Разработка автоматизированной системы анализа защищенности информационных ресурсов вуза

С.В.Окладникова, Д.Ф.Файзулаев, О.И.Евдошенко, Б.Б.Морозов, Т.А.Жирнова

Астраханский государственный университет

Аннотация: Анализ степени защищенности вуза является трудоемким и сложным процессом, т.к. необходимо анализировать большой объем данных (в т.ч. персональных). При этом возникает сложность в их обработке, т.к. необходимы значительные затраты времени и человеческих ресурсов. Авторами статьи разработан алгоритм расчета оценки уровня защищенности информационных ресурсов на основе коэффициента мощности мер защиты, позволяющий определить насколько адекватно и эффективно применяются реализуемые механизмы защиты информационной системы. Разработанная информационно-логическая модель информационной системы описана с помощью инструментов UML. Описана архитектура, основные классы системы. Предложенное авторами решение по автоматизации процесса проведения анализа защищенности реализовано в виде Web_сервиса. На примере анализа объекта «1С бухгалтерия» рассмотрено представление разработанной информационной системы.
Ключевые слова: информационная система, информационная безопасность, анализ защищенности, информационно-логическая модель, Web-приложение.

Введение

Одной из задач, решаемых вузами в рамках формирования своей информационной политики, является обеспечение безопасности информационных ресурсов. Активное внедрение в образовательную деятельность электронных технологий, а также автоматизация процессов, связанных с организацией научно-исследовательской, проектно-конструкторской и учебной деятельности, приводит к увеличению соответствующих угроз и снижению информационной защищенности вуза, а, следовательно, необходимости управления информационной безопасностью [1].

В вузе хранится служебная, коммерческая, конфиденциальная информация, персональные данные студентов и сотрудников и т.п. Специфика обеспечения безопасности информационных ресурсов обусловлена тем, что вуз – это открытое «предприятие» с большой и непостоянной аудиторией студентов, а также сотрудников, которые могут получать доступ к информационным ресурсам с различным уровнем. При

этом информационные ресурсы могут быть случайно или умышленно подвергнуты негативным воздействиям, что в свою очередь приведет к нарушению информационной безопасности вуза и нанесет ущерб всем участникам образовательного процесса [2].

Управление информационной безопасностью в вузе в т.ч. предполагает разработку мероприятий, направленных на предотвращение негативных воздействия различного вида. Объем и виды данных мероприятий определяются ФСТЭК России, ФСБ России, Роскомнадзором и др.

При создании эффективных механизмов управления информационной безопасностью в вузе, в первую очередь, необходимо провести анализ степени защищенности информационных ресурсов, который позволяет определить адекватность реализованных механизмов безопасности существующим рискам, способность обрабатывать (хранить, передавать) конфиденциальную информацию, уровень защищенности и его достаточность в данной среде функционирования, выявить уязвимости и т.п.

Существующие подходы к автоматизированному анализу защищенности информационных ресурсов

Проведенный авторами статьи обзор существующих подходов анализа защищенности [3,4] показал, что реализуемые методики анализа защищенности включают в себя расчет системы различных метрик защищенности и комплекса правил (формул), используемых для их расчета.

Проведение анализа может выполняться самостоятельно сотрудниками предприятия, специалистами по информационной безопасности, или с привлечением независимых экспертов, т.е. в основе процесса анализа защищенности лежит экспертный опрос и оценка полученных результатов [5].

В процессе проведения анализа защищенности выделяют следующие типовые этапы: определение объекта анализа; сбор сведений об объекте

анализа; классификация объекта анализа; определение требований к определенному классу; определение исходной защищенности объекта анализа; выявление актуальных угроз информационной безопасности; определение реализованных механизмов защиты информации; выработка рекомендаций, предложение механизмов защиты; формирование отчетов.

В качестве объекта анализа, как правило, выступают информационные системы (ИС), в т.ч. обрабатывающие конфиденциальную информацию и персональные данные; различные информационные активы. Сбор сведений об объекте анализа подразумевает составление анкет, опросов для экспертов, в качестве которых выступают специалисты по информационной безопасности. На основе собранных сведений проводится классификация объекта, т.е. определяется уровень защищенности, составляется перечень требований, которые необходимо выполнить. На завершающем этапе результаты анализа структурируются, и предоставляются специалистам в сфере информационной безопасности в виде отчетов в интерактивном режиме или иной документированной форме.

