УДК 004.08

А.Ю. Атисков

ИСПОЛЬЗОВАНИЕ ОНТОЛОГИЧЕСКОГО ПРОЕКТИРОВАНИЯ ДЛЯ АВТОМАТИЗИРОВАННОГО АНАЛИЗА ДОКУМЕНТОВ ПОЛИТИК БЕЗОПАСНОСТИ ПРЕДПРИЯТИЙ

Атисков А.Ю. **Использование онтологического проектирования для автоматизированного анализа документов политик безопасности предприятий.**
Аннотация. Информационные технологии активно внедряются во все сферы деятельности предприятий, что требует соблюдения определенных правил, обеспечивающих безопасность доступа к данным информационных систем и их сохранность. Такие правила объединяются в политики безопасности, которым присущи свойства противоречивости и двойного толкования. Для нивелирования этих свойств предлагается использовать онтологическую модель политики безопасности.
Ключевые слова: политика безопасности, онтологии, онтологическое проектирование, семантика, анализ противоречий.

Atiskov A.J. **Using ontological design for semi-automatic analysis of enterprise's security policy documents.**
Abstract. Information technologies are actively involved in every activity that requires observation of certain rules to ensure secure access to data information systems and their safety. Such rules are combined in a security policy, which is often full of contradictions and ambiguities. To overcome these troubles author proposes usage an ontological model of security policy. This allows tracking the entire structure of the organization to monitor the distribution of employees' rights to access corporate information, and keep track of how employees can work on the components of the organization. This approach will be useful for companies that have a large staff. Another advantage of ontological model is that it can expand the structure by adding staff and their responsibilities.
Keywords: security policy documents, ontology, ontological model, semantics, analysis of ambiguities.

1. Введение. На сегодняшний день развитие компьютерных технологий идет стремительными темпами. Информационные технологии активно внедряются во все сферы деятельности, они управляют работой кассовых аппаратов, следят за работой автомобильных систем зажигания, ведут учёт семейного бюджета, или просто используются в качестве развлекательного комплекса.

Для того чтобы сохранить в целостности и сохранности данные предприятий необходимо провести анализ структуры организации и определить права доступа каждого сотрудника к ценной информации. На сегодняшний день доступ сотрудников к корпоративной информации осуществляется путем распределения должностных обязанностей руководством компании. Однако бывают ситуации, когда служащие

имеют доступ к той информации, которой пользоваться не должны. Или же наоборот, доступ к какой-либо информации одновременно имеют несколько сотрудников, при отсутствии одного из которых, доступ к информации закрыт. Для того чтобы исключить ошибки в распределении доступа к информации, большинство организаций составляют специальный документ «политику безопасности», которого придерживаются директор компании и специалист по безопасности для обеспечения конфиденциальности корпоративных данных [8]. Для того чтобы исключить ошибки в распределении доступа, необходимо провести анализ политики безопасности.

Политика безопасности – совокупность правил, разрешающих пользователю выполнять операции над объектами. Целью создания политики безопасности является обеспечение защиты персонального компьютера от несанкционированной работы пользователя.

2. Способы описания политик безопасности. Аргументация о соответствии интерпретаций политики безопасности на различных уровнях рассмотрения, так же как и само описание политики безопасности, может быть выражено с использованием следующих методов описания:

1) Естественный язык. К недостаткам данного способа относятся противоречивость и различные интерпретации положений политики безопасности. В связи с возможными противоречиями, вызванными неформальностью метода, в описании политики безопасности должны быть четко определены попытки нарушения безопасности [1].
2) Математическое формальное описание (на основе соответствующей математической модели). Уменьшает противоречивость естественного языка, позволяет использовать средства верификации политики безопасности. К недостаткам данного метода можно отнести сложность описания, что сужает круг людей, понимающих политику безопасности, понижая вероятность того, что политика безопасности будет корректно реализована.
3) Нематематическое формальное описание. Промежуточное решение, наследующее достоинства и недостатки описания с использованием естественного языка и математического формального описания.

Таким образом, политика безопасности может быть разработана и описана с использованием как формального, так и неформального метода.

