Бауманский учебный центр «Специалист»

Программа курса Инженер защиты облачных вычислений от хакерских атак

Код курса: **ЦЦСЕ**

Тема	Ак. часов
Модуль 1. Введение в безопасность облачных вычислений • Основы облачных вычислений • Цели безопасности в облаке • Аналитика безопасности в облаке • Оценка безопасности провайдеров облачных вычислений • Модель общей ответственности в облаке Amazon • Модель общей ответственности в облаке Microsoft • Модель общей ответственности в облаке Google **Практическая работа** • Изучение основ облачных вычислений	**2**
Модуль 2. Безопасность платформы и инфраструктуры в облаке • Платформа и инфраструктура в облаке • Риски и угрозы, связанные с облачной платформой и инфраструктурой • Безопасность ключевых компонент • Проектирование безопасного центра обработки данных (ЦОД) в облаке • Безопасность платформы и инфраструктуры в Amazon Web Services (AWS) • Безопасность платформы и инфраструктуры в Google Cloud Platform (GCP) • Безопасность платформы и инфраструктуры в Microsoft Azure **Практическая работа** 1. Применение идентификации и доступа в AWS 2. Применение сервисов управления ключами AWS 3. Создание защищенных инстансов EC2 в AWS 4. Внедрение ролевого управления доступом в Microsoft Azure 5. Развертывание защищенной виртуальной машины в Azure 6. Блокировка портов управления с помощью Центра безопасности Azure, для защиты от атак на виртуальные машины в Azure 7. Применение управления доступом на основе ролей с помощью GCP IAM 8. Защита экземпляров GCP с помощью правил фаерволла 9. Безопасное развертывание в Google Kubernetes Engine (GKE) 10. Применение безопасного соединения между инстансами	**6**

Модуль 3. Безопасность приложений в облаке • Безопасность облачных приложений • Риски безопасности облачных приложений • Жизненный цикл безопасной разработки программного обеспечения (SSDLC) облачных приложений • DevOps и непрерывная интеграция / непрерывное развертывание (CI / CD) • Контроль безопасности облачных приложений • Безопасность приложений в AWS • Безопасность приложений в Azure • Безопасность приложений в GCP **Практическая работа** 1. Применение брандмауэра для интернет-приложений в AWS 2. Обеспечение принципа наименьших привилегий в Azure 3. Применение многофакторной аутентификации Azure AD 4. Ограничение доступа к приложениям App Engine в GCP	**2**
Модуль 4. Безопасность данных в облаке • Безопасность облачных данных • Основы облачного хранения данных • Архитектура облачного хранилища и этапы жизненного цикла • Оценка рисков, атаки и проблемы облачного хранилища данных • Стратегии и технологии безопасности облачных данных • Безопасность данных в AWS • Безопасность данных в GCP • Безопасность данных в Microsoft Azure **Практическая работа** 1. Ограничение доступа к корзине S3 с помощью CloudFront 2. Ограничение доступа к сегментам AWS S3 с помощью ACL и политики сегментов 3. Ограничение доступа к объектам S3 с помощью политик сегментов 4. Защита Amazon RDS от случайного удаления 5. Предотвращение удаления резервных копий с помощью политики доступа Amazon Backup Vault 6. Предотвращение случайного удаления и изменения объектов S3 с помощью блокировки объектов S3 7. Ограничение доступа к учетной записи Azure с помощью подписи общего доступа (SAS) 8. Отключение анонимного доступа к контейнеру в Azure 9. Предотвращение случайного удаления ресурсов с помощью блокировки ресурсов Azure 10. Ограничение сетевого доступа к учетной записи Azure с помощью конечных точек виртуальной сетевой службы 11. Защита секретов в Azure с помощью Key Vault 12. Применение шифрования данных в облаке Google 13. Применение DLP в облаке Google	**6**