Отличительной особенностью существующих методов анализа защищенности является использование различных математических методов, положенных в основу процедур оценивания рисков. В зависимости от этого они обладают разными возможностями адекватного учета реальных факторов, что в свою очередь, предопределяет точность и надежность полученных оценок риска [6-9].

Процесс анализа защищённости носит циклический характер, т.к. требует проведение периодического мониторинга информационной безопасности: регулярного обновления баз знаний и значений оценки рисков, проверки компетенции персонала, планирования проведения повторных оценок рисков, разработки мер по обеспечению безопасности и т.п.

Рассмотренный подход анализа защищенности, реализуемый на основе существующих методик не предусматривает группировку механизмов защиты, определение применимости реализованных мер защиты и расчет уровня защищенности объекта анализа, которые необходимы для проведения автоматизированного анализа защищенности.

Современный рынок информационных систем в области анализа защищенности широко представлен системами, автоматизирующими решение следующих задач: анализ рисков, оценка соответствия информационной безопасности организации требованиям определенных стандартов и руководящих документов, формирование комплексных решений, обладающих функционалом сканера безопасности с возможностью анализа полученных результатов.

Проведенный анализ показал, что около 20 % программных продуктов ориентированы для использования в банковской сфере, остальные имеют универсальное назначение и применимы в различных областях экономики. Тип лицензии у большинства систем проприетарный (включают демоверсии). Бесплатно распространяются такие системы как Microsoft Security Assessment Tool 4.0, Microsoft Corporation, США и Practical Threat Analysis (PTA), PTA Technologies, Израиль. Не все зарубежные системы анализа защищенности могут использоваться российскими компаниями, т.к. не обеспечивают требования законодательной и нормативной базы в области информационной безопасности РФ. В отечественных программных продуктах реализована возможность проверки соответствия системы защиты организации стандартам.

В большинстве информационных систем формируются рекомендации по повышению защищенности, которые в различных системах отличаются обоснованностью и качеством. Обоснование может быть экономическим или количественно подтверждать эффективность контрмер. Результаты анализа

представляются в виде отчетов, в т.ч. в графическом виде. В некоторых системах используется построение карты сети. В ИС, предусматривающих сбор информации (угроз, уязвимостей, контрмер и т.п.) посредством опросов сотрудников организации, аудиторов, с последующим ее хранением в базе знаний, отсутствует функционал, обеспечивающий сканирование сети для получения необходимой информации. Отсутствует возможность проведения анализа защищенности ИС на этапах их проектирования и дальнейшей эксплуатации.

Алгоритм оценки уровня защищенности информационных ресурсов вуза

Одним из этапов, реализуемых на основании сведений об объекте анализа и группировки реализованных мер защиты, является расчет общего уровня защищенности. Согласно Постановлению Правительства РФ от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» для классификации информационных систем, обрабатывающих персональные данные, применяются 4 уровня защищенности.

При расчете общего уровня защищенности авторами статьи предлагается ввести коэффициент значимости мер, определенный для каждого из уровня защищенности:

K1 = 1 для мер, применимых для 1-го уровня защищенности;

K2 = 0,75 для мер, применимых для 2-го уровня защищенности;

K3 = 0,5 для мер, применимых для 3-го уровня защищенности;

K4 = 0,25 для мер, применимых для 4-го уровня защищенности;

K5 = 0,25 для компенсирующих мер защиты.

Для расчета общего уровня защищенности вычисляется коэффициент мощности мер защиты (M). Например, если после классификации информационной системы определен 4-ый уровень защищенности, то коэффициент мощности рассчитывается по формуле (1):

$$M = \frac{K_1 n_1 + K_2 n_2 + K_3 n_3 + K_5 n_5}{m} \quad (1)$$

где Ki – коэффициенты значимости мер защиты,

ni – число мер каждой из групп,

m – количество коэффициентов значимости, зависящее от оправленного уровня защищенности ($1 \le m \le 4$).

Для каждого последующего уровня защищенности на уровень выше коэффициент для уровня защищенности на уровень ниже и текущего уровня защищенности не вычисляется, кроме коэффициента компенсирующих мер, то есть для 3-го уровня защищенности рассматриваются коэффициенты K1, K2 и K5, 2-го – K1 и K5, 1-го – K5 (рис. 1).

