EMSEC: TEMPEST, NONSTOP и HIJACK. Атака Ван Ика. Методы защиты - бункера, покрытия и напыления, материалы, белый шум и другие способы противодействия. Основы TSCM. Частоты, каналы и методы передачи. Способы сокрытия сигнала, наведенное прослушивание. Перехват аудио и видеоинформации, прослушка телефонных сетей. Типы устройств для перехвата и передачи информации. Принципы их обнаружения. Обзор необходимого оборудования для обнаружения подобных устройств: счетчики и анализаторы частот, измерители силы сигнала, нелинейные детекторы соединений (NJLD) и так далее. Оптический и акустический EMSEC и способы противодействия против подобных атак. Физические кейлоггеры - модифицированные клавиатуры, переходники PS2-на-PS2 и другие подобные устройства. Способы их обнаружения.

Биометрика. Различные методы биометрической идентификации и их сравнительная эффективность. Биометрические устройства и их надежность. Биометрические паспорта и идентификационные карты. Физическая аутентикация с помощью токенов и карт. Виды токенов и карт. Принципы их работы. Генерация единовременных

паролей. Возможность перехвата данных с токена и подделки карт. Физическая защита оборудования: системы сигнализации, детекторы движения, камеры дневного и ночного обзора, замки для мобильного оборудования. Методы уничтожения разнообразных носителей информации.

Лабораторные работы: генерация осмысленного сигнала с помощью монитора и его перехват. Нахождение коммерческого устройства для прослушивания. Использование физического кейлоггера.

Модуль 8. Прикладная криптография. Содержание модуля:
Принципы и законы криптографии. Исторические шифры. Основы криптоанализа. Обзор стандартных и основных симметричных шифров. DES, ГОСТ, AES, AES кандидаты, 64-блочные шифры. Режимы операции симметричных шифров и практическое использование этих режимов. Поточные шифры. Сравнение безопасности симметричных шифров. Сравнение эффективности работы блочных и поточных шифров на различных аппаратных архитектурах. Выбор симметричного шифра для программистов и системных администраторов. Шифрование паролей доступа в различных операционных системах.

Функции хэширования. Блочные симметричные алгоритмы в качестве функций хэширования. Поиск столкновений и другие методы атаки этих функций. Сравнительный анализ безопасности и эффективности работы различных функций хэширования. Практическое использование функций хэширования - сохранение целостности передаваемых данных, целостность сохраняемых файлов, шифрование паролей. Проверочные суммы файлов и протоколов (CRC32, Internet Checksum, Cisco IOS checksum) и их недостатки по сравнению с функциями хэширования. MIC в системе беспроводной безопасности WPAv1 и ее недостатки. Коды HMAC.

Модульная арифметика. Трудные задачи и асимметричная криптография. Диффи-Хеллман, Эль Гамаль, RSA и эллиптические кривые. Практические области приложения асимметрической криптографии: безопасный обмен ключами, аутентикация и алгоритмы цифровой подписи. DSA, RSA и ГОСТ. Цифровые сертификаты. Формат сертификата x.509.

Общая безопасность паролей. Выбор сильных паролей. Вспомогательные программы и команды для этого выбора. Ротация паролей. Определение чем зашифрован пароль в файле паролей. Атаки паролей по словарю и перебором, распространенные утилиты для этих атак.

Лабораторные работы: установка и конфигурация PGP или GnuPG. Взлом паролей к распространенным операционным системам (Windows NTLM hashes, UNIX DES, MD5, Blowfish) с помощью атак по словарю и перебора (L0phtCrack, John the Ripper, md5crack). Взлом Циско vigenere с помощью карандаша и бумаги.

Модуль 9. ***Основные протоколы сетевой безопасности.*** Содержание модуля:
Операции и безопасность SSH. Уязвимость SSHv1 к атаке "человек в середине". Операции и безопасность SSL/TLS. Уязвимость SSL/TLS к тайминг атаке. Операции и безопасность PPTP. Уязвимость PPTP к атакам, Anger и Ettercap. Операции и безопасность IPSec. Параметры безопасности, протоколы и режимы функционирования. Выбор шифров и имплементаций. Аппаратные и программные имплементации IPSec. Уязвимость агрессивного режима и различных имплементаций (e.g. WaveSec) к атакам. Общий обзор других VPN протоколов (cIPE, VTun, OpenVPN).

