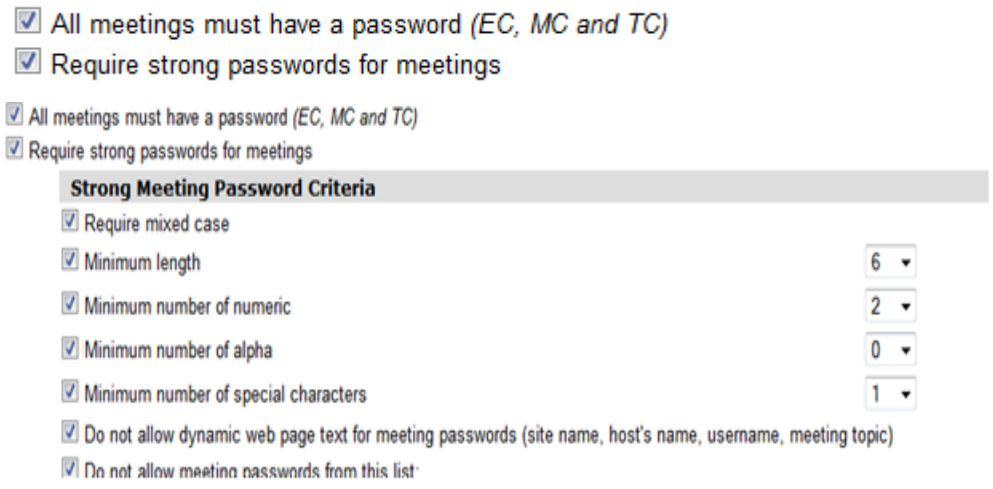
Рекомендации для обеспечения безопасности совещаний для администраторов и организаторов

Обзор конфиденциальности WebEx	Онлайновые решения Cisco WebEx помогают сотрудникам в разных офисах и виртуальным командам встречаться и работать в реальном времени, будто они находятся в одной комнате. Различные организации, предприятия и государственные учреждения всего мира полагаются на решения Cisco WebEx для упрощения рабочих процессов и повышения результатов программ по продажам, маркетингу, обучению, проектному менеджменту и поддержке. Для всех этих организаций и их пользователей конфиденциальность является важнейшим требованием. Сотрудничество онлайн должно обеспечивать многоуровневую безопасность: от планирования совещаний до аутентификации участников для совместного доступа к контенту. Cisco WebEx – это очень безопасное окружение, однако его также можно сделать очень открытым местом для сотрудничества. Понимание функций конфиденциальности администраторами сайта и конечными пользователями позволяет подогнать WebEx под конкретные корпоративные требования.
Администрирование веб-сайта WebEx	Полная конфиденциальность начинается с администрирования веб-сайта WebEx, с помощью которой администраторы могут управлять и использовать политику конфиденциальности для раздачи прав организатора и докладчика. Например, авторизованный администратор может отключить в сеансе для докладчика функции совместного доступа к приложениям или отправки файлов пользователям или сайтам. Для защиты совещаний Cisco рекомендует использовать следующие функции.
Функция	**Преимущества**
Все совещания должны быть скрытыми.	Даже из названий совещаний можно получить конфиденциальную информацию. Например, совещание под названием "Обсуждение приобретения компании A" может иметь финансовые последствия, если

Рекомендации для обеспечения безопасности совещаний для администраторов и организаторов

	название будет озвучено раньше времени. Создание скрытых совещаний обеспечивает конфиденциальность важной информации. ▪ Темы и другая информация совещаний **в списке** отображаются на сайте для авторизированных пользователей, а также неавторизированных пользователей и гостей. Если только в вашей организации нет специального корпоративного требования о публичном отображении названий и информации, все совещания должны быть **скрытыми**. ▪ Включение этого параметра для всех пользователей. На портале администрирования веб-сайта установите флажок ниже. ☑ All meetings must be unlisted *(EC, MC and TC)*

Рекомендации для обеспечения безопасности совещаний для администраторов и организаторов