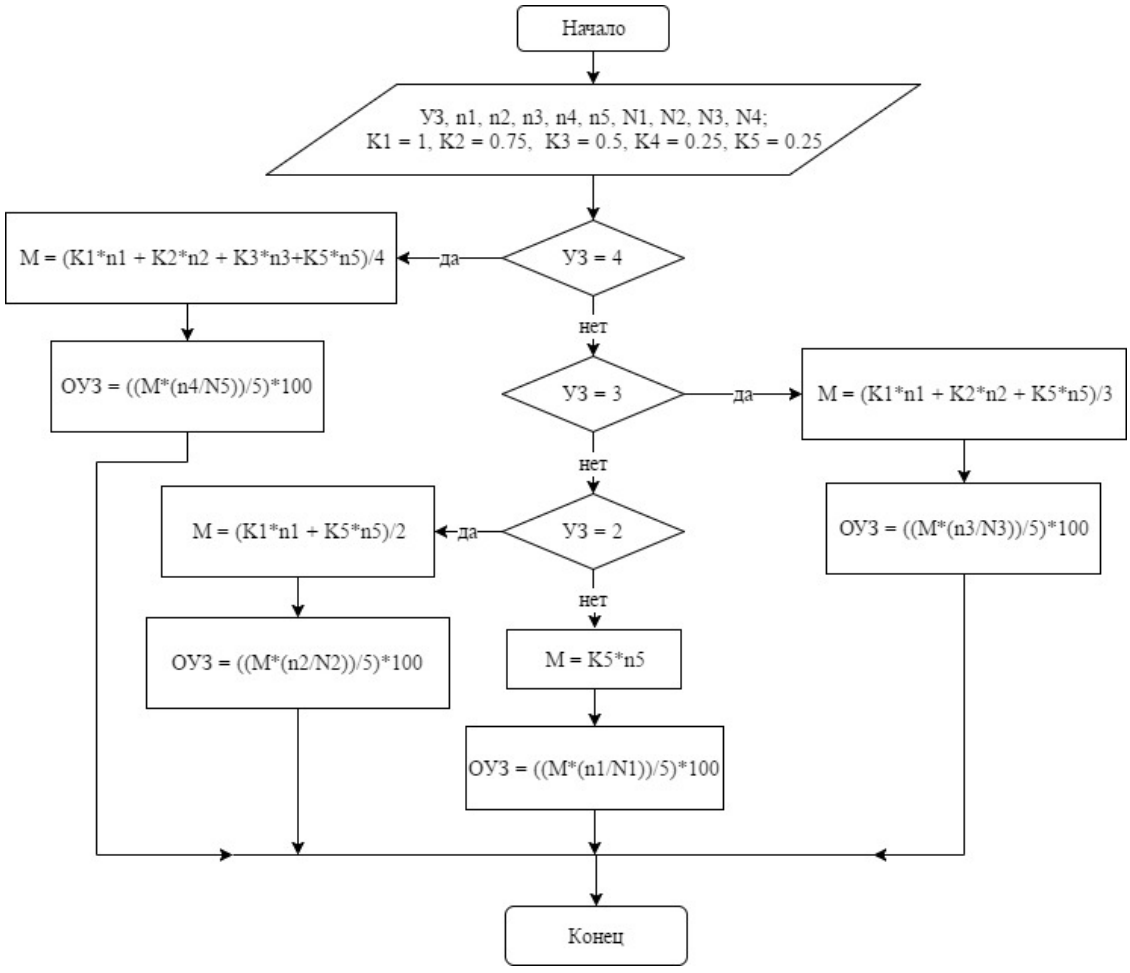

Рис. 1. Блок-схема алгоритма расчета оценки уровня защищенности информационных ресурсов вуза

На заключительном этапе вычисления общего уровня защищенности полученный коэффициент мощности М умножается на процент применяемых мер защиты для определенного «уровня защищенности». Полученная оценка общего уровня защищенности (ОУЗ) носит количественный характер, поэтому необходимо ввести систему ранжирования рассчитанной величины, для перевода в качественную оценку:

если ОУЗ $\leq$ 55%, ОУЗ считается низким;

если 55%< ОУЗ $\leq$ 85%, ОУЗ считается средним;

если ОУЗ > 85%, ОУЗ считается высоким.

