



Мобильность и Безопасность Microsoft 365

Код курса: MS-101T00

Мобильность и Безопасность Microsoft 365

Код курса: MS-101T00

Длительность	40 ак. часов
Формат	Очно; Дистанционно
Разработчик курса	Microsoft
Тип	Учебный курс
Способ обучения	Под руководством тренера

О курсе

Этот курс охватывает три центральных элемента корпоративного администрирования Microsoft 365 - управление безопасностью Microsoft 365, управление соответствием требованиям Microsoft 365 и управление устройствами Microsoft 365. В управлении безопасностью Microsoft 365 вы изучите все распространенные типы векторов угроз и утечек данных, с которыми сталкиваются сегодня организации, и узнаете, как решения Microsoft 365 для обеспечения безопасности позволяют устранить эти угрозы безопасности. Вы будете использовать Microsoft Secure Score, а также в Azure Active Directory Identity Protection. Затем вы узнаете, как управлять службами безопасности Microsoft 365, включая защиту Exchange Online, расширенную защиту от угроз, безопасные вложения и безопасные ссылки. Наконец, вы будете ознакомлены с различными отчетами, которые отслеживают состояние вашей безопасности. После этого вы перейдете от служб безопасности к разведке угроз; в частности, использование панели мониторинга безопасности и расширенного анализа угроз позволяющего опережать потенциальные нарушения безопасности. Теперь, когда ваши компоненты безопасности Microsoft 365 полностью установлены, вы изучите ключевые компоненты управления соответствием Microsoft 365. Начиная с обзора всех ключевых аспектов управления данными, включая архивирование и хранение данных, управление правами на доступ к информации, безопасное многоцелевое расширение Интернет-почты (S/MIME), шифрование сообщений Office 365 и предотвращение потери данных (DLP). Затем вы углубитесь в архивирование и хранение, уделяя особое внимание управлению записями на месте в SharePoint, архивированию и хранению в Exchange и политикам хранения в Центре обеспечения безопасности и соответствия нормативным требованиям. Ознакомившись с ключевыми аспектами управления данными, вы изучите способы их реализации, включая построение этических стен в Exchange Online, создание политик DLP из встроенных шаблонов, создание пользовательских политик DLP, создание политик DLP для защиты документов и создание советов по политикам. Затем вы сосредоточитесь на управлении данными в Microsoft 365, в том числе на управлении сроками хранения электронной почты, устранении неполадок с политиками хранения и советами по политикам, которые завершаются неудачей, а также на устранении неполадок с конфиденциальными данными. Затем вы узнаете, как внедрить Azure Information Protection и Windows Information Protection. Завершая этот раздел, вы узнаете, как управлять поиском и расследованиями, включая поиск содержимого в Центре обеспечения безопасности и соответствия нормативам, аудит журналов и управление расширенным раскрытием электронных данных. Курс завершается углубленным изучением управления устройствами Microsoft 365. Начиная с планирования различных аспектов управления устройствами, включая подготовку устройств под управлением Windows 10 к совместному

управлению. Вы узнаете, как перейти от Configuration Manager к Intune и познакомитесь с Microsoft Store for Business и Mobile Application Management. На этом этапе осуществляется переход от планирования к внедрению управления устройствами; в частности, стратегия развертывания Windows 10. Она включает в себя обучение, как реализовать автопилот Windows, Windows Analytics, и управление мобильным устройством (МДМ). При рассмотрении МДМ, вы узнаете, как развернуть его, как зарегистрировать устройства МДМ, и как управлять соответствием устройства. Данный курс является официальным курсом Microsoft, который помогает подготовить слушателей к экзамену MS-101: Microsoft 365 Mobility and Security. Сдача этого экзамена необходима для получения сертификации Microsoft 365 Certified: Enterprise Administrator Expert.

Подробная информация

Профиль аудитории:

- ИТ специалисты, стремящиеся получить роль корпоративного администратора Microsoft 365 (Microsoft 365 Enterprise Admin) и завершивших один из путей сертификации Microsoft 365 role-based administrator;
- ИТ специалисты, желающие получить опыт в области управления устройствами, безопасностью и соответствием требованиям в Microsoft 365;
- ИТ специалисты, желающие подготовиться к сдаче сертификационного экзамена MS-101 «Microsoft 365 Mobility and Security».

Предварительные требования:

Для успешного прохождения курса слушатели должны удовлетворять следующим требованиям:

- пройти курс (или иметь эквивалентные знания) для администраторов на основе ролей, например, "Обмен сообщениями", "Командная работа", "Безопасность и соответствие требованиям регулирования" или "Совместная работа";
- обладать пониманием DNS и базовых функциональных возможностей служб Microsoft 365;
- обладать глубоким пониманием общих практик ИТ.

По окончании курса слушатели смогут:

- планировать совместное управление;
- подготавливать устройства с Windows 10 к совместному управлению;
- осуществлять переход от Configuration Manager к Intune;
- настраивать Microsoft Store for Business;
- планировать управление мобильными приложениями;
- планировать стратегии развертывания Windows 10;
- планировать стратегии активации подписки Windows 10;
- устранять ошибки обновления Windows 10;
- использовать аналитику Windows 10;
- развертывание Управления Мобильными Устройствами;
- управлять устройствами с помощью Mobile Device Management;
- регистрировать устройства в Mobile Device Management (MDM);
- управлять соответствием устройств;
- управлять показателями безопасности;
- реализовывать решения безопасности в Microsoft 365;

