Электронный научный журнал «Век качества» ISSN 2500-1841 http://www.agequal.ru

2020, №4 http://www.agequal.ru/pdf/2020/AGE_QUALITY_4_2020.pdf

Ссылка для цитирования этой статьи:

Поначугин А.В., Пичужкина Д.Ю., Смекалова Е.С. Подбор оптимальной модели поиска и устранения ошибок в работе системного администратора // Электронный научный журнал «Век качества». 2020. №4. С. 139-150. Режим доступа: http://www.agequal.ru/pdf/2020/420010.pdf (доступ свободный). Загл. с экрана. Яз. рус., англ.

УДК 004.05

Подбор оптимальной модели поиска и устранения ошибок в работе системного администратора

Поначугин Александр Викторович,
кандидат экономических наук, доцент, преподаватель,
Нижегородский государственный педагогический университет им. Козьмы Минина,
603005, Российская Федерация, г. Нижний Новгород, Ульянова, 1
sasha3@bk.ru

Пичужкина Дарья Юрьевна
студент, Нижегородский государственный педагогический университет им. Козьмы Минина,
603005, Российская Федерация, г. Нижний Новгород, Ульянова, 1
dpichuzhkina@list.ru

Смекалова Екатерина Сергеевна
студент, Нижегородский государственный педагогический университет им. Козьмы Минина,
603005, Российская Федерация, г. Нижний Новгород, Ульянова, 1
skas.99@mail.ru

Аннотация: Ошибки в администрировании системы случаются довольно часто и могут внести необратимые изменения даже в самую хорошую модель безопасности. В данной статье особое внимание уделено наиболее распространенным ошибкам в администрировании, стратегиям определения ошибок и средствам администратора для поиска и устранения ошибок, рассмотрены различные модели поиска ошибок и выявление наиболее оптимальной. Также представлены результаты анкетирования «Модели поиска и устранения ошибок в работе системного администратора» студентов НГПУ им. Козьмы Минина, проведённого в 2020 г.

Проблематика: Образование ошибок, их выявление и устранение является главной проблемой в системном администрировании, которая сопровождает профессию, и неотъемлемой её частью.

Актуальность: Решение проблем, связанных с ошибками в администрировании системы, является неотъемлемой частью в деятельности системного администратора, поскольку данная сфера активно развивается, и происходит постоянное обновление программных систем. Это и приводит к возникновению различных новых ошибок, решение которых требует достаточных временных затрат, и чтобы их минимизировать следует подобрать оптимальную модель действий поиска и устранения ошибок. Правильно подобранная модель действий приведет к положительному решению поставленной задачи.

Ключевые слова: информационная безопасность; системный администратор; устранение ошибок; модель; поиск ошибок; информация; администрирование; информационная система.

Появление ошибок в области администрирования информационных систем - не редкость, что связано с постоянно меняющимися техническими требованиям, обновлениями программного обеспечения, сетевыми перебоями и т.д. [1, 2, 10]. Решением проблем возникновения ошибок и их устранением в администрировании занимается системный администратор - сотрудник, должностные обязанности которого подразумевают обеспечение слаженной работы парка компьютерной техники, сети и программного обеспечения.

Данную тему поднимают многие профессионалы из IT-сферы, такие как Л. Шапиро[10], В.В. Рабданова, И.Б. Елтунова [9], Г.Е. Кокиева, С.Ю. Исхаков [1] и др. Они рассматривают основные процессы администрирования локально-вычислительной сети, выявляют основные этапы обслуживания любого объекта сети, определяют типовые задачи системного администратора, а также пути решения проблем.