Для неформальных способов описания политик при разработке информационно-безопасных технологий разграничения доступа широкое распространение получило описание правил доступа субъектов к объектам в виде таблиц, наглядно представляющих правила доступа. Обычно такие таблицы подразумевают, что субъекты, объекты и типы доступа для данной системы заранее определены. Это позволяет составить таблицу в виде одной колонки для различных типов доступа, определенных в системе, и другой колонки, описывающей правила, регламентирующие доступ субъектов к объектам

Описание поддерживающих политик безопасности целесообразно выполнять в форме списков, определяющих соответствующие требования.

Существующие недостатки использования формальных методов сводятся к таким проблемам [2, 6, 7] как:

1) Неразрешимость некоторых проблем безопасности с использованием формальных методов.
2) Использование формальных методов при разработке систем может привести к появлению систем, практическое использование которых весьма неудобно.
3) Использование формальных методов при разработке систем приводит к дорогостоящим и отнимающим много времени проектам.
4) Многие нарушения безопасности происходят вследствие некорректного использования пользователями компьютерных систем; безопасность системы может быть нарушена в результате использования слабого пароля или ошибки реализации.
5) Модели безопасности часто не обеспечивают безопасности реальной системы; безопасность обеспечивается только в рамках формальной модели, которая часто бывает упрощенной; любой выход за пределы модели влечет нарушение безопасности.

Процесс создания онтологий заключается в подготовке чернового варианта, а затем итерационном его уточнении для определения деталей, пока онтология не будет отражать концепцию предметной области с определенной степенью [5, 9]. На практике, создание онтологий включает: определение классов в онтологии; организацию классов в некоторую иерархию (базовый класс и подклассы); определение слотов и их допустимых значений; заполнение значений слотов для экземпляров классов.

В последние годы в качестве языков концептуального моделирования, особенно в реализациях экспериментальных проектов для научных исследований, стал применяться язык RDF [11] вместе с языком запросов SPARQL для доступа к RDF-спецификации предметной области. Совокупность этих языков определяет полнофункциональную (включающую как дескриптивные, так и операционные средства) семантическую модель данных. Более широкому использованию языка RDF для концептуального моделирования будет способствовать осуществляемая в консорциуме W3C разработка нового стандарта описания отображения реляционных данных в RDF [11]. В ряде исследовательских проектов в качестве языка концептуального моделирования стали использоваться также версии языка описания онтологий консорциума W3C - OWL и OWL2.

В конце 2009 года консорциум W3C одобрил продвинутую версию стандарта языка описания онтологий - OWL2. В нем появились полезные новые конструкции, обогащающие выразительные возможности, но не нарушающие, тем не менее, разрешимость и вычислимость в тех рамках, в которых они обеспечивались прежней версией языка. Для OWL2 разработаны его профили OWL2 EL, OWL2 QL и OWL2 RL [4], также одобренные консорциумом. Эти подъязыки OWL2 за счет ограничений его выразительной силы обеспечивают определенные преимущества в аспекте реализации в некоторых конкретных областях применения по сравнению с полным языком.

3. Пример разработки онтологической модели политики безопасности для интернет-магазина. Для того чтобы разработать онтологическую модель политики безопасности необходимо определить классы онтологии организации, то есть определить термины предметной области [3].

Разрабатываемая система должна проанализировать политику безопасности и выявить наиболее критичные места в модели. Для этого выбирается предварительный список терминов в онтологии, далее на основе анализа структуры предприятия и видов деятельности выбираются конкретные классы.

Два базовых понятия - это сотрудники и информация. Каждый сотрудник имеет свой доступ к информации.

Определим классы онтологии, описывающие понятия предметной области. Каждый из классов может иметь свой подкласс, который изображает более подробное описание, чем его надкласс [11].

Общая структура организации представлена на рис. 1.

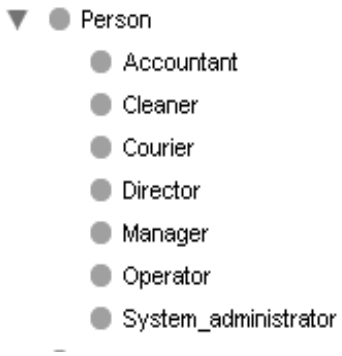

Рис. 1. Общий вид структуры организации интернет магазина.

На данном рисунке изображены все классы сотрудников организации: директор, менеджер, операторы, системный администратор, бухгалтер, курьер и уборщица.

Далее представим классы онтологии – способ хранения и доступ к информации (см. рис. 2).