Рассмотренный алгоритм оценки общего уровня защищенности определяет насколько адекватно и эффективно применяются все реализуемые механизмы защиты информационной системы, учитывая различные группы мер обеспечения информационной безопасности.

Информационно-логическая модель информационной системы анализа защищенности

Предлагаемое авторами статьи решение по автоматизации процесса проведения анализа защищенности реализовано в виде Web_сервиса. На рисунке 2 с помощью инструментов UML описаны компоненты ИС [10].

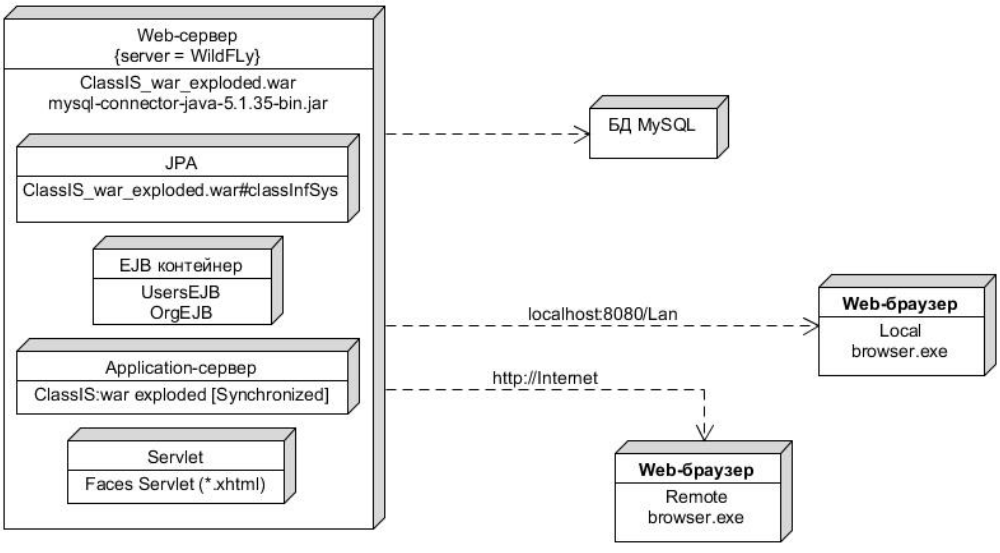

Рис. 2. Диаграмма развертывания

Разработанная ИС развернута на виртуальном сервере приложений «WildFly» версии 10.1.0. Достоинством WildFly является наличие поддержки одиночного отказоустойчивого развёртывания приложения («singleton deployment»), при котором в случае использования группы кластеризованных серверов развёртывание будет произведено только на одном узле, но в случае выхода этого узла из строя, приложение будет автоматически перенесено на другой узел. Реализованные функции настройки внешних подключений позволяют осуществить настройку сервера, таким образом, чтобы пользователи локальной сети могли подключаться к нему с любого автоматизированного рабочего места, в том числе с мобильных устройств, подключенных к сети.

База данных реализована на MySQL. Для быстрого соединения с базой данных и её модификации использована технология «JPA», которая предоставляет возможность сохранять в удобном виде Java-объекты в БД. Информационная система состоит из 7 классов (рис. 3).

