СТАТУС CISSP: КАК ПОЛУЧИТЬ И НЕ ПОТЕРЯТЬ?

***Дорофеев Александр Владимирович**, CISSP, CISA*

Рассмотрены вопросы международной сертификации специалистов в области информационной безопасности. Представлено описание основных учебных разделов и сложности подготовки.

***Ключевые слова:** сертификация специалиста, обучение по информационной безопасности, сертифицированный профессионал по информационной безопасности*

STATUS CISSP: HOW TO GAIN AND NOT TO LOSE?

***Alexander Dorofeev**, CISSP, CISA*

The problems of international certification of specialists in the field of information security are considered. The description of the main education sections and complexity of training is presented.

***Keywords:** professional certification, information security training, CISSP*

Аббревиатура CISSP (Certified Information Systems Security Professional), которую можно перевести как «сертифицированный специалист по информационной безопасности» появилась в начале 90-х годов, благодаря ассоциации ISC2 (International Information Systems Security Certification Consortium). Сейчас данным статусом уже обладают почти 90 000 человек в 146 странах мира. Что же стоит за статусом CISSP? Признают ли его в нашей стране? Как подготовиться к экзамену? Ответы на эти вопросы мы и дадим в первой статье цикла материалов, посвященных подготовке к экзамену.

Получить статус CISSP может специалист, сдавший сертификационный экзамен и имеющий необходимый практический опыт в области информационных технологий и информационной безопасности.

Экзамен представляет собой 6-ти часовой компьютерный тест на английском языке. Структурно он состоит из набора кейсов и ассоциированных с ними вопросов. Вопросы касаются тем, определенных в CISSP CBK (Common Body of Knowledge).

Согласно CISSP CBK специалист по информационной безопасности должен обладать знаниями и опытом в следующих 10 областях:

- управление доступом
- телекоммуникации и сетевая безопасность
- управление информационной безопасностью, риск-менеджмент
- безопасная разработка программного обеспечения
- криптография
- разработка безопасных архитектур
- обеспечение информационной безопасности на операционном уровне
- обеспечение непрерывности бизнеса и восстановления после сбоев
- законодательство, расследование инцидентов, выполнение требований
- физическая безопасность

Кратко рассмотрим содержание доменов CISSP CBK, знание которых проверяется в ходе экзамена.

Управление доступом.

В данном разделе рассматриваются виды управления доступом, а также способы аутентификации: пароли, биометрия и др. Значительное внимание уделено основным принципам информационной безопасности, таким как: принцип «наименьших привилегий», принцип «need-to-know» и принцип разделения полномочий.

Телекоммуникации и безопасность.

Это самый объемный раздел, который можно разделить на три логических блока: основные концепции построения локальных и глобальных сетей, технологии обеспечения безопасности в сетях и сетевые атаки.

Специалист по информационной безопасности должен в первую очередь хорошо представлять себе концепцию межсетевого взаимодействия: модель OSI, понимать термины «инкапсуляция» и «деинкапсуляция», ориентироваться в модели TCP/IP. В раздел попали технологии LAN, а также рассматриваются такие компоненты сети как коммутаторы, маршрутизаторы, межсетевые экраны и другие.

Что касается технологий обеспечения безопасности, то в первую очередь будущие обладатели статуса CISSP должны ориентироваться в технологиях построения виртуальных частных сетей (VPN), применении трансляции сетевых адресов (NAT) и сегментировании сетей. Также важно понимать механизмы обеспечения безопасности беспроводных сетей, и обеспечения безопасности электронной почты.

Невозможно представить себе эксперта в области информационной безопасности, который бы не разбирался в технологиях организации сетевых компьютерных атак, как минимум, в таких как:

- атаки методом перебора паролей и подбора по словарю;
- атаки «отказ в обслуживании»;
- spoofing-атаки;
- перехват трафика;
- атаки «человек посередине»;
- спамерские атаки;
- социальная инженерия;
- фишинг-атаки;
- атаки типа «Маскарад»;
- перехват сессии;
- ARP-spoofing;
- DNS-атаки.

Управление информационной безопасностью. Риск-менеджмент.