Протоколы аутентикации: RADIUS, TACACS+ и Керберос. Структура, операции и имплементации этих протоколов. Выбор необходимой имплементации. Уязвимости Керберос 4. Атаки на RADIUS. Стандарт аутентикации 802.1x и типы расширяемого протокола аутентикации (EAP). Правильный и безопасный выбор типа EAP. Уязвимости отдельных типов EAP. Служба каталогов LDAP. Её использование для централизованной аутентикации. LDAP и аутентикация мобильных устройств. Имплементации и инструментарий LDAP.

Лабораторные работы: установка и конфигурация защищенных IPSec и PPTP туннелей. Перенаправление портов по протоколу SSH. Установка RADIUS сервера, службы каталогов LDAP и практическая аутентикация пользователей. Атаки против уязвимых версий и режимов SSH, SSL/TLS, PPTP и IPSec.

Модуль 10. Зловредный код (malware) и борьба с ним. Содержание модуля:
Вирусы и их классификация. Методы распространения, внедрения и сокрытия от обнаружения. Приносимый вред. Черви и их классификация. Методы и алгоритмы распространения, внедрения и сокрытия от обнаружения. Известные черви от Морриса до наших дней. Приносимый вред, включая истощение сетевых ресурсов. Бэкдоры: трояны и руткиты. Функциональность, включая кейлоггинг. Патчеры файлов. Бэкдоры для систем Windows и UNIX. Методы их сокрытия и перезапуска. Способы коммуникации с удаленным бэкдором - обратные соединения, сокрытие и шифрование каналов коммуникации. Утилиты для проведения DDoS атак и методы их проведения. Другие виды зловредного кода. Spyware, его коммерческое значение и приносимый вред. Легальная сторона Spyware на примере Gator'a. Дайалеры и наносимый ими ущерб. Форк-бомбы. Автоматические генераторы зловредного кода. Методы обнаружения и удаления зловредного кода разных типов. Основы вскрытия и анализа обнаруженного зловредного кода, включая анализ бинарных файлов. Локальная и централизованная фильтрация зловредного кода. *Проект: написание простого бэкдора и описание методологии его обнаружения.*

Модуль 11. Аудит безопасности. Содержание модуля:
Типы аудитов безопасности. "Black box", "grey box" и "white box" тестирование. Общая последовательность и стадии тестирования. Что является и что не является аудитом безопасности. Преимущества и недостатки использования автоматизированных систем проверки безопасности. Оценка риска обнаруженных уязвимостей. Этическая сторона аудита и тестирование на DoS атаки. Составление рекомендаций по устранению обнаруженных уязвимостей. Написание и формат отчета об аудите безопасности.

Удаленный аудит безопасности через Интернет. Особенности и методология. Влияние промежуточных сетевых узлов на результаты тестирования. Методы преодоления межсетевых экранов и систем обнаружения несанкционированного вторжения. Проверка работы систем обнаружения несанкционированного вторжения.

Локальный аудит безопасности. Отличия его от удаленного. Атаки на низких уровнях OSI модели. Атаки "человек в середине". Перехват и анализ данных. Обнаружение и избежание систем обнаружения несанкционированного вторжения и проверка их функционирования. Оценка риска сети со стороны внутренних атакующих.

Беспроводной аудит безопасности и его специфика. Последовательность, методология, необходимое оборудование. Атаки против беспроводных протоколов, точек доступа и шлюзов. Атаки "человек в середине", фишинг и беспроводные DoS атаки. Оценка разделения проводной и беспроводной сети. Обнаружение и устранение пиратских устройств в процессе аудита. Оценка риска безопасности беспроводной сети.

Аудит безопасности отдельно взятого сетевого узла с наличием доступа в систему. Анализ безопасности установленных на нем приложений. Способы повышения привилегий. DoS атаки на локальном узле. Бета-тестирование безопасности нового сетевого устройства: форма, подход, методология и проверка на соответствие промышленным стандартам безопасности.

Лабораторная работа: проверка безопасности узлов-мишеней с последующим написанием полного отчета о проделанном аудите безопасности, включающим в себя оценку риска обнаруженных уязвимостей и предложения по их практическому устранению. Предлагаемая структура сети-мишени - маршрутизатор, коммутатор, Windows сервер, Линукс сервер.