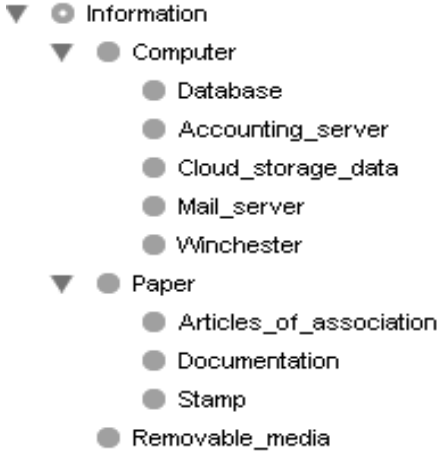

Рис. 2. Общий вид класса: «Способы хранения и доступ к информации».

Здесь изображено три вида носителя информации: бумажный (различные документы, устав компании, печать и т.д.); информация, хранящаяся в компьютерах (на почте, винчестерах, облачное храни-

лище данных) и на электронных носителях (флеш-карты, дискеты).

4. Определение и создание свойств (слотов) и их аспектов (ограничений). Задача слота – описать свойства класса и экземпляра. Свойства дают возможность, утверждать общие факты о членах классов. Свойство - это бинарное отношение. Различают два типа свойств: свойства-значения (отношения между представителями классов и типами данных) и свойства-объекты отношения между представителями двух классов).

Для начала, необходимо определить перечень свойств каждого из классов. Возьмем класс «Директор». Директору разрешено подписание документов (signing documents), управление персоналом (personnel management), решение кадровых вопросов (Personnel matters), организация работы сотрудников (Organization of work of employees), и проводить инструктаж с подчиненными по технике безопасности, правилами работы с клиентами и ведением отчетности (Instructing subordinates safety). Имеет доступ к документации и компьютерам.

Класс «Оператор» проводит прием заявок через интернет (Accepting applications online), прием заявок на товар по телефону (Accepting applications on the phone), проводит консультации клиентов по товару (Assist customers by product) и занимается ведением базы данных клиентов (Maintaining customer database), имеет доступ к компьютерам.

Класс «Менеджер» занимается консультациями клиентов при самовывозе (Assist customers with Pickup) и работой с клиентами при самовывозе товара (Working with clients with Pickup).

Класс «Курьер» занимается приемом оформленных заявок (Admission processing applications), доставкой товара (delivery of goods), отчетом о продаже товара (The report of the sale of goods).

Класс «Бухгалтер» занимается оформлением чеков (Making checks), проводит учет товара (integration product), ведет бухгалтерскую книгу (Maintain ledger), занимается расчетом налогов (tax Preparation), оплатой налогов (Payment of taxes), работой с безналичным расчетом (Working with bank transfer), проведением платежей после согласования с директором (Making payments), а также работой с кассой (Work with cash register).

Класс «Администратор сети» занимается Редактированием (добавление/удаление) товара в интернет-магазине (Edit (add / remove) product in the online store), редактированием сайта (Edit site), проводит контроль безопасности данных компании и сайта (Control of data security company and website), созданием и сменой паролей к серверам,

рабочим компьютерам сотрудников (Creating / changing passwords for servers, desktops, workstations), контролем над переносными устройствами (Control of portable devices), занимается службой безопасности баз данных и обновлением программного обеспечения (software update).

Класс «Уборщица», проводит уборку в помещении, и также может иметь доступ к компьютеру.

Приведем пример того, как может быть реализована угроза неправильного распределения прав доступа сотрудников к корпоративной информации. Например, уборщица, во время проведения уборки помещения, имеет доступ ко всем компьютерам. Она может случайно (или целенаправленно) отключить систему, тем самым запустив возможное обновление программного обеспечения. И вся не сохраненная информация на компьютере будет удалена, что нанесет серьезный ущерб компании.

Для решения данной задачи, создадим новый класс и назовем его «Последствия». Тогда последовательность переходов будет состоять в том, что уборщица, во время уборки помещение, задевает компьютер, тем самым происходит «выключение компьютера», что введет к классу «Последствия». Далее, на следующем этапе, процесс начинается с класса «Последствия» и ведет к «обновлению программного обеспечения». Тем самым, система компьютера обновляется и происходит утеря корпоративной информации.