Специалист, обладающий статусом CISSP должен глубоко разбираться в вопросах управления информационной безопасностью.

Фактически для успешной сдачи экзамена необходимо разобраться в основных элементах управления информационной безопасностью: управление активами, количественные и качественные методики оценки рисков информационной безопасности, применение контролей (мер безопасности) для минимизации рисков, процессы разработки и внедрения эффективных политик и процедур, обучение персонала и аудит информационной безопасности.

Криптография

Нельзя представить себе информационную безопасность без криптографии. От будущих CISSP'ов не требуется глубокого понимания математической теории, лежащей в основе алгоритмов шифрования, но нужно очень хорошо ориентироваться в базовых понятиях, названиях алгоритмов и их назначении. В домен включены алгоритмы симметричного и асимметричного шифрования, алгоритмы хеширования, алгоритмы цифровые подписи, инфраструктура открытых ключей (PKI). Дополнительно рассматриваются альтернативные методы сокрытия информации (например, стеганография).

Безопасность разработки программного обеспечения

Большинство проблем информационной безопасности связаны с уязвимостями в программном обеспечении, поэтому в CISSP CBK включен домен по безопасной разработке ПО. Эксперт в области ИБ должен разбираться в таких вопросах, как жизненный цикл разработки программного обеспечения (SDLC), модели разработки и тестирования, угрозы, уязвимости и меры безопасности в приложениях.

Архитектура безопасности

Домен содержит такие фундаментальные вопросы, как фундаментальные концепции моделей безопасности, модели подсистем управления доступом, стандарты и критерии безопасности, принципы работы контрмер.

Безопасность операций

В данном домене рассматриваются вопросы операционного управления информационной безопасностью: антивирусная защита, управление патчами и уязвимостями, резервное копирование и восстановление данных, выполнение законодательных требований, мониторинг информационной безопасности.

Обеспечение непрерывности бизнеса и восстановление после сбоев

Эксперт в области информационной безопасности должен хорошо разбираться в вопросах

обеспечения непрерывности бизнеса и восстановления после сбоев, оценке влияния сбоев на бизнес (BIA), тестировании планов и обучении персонала.

Выполнение требований законодательства

Выполнение требований законодательства является важной составляющей обеспечения информационной безопасности. В частности специалисты по ИБ должны хорошо ориентироваться в требованиях законодательства в отношении следующих вопросов расследования компьютерных преступлений, защиты интеллектуальной собственности и лицензирования.

Физическая безопасность

Без обеспечения эффективной физической безопасности обеспечение информационной безопасности невозможно, поэтому будущие обладатели статуса CISSP должны хорошо разбираться в угрозах физической безопасности, вопросах защиты периметра, серверных помещений.

Формат экзамена

Сам экзамен состоит из 250 вопросов и длится 6 часов. Каждый вопрос предполагает 4 варианта ответа, из которых только один верный. Максимальное количество баллов, которое можно получить равно 1000. Для сдачи экзамена необходимо набрать не менее 700 баллов.

В качестве примера можно привести следующий вариант вопроса из распространяемого ассоциацией ISC2 информационного бюллетеня (CISSP candidate information bulletin):

Какое из следующих описаний подходит для определения атаки SYN flood?

(A) Быстрая передача сообщений по протоколу Internet Relay Chat (IRC)
(B) Создание большого количества полуоткрытых соединений
(C) Отключение сервера DNS
(D) Чрезмерное линкование учетных записей пользователей и файлов

Правильный ответ: B

Требования к опыту

Соискатель статуса CISSP должен обладать 5 летним опытом, как минимум, в двух из обозначенных выше областей. При этом один год опыта может быть засчитан, если у кандидата есть высшее образование в области информационной безопасности.

Признание

Что касается признания статуса, то в США данный статус официально признается таким ведомством, как Министерство Обороны. В России специалист по информационной безопасности «обязан» обладать сертификатом CISSP, если он хочет занимать руководящую позицию в области ИБ или работать в консалтинговой или интеграционной компании. Чтобы самостоятельно оценить востребованность данного статуса предлагаю читателю просмотреть страницы «CISSP'ов» в социальных сетях и убедиться, что в такой компании профессионалов оказаться весьма почетно.