Совещания должны иметь пароль (сложный).	▪ Самым надежным способом повысить безопасность совещания является создание необычного пароля высокой степени сложности (сложного пароля). Сложный пароль должен содержать буквы верхнего и нижнего регистров, цифры и специальные символы (например, $Tu0psrOx!). Пароль защищает от неавторизованного доступа, поскольку только пользователи с паролем смогут присоединиться к совещанию. Благодаря требованию создания пароля для всех совещаний, все совещания, созданные организаторами, будут защищенными. ▪ **Обратите внимание.** Использование сложного пароля не повлияет на присоединение авторизованных посетителей. Участники могут с легкостью присоединиться к совещанию, щелкнув URL в электронном приглашении, с помощью мобильного приложения WebEx и других каналов, например Jabber. ▪ Включение этого параметра. На портале администрирования установите и настройте флажки ниже. 

Рекомендации для обеспечения безопасности совещаний для администраторов и организаторов

Не позволять присоединяться раньше организатора.	▪ Подумайте о выборе этого варианта для всех организаторов. Этот вариант рекомендуется для всех совещаний в списке, поскольку внешние посетители могут использовать запланированное совещание в собственных целях без уведомления и согласия организатора. ▪ Для включения этого параметра в администрировании веб-сайта удалите флажки ниже, чтобы исключить ситуацию, в которой пользователи могут позволить посетителям присоединяться до организатора. ☐ Allow attendees or panelists to join before host *(EC, MC and TC)* ☐ The first attendee to join will be the presenter *(MC only)* ☐ Allow attendees or panelists to join teleconference before host *(EC,MC and TC)*

Для управления параметрами политики для всех пользователей на вашем веб-сайте доступны также другие функции администрирования веб-сайта WebEx ниже.

Функция	Функциональность
Управление учетной записью организатора.	▪ Блокировать учетную запись после настраиваемого количества неудачных попыток входа. ▪ Автоматически разблокировать заблокированную учетную запись после указанного интервала времени. ▪ Деактивировать учетные записи после определенного периода неактивности. ▪ Требовать от пользователя изменить пароль при следующем входе. ▪ Блокировать или разблокировать учетную запись пользователя. ▪ Активировать или дезактивировать учетную запись пользователя.
Создание учетной записи.	▪ Требовать текст безопасности при запросах новых учетных записей. ▪ Требовать электронное подтверждение регистрации новых учетных записей. ▪ Настроить правила для самостоятельной регистрации новых учетных записей.

Рекомендации для обеспечения безопасности совещаний для администраторов и организаторов

Пароли учетных записей.	▪ Требовать специальные правила для формата, длины и повторного использования пароля. ▪ Запрещать пароли, которые легко подобрать (например, "password"). ▪ Установить минимальный интервал времени, прежде чем можно будет изменить пароль.

Рекомендации по безопасности для организаторов

Как организатор, вы принимаете окончательное решение в отношении безопасности вашего совещания. Помните, что вы контролируете практически каждый аспект совещания, включая время его начала и окончания.

Следуйте рекомендациям по безопасности ниже при планировании и организации совещаний на основании ваших корпоративных требований в отношении защиты совещаний и информации.

При планировании совещания...	**Преимущество**
Планировать скрытые совещания.	Для повышения уровня безопасности совещания организаторы могут не указывать его в календаре совещаний. Для этого удалите флажок рядом с этим вариантом, чтобы предотвратить неавторизованный доступ к совещанию и скрыть информацию о нем, например, имя организатора, тему и время начала. ▪ Такое совещание не отображается в календаре совещаний на странице "Обзор совещаний" и на вашей странице "Персональные совещания". ▪ Чтобы присоединиться к скрытому совещанию, посетители должны указать его уникальный номер. ▪ Для скрытого совещания необходимо, чтобы организатор сообщил о нем посетителям, отправив ссылку в электронном приглашении, или же ввел номер совещания на странице "Присоединиться к совещанию". ▪ **Обратите внимание.** При указании совещания в списке для пользователей отображаются его название и информация. Если совещание не защищено паролем, любой пользователь может к нему присоединиться. **Подсказка.** Выбирайте уровень безопасности, исходя из цели совещания.

