Ученые записки Крымского федерального университета имени В. И. Вернадского. Экономика и управление. Том 3 (69). 2017 г. № 2. С. 11–17.

УДК 004.056.4

ОТКАЗОУСТОЙЧИВОСТЬ ЭКОНОМИЧЕСКИХ КОМПЬЮТЕРНЫХ СИСТЕМ УПРАВЛЕНИЯ

Бойченко О. В., Тупота Е. С.

Крымский федеральный университет имени В. И. Вернадского, Симферополь, Российская Федерация
E-mail: bolek61@mail.ru

В статье исследованы современные концепции и практики использования отказоустойчивых информационных систем для управления экономической сферой. Выявлены пробелы концепций отказоустойчивости информационных систем, уязвимости которых определены современным состоянием кибербезопасности. Предложена концепция отказоустойчивых информационных систем управления, которая позволяет создать условия эффективности процессов управления за счет инновационных подходов в учете современной проблематики рисков сетевых информационных технологий, связанных с кибербезопасностью.
Ключевые слова: информационная система управления, отказоустойчивость, концепция, кибербезопасность, риски, сетевые технологии.

ВВЕДЕНИЕ

Современные тенденции развития информационно-коммуникационных технологий влекут за собой большие риски, связанные с киберпреступностью. В связи с этим на предприятиях остро встает вопрос защиты коммерческих и пользовательских данных. В таком случае острой необходимостью является разработка новых подходов в концепции внедрения отказоустойчивых систем, обеспечивающих защищенность информационных ресурсов предприятия.

Цель исследования состоит в анализе используемых моделей отказоустойчивой компьютерной системы управления в обеспечении защищенности информационных ресурсов предприятия, а также в структурировании современной концепции отказоустойчивых систем управления экономической сферой.

ОСНОВНОЙ МАТЕРИАЛ

Отказоустойчивость – это свойство системы сохранять свою функциональность даже при наличии неисправностей. Данный вопрос широко рассматривался такими учеными, как Ж. К. Лапри, А. Авиценис, Д. Пауэлл, Д. Рашби и др. В работах этих исследователей представлена основная концепция понятия отказоустойчивости информационных систем управления, впервые введены два основных понятия для обеспечения отказоустойчивости (режим сбоя и допускаемое покрытие), а также представлена система классификации отказоустойчивости в режиме реального времени [1].

Основываясь на положениях указанных научных трудов и практическом опыте специалистов, следует отметить, что для более подробного рассмотрения ошибок

внутри системы необходимо, прежде всего, введение базовых понятий неисправности, сбоя и ошибки. Неисправность представляет собой дефект или недостаток, который возникает в некоторых аппаратных или программных компонентах системы. Сбой – это отклонение системы за рамки установленных системных ограничений. Ошибка – это возникшая неисправность и непригодность эксплуатации системы в целом. Отметим, что сбой в работе в одной из подсистем также может быть рассмотрен как неисправность системы в целом. Таким образом, становится возможным представить модель отказа системы (рис. 1):

Рис. 1. Модель отказа системы
Источник: составлено авторами.

Рассматривая систему, работающую на многопроцессорной архитектуре, следует отметить, что неисправность в одном процессе может привести к отказу всей системы, что мы рассматриваем как ошибки системы. В таком случае способность системы функционировать даже при наличии ошибки в одном процессе определяется отказоустойчивостью.

Следует отметить, что большинство ошибок не сразу приводит систему к сбою, некоторым свойственно накапливаться (не влиять на систему вовсе). В таком случае неисправности можно разделить на несколько видов: латентная (активированная, не проявляемая на уровне эксплуатации), и эффектная (влияющая на уровень эксплуатации).

Перечисленные факторы необходимо учитывать при проектировании отказоустойчивой системы, начиная с определения гипотезы системы соответственно конкретному продукту с учетом прогнозируемых ошибок и сбоев системы, а также уязвимостей, учитываемых проектируемой отказоустойчивой системой.

Практика свидетельствует о существовании большого количества подходов в создании отказоустойчивых систем управления. Так, например, концепция «Синтез регулятора» [2] (основана на автоматической генерации отказоустойчивого программного обеспечения) направлена на разработку инструмента, который должен выявлять критические ошибки и учитывать все возможные состояния системы (нормальное состояние системы и состояние системы с неисправностями) за счет использования регулятора, определяющего возможность одновременного возникновения неисправностей и сбоев. Преимущество данной концепции заключается в возможности нахождения автоматического контроллера (модуля безопасности) системы управления, представленной динамической (механизм для обработки ошибок) и статической (гарантия пресечения указанных недостатков во время исполнения) компонентами.