В данной работе представлен подбор наиболее оптимальной модели для поиска и решения ошибок, встречающихся в системном администрировании, наиболее распространёнными из которых являются:

1. Наличие права на запись в системный каталог - включает в себя наличие возможности записи в один из каталогов, используемых в файле начальной загрузки. Приводит к тому, что злоумышленник может взломать одну из запускаемых программ, таких как различные драйвера или операционные

оболочки так, чтобы та совершала некоторые несанкционированные действия, например, запоминала пароль, под которым пользователь вошел в систему;

2. Наличие права на чтение sys:system - наличие данного права автоматически приводит к доступности копии файлов базы данных, связок NET$*.OLD, что в результате может привести к прочтению хэш-значения пароля любого пользователя;

3. Регулярное обновление системы - включает в себя регулярные установки, свежие обновления безопасности, которые позволяют предотвратить возможные сбои, потерю данных и прочие неприятные последствия хакерских атак, но некоторые обновления могут нарушить нормальную работу сети;

4. Обязательное включение аудита - данная функция позволяет отслеживать все попытки входа в систему, доступа к файлам, папкам и службе каталогов, но без встроенного аудита проанализировать причины уязвимости системы практически невозможно;

5. Документация всех изменений и исправлений - это систематическое документирование любых проделанных операций, которое значительно облегчает задачу сетевого администратора и его потенциальных преемников, в результате чего минимизируются ошибки лишней проделанной работы [3].

Действия системного администратора всегда направлены на решение технических проблем, но не стоит забывать, что все они базируются на стратегии управления ошибками, которые разбивают сложную задачу идентификации и диагностики на четыре простых подзадачи:

1. Определение ошибки.

2. Генерация тревожного сигнала.

3. Изоляция ошибки.

4. Коррекция ошибки.

Для работы с данными стратегиями применяется две технологии NMS (система управления локальной сетью компании) - пассивная и активная.

Пассивная технология работы NMS оповещает управляющую систему о выполнении заранее предусмотренного и заданного параметрами системы

условия и применяется администратором системы при идентификации проблем, не связанных с аппаратными сбоями.

Активная технология NMS тестирует ИС и опрашивает каждое из устройств на регулярной основе, и если какое-либо устройство не реагирует в заданный системным администратором интервал времени или его параметры отличаются от желаемых, то посылается сообщение администратору системы о сбое устройства.

Системный администратор должен выбрать такую систему управления, которая позволяет использовать обе стратегии. Таким образом, правильно спроектированная система управления дает возможность администратору системы выполнять далее перечисленные логические действия по управлению ошибками:

1. Выбор времени, когда управление ошибками осуществляется полностью, не осуществляется вовсе или осуществляется частично. Если это требование выполняется, то считается, что ошибок нет. Время работы информационной системы определяется в специальном документе - соглашении об уровне сервиса SLA (Service Level Agreement).

2. При настройке системы создаются специальные триггеры, определяющие, какую ситуацию в данной системе следует рассматривать как ошибочную.

3. Настройка времени автоматической перезагрузки системы и переустановки параметров. Можно настроить параметры так, чтобы в определенных случаях система сама перезагружалась и устанавливала определенные параметры в номинальные значения.

4. Установка предупреждений об ошибках [4, 5].

Встроенные средства администрирования не всегда являются удобными, поэтому в помощь системному администратору постоянно разрабатываются программные утилиты, которые направлены на определение и решение проблем, такие как Wireshark, PowerShell ISE, RSAT, инструменты Sysinternals, и др. [7].

Не только утилиты, но и знания большинства технических проблем и стратегий подхода для их решения могут помочь устранить проблему, так как

основная сложность лежит в её поиске. На данном этапе может использоваться базовая модель поиска ошибок каскадного типа, которая представляет собой последовательное выполнение системным администратором определенных действий (рис. 1), к примеру, убедиться в том, что ошибка имеет место быть, провести инвентаризацию, сделать копию информационной системы, сделать перезагрузку всех компонентов, проверить права пользователей, убедиться, что версия программного обеспечения является текущей, собрать информацию об ошибке или ошибках, разработать план по решению проблемы, проверить все гипотезы ее возникновения и задокументировать все действия в специальном журнале [2, 6].

