

ОСНОВНЫЕ ФУНКЦИИ БЕЗОПАСНОСТИ SALESFORCE

М.В. Стержанов

Функции безопасности Salesforce дают пользователям возможность безопасно и эффективно проводить работу в системе, разграничив доступ к данным для разных групп пользователей. Рассмотрим основные способы защиты данных от несанкционированного доступа внутри организации и от ненадлежащего использования пользователями.

Salesforce отображает информацию о производительности и безопасности системы в режиме реального времени на сайте <http://trust.salesforce.com>. Ресурс <http://trust.salesforce.com/security> предоставляет оперативные данные о производительности

системы, предупреждения о текущих и недавних попытках фишинга и вредоносного ПО, а также советы по передовым методам обеспечения безопасности.

Администратор может использовать механизм Health Check для выявления и устранения потенциальных уязвимостей в настройках безопасности. Сводная оценка показывает степень соответствия с базовыми показателями и стандартами безопасности. Имеется возможность загрузить до пяти настраиваемых базовых показателей вместо стандартного базового плана Salesforce.

Функции аудита Salesforce непосредственно не защищают организацию, однако предоставляют важную информацию об использовании системы, которая может иметь решающее значение для диагностики потенциальных или реальных проблем безопасности.

Salesforce Shield – это три инструмента безопасности, которые помогают создавать дополнительные уровни доверия, соответствия и управления прямо в критически важных для бизнеса приложениях. Он включает в себя шифрование платформы Shield, мониторинг событий и журнал аудита [1].

Литература

1. Salesforce Security Basics [Электронный ресурс]. – Режим доступа: https://developer.salesforce.com/docs/atlas.en-us.securityImplGuide.meta/securityImplGuide/overview_security.htm. – Дата доступа: 10.04.2021.