Основой концепции является функция обнаружения состояния ошибки, позволяющая своевременно произвести корректировку процесса обработки данных системы управления. Применение механизма контрольных точек позволяет производить необходимую операцию по восстановлению системы путем дробления основной ошибки на части, исправление которых менее трудоемко и более эффективно.

Вторая концепция построения отказоустойчивой системы направлена на использование аспектно-ориентированного программирования [3]. Данная концепция подразумевает модернизацию исходной системы на основе принципов аспектно-ориентированного программирования путем осуществления контроля над функционированием системы с использованием контрольных точек в режиме реального времени (с определением временного промежутка между контрольными точками). Большие интервалы приводят к увеличению временной составляющей между действующей неработающей системой и «эталонной». В то же время слишком маленькие интервалы увеличивают расходы на оборудование и программное обеспечение, так как необходимо выделять большие производительные мощности. В результате определения оптимальной продолжительности интервалов времени расходы сводятся к минимуму, а вероятность работоспособности системы стремится к максимуму.

Проведенный анализ рассмотренных ранее концепций отказоустойчивости информационных систем управления экономической сферой определяет ряд пробелов, связанных с современными аспектами уязвимостей распределенных корпоративных сетей (прежде всего, это актуальные вопросы киберпреступности, стремительный рост которой вызывает большое беспокойство не только в России, но и во всем мире). Это требует разработки новых подходов для создания концепции отказоустойчивых систем управления экономической сферой.

Прежде всего, следует отметить, что отказоустойчивость системы управления определяется двумя основными критериями: доступность (доли времени, при котором система находится в рабочем состоянии) и надежность (вероятность того, что система будет находиться в рабочем состоянии). Отметим, что система с высокой доступностью как раз наиболее уязвима по отношению к отказу. Высокая надежность информационной системы является самым важным аспектом в любой отрасли ее внедрения (отказ может означать потерю времени, средств либо человеческих ресурсов) [4].

При разработке концепции также необходимо учитывать, что информационные системы отказываются грамотно работать по разным причинам:

1. Ошибка проектирования на программном уровне.

2. Ошибка, которая проявляется только при отдельных условиях (которые не были протестированы разработчиками).

3. Сбой системы со стороны внешней среды.

4. Сбой системы вследствие конфликта прикладного программного обеспечения.

5. Сбои из-за старения аппаратной или программной части системы.

6. Ошибки неправильной спецификации и конструктивных недостатков системы.

7. Ошибки оператора по сбою в работе системы (отсутствие необходимой компетенции).

8. Ошибки, вызванные отсутствием конструкций по соответствующим действиям оператора для восстановления системы (контекстные подсказки).

Таким образом, информационная безопасность представляет собой концепцию защиты информации и информационной системы от несанкционированного доступа, использования, раскрытия, разрушения, модификации или уничтожения в целях обеспечения конфиденциальности, целостности и доступности.

При этом гарантия безопасности представляет собой меры по охране и защите информационных систем путем обеспечения их доступности, целостности, подлинности, конфиденциальности и отказоустойчивости (обеспечение восстановления информационных систем посредством обнаружения уязвимостей и реагирования на угрозы, а также включения системы защиты).

Во время повсеместного использования сетевых информационных технологий для управления деятельностью предприятий, уязвимости веб-приложений являются одними из самых серьезных угроз информационной безопасности, что, прежде всего, связано с одной из самых главных проблем в ИТ-индустрии – кибербезопасностью.

В концепции учтены выводы экспертного анализа, свидетельствующего о существовании четырех основных проблем сетевой информационной безопасности:

1. Уязвимость веб-приложений.
2. Устаревшие патчи.
3. Ошибки, связанные с шифрованием и обеспечением конфиденциальности данных на ПК.
4. Очень простые либо полное отсутствие паролей на корпоративных почтах или в приложениях операторов на предприятии.

Прежде всего, следует обратить внимание на первый пункт угрозы безопасности, связанной с веб-приложениями, поскольку на практике использование данного сервиса является наиболее популярным для администраторов сети и наиболее непонятным в использовании для руководителей предприятия. Поскольку для веб-приложений зачастую используют уже готовые программные решения, то для внедрения на предприятии готового решения необходимо оценить соответствие разработанного приложения требованиям безопасности на основе указаний нормативных документов. При этом особо важным вопросом в решении проблем безопасности информационной системы управления является внедрение механизмов защиты в начале разработки проекта информатизации, что обеспечит корректную работу системы на всех уровнях

модели OSI. В противном случае (наращивание подсистемы защиты в разработанный проект) приложение будет работать неправильно, имея просто оболочку безопасности, которую взломать хакерам будет весьма просто.