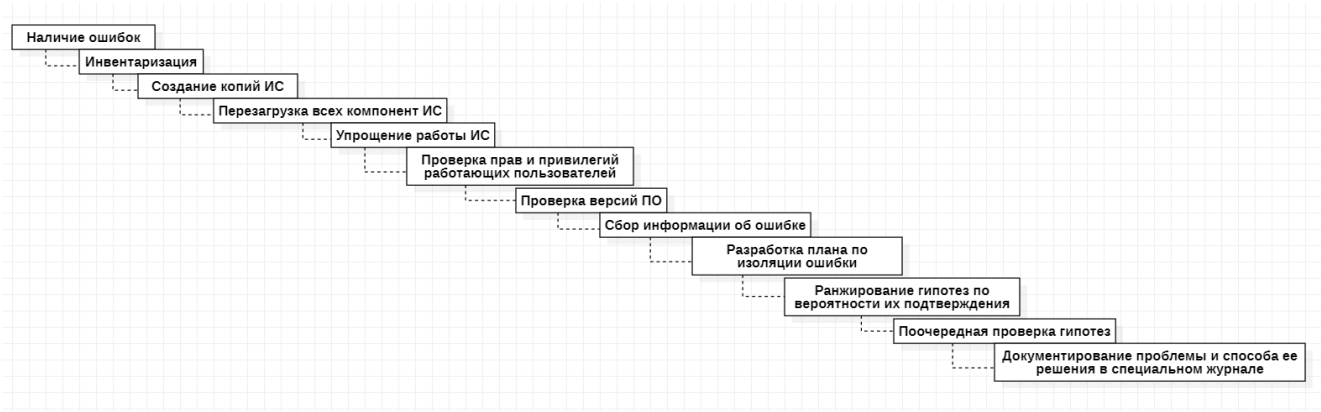


Рис. 1. Каскадная UML-диаграмма «Базовая модель поиска ошибок системного администратора»

Каскадная модель поиска ошибок системного администратора хоть и является базовой, но не единственной. В данной работе также представлены ещё два варианта моделей для поиска ошибок: спиральная модель и поэтапная модель с промежуточным контролем.

Спиральная модель представляет собой процесс, сочетающий в себе как итеративность действий, так и этапность. Спиральная модель поиска ошибок включает в себя: наличие ошибок, создание копий ИС и проверку прав ПО, сбор информации о существующих ошибках, разработку плана по их изоляции и устранению, проверку результата и документирование действий, причем действия повторяются до тех пор пока ошибки не будут устранены (рис. 2).

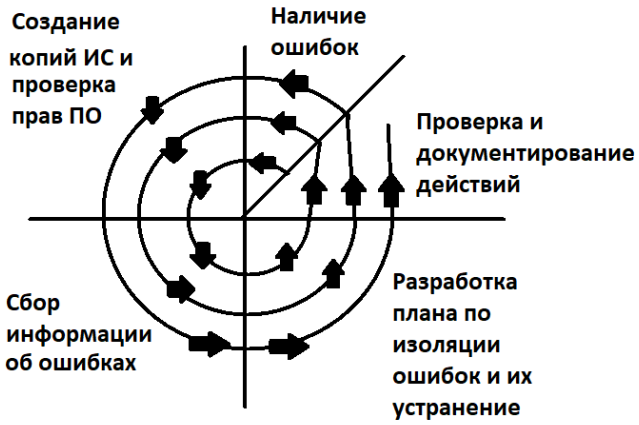


Рис. 2. Спиральная модель «Базовая модель поиска ошибок системного администратора»

Поэтапная модель с промежуточным контролем является развитием каскадной модели, только здесь стрелочки позволяют вернуться на предыдущие этапы для устранения найденных ошибок. Эта модель включает в себя: наличие ошибок, создание копий ИС, проверку прав и версий ПО, сбор информации о существующих ошибках, разработку плана по изоляции и устранению ошибок, проверку результата и документирование (рис. 3).

