Для своевременного выявления постепенной деградации параметра в процессе эксплуатации используется диагностическое устройство (далее – ДУ). Поскольку отклонение фактического параметра от эталонного параметра и переход в опасную зону являются постепенным процессом, регулярный контроль позволяет обнаружить критическое отклонение и вовремя вывести изделие из эксплуатации. Наличие исправно функционирующего диагностического оборудования «преобразует» зону потенциально опасного состояния в зону «компенсации», где риск реализации отказа снижается за счет его раннего обнаружения (рисунок 3). При этом собственные неисправности ДУ не формируют самостоятельного дополнительного риска, так как они проявляются в области крайне маловероятных значений параметра (в «хвостах» распределения), где плотность вероятности возникновения отказа мала.

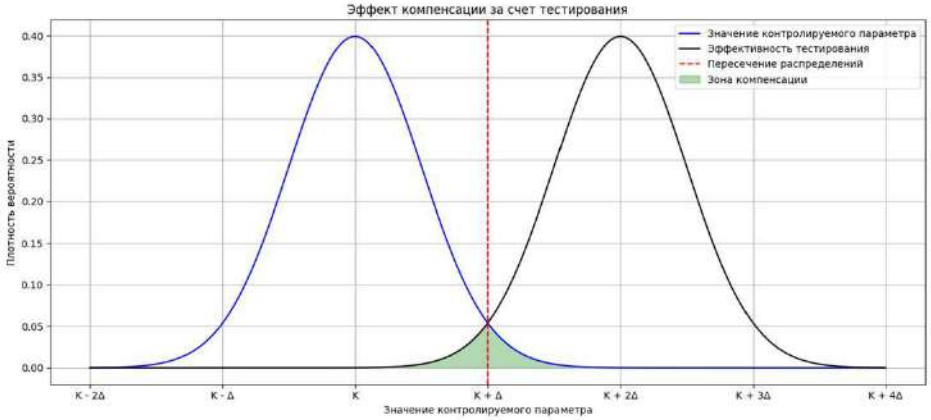

Рисунок 3 – Влияние диагностики на уменьшение последствий опасного отклонения фактического значения параметра от эталонного

Выводы:

1 Системы автоматики подвержены случайным отказам, которые можно моделировать с помощью простейших потоков отказов и вероятностных моделей (например, модели Маркова). Механические элементы также подвержены отказам, но они носят постепенный характер и зависят от качества производства и условий эксплуатации и технического обслуживания.

2 Отказом механического изделия считается такое отклонение значения его параметра от эталонного, которое приводит к нежелательным последствиям при организации перевозочного процесса. Эти аспекты приводят к тому, что отказы механических изделий имеют вероятностную природу, поэтому требуют расчета вероятностей возникновения опасных ситуаций и критериев оценки рисков.

3 Методы контроля. Контроль состояния механического изделия может осуществляться двумя методами: абсолютным – визуальный осмотр, вероятностным – автоматический контроль с учетом метрологических характеристик.

4 Текущие задачи:

– унификация критериев оценки – номинальные параметры; допустимые отклонения; критические изменения; аварийные состояния;

– разработка прогнозных моделей;

– внедрение автоматизированных систем мониторинга;

– адаптация международного опыта.

УДК 625.8

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СИСТЕМЫ ДИСТАНЦИОННОГО ОБУЧЕНИЯ

Н. В. РЯЗАНЦЕВА, В. Е. МИНИН, И. С. КУХАРЕНКО
Белорусский государственный университет транспорта, г. Гомель

В современных условиях разработка программного обеспечения становится все более сложной и затратной. Растут требования к функциональности и масштабированию, увеличивается число интеграций с внешними сервисами, и ужесточаются критерии соответствия нормативам. В универси-

тете ведется активная работа над созданием и внедрением системы дистанционного обучения (СДО) и защита информации является одной из основных задач. Для такой системы необходим сбалансированный подход: избыточная защита ведет к удорожанию и усложнению эксплуатации, в то время как пренебрежение базовыми мерами создает неприемлемые риски компрометации.

К числу критически важных уязвимостей относятся недостатки в механизмах аутентификации и управления сессиями. Основными проявлениями их являются использование слабых паролей и отсутствие многофакторной аутентификации для пользователей с повышенными привилегиями. В качестве мер по снижению рисков предлагается ввести минимальные требования к сложности паролей, хранить пароли с помощью современных адаптивных алгоритмов хеширования, внедрить многофакторную аутентификацию для администраторов и ответственных ролей, а также обеспечить корректные настройки cookie (HttpOnly, Secure) и политики истечения сессий.

Серьезные риски связаны с проблемами управления доступом, когда пользователи получают права, не соответствующие их роли. Решением являются внедрение централизованной авторизации по принципу наименьших привилегий, обязательная серверная проверка прав для критичных запросов и регулярный аудит системы доступа.

Высокую критичность имеют SQL-инъекции, последствия которых является выполнение произвольного кода и полный компрометацию данных. Надежная защита от этого вектора атак строится на трех китах: повсеместное применение параметризованных запросов (или ORM), строгая валидация входных данных и их корректное экранирование.

Утечка чувствительных данных – еще одна значимая категория рисков. Были замечены случаи передачи данных без шифрования, хранение резервных копий без защиты и избыточное хранение персональной информации. В качестве контрмер рекомендовано применять TLS для всех каналов передачи, шифровать важные данные, маскировать и минимизировать хранение персональных данных, а также внедрить политики управления логами и резервными копиями с учетом сроков хранения и процедур безопасного удаления.

Использование устаревших или уязвимых компонентов также отмечено как типичная проблема. Библиотеки и плагины со старыми версиями легко становятся вектором атак. Для этого необходимо вести учет зависимостей, регулярно сканировать проект на известные уязвимости и оперативно обновлять компоненты с проверкой совместимости.

К числу важнейших практик обеспечения безопасности относится регистрация действий и мониторинг. При их отсутствии инциденты могут оставаться незамеченными длительное время. Рекомендуется настроить централизованный сбор логов, внедрить мониторинг аномалий и оповещений, а также разработать регламент реагирования на инциденты.

Авторами было отмечено, что для СДО в университете оптимальным является набор мер, предоставляющий наилучшее соотношение риска к стоимости:

– обязательное шифрование каналов связи (TLS);
– безопасное хранение паролей и управление сессиями;
– проверка прав доступа на сервере;
– регулярное сканирование зависимостей и базовый механизм логирования с оповещениями.

В дополнение к техническим мерам рекомендуется интегрировать процессы тестирования безопасности (статический и динамический анализ, периодическое тестирование безопасности и анализ конфигураций) в цикл разработки, ведь безопасность должна быть непрерывным и эволюционным процессом, а не разовой задачей.

УДК 656.257.073

ОПОРНОЕ УПРАВЛЕНИЕ ИСПОЛНИТЕЛЬНОЙ СТАНЦИЕЙ НА БАЗЕ ТИПОВЫХ РЕШЕНИЙ ДЦ «НЕМАН»

Ф. Е. САТЫРЕВ, В. Н. ЛИТВИН
Белорусский государственный университет транспорта, г. Гомель

В рамках работ по оптимизации структуры оперативного управления перевозочным процессом, внедрению на железной дороге современных информационных технологий, эффективному исполь-