5. Создание и трансляция запросов. В инструменте онтологического проектирования Protégé [10] существует закладка запросов, при помощи которой получают нужные сведения из созданного проекта по всем экземплярам классов.

Допустим нужно определить, кто имеет право обновить программное обеспечение на компьютерах сотрудников. Для этого в поле Slot выбирается software update и в последнем поле экземпляров выбирается соответствующий экземпляр Computer, после нажатия кнопки Find, результат запроса отобразится в поле Search Results справа (см. рис. 3).

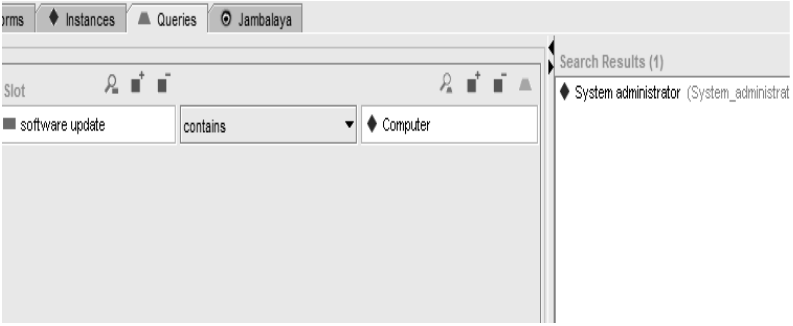

Рис. 3. Создание запроса software update.

Для того чтобы узнать, кто занимается оплатой налогов, в поле Slot выбирается payment of taxes и в последнем поле экземпляров выбирается соответствующий экземпляр Documentation, после нажатия кнопки Find, результат запроса отобразится в поле Search Results справа.

Рассмотрим ситуацию с уборкой помещения, когда уборщица, случайно задевает какой-либо компьютер, тем самым, запуская процесс перезагрузки машины. В поле Slot выбирается turn off и в последнем поле экземпляров выбирается соответствующий экземпляр computer, после нажатия кнопки Find, результат запроса отобразится в поле Search Results справа (см. рис. 4).

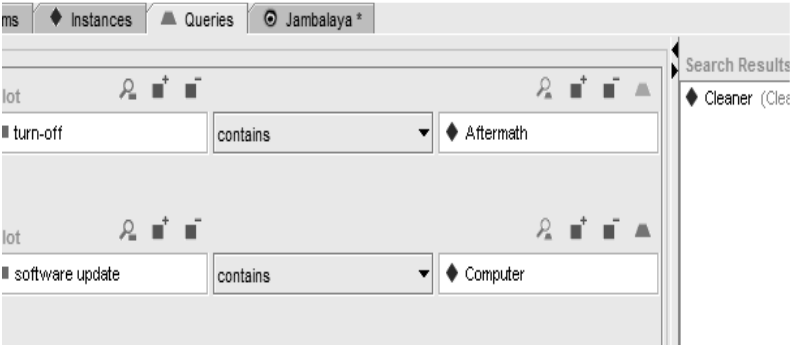

Рис. 4. Создание запроса turn off.

Результат показывает, что в случае ошибки уборщицы есть риск подвергнуться переустановке программного обеспечения, вследствие

чего вся несохраненная корпоративная информация будет удалена.

Чтобы узнать, кто имеет доступ (чтение и запись) к бухгалтерскому серверу выбирается read and change и в последнем поле экземпляров выбирается соответствующий экземпляр Accounting server, после нажатия кнопки Find, результат запроса отобразится в поле Search Results справа (см. рис. 5).

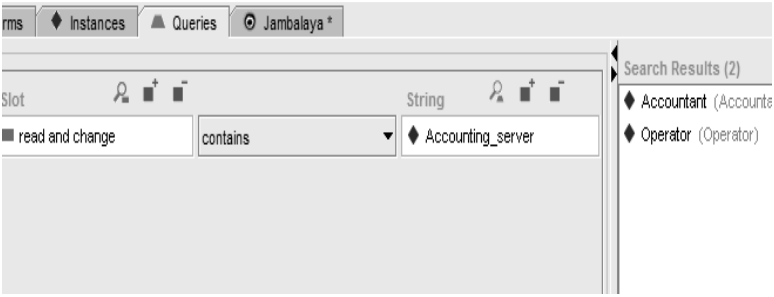

Рис. 5. Создание запроса read and change.

