ИЗМЕНЕНИЯ В CISSP: ЧТО НОВОГО И ИНТЕРЕСНОГО?

Дорофеев А.В.[1]

Публикация продолжает серию наших статей по подготовке к сдаче экзамена на статус сертифицированного специалиста по информационной безопасности (Certified Information Systems Security Professional). В данной короткой статье рассмотрены последние изменения в CISSP CBK (common body of knowledge).

***Ключевые слова**: сертификация специалистов, CISSP CBK.*

С 15-го апреля 2015 ассоциация ISC2 ввела изменения в экзамен CISSP (Certified Information Systems Security Professional). Была изменена структура доменов и их количество изменилось. В данной статье мы вкратце рассмотрим нововведения.

Перегруппировка доменов

Теперь в CISSP CBK (common body of knowledge) 8 доменов (вместо 10), которые сгруппированы следующим образом:

- Менеджмент безопасности и риска (Security and Risk Management);
- Безопасность информационных ресурсов (Asset Security);
- Проектирование систем безопасности (Security Engineering);
- Безопасность коммуникаций и сети (Communications and Network Security);
- Управление учетными записям и доступом (Identity and Access Management);
- Тестирование защищенности (Security Assessment and Testing);
- Процессы информационной безопасности (Security Operations);
- Безопасность при разработке программного обеспечения (Software Development Security).

Домен «Менеджмент безопасности и риска» посвящен фундаментальным концепциям информационной безопасности: угроза, риск, выполнение требований и др. «Безопасность информационных ресурсов» группирует вопросы управления информационными ресурсами или активами. Домен «Проектирование систем безопасности» объединяет вопросы от применения криптографии до физической безопасности (системы вентиляции, кондиционирования, пожаротушения и т.п.). «Безопасность коммуникаций и сети» остался таким же всеобъемлющим доменом по сетевой безопасности, аналогичная ситуация с доменами: «Управление учетными записям и доступом», «Процессы информационной безопасности», «Безопасность при разработке программного обеспечения». Вопросы технического аудита, которые ранее были в сетевой безопасности, вынесены в отдельный домен «Тестирование защищенности».

«Исчезнувшие» из отдельных доменов вопросы непрерывности бизнеса и восстановления после сбоев, а также криптографии теперь «размазаны» по новым доменам.

По факту содержимое CBK не изменилось, а лишь было реорганизовано и стало ближе к структуре доменов, определенной, например, в стандарте ISO 27001. Ассоциация ISC2 в своих материалах отдельно сообщает, что ничего не было удалено. Тем не менее в обновленном буклете для экзаменующихся можно найти такие современные темы, как Internet of Things (IoT), SCADA, SaaS и др.

Формат экзамена

Что касается длительности экзамена и количества вопросов, то они не претерпели изменений. В CISSP так и осталось 250 вопросов, на которые дается 6 часов. Проходной балл остался тем же: 700 из 1000.

Новые типы вопросов

Необходимо отметить, что в тесте CISSP помимо стандартных вопросов с несколькими вариантами ответов (multiple choice questions) с февраля 2014 добавлены вопросы типа «Drag & Drop» и «Hotspot». В первом случае экзаменуемому нужно будет выбрать правильные ответы и перенести их на область ответа, а во втором случае указать правильную точку на диаграмме.

Таким образом, нововведения не окажут серьезного влияния на подготовку к экзамену, все предыдущие публикации остаются актуальными по сути [1-10]. Наши последующие статьи для подготовки к экзамену также будут отражать новую структуру CISSP CBK.