Практика эксплуатации распределенных компьютерных систем управления свидетельствует о наличии довольно существенной проблемы в защите веб-приложений, связанной с отсутствием надежного механизма проверки входных данных на аутентичность, что создает условия для успешных действий злоумышленников по проникновению в систему и получению несанкционированного доступа к информационным ресурсам [5].

Для решения указанной проблемы концептуально может быть предложено использование механизма управления сеансами, позволяющего создать условия исключения перехода пользователя в другую пользовательскую сессию и просматривания конфиденциальной информации.

В предложенной концепции определено, что следующим важным инструментом безопасности распределенной компьютерной информационной системы управления является шифрование данных сразу после ввода в систему. Следует отметить, что шифрование при хранении и передаче данных имеет решающее значение для безопасности компании и исключения утечки корпоративной информации.

Важным элементом в структуре разработанной концепции является проведение мониторинга уязвимостей, оперативное реагирование на компьютерные атаки, а также контроль состояния системы безопасности на основе строгих тестов на проникновение, что является залогом успешной работоспособности веб-приложений и отказоустойчивости системы управления в целом.

Таким образом, становится возможным представить инновационный подход в разработке структуры концепции отказоустойчивых систем управления экономической сферой (рис. 2).

Отдельного внимания заслуживает блок информационного режима управления рисками, определяющего потенциальные и прогнозируемые риски безопасности и меры по их ликвидации.

Прежде всего, это касается мер по принятию стандартных мер безопасности:

- отключение ненужных функций системы;
- поддержка своевременного обновления приложений;
- защита от вредоносных программ;
- контроль электронной почты, веб-серфинга;
- контроль правильной настройки устройств системы;
- проверка съемных носителей на наличие вредоносного программного обеспечения.

Пользовательский блок также заслуживает отдельного рассмотрения в структуре разработанной концепции отказоустойчивых систем управления

экономической сферой, где ключевую роль играет администрирование системы, в котором необходимо указать следующие меры:

- обеспечение пользователей системы рабочим местом с уникальным доступом и привилегиями;
- исключение использования учетных записей, используемых системным администратором и администратором баз данных, для рискованных действий;
- контроль действий пользователя по доступу к конфиденциальной информации;
- контроль действий пользователя по изменению пароля и удалению учетных записей;
- регулярное обучение пользователей по проблемам, связанным с кибер-рисками;
- постоянное сканирование входящего и исходящего трафика для обнаружения подозрительной активности;
- использование специализированных систем обнаружения и предотвращения вторжений.

Рис. 2. Концепция отказоустойчивых информационных систем управления экономической сферой

Источник: составлено авторами.

Предложенная концепция отказоустойчивых информационных систем управления экономической сферой позволяет создать условия надежности и эффективности процессов управления за счет инновационных подходов в учете

современной проблематики рисков сетевых информационных технологий, связанных с кибербезопасностью.

ВЫВОДЫ

Уникальность разработанной концепции состоит в создании новых подходов по характеристике отказоустойчивых информационных систем управления на основе сетевых технологий, а также создании системы сетевой безопасности распределенной информационной системы в составе стандартных мер безопасности и предупреждения потенциальных и прогнозируемых рисков. Особого внимания в разработанной концепции заслуживают специальные методы, обеспечивающие защиту пользовательских и коммерческих данных предприятия по администрированию распределенной корпоративной сети.

Список литературы

1. Laprie J. C. Dependable Computing and Fault Tolerance: Concepts and Terminology // Proceedings of 15th International Symposium on Fault-Tolerant Computing (FTSC-15), 1985. P. 2–11.

2. Бесекерский В. А., Попов Е. П. Теория систем автоматического управления / Изд. 4-е, перераб. и доп. СПб.: Профессия, 2003. 752 с.

3. Семенов Н. А., Гончаров А. А. Аспектно-ориентированное программирование в контексте решения вопросов повышения эффективности экономических показателей ИТ-проектов // Программные продукты и системы. Тверь: ТГУ. № 3. 2016. С. 149–153.

4. Информационная безопасность социально-экономических систем: монография / Апатова Н. В., Акинина Л. Н., Байздренко Е. А., Бойченко О. В., Гапонов А. И., Герасимова С. В., Королев О. Л., Писарюк С. Н., Потанина М. В., Рыбников А. М., Рыбников М. С., Ремесник Е. С., Смирнова О. Ю., Титаренко Д. В. и др. / под ред. проф. О. В. Бойченко. Симферополь: ИП Зуева Т. В., 2017. 302 с.

5. Бойченко О. В., Бахши Д. Г. Механизмы защиты данных сетевых информационных технологий // Проблемы информационной безопасности: III Междунар. науч.-технич. конф., 16–18 февраля 2017 г.: тезисы докладов. Симферополь, 2017. С. 153–154.

Статья поступила в редакцию 11.09.2017