- планировать и настраивать Azure Identity Protection;
- реализовывать Microsoft Secure Score;
- реализовать защиту Exchange Online;
- внедрять расширенную защиту от угроз;
- управлять безопасностью вложений и ссылок;
- реализовывать аналитику угроз Microsoft 365;
- использовать панель мониторинга безопасности Microsoft 365;
- настраивать расширенную Аналитику угроз;
- реализовывать безопасность облачных приложений;
- внедрять управление записями на месте в SharePoint (in-place hold);
- осуществлять архивирование и хранение в Exchange;
- создавать политики хранения в Центре безопасности и соответствия требованиям;
- планировать потребности в области безопасности и соответствия требованиям;
- строить этические стены в Exchange Online;
- создавать политики DLP из встроенных шаблонов;
- создавать пользовательские политики DLP;
- создавать политики DLP для защиты документов;
- управлять подсказками политик;
- управлять удержанием в электронной почте;
- устранять неполадки управления данными;
- внедрять защиту информации;
- внедрять расширенную защиту информации;
- понимать защиты информации Windows;
- искать содержимое в центре безопасности и соответствия требованиям;
- проводить исследование журнала аудита;
- управлять расширенными политиками eDiscovery.

Программа курса

Модуль 1 "Введение в Метрики безопасности Microsoft 365"

- Векторы угроз и утечки данных
- Решения безопасности в Microsoft 365
- Введение в Secure Score
- Введение в защиту удостоверений Azure Active Directory

Модуль 2 "Управление службами безопасности Microsoft 365"

- Введение в защиту Exchange Online
- Введение в расширенную защиту от угроз
- Управление безопасными вложениями
- Управление безопасными ссылками
- Мониторинг и отчеты

Модуль 3 "Лабораторная работа 1"

- Лабораторная работа 1: Управление службами безопасности Microsoft 365

Модуль 4 "Аналитика угроз Microsoft 365"

- Обзор аналитики угроз Microsoft 365
- Использование панели мониторинга безопасности
- Настройка расширенного анализа угроз
- Внедрение безопасности облачных приложений

Модуль 5 "Лабораторная работа 2"

- Лабораторная работа: Внедрение оповещений с помощью панели мониторинга безопасности

Модуль 6 "Введение в управление данными в Microsoft 365"

- Введение в архивацию в Microsoft 365
- Введение в хранение в Microsoft 365
- Введение в управление информационными правами
- Введение в S/MIME
- Введение в шифрование сообщений Office 365
- Введение в предотвращение потери данных

Модуль 7 "Архивация и хранение в Microsoft 365"

- Управление записями на месте в SharePoint
- Архивирование и хранение в Exchange
- Политика хранения в SCC

Модуль 8 "Лабораторная работа 3"

- Лабораторная работа: Внедрение архивирования и хранения

Модуль 9 "Внедрение управления данными в Microsoft 365 Intelligence"

- Планирование безопасности и соответствия требованиям
- Построение этических стен в Exchange Online
- Создание простой политики DLP из встроенного шаблона
- Создание пользовательской политики DLP
- Создание политики DLP для защиты документов
- Работа с подсказками политик

Модуль 10 "Лабораторная работа 4"

- Лабораторная работа 4: Внедрение политик DLP

Модуль 11 "Управление данными в Microsoft 365"

- Управление удержанием в электронной почте
- Устранение неполадок управления данными
- Внедрение защиты информации
- Внедрение расширенной защиты информации
- Введение в информационную защиту Windows

Модуль 12 "Лабораторная работа 5"

- Лабораторная работа 5: Внедрение AIP и WIP

Модуль 13 "Управление поиском и расследованиями"

- Поиск контента в Центре безопасности и соответствия требованиям
- Расследование журнала аудита
- Расширенное управление eDiscovery

Модуль 14 "Лабораторная работа 6"

- Лабораторная работа: Управление поиском и расследованиями

Модуль 15 "Планирование управления устройствами"

- Введение в совместное управление
- Подготовка устройств с Windows 10 к совместному управлению
- Переход от Configuration Manager к Intune
- Введение в Майкрософт Store for Business
- Планирование управления мобильными приложениями

Модуль 16 "Лабораторная работа 7"

- Лабораторная работа: Внедрение Microsoft Store для бизнеса

Модуль 17 "Планирование стратегии развертывания Windows 10"

- Сценарии развертывания Windows 10
- Осуществление Windows Autopilot
- Планирование стратегий активации подписки Windows 10
- Устранение ошибок обновления Windows 10
- Введение в аналитику Windows

Модуль 18 "Внедрение управления мобильными устройствами"

- Планирование MDM
- Развертывание MDM
- Регистрация устройств в MDM
- Управление соответствием устройств

Модуль 19 "Лабораторная работа 8"

- Лабораторная работа: Управление устройствами с помощью Intune

[Посмотреть расписание курса и записаться на обучение](#)

Обращайтесь по любым вопросам
к менеджерам Учебного центра Softline

8 (800) 505-05-07 | edusales@softline.com

Ждём вас на занятиях в Учебном центре Softline!



Почему Учебный центр Softline?

Лидер на рынке корпоративного обучения.

Более 300 тысяч подготовленных IT-специалистов.

Гибкий индивидуальный подход в обучении, скидки и акции.

Широкая сеть представительств в крупнейших городах РФ и СНГ; дистанционный формат обучение на вашей территории или в арендованном классе в любой точке мира.

Высокотехнологичное оборудование

Более **18 лет** опыта работы

Международные сертификаты для IT-специалистов и пользователей в Центрах тестирования

Сертифицированные тренеры с богатым практическим опытом работы

Авторизации от мировых производителей ПО (Microsoft, Cisco, VMware, Citrix, Лаборатория Касперского, Oracle, Autodesk, Код безопасности и других).

Разработка курсов и тестов под заказ, внедрение корпоративных систем обучения.

Подробнее об Учебном центре Softline

Вы можете узнать из [профайла](#).