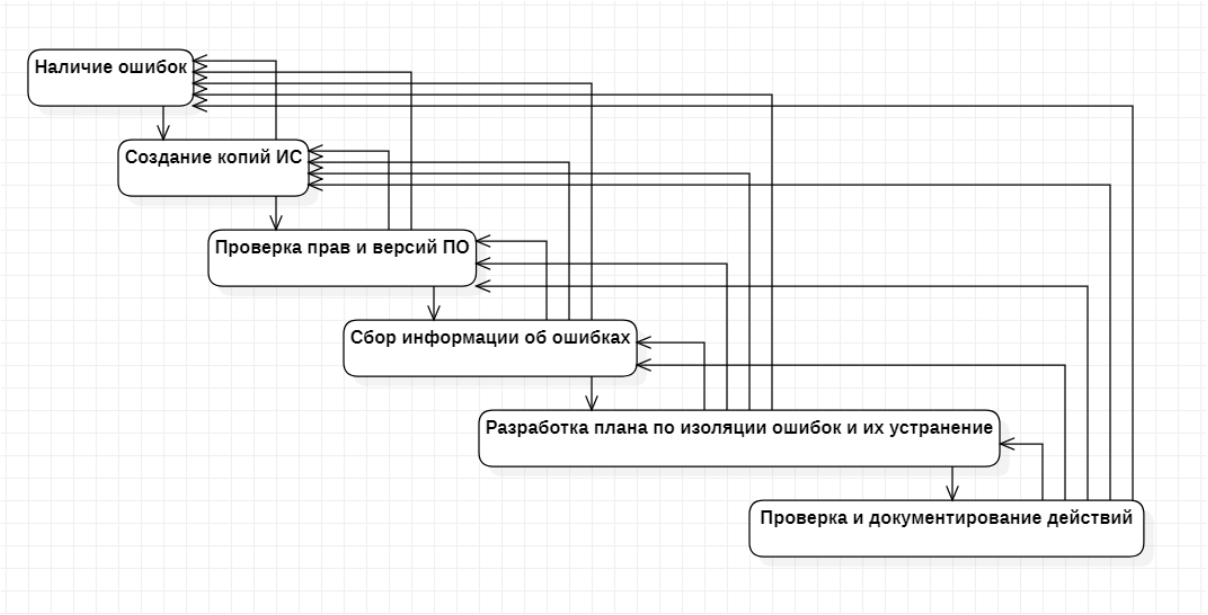
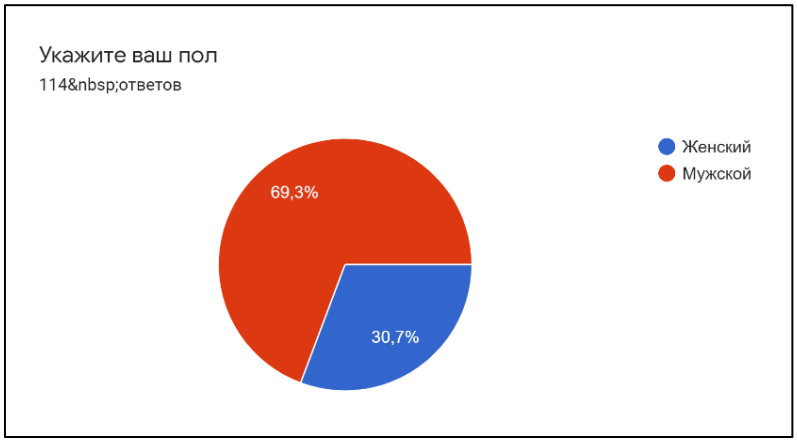


Рис. 3. Поэтапная модель с промежуточным контролем.
UML-диаграмма «Базовая модель поиска ошибок системного администратора»

По данной теме было проведено исследование в виде опроса на тему «Модели поиска и устранения ошибок в работе системного администратора», в котором принимали участие студенты 1-4 курсов НГПУ им. Козьмы Минина. Всего опрос прошли 114 человек, из которых большинство составляли мужчины (69,3%), а остальные женщины – 30,7% (рис. 4).



