# Бауманский учебный центр «Специалист»

## Программа курса ALTSEC. Информационная безопасность в ОС Альт

Код курса: **АЛЬТ-ИБ**

| Тема | Ак. часов |
|---|---|
| **Модуль 1. Законодательное регулирование IT-сферы в РФ**<br>• Основы информационной безопасности.<br>• Лицензионность ПО.<br>• Реестр Российского ПО Минкомсвязи.<br>• Защита персональных данных.<br>• КИИ. | **4** |
| **Модуль 2. Основы обеспечения безопасности при использовании ОС Альт**<br>• Механизмы разграничения доступа в Linux:<br>  ◦ Дискреционный доступ;<br>  ◦ Мандатный доступ;<br>  ◦ Ролевой доступ.<br>• Отличия ОС Альт с точки зрения безопасности.<br>• Средства очистки оперативной и дисковой памяти. | **4** |
| **Модуль 3. Подсистема аутентификации ОС Альт**<br>• Архитектура PAM.<br>• Настройка хэширования паролей (ГОСТ Р 34.11–2012).<br>• Настройка требований сложности паролей.<br>• Хранение истории паролей.<br>• Блокировка пользовательских УЗ.<br>• Ограничение возможности входа пользователей. | **4** |
| **Модуль 4. Контроль целости системы**<br>• Возможности менеджера пакетов для контроля целостности системы.<br>• Настройка контроля целостности средствами osec.<br>• Подсистема IMA/EVM. | **4** |
| **Модуль 5. Контроль ввода-вывода**<br>• Ограничения при помощи правил udev.<br>• Ограничение и контроль использования съемных носителей (usbguard, alterator-ports-access).<br>• Контроль ввода-вывода средствами библиотеки PolKit. | **4** |
| **Модуль 6. Управление протоколированием событий**<br>• Система журналирования.<br>• Система аудита.<br>• Централизация данных журналирования и аудита. | **4** |
| **Модуль 7. Шифрование данных**<br>• Симметричные и ассиметричные алгоритмы шифрования.<br>• Шифрование отдельных файлов средствами openssl и gnupg.<br>• Использование зашифрованных разделов средствами LUKS.<br>• Использование криптоконтейнеров eCryptFS.<br>• Использование отечественных криптопровайдеров в ОС Альт (на примере Криптопро). | **4** |

| | |
|---|---|
| **Модуль 8. Инфраструктура публичных ключей и SSL/TLS**<br>• Ассиметричная криптография и инфрастурктура публичных ключей.<br>• Использование openssl для генерации сертификатов.<br>• Инспользование EasyRSA для генерации сертифкатов. | **4** |
| **Модуль 9. Использование технологий VPN для соединения удаленных офисов**<br>• Основы технологии VPN.<br>• Развертывание OpenVPN-сервера средствами alterator-openvpnserver.<br>• Подключение к серверу OpenVPN.<br>• Управление туннелированием трафика при помощи маршрутизации.<br>• Установка защищенных соединений с использованием WireGuard. | **4** |
| **Модуль 10. Обнаружение и предотвращение сетевых атак**<br>• Обнаружение руткитов средствами Rkhunter/chkrootkit.<br>• Использование антивирусного ПО ClamAV.<br>• Настройка fail2ban.<br>• Использование сетевой СОВ suricat. | **4** |
| 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
**+7 (495) 232-32-16**

Для организаций
**+7 (495) 780-48-44**

E-mail
**info@specialist.ru**