О ПЕРВОЙ РОССИЙСКОЙ ПРОФЕССИОНАЛЬНОЙ СЕРТИФИКАЦИИ В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ «СЕРТИФИЦИРОВАННЫЙ СПЕЦИАЛИСТ ПО КИБЕРБЕЗОПАСНОСТИ»

Дорофеев А. В.[1]

DOI: 10.21681/2311-3456-2025-1-147-149

Введение

Специалистам по информационной безопасности, как и другим ИТ-профессионалам, часто требуется подтверждение своих знаний в различных ситуациях: на собеседованиях, при переходе на новую работу или в борьбе за выгодный контракт. Наличие широко признаваемого сертификата может значительно упростить решение данных задач [1–4].

В мировой практике существует более десятка сертификаций для специалистов нашего профиля, каждая из которых имеет свою направленность. Самые известные из них: Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA), CompTIA Security+ и Offensive Security Certified Professional (OSCP).

К примеру, общее количество сертифицированных специалистов CISSP составляет более 156 000 человек. Данная независимая сертификация всячески поддерживается государством, например, прохождение ее рекомендуется для ряда категорий служащих США, в том числе в Министерстве обороны.

Требования Министерства обороны США по наличию сертификатов у персонала

Вид сертификата		
IAM Level I	IAM Level II	IAM Level III
CAP, CND, Cloud+, GSLC, Security+ CE, H CISPP	CAP, CASP+ CE, CISM, CISSP (или Associate CISSP), GSLC, CCISO, HCISPP	CISM, CISSP (или Associate CISSP), GSLC, CCISO
IASAE I	IASAE II	IASAE III
CASP+ CE, CISSP (или Associate CISSP), CSSLP	CASP+ CE, CISSP (или Associate CISSP), CSSLP	CISSP-ISSAP, CISSP-ISSEP, CCSP

Рис. 1. Требования к специалистам по директиве US DoD 8570

Что касается нашей страны, то обычной практикой является включение требований по наличию сертифицированных специалистов CISSP в условиях контрактов на выполнение работ в ИТ-области. Это является объективным фактором востребованности сертификации специалистов.

Однако после 2022 года доступ для российских специалистов к получению этих международных сертификатов значительно затруднился.

Для заполнения этого пробела авторы данной статьи предложили создание российского аналога для CISSP и CISM — сертификацию ССК (Сертифицированный специалист по кибербезопасности). Были организованы подготовительные курсы, а также сдача сертификационных экзаменов.

Ниже мы поделимся своим опытом создания системы профессиональной сертификации.

Обзор доменов

Основным элементом любой системы профессиональной сертификации является набор доменов, на основе которых формулируются вопросы экзамена [5–10]. В системе сертификации мы выбрали следующие восемь ключевых доменов:

1. Менеджмент информационной безопасности;
2. Законодательство в области информационной безопасности;
3. Безопасный доступ;
4. Сетевая безопасность;
5. Криптография;
6. Обеспечение непрерывности и восстановления;
7. Контроль и мониторинг информационной безопасности;
8. Разработка безопасного программного обеспечения.

Эти домены охватывают основные аспекты профессиональных знаний в области кибербезопасности, и их понимание позволяет специалистам решать актуальные задачи в своих организациях.

«Менеджмент информационной безопасности» является ключевым доменом, так как основная задача специалистов по кибербезопасности — защитить организацию, которая их наняла. Для этого важно не только уметь применять современные технологии информационной безопасности, но и управлять процессами информационной безопасности в организации. Ведь в конечном итоге информационная безопасность в организации зависит от каждого, кто имеет доступ к защищаемой информации.

В ходе подготовительных курсов в рамках данного домена мы рассматриваем основные понятия информационной безопасности: активы, угрозы, меры безопасности, риски и СМИБ (система менеджмента

1 Дорофеев Александр Владимирович, CISSP, CISA, CISM, директор Учебного центра «Эшелон». Россия. Москва. E-mail: ad@cnpo.ru

информационной безопасности). Подробно разбираем цикл Деминга (PDCA) и ГОСТ Р ИСО/МЭК ИСО 27001. Отдельное внимание уделяется формированию в организации понятной системы организационно-распорядительной документации, а также проведению внутреннего аудита СМИБ.

Одной из ключевых целей информационной безопасности в организации является выполнение нормативных требований. Эти требования существуют не только для самой организации и её конкретных процессов, но и для информационных систем, используемых для поддержки этих процессов, а также для средств защиты информации.

