auth

Многофакторная аутентификация

Технические специалисты ООО «Открытые технологии» уделяют большое внимание поддержанию безопасности программного продукта на должном уровне и оперативно обновляют СЭО 3KL при обнаружении критических уязвимостей или внеочередных выпусках Moodle патчей безопасности. Однако, подавляющее большинство взломов по-прежнему происходит из-за того. что преподаватели (а, зачастую, и администраторы СЭО) устанавливают себе слишком очевидные пароли и хранят их в общедоступном месте.

Решением проблемы может стать многофакторная аутентификация (МФА). Если в СЭО 3KL включена и настроена многофакторная аутентификация, то пользователю, для авторизации и входа в систему, кроме ввода логина и пароля, необходимо успешно пройти дополнительную проверку (или несколько проверок): ввести одноразовый пароль из приложения, вставить аппаратный ключ, подтвердить биометрию, зайти с устройства с определенным IP-адресом и т. п. И теперь, даже если злоумышленнику удалось раздобыть пароль и логин, то со вводом, например, кода из СМС, у него возникнут проблемы. Метод перебора здесь тоже не сработает — количество попыток ввода ограничено, после их окончания учетная запись пользователя будет заблокирована и без вмешательства администратора восстановить доступ не получится.

Функционал МФА позволяет создавать как последовательные сценарии подтверждения личности пользователя (когда надо успешно пройти несколько проверок, друг за другом), так и сценарии с возможностью выбора: например, сегодня пользователь забыл свой аппаратный ключ на рояле, но он смело выбирает получение секретного кода на почту, вводит его и входит в систему.

Вид и количество необходимых для входа проверок (факторов аутентификации) выбираются и настраиваются администратором СЭО при включении в среде электронного обучения МФА. Разумеется, после того, как такой важный шаг будет регламентирован и одобрен руководством организации. :-)

И, кстати, в СЭО 3KL можно настроить МФА на получение секретного кода в мессенджере «MAX»!

А все нюансы применения многофакторной аутентификации и ее правильной настройки мы описали для вас в тематической статье нашей базы знаний.

Уникальный ID ответа: #2002
Опубликовал: : Сергей Гусев
Последние обновление: 2026-11-19 17:02

(c) 2026 ООО "Открытые технологии" <sp-other@opentechnology.ru> | 19.11.2026
URL: https://kb.opentechnology.ru/content/46/993/ru/mnogofaktornaa-autentifikacia.html