Рекомендации для обеспечения безопасности совещаний для администраторов и организаторов

	Например, для доступа к совещанию для обсуждения корпоративного пикника достаточно только пароля. С другой стороны, планируя совещание, где будут обсуждаться конфиденциальные финансовые данные, лучше не указывать его в календаре совещаний. Кроме того, можно ограничить доступ к совещанию после присоединения всех посетителей.
Внимательно выбирать тему совещания.	▪ Совещание в списке или пересланное электронное приглашение по меньшей мере может сообщить названия совещаний непредусмотренным пользователям. Названия совещаний могут непреднамеренно раскрыть конфиденциальную информацию, поэтому убедитесь в том, что название не содержит никаких конфиденциальных данных, например имен компаний и мероприятий.
Защищать совещания сложным паролем.	▪ Использование сложных паролей совещаний для каждого сеанса – самый верный способ защитить ваши совещания. Хоть это и необычно, но администраторы веб-сайта могут разрешать создание совещаний без паролей. В большинстве случаев настоятельно рекомендуется защищать все совещания сложными паролями. ▪ **Обратите внимание.** Добавление паролей к совещаниям не влияет на присоединение к совещаниям авторизованных посетителей. Участники могут с легкостью присоединиться к совещанию, щелкнув URL в электронном приглашении, с помощью мобильного приложения WebEx и других средств, например Jabber. ▪ **Не используйте пароли** для совещаний повторно. Планирование совещаний с одинаковыми паролями значительно снижает уровень защиты совещания.

Рекомендации для обеспечения безопасности совещаний для администраторов и организаторов

Исключать пароли совещаний из приглашений.	▪ Если вы приглашаете посетителей на совещание, пароль доступа к нему не указывается в получаемых посетителями электронных приглашениях. Нужно сообщить посетителям пароль другими средствами, например, по телефону. ▪ Для чрезвычайно конфиденциальных совещаний не указывайте пароли совещаний в электронных приглашениях. Это исключает возможность неавторизованного доступа к информации о совещании, если сообщение электронной почты пересылается ненадлежащим получателям.
Посетители должны иметь учетную запись на вашем сайте.	▪ Когда этот параметр включен, чтобы присутствовать на совещании, все посетители должны иметь учетные записи пользователя на вашем сайте. За информацией о том, как посетители могут получить учетные записи, обратитесь к администратору вашего сайта. ▪ Инструкции по включению этого параметра приведены ниже. ☐ Require attendees to have an account on this Website in order to join this meeting
Использовать звук входа и выхода или сообщение имени.	▪ Использование этой функции предотвращает присоединение пользователей к аудиочасти совещания без вашего ведома. ▪ Эта функция включена по умолчанию. Для выбора этого параметра нажмите Выбрать **участника** > **Звук входа и выхода** *(недоступно для Training Center).*
Ограничить доступность.	▪ Ограничьте доступность, например чата и аудио, если вы разрешаете пользователям присоединяться к совещанию до организатора.
Запрещать пересылку приглашений.	▪ Попросите, чтобы ваши приглашенные пользователи не пересылали приглашения, в частности это касается конфиденциальных совещаний.
Назначить альтернативного организатора.	▪ Назначьте альтернативного организатора, чтобы начать и контролировать совещание. Это помогает повысить безопасность совещаний, устранив ситуацию, при которой роль организатора будет назначена незапланированному или неавторизованному посетителю, если вы вдруг потеряете связь с совещанием. ▪ **Примечание.** Приглашая посетителей на запланированное совещание, можно назначить одного или нескольких посетителей в качестве альтернативных организаторов совещания. Альтернативный организатор

Рекомендации для обеспечения безопасности совещаний для администраторов и организаторов