1 Дорофеев Александр Владимирович, ЗАО «НПО «Эшелон», Москва, a.dorofeev@cnpo.ru

Литература:

1. Дорофеев А.В. Статус CISSP: как получить и не потерять? // Вопросы кибербезопасности. 2013. № 1(1). С.65-68.
2. Дорофеев А.В., Марков А.С. Менеджмент информационной безопасности: основные концепции // Вопросы кибербезопасности. 2014. № 1 (2). С. 67-73.
3. Дорофеев А.В. Менеджмент информационной безопасности: управление рисками // Вопросы кибербезопасности. 2014. № 2(3). С.66-73.
4. Дорофеев А.В. Менеджмент информационной безопасности: переход на ISO 27001:2013 // Вопросы кибербезопасности. 2014. № 3(4). С.69-73.
5. Дорофеев А.В. Подготовка к CISSP: телекоммуникации и сетевая безопасность // Вопросы кибербезопасности. 2014. № 4(7). С. 69-74.
6. Барабанов А.В. Подготовка к сдаче CISSP: модели информационной безопасности // Вопросы кибербезопасности. 2014. № 5(8). С. 59-67.
7. Марков А.С., Цирлов В.Л. Основы криптографии: подготовка к CISSP // Вопросы кибербезопасности. 2015. № 1 (9). С. 65-73.
8. Марков А.С., Цирлов В.Л. Безопасность доступа: подготовка к CISSP // Вопросы кибербезопасности. 2015. № 2 (10). С. 60-68.
9. Дорофеев А.В., Марков А.С. Планирование обеспечения непрерывности бизнеса и восстановления // Вопросы кибербезопасности. 2015. № 3 (11). С. 68-73.
10. Марков Г.А. Вопросы физической безопасности информации // Вопросы кибербезопасности. 2015. № 4 (12). С. 70-76.

CISSP CHANGES: WHAT IS NEW AND INTERESTING?

***Dorofeev A.V.*[2]**

Publication continues the series of our articles devoted to preparation for the CISSP (Certified Information Systems Security Professional) exam. In this short article we will review the latest changes in the structure of CISSP CBK.

***Keywords**: expert certification, CISSP CBK*

References:

1. Dorofeev A.V. Status CISSP: kak poluchit' i ne poteryat'? Voprosy kiberbezopasnosti. 2013. No 1(1), pp.65-68.
2. Dorofeev A.V., Markov A.S. Menedzhment informatsionnoy bezopasnosti: osnovnye kontseptsii, Voprosy kiberbezopasnosti. 2014. No 1 (2), pp. 67-73.
3. Dorofeev A.V. Menedzhment informatsionnoy bezopasnosti: upravlenie riskami, Voprosy kiberbezopasnosti. 2014. No 2(3), pp.66-73.
4. Dorofeev A.V. Menedzhment informatsionnoy bezopasnosti: perekhod na ISO 27001:2013, Voprosy kiberbezopasnosti. 2014. No 3(4), pp.69-73.
5. Dorofeev A.V. Podgotovka k CISSP: telekommunikatsii i setevaya bezopasnost', Voprosy kiberbezopasnosti. 2014. No 4(7), pp. 69-74.
6. Barabanov A.V. Podgotovka k sdache CISSP: modeli informatsionnoy bezopasnosti, Voprosy kiberbezopasnosti. 2014. No 5(8), pp. 59-67.
7. Markov A.S., Tsirlov V.L. Osnovy kriptografii: podgotovka k CISSP, Voprosy kiberbezopasnosti. 2015. No 1 (9), pp. 65-73.
8. Markov A.S., Tsirlov V.L. Bezopasnost' dostupa: podgotovka k CISSP, Voprosy kiberbezopasnosti. 2015. No 2 (10), pp. 60-68.
9. Dorofeev A.V., Markov A.S. Planirovanie obespecheniya nepreryvnosti biznesa i vosstanovleniya, Voprosy kiberbezopasnosti. 2015. No 3 (11), pp. 68-73.
10. Markov G.A. Voprosy fizicheskoy bezopasnosti informatsii, Voprosy kiberbezopasnosti. 2015. No 4 (12), pp. 70-76.

2 Alexander Dorofeev, NPO Echelon, Moscow, a.dorofeev@cnpo.ru