Источник: составлено авторами
Рис. 4. Пол респондентов опроса на тему «Модели поиска и устранения ошибок в работе системного администратора»

В результате проведенного опроса было важно узнать, связаны ли респонденты с профессией системного администратора или просто сталкивались со схожими проблемами. Второй вопрос звучал так: «Связаны ли вы были с системным администрированием?». Ответы распределились следующим образом:

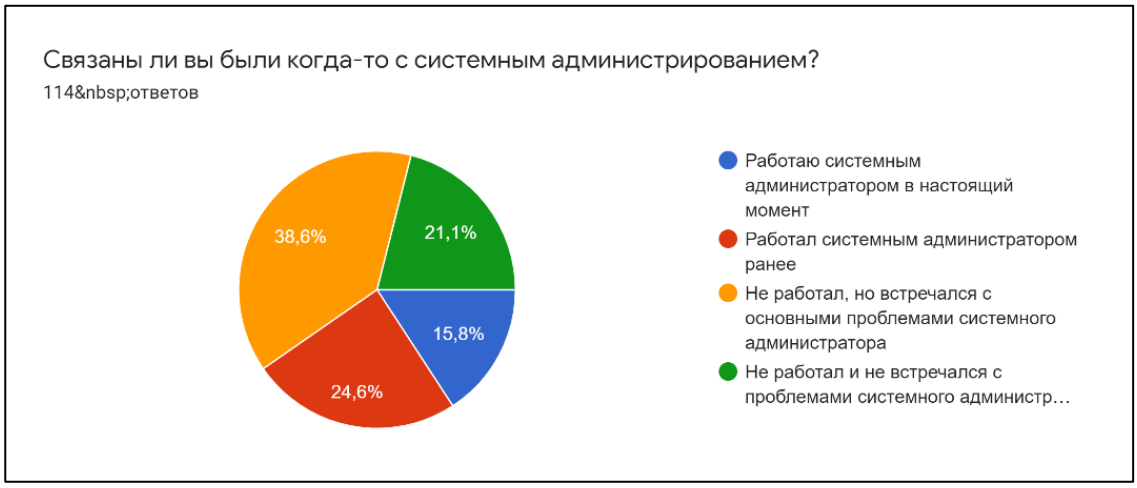
38,6% - не работали, но встречались с основными проблемами системного администратора;

24,6% - уже работали системным администратором ранее;

21,1% - не работали системным администратором и не встречалась с проблемами из данной сферы;

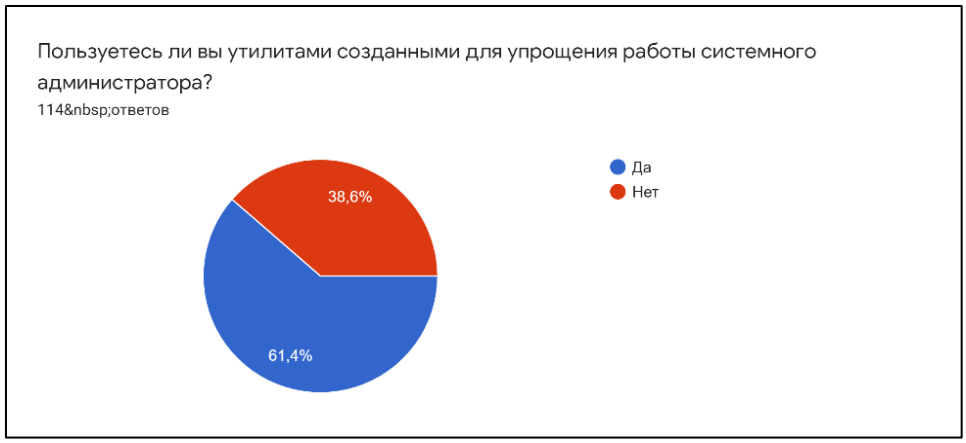
15,8% - работают системным администратором в настоящий момент (что составляет достаточно большой процент среди студентов НГПУ им. Козьмы Минина) (рис. 5).