Что нужно сделать, чтобы успешно сдать экзамен?

На взгляд автора самым важным для успешной сдачи экзамена является владение техническим английским языком на уровне чтения без словаря. Если базовые навыки по владению языком уже есть, то лучше всего начать подготовку с освоения английских терминов в области информационной безопасности. Хороший набор глоссариев подготовлен и опубликован в сети Интернет ассоциацией ISACA: http://www.isaca.org/Pages/Glossary.aspx

Для того, чтобы эффективно спланировать свою подготовку лучше сначала потренироваться на различных банках вопросов, доступных в Интернет. Единственное, нужно помнить, что точно такие вопросы вы практически никогда не встретите на экзамене, так как все сдающие его обязуются не разглашать материалы экзамена (да и объем экзамена не позволяет это сделать). Работа с вопросами позволит определить ваши слабые области, требующие наибольшего внимания. Что касается времени подготовки, то лучше выделить на нее, как минимум, три месяца. Сдать экзамен CISSP студенческим способом - потратив ночь на зубрежку и написание шпаргалок не получится. Объем знаний слишком большой, а списывание жестоко пресекается организаторами экзамена.

Даже если тренировка на вопросах показала, что ваш уровень довольно высок, очень важно глубоко разобраться в такой теме, как управление информационной безопасностью. Несмотря на то, что ряд доменов CISSP сугубо технические, вопросы управления ИБ все чаще и чаще доминируют в экзамене. Здесь лучше

поработать с такими первоисточниками практик управления ИБ, как стандарты серии ISO 27000 (в особенности ISO 27001 и ISO 27002) и соответствующие публикации американского института стандартов (NIST).

Подготовиться к экзамену позволяют и специализированные курсы, но стоит понимать, что ни один курс не «загрузит» в голову специалиста знания и опыт, которые приобретаются профессионалами годами. Наиболее удобный формат подготовительных курсов - это разнесенные по времени семинары длительностью 1-2 часа, на каждом из которых дается обзор одного из доменов и рассматриваются наиболее «коварные» понятия и примерные вопросы. Современные технологии проведения вебинаров позволяют участвовать в таком обучении удаленно и в удобное вечернее время.

Все мы знаем, что готовиться веселее с кем-нибудь и здесь помимо общения с одногруппниками, подключающимися к вебинарам, лучше стать завсегдатаем специализированных форумов, на которых будущие обладатели статуса CISSP обсуждают вопросы для подготовки к экзамену и обмениваются впечатлениями после сдачи экзамена.

Дополнительно необходимо обзавестись хорошим учебником. Можно пользоваться как официальным руководством от ISC2, так и учебниками от признанных профессионалов.

Таким образом, хороший английский, понимание вопросов управления ИБ, подготовительные семинары и толковый учебник позволят эффективно подготовиться к экзамену.

Поддержание статуса сертифицированного специалиста

После успешной сдачи экзамена и получения статуса CISSP специалист должен каждый год демонстрировать, что он поддерживает свой высокий профессиональный уровень: участвует в конференциях и тренингах, читает профессиональную литературу, пишет технические статьи и т.п. В ассоциации ISC2 есть своеобразный прейскурант, сопоставляющий каждую из подобных активностей определенному числу баллов CPE (continuing professional education credits). Только регулярно набирая необходимый минимум баллов и оплачивая членские взносы профессионал поддерживает действующий статус CISSP.

В следующей статье мы рассмотрим основные понятия, владение которыми позволит быстро погрузиться в предметную область.

Литература (References)

1. Steven Hernandez. Official (ISC)2 Guide to the CISSP CBK, Third Edition. - ISC2 Press, 2012. 968 p.
2. James M. Stewart, Mike Chapple, Darril Gibson. CISSP: Certified Information Systems Security Professional Study Guide, 6th Edition. - Sybex, 2012. 936 p.
3. Shon Harris, CISSP All-in-One Exam Guide, 6th Edition - McGrawHill, 2012. 1216 p.
4. Eric Conrad, Seth Misenar, Joshua Feldman. CISSP Study Guide, Second Edition - Syngress, 2012. 600 p.