Специалист по кибербезопасности должен хорошо ориентироваться в требованиях законодательства в области информационной безопасности, так как они служат основой для формирования внутренних документов организации по информационной безопасности и являются критериями для проведения различных проверок со стороны регулирующих органов.

Домен «Безопасный доступ» посвящен ряду важных тем, связанных с управлением доступом к данным. Основными темами домена являются различные типы моделей управления доступом, технологии аутентификации и идентификации и современные атаки на данные системы.

Другим ключевым доменом является «Сетевая безопасность». Специалист по кибербезопасности должен понимать, как функционируют сети, хорошо ориентироваться в угрозах, которые могут быть реализованы на различных уровнях семиуровневой модели ISO/OSI, а также уметь применять ключевые технологии сетевой безопасности: IDS/IPS, межсетевое экранирование и т.п.

Домен «Криптография» посвящён криптографической защите информации при ее хранении и передаче. Домен включает в себя темы, посвященные алгоритмам шифрования с секретным/открытым ключом, хеш-функциям, протоколам безопасности. В ходе подготовительных курсов по этому домену рассматриваются как российские, так и зарубежные стандарты.

Обеспечение доступности информационных систем и данных является ключевой задачей обеспечения информационной безопасности. Поэтому в системе сертификации специалиста по кибербезопасности нельзя не включить домен, посвященный обеспечению непрерывности бизнеса и восстановлению организации после разрушений, бедствий, критических ситуаций или аварий. Хорошее знание этого домена позволит подготовить организацию к оперативному реагированию на различные негативные события, а также обеспечить ее непрерывное функционирование.

Специалист по кибербезопасности должен быть максимально компетентен в таких аспектах, как выявление киберугроз, попыток вторжения злоумышленников, а также реагирования на инциденты информационной безопасности. Именно этим вопросам посвящен домен «Контроль и мониторинг информационной безопасности».

Уязвимое программное обеспечение представляет значительный риск для безопасности любой организации. Чтобы минимизировать уязвимости, компании-производители программного обеспечения внедряют процессы безопасной разработки, предусматривающие различные меры на всех стадиях цикла создания программного обеспечения. В этом контексте мы добавили отдельный домен, посвящённый разработке безопасного программного обеспечения. В ходе подготовительных курсов мы подробно рассматриваем положения ГОСТ Р 56939, активное участие в создании которого принимали участие эксперты нашей испытательной лаборатории.

Форматы экзаменов

Система сертификации предусматривает два вида экзаменов: экзамен на статус кандидата и на статус специалиста (рис. 2). Первый экзамен проводится в онлайн формате и является бесплатным, что позволяет попробовать свои силы неограниченному кругу российских специалистов. Второй экзамен доступен пока только в оффлайн формате, в рамках которого не допускается возможность списывания. Длительность кандитатского экзамена – 2 часа, в ходе которых нужно ответить на 100 вопросов, а экзамена на статус специалиста – 4 часа, и количество вопросов уже – 200. Проходной балл – 70 % правильных ответов.

Каждый вопрос содержит четыре варианта ответа, и испытуемому необходимо выбрать наилучший.

Для подготовки к экзаменам имеются онлайн и оффлайн курсы, которые проводятся экспертами группы компаний «Эшелон». Причём доступен бесплатный онлайн курс, к которому можно присоединиться, пройдя регистрацию по ссылке https://etecs.ru/ssc/. Видео с прошлого курса выложено на наших каналах в YouTube https://www.youtube.com/playlist?list=PLAs36PQnfDQ0-U7iGV2Z6_1v-s9RXktHc и RuTube https://rutube.ru/plst/429175/. Для общения слушателей курса и разбора вопросов в Telegram организованы канал https://t.me/sskquestions и группа https://t.me/cybersecspec. Также в настоящее время идет работа по написанию учебного пособия.

Отдельно стоит обратить внимание, что статус «Сертифицированный специалист по кибербезопасности» присваивается специалистам, которые успешно сдали оффлайн-экзамен, а также подтвердили наличие опыта по нескольким доменам экзамена не менее 5 лет. В случае наличия высшего образования в области информационной безопасности необходимо подтвердить опыт не менее 4 лет.