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru



Источник: составлено авторами
Рис.5. Отношение респондентов к системному администрированию

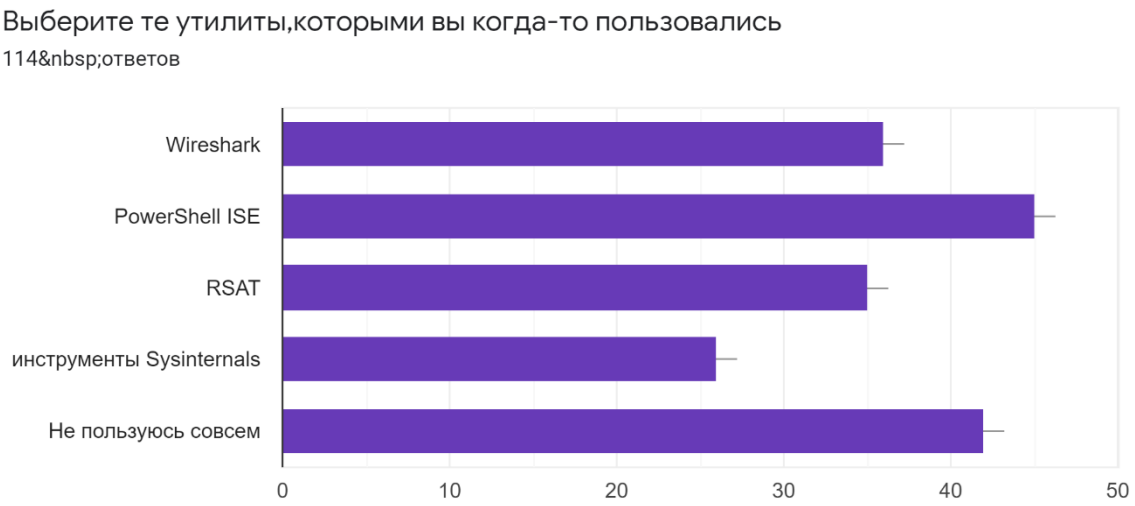
На вопрос «Пользуетесь ли вы утилитами, созданными для упрощения работы системного администратора?» больше половины опрошенных ответили «да» (61,4%), что связано с удобством использования этих программ, так как они ускоряют работу процесса поиска ошибок (рис. 6).



Источник: составлено авторами
Рис. 6. Использование респондентами утилит

Четвертый вопрос формировался из предыдущего: «Выберите те утилиты, которыми вы когда-то пользовались». Самой популярной утилитой является PowerShell ISE - 39,5%, далее идет Wireshark – 31,6%, RSAT - 30,7%, и закрывают этот список инструменты Sysinternals – 22,8% (рис. 7).

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru



Источник: составлено авторами

Рис.7. Соотношение использования популярных утилит

Одним из важных вопросов данного опроса является «Выбор наиболее оптимальной модель поиска ошибок системного администратора для конкретного пользователя». Стоит заметить, что опора идет на каскадную модель, которая является базовой, но не популярной среди пользователей – 16,7%. За ней идёт поэтапная модель с промежуточным контролем – 24,6%, а лидером использования является спиральная модель поиска и устранения ошибок – 58,8% (рис. 8).

Источник: составлено авторами

Рис. 8. Выбор оптимальной модели поиска ошибок

Действительно, спиральная модель по праву является популярной среди системных администраторов, так как включает в себя поэтапный и итерационный подход в поиске и устранение ошибок.

Диагностика и решение ошибок имеет комплексный подход. На поиск и устранение проблем системного администрирования требуется много времени и сил, поэтому задачей современного системного администратора является максимальное сокращение времени и упрощение способов нахождения ошибок [11, 12]. Решение всех этих проблем осуществляет наиболее подходящая модель поиска и устранения ошибок, в результате чего также автоматизируется вся работа предприятия, и решаются проблемы его простоя из-за технических сбоев, связанных с системным администрированием. Стоит также заметить, что все модели действенны, носят практический характер, но подбираются индивидуально под предприятие и сотрудника, решающего возникшие проблемы. Нет проблем, которые нельзя решить, но есть неправильно подобранные методы их решения [9].

Список литературы

1. Исхаков С.Ю. Постановка задачи системного администрирования / С.Ю. Исхаков // Электронные средства и системы управления. Материалы докладов международной научно- практической конференции. 2010. № 2. С. 36-38.