Модуль 12. Реверс Инженерия. Содержание модуля:
Дебаггеры, дизассемблеры, дамперы, эмуляторы и редакторы шестнадцатиричного кода для систем Windows и UNIX. Их сравнительные характеристики. Использование дебаггера, дизассемблера и дизассемблера вместе с дебаггером. Идентификация ключевых структур языков высокого уровня. Анализ критических ошибок приложений и операционных систем. Вскрытие файлов "core dump". Методы защиты программного обеспечения от дизассемблеров, дебаггеров, мониторов и дамперов. Преодоление методов защиты программного обеспечения от реверс инженерии. *Проект: реверс инженерия "неизвестного трояна" с предоставлением отчета о результатах.*

Модуль 13. Обнаружение и расследование атак. Содержание модуля:
Журналирование на различных системах и его централизация. Защита процесса журналирования и самих журналов, процедура их анализа, вспомогательные утилиты для просмотра и анализа журналов. Признаки нестандартного поведения систем и сигнатуры атак. Основы наблюдения за сетями. Системы обнаружения и предотвращения несанкционированного доступа (IDS/IPS). Сигнатурные и статистические IDS/IPS. Архитектура распределенных IDS/IPS. Беспроводные IDS/IPS. Истинные и ложные срабатывания. Обнаружение атак на всех уровнях OSI модели. Активная защита и ее проблемы. IDS/IPS на отдельно взятом узле: Tripwire, Cisco Secure Agent и так далее.

Правовые основы расследования вторжения. Преступление и наказание: законы о компьютерной безопасности и уголовная ответственность за несанкционированный доступ, DoS/DDoS атаки, пиратство и взлом коммерческого программного обеспечения. Типы компьютерных преступлений с юридической точки зрения. Инстанции, занимающиеся расследованием компьютерных преступлений и как с ними связаться. Юридические процедуры сбора, сохранения и предоставления доказательств. Стратегия расследования, управление расследованием и предварительная подготовка к инцидентам атак.

Технические процедуры расследования вторжения и сбора доказательств. Дупликация систем и сохранение доказательств. Используемые утилиты и методологии. Анализ доказательств. Приложение всего перечисленного к различным системам, включая Windows, UNIX и сетевые устройства Циско. Признаки вторжения на этих системах. Идентификация и отслеживание атакующих на Интернете, в локальных и беспроводных сетях. Технические и юридические стороны вопроса. Используемые методы и утилиты.

Лабораторная работа: установка и настройка Snort + ACID, установка и настройка Tripwire. Проведение анализа "взломанной машины" с учетом всех процедуральных деталей. Предоставление формы описания обнаруженных доказательств в качестве отчета.

Модуль 14. Управление информационной безопасностью. Содержание модуля:

Обязанности главы по информационной безопасности компании или организации. Планы безопасности и обязанности сотрудников в соответствии с этими планами. Стандарты, регуляции и процедуры. Классификация информации и систем согласно уровням безопасности. Уставы по безопасности (security policy). Их предназначение, структура и содержание. Написание устава по безопасности с учетом специфики и требований компании или организации. Качественная и количественная оценка риска информационных инфраструктур. Оценка финансового риска и финансовых потерь вследствие атак на информационные инфраструктуры. Страховые аспекты вопроса. Сравнительная оценка рентабельности решений и услуг по информационной безопасности. Последствия успешных атак для имиджа компании и их смягчение. Работа с юристами и средствами массовой информации.

Социальная инженерия. Типы "социальных атак" и их последствия. Звенья цепи, наиболее уязвимые для социальных инженеров. Обнаружение и защита от социальной инженерии. Работа с персоналом. Безопасный прием на работу и увольнение сотрудников. Права и обязанности пользователей на сети. Юридические и административные аспекты отслеживания поведения пользователей. Повышение уровня образованности пользователей и технического персонала в области информационной безопасности.

Информационная безопасность в непредвиденных обстоятельствах. Сохранение контроля. Планы на случай непредвиденных обстоятельств, их составление и роль в уставе безопасности. Описание процедур расследования атаки в уставе безопасности. Резервное копирование и его безопасность. Резервные центры трех типов. Резервные линии и защита от DDoS атак. Восстановление утерянной информации.

Открытие собственной компании, оказывающей услуги в сфере информационной безопасности. Анализ рынка. Определение рыночной ниши. Услуги vs. разработка программного и аппаратного обеспечения. Написание бизнес-плана. Стартовый капитал и инвестиции. Необходимые специалисты, их поиск, отбор и наем. Стандарты аккредитации компаний, оказывающих услуги в области информационной безопасности. Модели маркетинга и отношений с клиентами. Рост компании и диверсификация услуг. Патенты и интеллектуальная собственность.

