Марков В.М.
*Канд. тех. наук Провоторов А.В.*
*Муромский институт (филиал) федерального государственного образовательного учреждения высшего образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»*
*602264, г. Муром, Владимирская обл., ул. Орловская, 23*
*Россия, 602264, Владимирская область, г. Муром, ул. Орловская, д.23.*
*vladmarkov7@mail.ru*

**Разработка приложения мониторинга действий пользователя и системы на предприятии.**

На современном этапе развития компании стали зависимыми от информационных систем, в следствии этого появились уязвимости к хакерским атакам, человеческому и государственному фактору, а также вирусам, настолько, что многие руководители бизнеса уже не чувствуют себя в безопасности.

Системы мониторинга выступают решением данной проблемы, а именно реализовывают наблюдение за действиями работников, а также проверяют на соответствия корпоративным нормам.

Из-за увеличения инсайдерских угроз, появилась необходимость таких систем. Сотрудники тратят много рабочего времени на задачи, не связанные со своими обязанностями. В повышении производительности сотрудников, заинтересован каждый работодатель, именно этому поспособствует собранная информация о том, чем занимаются работники в рабочее время.

Инсайдерские угрозы — это угрозы организации, которые исходят от кампании, таких как бывшие сотрудники, работники или деловые партнеры, которые обладают информацией о методах защиты информации внутри предприятия, компьютерных системах и данных.

Приложение мониторинга предоставит актуальную информацию для анализа состояния ИТ-инфраструктуры и работоспособности сотрудников, а также оперативное устранение, обнаруженной в угрозы. Постоянный мониторинг помогает поддерживать сервисы в рабочем состоянии и сохранять необходимый уровень их качества, а также избежать простоев в работе.

Если сотрудник использует ресурсы не по назначению, ему будет очень легко замести следы, стерев данные или удалив журналы посещений и файлы. Но разрабатываемое приложение мониторинга действий пользователя и системы позволит сохранить запись каждого действия, произведенного пользователем, вне зависимости от того, что он делал и какую информацию стер.

Основные функций мониторинга:

- Слежение. Основная функция, включающая в себя периодический сбор информации.
- Хранение информации. Дополнение к слежению. Осуществляется сбор информации по основным показателям каждого объекта мониторинга, для хранения обычно используются базы данных.
- Построение отчётов. Осуществляется как на основе текущих данных слежения, так и по долговременно хранимой информации.

Использование разработанного приложения мониторинга позволит:

- оптимизировать использование информационных ресурсов;
- Минимизировать время простоя, а также повысить качество ИТ-сервисов;
- обеспечить безопасность информации, надежность, и согласованное функционирование всех компонентов ИТ-инфраструктуры;
- Повысить в несколько раз эффективность работы ИТ-подразделения.

Итогом работы являться разработанное приложение мониторинга действий пользователя и системы.