Модуль 5. Безопасность операций в облаке • Безопасность операций • Состав операций облачного центра обработки данных • Операции по обеспечению безопасности облачной инфраструктуры • Безопасность операций в Microsoft Azure • Безопасность операций в AWS • Безопасность операций в GCP **Практическая работа** 1. Выявление потенциальных проблем безопасности с помощью Amazon Inspector 2. Мониторинг активности пользователей с помощью AWS CloudTrail 3. Мониторинг групп безопасности с помощью CloudTrail и CloudWatch 4. Ограничение доступа к удаленному рабочему столу виртуальных машин в Azure 5. Защита RDP / SSH доступа к виртуальным машинам Azure с помощью Azure Bastion 6. Сканирование уязвимостей в приложениях App Engine с помощью Google Cloud Web Security Scanner	**4**
Модуль 6. Тестирование на проникновение в облаке • Тестирование на проникновение в облачные вычисления • Общие шаги тестирования на проникновение в облаке • Шаги тестирования на проникновение для AWS • Шаги тестирования на проникновение для Azure • Шаги тестирования на проникновение для GCP **Практическая работа** 1. Выявление неправильно настроенных сегментов S3 в AWS 2. Выявление общедоступных данных с помощью ключей API в AWS	**2**
Модуль 7. Реагирование на инциденты в облаке • Реагирование на облачный инцидент • Жизненный цикл реагирования на инциденты в облаке • Реагирование на инциденты безопасности в AWS • Реагирование на инциденты безопасности в Microsoft Azure • Реагирование на инциденты безопасности в GCP **Практическая работа** 1. Обнаружение компрометации конфиденциальных данных в корзинах S3 с помощью Amazon Macie 2. Создание оповещений журнала активности с помощью Azure Monitor 3. Мониторинг подозрительного сетевого трафика с помощью журналов потоков VPC в GCP 4. Обнаружение инцидентов в GCP с помощью облачного мониторинга	**2**
Модуль 8. Криминалистические расследования в облаке • Облачная криминалистика • Расследование инцидентов безопасности в AWS • Расследование инцидентов безопасности в Microsoft Azure • Расследование инцидентов безопасности в Google GCP **Практическая работа** 1. Изучение журналов консоли Amazon CloudWatch 2. Криминалистическое исследование виртуальной машины в Microsoft Azure	**2**

Модуль 9. Непрерывность бизнеса и аварийное восстановление в облаке • Облачное аварийное восстановление и непрерывность бизнеса • Аварийное восстановление и планирование непрерывности бизнеса • Реализация восстановления и отказоустойчивости • Непрерывность бизнеса и аварийное восстановление в AWS • Непрерывность бизнеса и аварийное восстановление в Azure • Непрерывность бизнеса и аварийное восстановление в GCP **Практическая работа** 1. Резервное копирование и восстановление отказавшего инстанса EC2 с помощью снимка состояния в AWS 2. Реализация резервного копирования объектов Amazon S3 с межрегиональной репликацией 3. Восстановление инстанса EC2 с использованием опции резервного копирования Amazon Machine Image (AMI) 4. Реализация аварийного восстановления в Azure с использованием репликации данных хранилища и отработки отказа 5. Реализация резервного копирования и восстановления виртуальных машин с помощью службы архивации Azure 6. Создание снимка экземпляра виртуальной машины и восстановление экземпляра с помощью снимка в GCP 7. Обеспечение доступности службы с помощью балансировки нагрузки в GCP	**6**
Модуль 10. Корпоративное управление, управление рисками и соответствие требованиям в облаке • Управление облачными вычислениями (Governance) • Управление рисками в облаке (Risk) • Соответствие требованиям в облаке (Compliance) • GRC в AWS • GRC в Azure • GRC в GCP **Практическая работа** 1. Ограничение развертывания сегментов S3 в определенном регионе с помощью политики IAM в AWS 2. Изучение результатов соответствия требованиям с помощью AWS Security Hub 3. Обеспечение соблюдения нормативных требований назначением встроенной политики и созданием настраиваемой политики в Azure	**4**
Модуль 11. Стандарты, политики и юридические аспекты в облаке • Законы, влияющие на облачные вычисления • Стандарты облачных вычислений • Планирование облачного аудита и отчетность • Стандарты, политики и аудит в AWS • Стандарты, политики и аудит в Azure • Стандарты, политики и аудит в GCP **Практическая работа** 1. Проведение аудита безопасности в AWS с помощью AWS Trusted Advisor 2. Проведение аудита соответствия в Azure 3. Проведение аудита в GCP	**2**
Модуль 12. Обзор курса и заключительное тестирование	**2**
Аудиторная нагрузка в классе с преподавателем	**40 ак.ч. + 40 ак.ч. самостоятельно**

По окончании обучения на курсе проводится итоговая аттестация. Аттестация проводится в виде теста на последнем занятии или на основании оценок практических работ, выполняемых во время обучения на курсе.

Контакты центра

Для частных лиц	Для организаций	E-mail
+7 (495) 232-32-16	**+7 (495) 780-48-44**	**info@specialist.ru**