Рис. 2. Сертификаты специалистов

Первые итоги

Первый эксперимент показал, что созданная система сертификации вызвала большую заинтересованность у российских специалистов в области информационной безопасности. На онлайн курсы по подготовке к экзамену «Сертифицированный специалист по кибербезопасности» (ССК) от учебного центра «Эшелон» получено уже более 3 тыс. регистраций. По итогам первого курса, проведенного в 2024-м году, 269 участников участвовало в сдаче онлайн-экзамена, из которых 163 набрали более 70 баллов из 100 возможных и стали кандидатами ССК. Среди слушателей специалисты из России, Узбекистана, Казахстана и других стран СНГ. Размер группы слушателей в Telegram уже более 760 подписчиков.

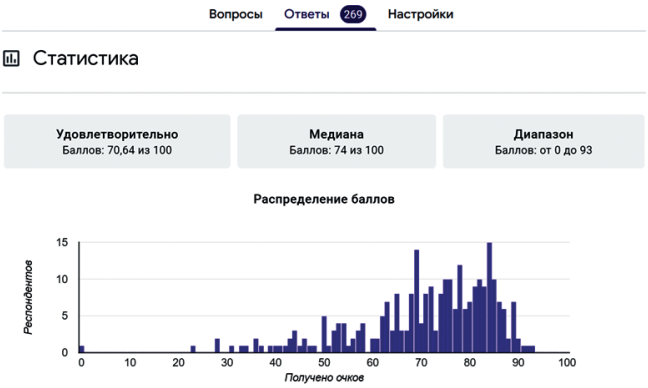

Рис.3. Распределение результатов онлайн теста ССК

В результате проведения оффлайн-экзамена, а также акции выдачи сертификата российским специалистам, обладающим действующими сертификатами CISSP и CISM, количество обладателей статуса ССК уже превысило 30 человек.

Заключение

Учебный центр «Эшелон» провел указанный эксперимент с целью демонстрации возможности альтернативной (негосударственной) независимой сертификации специалистов в нашей стране с привлечением всех заинтересованных лиц от ведущих компаний и ВУЗов страны. Возможно, данная идея покажется привлекательной специалистам Союзного государства и ОДКБ [11].

В планах активистов ССК в настоящее время стоят следующие задачи:

- расширение списка организаций-партнеров, отвечающих за создание и развитие базы вопросов сертификационного экзамена;
- расширение списка учебных заведений, проводящих подготовительные курсы и прием экзамена.

Литература

1. *Дорофеев А. В. Статус CISSP: как получить и не потерять? // Вопросы кибербезопасности. 2013. № 1(1). С. 65–68.*
2. *Лившиц И. И. Проблемы подготовки специалистов в области информационной безопасности // Вестник ДГТУ. Технические науки. 2024. Т. 51. № 1. С. 123–131. DOI: 10.21822/2073-6185-2024-51-1-123-131.*
3. *Чванова М. С., Киселева И. А., Анурьева М. С. Зарубежный опыт подготовки специалистов для наукоемких технологий // Вестник Тамбовского университета. Серия: Гуманитарные науки. 2021. Т. 26. № 190. С. 7–24. DOI: 10.20310/1810-0201-2021-26-190-7-24.*
4. *Seidakhmetova F., Pasekova M., Sarygulova R., Sholpanbayeva K. Training of Specialists in the Field of Information Security // Statistics, Accounting and Audit. 2023. № 2 (89). С. 40–46. DOI:10.31992/0869-3617-2022-31-2-82-93.*
5. *Барабанов А. В., Дорофеев А. В., Марков А. С., Цирлов В. Л. Семь безопасных информационных технологий / Под. ред. А. С. Маркова. М.: ДМК Пресс, 2017. 221 с.*
6. *Дорофеев А. В., Марков А. С. Менеджмент информационной безопасности: основные концепции // Вопросы кибербезопасности. 2014. № 1 (2). С. 67–73.*
7. *Дорофеев А. В., Марков А. С. Планирование обеспечения непрерывности бизнеса и восстановления // Вопросы кибербезопасности. 2015. № 3 (11). С. 68–73.*
8. *Марков А. С., Цирлов В. Л. Безопасность доступа: подготовка к CISSP // Вопросы кибербезопасности. 2015. № 2 (10). С. 60–68.*
9. *Марков А. С., Цирлов В. Л. Основы криптографии: подготовка к CISSP // Вопросы кибербезопасности. 2015. № 1 (9). С. 65–73.*
10. *Петренко Ю. А., Петренко С. А. Лучшая практика управления непрерывностью бизнеса // Защита информации. Инсайд. 2010. № 5 (35). С. 12–21.*
11. *Марков А. С. Проблемные вопросы международной сертификации специалистов по информационной безопасности // В сб. трудов XVIII Международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности». М.: НАМИБ, 2024. С. 82–85.*