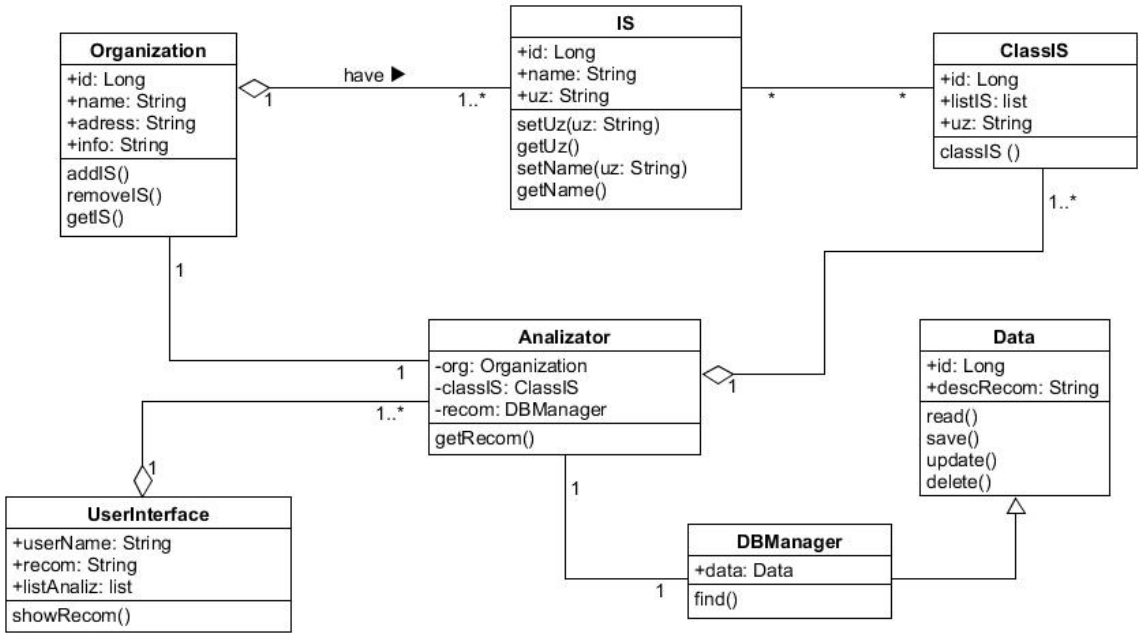

Рис. 3. Диаграмма классов

Класс «Organization» обрабатывает данные об организации, в которой проводится анализ защищенности различных (ИС), в том числе обрабатывающих персональные данные. Работа с сущностью ИС осуществляется с помощью класса «IS», содержащий сведения о ней. Далее данные об ИС получает класс «ClassIS», который классифицирует ее и отправляет сведения в класс «Analizator». Последний указанный класс производит анализ собранных данных, передает информацию классу «UserInteface» для отображения результатов выполнения своей работы. «DBManager» и «Data» позволяют взаимодействовать с базой данных, производя поиск, сохранение и модификацию полученных в ходе анализа сведений. В ИС предусмотрены три группы пользователей:

- администратор системы имеет все права и доступ ко всем страницам и ресурсам системы, обеспечивает управление и мониторинг базы данных;
- пользователь заполняет опросные листы, знакомится с отчетами;
- эксперт (специалист по информационной безопасности) создает формы для проведения опроса, обеспечивает выполнение рекомендаций и т.д.

Для взаимодействия пользователя с ИС анализа защищенности вуза был создан Web-интерфейс, основанный на фреймворке «JSF», а также «PrimeFaces». Данные, полученные системой от пользователя анализируются классами, реализующими основную логику системы, благодаря подходу «EJB» (спецификация технологии написания и поддержки серверных компонентов, содержащих бизнес-логику).

Описание разработанной информационной системы

Информационная система представляет собой набор различных взаимосвязанных модулей, которые после выполнения своей работы передают обработанные данные друг другу.

Модуль формирования и назначения опросных листов позволяет пользователю системы создать новый опросник, заполнить необходимыми

вопросами и ответам, а также направить его для прохождения всем отделам и сотрудникам, выбранным отделам или выбранным сотрудникам организации.

Модуль категорирования вопросов в опросном листе предусмотрен для разбиения вопросов на подгруппы (категории) с целью простого и ясного отображения сформированного опросника для пользователя.

Модуль записи в журнал результатов прохождения опросных листов необходим для просмотра информации о том, кто является автором опросника, когда и кому он направлен, когда и кто его заполнил и отправил. Также данный модуль позволяет ознакомиться с содержимым заполненного опросного листа, то есть с ответами.

Модуль анализа данных обрабатывает полученную информацию, затем выдает результат, в который входят сведения об анализируемой информационной системе, список требований, перечень актуальных угроз информационной безопасности, оценка общего уровня защищенности, рекомендации для повышения полученной оценки.

Модуль формирования отчетов на основе сведений, полученных от вышеописанного модуля, создает документ, в который записывается более подробная информация об анализируемой ИС.

Модуль работы с базой данных позволяет выполнять все манипуляции с записями в базе, добавлять новые записи, а также хранит данные о вопросах для опросных листов, сотрудниках, отделах, пользователях, группах пользователей, анализируемых информационных системах, мерах защиты и угрозах информационной безопасности.