Проект: написать устав по безопасности для воображаемой компании или организации либо написать краткий бизнес-план для открытия собственной компании, оказывающей услуги в сфере информационной безопасности либо производящей имеющее отношение к безопасности программное или аппаратное обеспечение.

Основные преимущества описанной программы по сравнению с западными аналогами
Предложенная программа резко отличается от её возможных эквивалентов, таких как курсы MSc в области информационной безопасности, предлагаемые некоторыми западными университетами. В чем же заключаются основные различия?

1. Наша программа устраняет недостатки и проблемы, перечисленные в начале этого доклада.
2. Она является более глубокой и логичной, перемещаясь от общего к частному, от теории к практике, от массивных сетей до отдельных участков кода, от алгоритмов шифрования до использующих их протоколов безопасности.
3. Основы управления информационной безопасностью даются не в начале, как в западных программах, а в конце. Согласно нашей точке зрения, менеджер обязан полностью понимать системы, методологии и процедуры, за которые он ответственнен.
4. Покрываются все сферы информационной безопасности без исключения. Огромное значение уделяется практике - см. перечисленные лабораторные работы и проекты. В результате получается специалист, способный выжить и трудоустроиться в условиях даже самой жесткой конкуренции, с навыками и умениями, которые всегда кому-либо пригодятся и в частном, и в государственном секторе. Подобный специалист способен открыть и развивать свою собственную компанию в этой сфере, либо работать независимым консультантом-одиночкой. Именно поэтому в последний модуль по управлению мы включили секцию об открытии и продвижении собственной компании по информационной безопасности. Подобный материал полностью отсутствует в западных программах.
5. Мы стараемся покрыть основные существующие платформы и типы сетей. Перекрываются все 7 уровней OSI модели. Значительное внимание уделяется использованию свободного программного обеспечения с открытым кодом. Для этого есть существенные причины. Во-первых, по нашим наблюдениям, наличие доступа к коду значительно облегчает обучение, стимулирует понимание, любопытство и творческий подход. Во-вторых, учитывается специфика российского рынка. Далеко не многие компании, особенно компании начинающие, способны платить по 10 - 20 тысяч в год за лицензию пользователя на необходимое коммерческое программное или аппаратное обеспечение. Тем более это относится к учебным и научным учереждениям и организациям, не говоря уже о консультантах-одиночках. Впридачу, мы не приветствуем пиратство, и считаем, что более активное использование свободного программного обеспечения с открытым кодом поможет его ограничить, заодно значительно уменьшив сложившийся негативный имидж России, как "страны софтварных пиратов" за рубежом. Западные курсы акцентируются на коммерческих решениях - таковы законы рынка.
6. Как вы уже очевидно заметили, в отличие от западных наработок. в нашей программе уделяется большое значение не только методам защиты, но и методам нападения. Во-первых, без способности смотреть на системы "через прицел атакующего" их невозможно эффективно защитить. Специалист по информационной безопасности должен быть способным понимать образ мышления кракера, чтобы предсказать его действия, методы и подходы,

знать, на что способны утилиты и устройства, используемые нападающим. Во-вторых, рынок для аудиторов безопасности существует и продолжает активно расширяться. Тем не менее, реального стандарта по их подготовке нет. В данную специализацию уходят многие, считающие ее хорошим карьерным ходом или способом заработать. При этом большинство курсов по подготовке "этических хакеров" явно читаются подобного-же рода "гуру".

Хотелось-бы остановиться на этом подробнее. Так как мы хорошо знакомы с рынком аудитов сетевой безопасности, мы можем изложить основные ошибки и пробелы многих участников этого рынка:

- одни и те же методики и утилиты используются при проведении удаленных и локальных аудитов безопасности. Никогда не следует забывать о тестировании низкоуровневых протоколов!