	может начать совещание и выполнять обязанности организатора. Таким образом, у альтернативного организатора должна быть учетная запись пользователя на вашем веб-сайте Meeting Center.
Во время совещания	
Ограничить доступ к совещанию.	▪ Блокируйте совещание после того, как все посетители присоединились к нему. Это предотвратит присоединение дополнительных посетителей. Организаторы могут блокировать и разблокировать совещания в любое время на протяжении всего сеанса. ▪ Чтобы **заблокировать** совещание, выберите **Совещание > Ограничить доступ.** ▪ **Подсказка.** Этот параметр предотвращает присоединение кого-либо к совещанию, в том числе участников, приглашенных на совещание, но еще не присоединившихся к нему. Чтобы **разблокировать** совещание, выберите **Совещание > Восстановить доступ.**
Проверять личности всех пользователей в вызове.	▪ Учет всех пользователей посредством переклички – отличная практика. Попросите пользователей включить их видео или представиться, чтобы подтвердить свою личность. ▪ Обратите внимание. o Для посещения совещания с помощью телефона звонящему необходимо только знать действительный номер телефона системы WebEx и девятизначный идентификатор совещания. Установка паролей на совещания не предотвращает присоединение пользователей к аудиоконференции WebEx. o Если пользователям без учетной записи позволяется присоединяться к совещанию, неавторизованные пользователи в вашем совещании могут назваться любым именем.
Удалить участника из совещания.	▪ Участников можно исключить из совещания в любое время. ▪ Выберите имя участника и нажмите **Участник>Вывести.**
Предоставлять совместный доступ к контенту и приложениям, но не рабочему столу.	▪ Используйте функцию **Совместный доступ >Приложение** вместо **Совместный доступ >Рабочий стол**, чтобы поделиться приложением и избежать случайного раскрытия конфиденциальной информации на рабочем столе.

Рекомендации для обеспечения безопасности совещаний для администраторов и организаторов

После совещания	
Создавать пароли для записей.	▪ Лучший способ предотвратить неавторизованный доступ к записям – не создавать их. ▪ Если же записать совещание необходимо, для защиты информации можно отредактировать запись совещания и добавить к ней пароль до того, как предоставлять совместный доступ. Для доступа к защищенным паролем записям необходимо знать пароль.
Удалить записи.	▪ Удаляйте записи, если они уже неактуальны.

Рекомендации для обеспечения безопасности совещаний для администраторов и организаторов

Персональные совещания WebEx (совещания PCN)	
Проведение персональных совещаний (PCN) в администрировании веб-сайта	▪ **Не включайте функцию "Присоединяться до организатора" для персональных совещаний** для каких-либо пользователей, если только вы не понимаете в полной мере последствий для безопасности и вам не нужна эта функция. . ▪ Персональные совещания предполагают два случайных 8-значных кода доступа для управления персональным совещанием и доступа к нему (код доступа организатора и код доступа посетителя). Эти коды статичны и всегда доступны без предварительного планирования. Если персональное совещание запланировано заранее, организатор получает приглашение с кодами доступа организатора и посетителя, а приглашенные получают отдельное приглашение, содержащее (только) код доступа посетителя. ▪ Если функция "Присоединиться до организатора" выключена (рекомендуется), организатор должен набрать номер доступа WebEx для аудиомоста и ввести ПИН и код доступа организатора, прежде чем посетители смогут присоединиться к совещанию. ▪ Если функция "Присоединиться до организатора" включена, посетители смогут присоединиться к совещанию без присутствия организатора. Включение этой функции может привести к непредвиденным последствиям, включая ненадлежащее использование минут телеконференции.
Безопасность персональных совещаний для организаторов	▪ **Создайте сложный ПИН организатора и обеспечьте его защиту.** ▪ Ваш ПИН является последним уровнем защиты от неавторизованного доступа для вашей учетной записи персонального совещания. Если другой пользователь узнал код доступа к персональному совещанию, совещание все равно невозможно будет начать без ПИН организатора. Обеспечьте сохранность своего ПИН, и не разглашайте его.
Заключение	Несколько дополнительных шагов при настройке параметров сайта, планировании совещаний WebEx и участии в них могут значительно повысить уровень безопасности и конфиденциальности совещания.

Рекомендации для обеспечения безопасности совещаний для администраторов и организаторов

Руководства пользователей и статьи базы знаний для повышения уровня безопасности и конфиденциальности	▪ Руководство по быстрому началу работы Cisco WebEx ▪ Официальный документ по безопасности WebEx ▪ Какой уровень безопасности мне следует обеспечить для моего запланированного совещания? ▪ Как установить требование к тому, чтобы все совещания и сеансы обучения были скрытыми для всего сайта? ▪ Как запланировать скрытое совещание? ▪ Как изменить "скрытое совещание" на "совещание в списке"?