Благодаря такому подходу архитектура системы становится более гибкой, расширяемой и надежной в случае сбоя в работе оного из модулей.

Главное меню ИС содержит следующие пункты: Операции, Анализ данных, База данных, Отчеты. Пункт меню «Операции» реализует функции управления модулями формирования и назначения опросных листов и

категорирования вопросов. Пункт «Базы данных» обеспечивает контроль работы с базой данных.

Рассмотрим работу информационной системы проведем на примере интерфейса пользователя. На рисунке 4 изображена главная страница пользователя, содержащая информацию о назначенных и отправленных (пройденных) опросных листах.

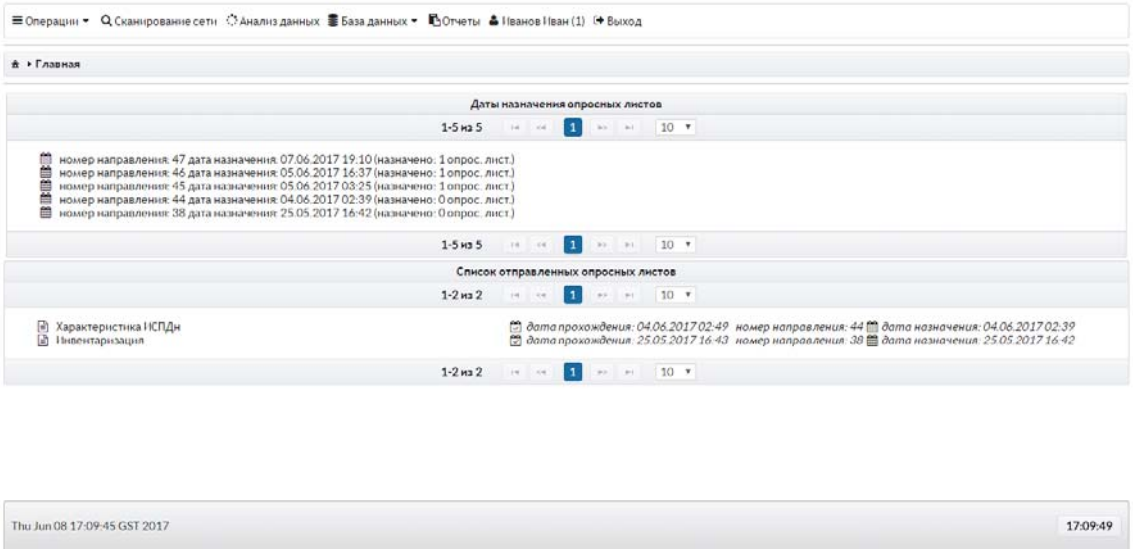

Рис. 4. Главная страница пользователя

Опросный лист содержит 178 вопросов, сгруппированных по категориям: сведения об информационной системе; уровень исходной защищенности; вероятность реализации угрозы; реализация мер защиты информации; определение опасности угроз безопасности защищаемой информации.

Для удобства работы пользователя предусмотрена возможность сохранения промежуточных результатов опроса. Отправление опроса для анализа системе выполняется после того, как пользователь изменит статус опросного листа на «Готов». Результаты анализа защищенности объекта анализа содержат: основные сведения об объекте анализа, требования, актуальные угрозы информационной безопасности, оценку уровня

защищенности, а также рекомендации для повышения определенного уровня (рис. 5).