Таким образом, благодаря построенной модели политики безопасности, была найдена ошибка в распределении прав доступа сотрудников к корпоративной информации - оператор может иметь доступ к бухгалтерскому серверу, причем он имеет право чтения и удаления информации, где хранится важная документация. Это ошибка является очень грубой и ее необходимо устранить.

6. Заключение. В результате проделанной работы была разработана онтологическая модель политики безопасности, которая при анализе данного документа, может выявлять ошибки в распределении прав доступа сотрудников к корпоративной информации. Данный проект позволяет прослеживать всю структуру организации, следить за распределением прав доступа сотрудников к корпоративной информации, и отслеживать, как сотрудники могут воздействовать на компоненты организации.

Данный подход будет полезен тем компаниям, которые имеют большой штат сотрудников. Главным преимуществом онтологической модели является то, что при необходимости можно расширить структуру путем добавления сотрудников и их обязанностей, сделав процесс поиска ошибок автоматизированным.

Литература

1. *Анисимов А.В., Марченко А.А.* Система обработки текстов на естественном языке // Искусственный интеллект. 2002. № 4. С. 157–163.

2. *Варлатая С.К., Шаханова М.В.* Анализ методов описания политики безопасности при разработке информационно-безопасных технологий // Аудит безопасности. – 2010. № 1. С. 10–13. // URL: http://www.tusur.ru/filearchive/reports-magazine/2010-1/10-13.pdf (дата обращения: 22.07.2013).
3. *Гладун В.П., Величко В.Ю., Святогор Л.А.* Структурирование онтологии ассоциаций для конспектирования естественно-языковых текстов // Information Science and computing. 2008. № 2. С. 153–159. // URL: http://www.foibg.com/ibs_isc/ibs-02/IBS-02-p20.pdf (дата обращения: 22.07.2013).
4. *Когаловский М.Р.* Системы доступа к данным, основанные на онтологиях // Программирование. Базы данных и базы знаний. 2012. № 4. С. 55–77.
5. *Константинова Н.С., Митрофанова О.А.* Онтология как системы хранения знаний // Всероссийский конкурсный отбор обзорно-аналитических статей по приоритетному направлению "Информационно-телекоммуникационные системы". 2008. 54 с. // URL: http://www.ict.edu.ru/ft/005706/68352e2-st08.pdf (дата обращения: 22.07.2013).
6. *Медведовский И.Д.* Программные средства проверки и создания политики безопасности // URL: http://computerlib.narod.ru/html/policies.htm (дата обращения: 22.07.2013).
7. *Медведовский И.Д.* Программные средства проверки политики безопасности на соответствие требованиям ISO 17799 // URL: http://www.activeaudit.narod.ru/progs.htm (дата обращения: 22.07.2013).
8. *Рэнди Франклин Смит.* Объясняем политику безопасности // Windows IT Pro. – 2006. – № 5. // URL: http://www.osp.ru/win2000/2006/05/2863216 (дата обращения: 22.07.2013).
9. *Noy Natalya, McGuinness Deborah.* Разработка онтологий 101: руководство по созданию вашей первой онтологии // Стэнфордский Университет, Стэнфорд, Калифорния // Stanford Knowledge Systems Laboratory Technical Report KSL-01-05 and Stanford Medical Informatics Technical Report SMI-2001-0880, March 2001 // URL: http://ifets.ieee.org/russian/depository/ontology101_rus.doc (дата обращения: 22.07.2013).
10. *Protégé* Ontology editor and knowledge-base framework // URL: http://protege.stanford.edu/ (дата обращения: 22.07.2013).
11. *RDF* Среда Описания Ресурса // URL: http://www.w3.org/2007/03/rdf_concepts_ru/#dfn-property (дата обращения: 22.07.2013).

Атисков Алексей Юрьевич — к.т.н.; научный сотрудник лаборатории информационно-вычислительных систем СПИИРАН. Область научных интересов: технологии автоматизированной трансформации диаграмм проектирования, OWL-описание предметных областей, метамоделирование информационных систем. Число научных публикаций — 9. atiskov@gmail.com; СПИИРАН, 14-я линия В.О., д. 39, г. Санкт-Петербург, 199178, РФ; р.т. +7(812)328-4369, факс +7(812)328-4450.