- отсутствует полный спектр услуг. В особенности, это относится к аудитам беспроводной безопасности (впервые стандартизованы в нашей "Wi-фу"), локальным аудитам с доступом к узлу, аудитам исходного кода, бета-тестированию новых и малопроверенных сетевых устройств (впервые стандартизирован для независимых консультантов в нашей "Hacking Exposed: Cisco Networks")

- чрезмерное доверие автоматизированным сканерам уязвимостей, либо просто неумение пользоваться чем-либо ещё. По нашему опыту, многие как бесплатные, так и коммерческие сканеры выдают до 50-60 % фальшивых позитивов (fasle positives), для устранения которых необходима детальная проверка полученных данных "вручную"

- недостаточное внимание, уделяемое оценке безопасности сетевых устройств. "Это всего-лишь коммутатор (кабельный "модем", точка беспроводного доступа, маломощный маршрутизатор), что кракеры могут реально с ним сделать?". Для по крайней мере некоторых ответов на этот вопрос, см. десятую главу выходящей "Hacking Exposed: Cisco Networks"

- недостаточное усердие при попытках пробить межсетевой экран при удаленном тестировании. "Если стандартный скан не проходит, значит сеть в безопасности"

- недостаточное использование латерального мышления в целом - если проблема не решается в лоб, она забрасывается вместо поиска обходных путей, вследствии недостатка кругозора

Программа, которую мы описали, способствует подготовке истинных аудиторов безопасности, не совершающих подобных ошибок.

Заключение.
Подготовка полноценных специалистов в сфере информационной безопасности возможна только в случае тщательного прохождения всех пунктов приведенной программы. Их можно разделить на 7+7, по 7 модулей в год, что является приемлемым для
- двухлетнего обучения на диплом Магистра
- двух последних лет обучения на диплом Бакалавра
Разница в содержании курса между обоими дипломами будет заключаться в глубине преподавания предложенных тем и количестве практических работ, которое для бакалавра может быть неполным (по сравнению с приведенным в программе). В чем-то приведенное расхождение напоминает разницу между (ISC)2 SSCP и CISSP сертификатами.

Говоря о промышленных сертификатах, было-бы весьма полезно, если бы выпускники с дипломами специалистов по информационной безопасности могли-бы получать статус CISSP Associate, либо получать иные сертификаты в данной области, такие как SANS GIAC и TIA Security+. Это явилось-бы подтверждением значимости курса известными международными организациями. Уже имеются прецеденты автоматического присвоения статуса CISSP Associate дипломникам в области управления информационной безопасностью, например в Royal Holloway колледже Лондонского университета. В любом случае, прохождение подобной программы автоматом подготовит студентов к сдаче на все вышеперечисленные сертификаты.

В том случае, если предложенная программа выглядит слишком емкой или даже непомерной, по крайней мере теоретически ее можно разделить на две ветви специализации. Первая ветвь, с уклоном в программирование и менеджмент безопасности проектов разработки, будет акцентирована на модулях, концентрирующихся на безопасности кода, реверс инженерии и безопасности отдельного сетевого узла. Вторая ветвь, с уклоном в системную администрацию, архитектуру сетей и менеджмент безопасности информационной инфраструктиры компании или организации, будет акцентирована на модулях, концентрирующихся на безопасности сетей, протоколах сетевой безопасности, физической безопасности и управлении информационной защитой. Таким образом, может быть достигнуто некоторое разграничение специальностей, которое способно оказаться полезным при разработке курса Магистра по Информационной Безопасности для тех, кто уже получил Бакалавра в данной области. Это разграничение позволит углубить уровень изучения материала профессионалами с уже имеющимся опытом в сфере информационной безопасности. Кроме того, отдельные модули предложенной программы можно использовать как полноценные курсы повышения квалификации специалистов, например в Академии

Информационных Систем (http://www.infosystem.ru/), где уже предоставляется набор на подобный курс, читаемый нами и посвященный прикладной безопасности беспроводных сетей стандарта 802.11.

Ссылки.

http://www.cs.utk.edu/~dunigan/security.html
http://heap.nologin.net/programming.html
http://www.owasp.org/index.jsp
http://www.drizzle.com/~aboba/IEEE/
http://www.eskimo.com/~joelm/tempest.html
http://www.tscm.com/
http://www.ee.oulu.fi/research/ouspg/sage/glossary/
http://www.ietf.org/rfc/rfc2196.txt
http://www.isg.rhul.ac.uk/msc/teaching/TM.shtml
https://www.isc2.org/
http://www.cccure.org/
http://csrc.nist.gov/
http://www.informaticsgroup.com/sg/ipdc/hacking.htm
http://conventions.coe.int/Treaty/RUS/v3DefaultRUS.asp
http://iso-17799.safemode.org/
http://www.citforum.ru/security/
http://www.ot.ru/print_version_press20041014.html#topofpage
http://www.boran.com/security/
http://www.isecom.org/
http://secinf.net/
http://www.l0t3k.org/security/