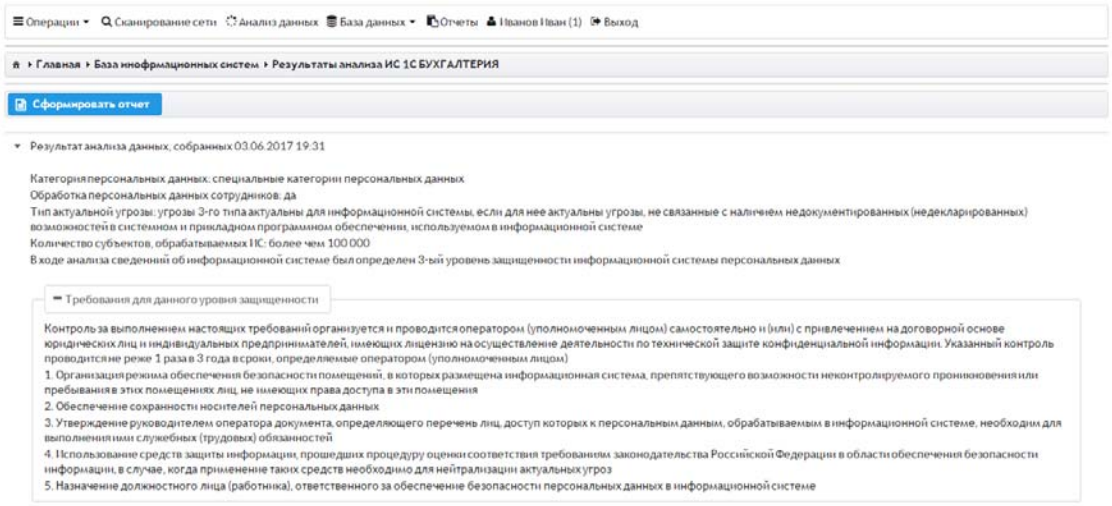

Рис. 5. Форма отчета

Результатом анализа является определение оценки общего уровня защищенности. На рисунке 6 показано, что оценка общего уровня защищенности измеряется в процентах и равна 90 для информационной системы «1С бухгалтерия» на конкретный период времени, то есть общий уровень защищенности рассматриваемой системы является высоким.

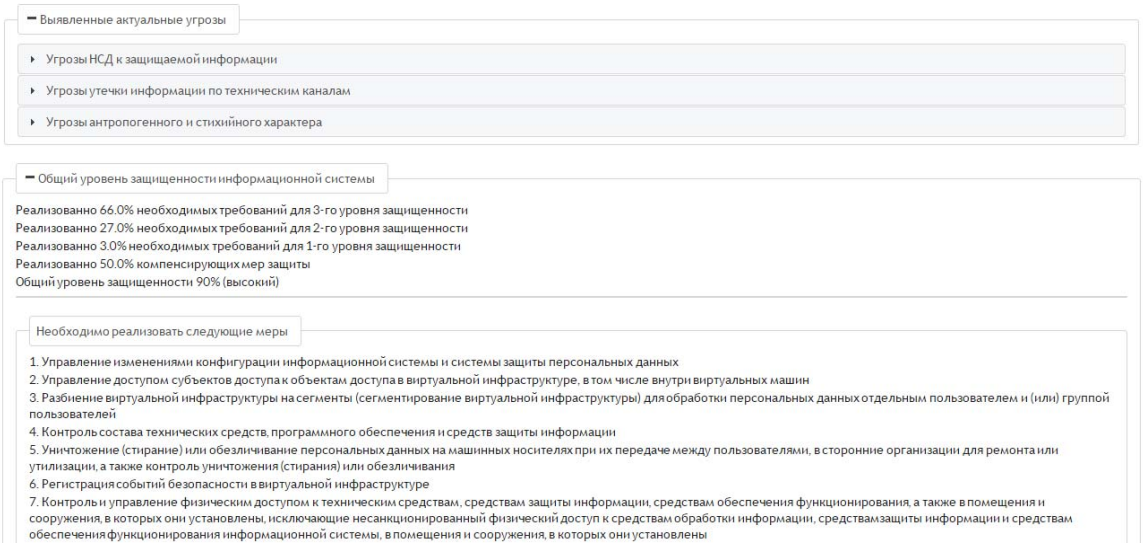

Рис. 6. Итоговый отчет

Согласно постановлению Правительства №1119 необходимо выполнения всех требуемых мер для 3-го уровня защищенности, поэтому

далее система вносит рекомендации, которые нужно применить. Также результаты анализа можно сформировать в отчет и скачать его с сервера в виде документа MS Word.

Заключение

Авторами статьи рассмотрены вопросы актуальности и особенности процесса автоматизации анализа защищенности вуза. Проведен сравнительный анализ существующих аналогов, сформулированы их основные недостатки и предложено решение по автоматизации процесса анализа защищенности, разработан алгоритм расчета оценки уровня защищенности информационных ресурсов на основе коэффициента мощности мер защиты. Предложенный алгоритм оценки общего уровня защищенности позволяет определить насколько адекватно и эффективно применяются все реализуемые механизмы защиты информационной системы, учитывая различные группы мер обеспечения информационной безопасности. Разработанная информационно-логическая модель информационной системы описана с помощью инструментов UML. Описана архитектура и основные классы системы. Предложенное авторами решение по автоматизации процесса проведения анализа защищенности реализовано в виде Web_сервиса. На примере анализа объекта «1С бухгалтерия» рассмотрено представление разработанной информационной системы. В целом, использование информационной системы позволит повысит эффективность проведение анализа защищенности вуза.