Atiskov Alexey Jurievich — Ph.D.; researcher, Laboratory of Computer and Informational Systems, SPIIRAS. Research interests: technologies of semi-automatic system that transforms modelling diagrams, OWL-description of subjects, metamodelling of informational systems. The number of publications — 9. atiskov@gmail.com; SPIIRAS, 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone +7(812)328-4369, fax +7(812)328-4450.

Рекомендовано лабораторией информационно-вычислительных систем СПИИРАН, заведующий лабораторией Воробьев В.И, д.т.н., проф.
Статья поступила в редакцию 10.09.2013.

РЕФЕРАТ

Атисков А.Ю. **Использование онтологического проектирования для автоматизированного анализа документов политик безопасности предприятий.**

Для того чтобы сохранить в целостности и сохранности данные предприятий, необходимо провести анализ структуры организации и определить права доступа каждого сотрудника к ценной информации. На сегодняшний день доступ сотрудников к корпоративной информации осуществляется путем распределения должностных обязанностей руководством компании. Однако бывают ситуации, когда служащие имеют доступ к той информации, которой пользоваться не должны. Или же наоборот, доступ к какой-либо информации одновременно имеют несколько сотрудников, при отсутствии одного из которых, доступ к информации закрыт. Для того чтобы исключить ошибки в распределении доступа к информации, большинство организаций составляют специальный документ «политику безопасности», которого придерживаются директор компании и специалист по безопасности для обеспечения конфиденциальности корпоративных данных. Для того чтобы исключить ошибки в распределении доступа, необходимо провести анализ политики безопасности.

Существующие недостатки использования формальных методов заключаются в неразрешимости некоторых проблем безопасности с использованием формальных методов; использование формальных методов при разработке систем может привести к появлению систем, практическое использование которых весьма неудобно; использование формальных методов при разработке систем приводит к дорогостоящим и отнимающим много времени проектам; многие нарушения безопасности происходят вследствие некорректного использования пользователями компьютерных систем; модели безопасности часто не обеспечивают безопасности реальной системы; безопасность обеспечивается только в рамках формальной модели, которая часто бывает упрощенной; любой выход за пределы модели влечет нарушение безопасности.

Анализ онтологической модели политики безопасности может выявлять ошибки в распределении прав доступа сотрудников к корпоративной информации. Позволяет прослеживать всю структуру организации, следить за распределением прав доступа сотрудников к корпоративной информации, и отслеживать, как сотрудники могут воздействовать на компоненты организации.

Данный подход будет полезен тем компаниям, которые имеют большой штат сотрудников. Главным преимуществом онтологической модели является то, что при необходимости можно расширить структуру путем добавления сотрудников и их обязанностей, сделав процесс поиска ошибок автоматизированным.

SUMMARY

Atiskov A.J. **Using ontological design for semi-automatic analysis of enterprise's security policy documents.**

In order to preserve the integrity and security to enterprise data it is necessary to analyze the structure of the organization and define the access rights of each employee to valuable information. To date, employees access to corporate information distribution is carried out by the company's management duties. However, there are situations where employees have access to the confidential information that they should not. Or conversely, it situation when access to any information should be done simultaneously by several workers in the absence of one of them, access to information is closed. In order to avoid errors in the distribution of access to information, most organizations have special document "security policy", which adhere to the director of the company and an expert on security to ensure the confidentiality of corporate data. In order to avoid errors in the distribution of access, it is necessary to analyze security policies.

Existing deficiencies of using formal methods are to insolubility of some security issues with the use of formal methods, the use of formal methods in the design of systems can lead to the emergence of systems, the practical use of which is very inconvenient, the use of formal methods in the development of systems leads to costly and time-consuming projects, many security breaches occur as a result of incorrect use of users of computer systems, security models often do not provide real security system, security is provided only as part of a formal model, which is often simplified , and anyone going beyond the model entails a breach of security.

Analysis of the ontological model of security policy can detect errors in the distribution of access rights of employees to corporate information. It allows to track the entire structure of the organization, to monitor the distribution of the rights of employees to access corporate information, and keep track of how employees can work on the components of the organization.

This approach will be useful for companies that have a large staff. The main advantage of the ontological model is the fact that it can be expanded by adding staff and their responsibilities by making the process of finding errors automated.