2. Куроуз Д., Росс К. Компьютерные сети / Д. Куроуз, К. Росс // Настольная книга системного администратора. – М.: Эксмо, 2016.

3. Михайлов В.В. Администрирование информационных систем: конспект лекций: учебное пособие / В.В. Михайлов. – Белгород: Изд-во БГТУ, 2017. – 112 с.

4. Олифер В., Олифер Н. Компьютерные сети. – СПб.: Питер, 2017; Фомин Д.В. Компьютерные сети: учеб. пособие. - М.: Директ-Медиа, 2015.

5. Пичужкина Д.Ю., Смекалова Е.С. Роль системного администратора в современном мире // Форум молодых ученых. 2019. № 6(34). С. 908-910.

6. Пичужкина Д.Ю., Смекалова Е.С., Болдин С.В. Роль системного администратора в эпоху облачных технологий // Образование в цифровую эпоху: сборник статей по материалам Международной научно-практической конференции преподавателей, студентов, аспирантов, докторантов и заинтересованных лиц, Нижний Новгород, 10-11 декабря 2019 г. - Н. Новгород, 2019. С. 182-183.

7. Поначугин А.В., Андреянова Л.С. Администрирование локально-вычислительных сетей, пути решения современных проблем // Вестник московского финансово-юридического университета. 2017. № 3. С. 168-174.

8. Поначугин А.В. Мониторинг качества образования как важный фактор подготовки бакалавров в области прикладной информатики // Вестник Мининского университета. 2020. Т. 8. № 1. С. 4.

9. Рабданова В. В., Елтунова И. Б., Кокиева Г. Е. Автоматизация работы системного администратора // Наука и образование сегодня. 2018. № 4 (27). С. 20-24.

10. Шапиро Л., Семь принципов Наполеона для системных администраторов // Системный администратор. 2010. № 10 (95). С. 18-20.

11. Самерханова Э.К., Балакин М.А. Подготовка руководителей профессиональных образовательных программ к работе в условиях цифровой среды вуза // Вестник Мининского университета. 2020. Т. 8. № 2. С. 4. – URL: https://vestnik.mininuniver.ru/jour/article/view/1084/777

12. Хогдал С.Д. Анализ и диагностика компьютерных сетей. – М.: Лори, 2015.

Selection of the optimal model for finding and eliminating errors in the work of the system administrator

Ponachugin Alexander Viktorovich,
candidate of economic sciences, associate professor,
Nizhny Novgorod State Pedagogical University. Kozma Minin,
603005, Russian Federation, Nizhny Novgorod, Ulyanova, 1
sasha3@bk.ru

Pichuzhkina Daria Yurievna,
student,
Nizhny Novgorod State Pedagogical University. Kozma Minin,
603005, Russian Federation, Nizhny Novgorod, Ulyanova, 1
dpichuzhkina@list.ru

Smekalova Ekaterina Sergeevna,
student,
Nizhny Novgorod State Pedagogical University. Kozma Minin,
603005, Russian Federation, Nizhny Novgorod, Ulyanova, 1
skas.99@mail.ru

Errors in system administration are popular and make irreversible changes to even the best security model. This article focuses on the most common errors in administration, strategies for identifying errors and administrative tools for troubleshooting errors, discusses various models for finding errors and identifying the most optimal one. Also, the results of the questionnaire "Models for finding and eliminating errors in the work of a system administrator" of students of the NSPU named after Kozma Minin, held in 2020, are presented.

Problems: The formation of errors, their identification and elimination is the main problem in system administration, which accompanies the profession, and is an integral part of it.

Relevance: Solving problems associated with errors in system administration is an integral part in the activities of a system administrator, since the field is actively developing and there is a constant update of software systems, which leads to the emergence of various new errors, the solution of which leads to sufficient time and in order to minimize them it is necessary to select the optimal model of actions for finding and eliminating errors. A correctly selected action model will lead to a positive solution to the task.

Keywords: information security; System Administrator; elimination of errors; model; search for errors; information; administration; Information system.