Литература

1. Бородина Н.А., Богданова И.Б., Особенности осуществления государственной политики в области информатизации образования в современной России // Инженерный вестник Дона. - 2012. - №1. URL: ivdon.ru/magazine/archive/n1y2012/635.

2. Проталинский О. М., Ажмухамедов И. М., Информационная безопасность вуза // Вестник Астраханского государственного технического университета. - 2009. - №1. - С. 18-23.
3. Оладько В.С., Микова С.Ю., Нестеренко М.А., Технологии защиты интернет- технологий и web-приложений // Международный научный журнал. - 2015. - №8. - С. 81-85.
4. Жукова М.Н., Коромыслов Н.А., Модель оценки защищенности автоматизированной системы с применением аппарата нечеткой логики // Известия ЮФУ. - 2013. - №12. - С. 63-69.
5. Avneet Pannu, M. Survey on Expert System and its Research Areas // International Journal of Engineering and Innovative Technology (IJEIT) // Volume 4, Issue 10, April 2015. – pp. 104 – 108. URL: ijeit.com/Vol%204/Issue%2010/IJEIT1412201504_20.pdf.
6. Пятков А.Г., Лубкин И.А. Оценка уровня защищенности компьютерных сетей при помощи метрик безопасности на основе общего графа // Актуальные проблемы авиации и космонавтики. - 2010. - №6. - С. 396-397.
7. Ажмухамедов И.М., Выборнова О.Н., Формализация понятий приемлемого и толерантного риска // Инженерный вестник Дона. - 2015. - №3. URL: ivdon.ru/uploads/article/pdf/IVD_177_azhmuhamedov_vybornova.pdf_4eae1c0752.pdf.
8. Созинова Е.Н. Применение экспертных систем для анализа и оценки информационной безопасности // Молодой ученый. - 2011. - №10. - С. 64-66.
9. Чусавитин М.О. Использование метода анализа иерархий при оценке рисков информационной безопасности образовательного учреждения. // Фундаментальные исследования. - 2013. - №10. - С. 2080-2084.

10. Documents Associated With Unified Modeling Language (UML) // Object Management Group, Inc. – URL: omg.org/spec/UML/2.4.1/

11. References

1. Borodina N.A., Bogdanova I.B. Inženernyj vestnik Dona (Rus). 2012. №1.
2. Protalinskiy O. M. Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. 2009. №1. pp. 18-23. URL: ivdon.ru/magazine/archive/n1y2012/635.
3. Olad'ko V.S., Mikova S.Yu., Nesterenko M.A. Mezhdunarodnyy nauchnyy zhurnal. 2015. №8.
4. Zhukova M.N., Koromyslov N.A. Izvestiya YuFU. 2013. №12. P. 63-69.
5. Avneet Pannu, M. International Journal of Engineering and Innovative Technology (IJEIT). Volume 4, Issue 10, April 2015. pp. 104 – 108. URL: ijeit.com/Vol%204/Issue%2010/IJEIT1412201504_20.pdf.
6. Pyatkov A.G., Lubkin I.A. Aktual'nye problemy aviatsii i kosmonavtiki. 2010. №6. pp. 396-397.
7. Azhmukhamedov I.M., Vybornova O.N. Inženernyj vestnik Dona (Rus). 2015. №3. URL: ivdon.ru/uploads/article/pdf/IVD_177_azhmuhamedov_vybornova.pdf_4eae1c0752.pdf.
8. Sozinova E.N. Molodoy uchenyy. 2011. №10. pp. 64-66.
9. Chusavitin M.O. Fundamental'nye issledovaniya. 2013. №10. pp. 2080-2084.
10. Documents Associated with Unified Modeling Language (UML) [Electronic resource]. Object Management Group, Inc. UML: omg.org/spec/UML/2.4.1 (free access).