УДК 004.413

ПРОГРАММНОЕ СРЕДСТВО ДЛЯ ПРОВЕДЕНИЯ АУДИТА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ОРГАНИЗАЦИИ

В.А. БОЙПРАВ, В.В. КОВАЛЕВ, Л.Л. УТИН

Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь

Поступила в редакцию 20 февраля 2018

Аннотация. На основе требований к системе защиты информации, представленных в приказе Оперативно-аналитического центра при Президенте Республики Беларусь от 30.08.2013 № 62, и положений СТБ ISO/IEC 27001-2016 составлен перечень вопросов и разработано программное средство, которые могут быть использованы для анкетирования сотрудников организаций при проведении аудита системы защиты информации последних. Представлен порядок использования разработанного программного средства.

Ключевые слова: аудит, защита информации, программное средство.

Abstract. Based on the requirements for the information security system presented in the Order of the Operational and Analytical Center under the President of the Republic of Belarus of August 30, 2013, No. 62 and the provisions of the STB ISO / IEC 27001-2016, the list of issues was drawn up and a software tool developed that can be used to question employees organizations during the audit of information security systems of the latter. The order of using the developed software is presented.

Keywords: audit, information protection, software.

Doklady BGUIR. 2018, Vol. 115, No. 5, pp. 44-49
Software for audit of information protection system of the organization
V.A. Boiprav, V.V. Kovalev, L.L. Utin

Введение

Одна из проблем, возникающих при проведении аудита систем защиты информации, связана с хранением и обработкой больших массивов полученных данных. В связи с этим в настоящее время на основе актуальных методик аудита (COBRA, КОНДОР+, RA Software Tool, CRAMM, MethodWare и др.) разрабатываются программные средства, использование которых способствует сокращению временных затрат на реализацию указанных процессов. Однако данные средства не могут быть использованы для проведения аудита систем защиты информации организаций Республики Беларусь, так как в них не учтены требования национального законодательства. Кроме того, существующие программные средства характеризуются высокой стоимостью.

В настоящей работе предложена методика реализации программного средства для проведения аудита системы защиты информации организаций Республики Беларусь, характеризующегося по сравнению с аналогами более низкой стоимостью.

Методика разработки программного средства

Для разработки программного средства авторами был использован стандартный продукт Visual Studio Code компании Microsoft, который может функционировать на трех

платформах (Linux, OS X и Window), а также сопутствующий дополнительный инструментарий: ASP.NET, NodeJS, Git, Yeoman, Generator-aspnet, Hottowel, Express, Bower, TypeScript, TypeScript.

В основу программного алгоритма заложен перечень вопросов, приведенный в работе [1]. Эти вопросы составлены на основе требований к системе защиты информации, представленных в приказе Оперативно-аналитического центра при Президенте Республики Беларусь от 30.08.2013 № 62 и положений СТБ ISO/IEC 27001-2016. Они касаются аспектов, связанных с соблюдением в организации требований к системе защиты информации, изложенных в указанных документах. Перечень анкетных вопросов, формируемый разработанным программным средством, зависит от класса объектов информатизации, которые эксплуатируются сотрудниками аудируемой организации. Формулировка каждого из вопросов предполагает получение от сотрудника аудируемой организации ответа «Да» или «Нет».

В созданном программном средстве реализована разработанная авторами методика обработки ответов на анкетные вопросы. Эта методика включает в себя следующие шаги [2].

Шаг 1. Отнесение каждого из опрашиваемых сотрудников к определенной группе, в зависимости от стажа его работы в организации. К группе 1 относятся сотрудники, стаж работы которых составляет менее 2 лет (молодые специалисты и вновь принятые сотрудники), к группам 2 и 3 – сотрудники, стаж работы которых соответственно составляет 3–5 лет (знающие специфику предприятия и его проблемы) и более 5 лет (наиболее консервативные).

Шаг 2. Присвоение каждому из ответов определенного абсолютного значения (балла). Величина этого значения зависит от выбранного ответа.

Если ответ на вопрос «Да», то этому ответу присваивается 1 балл.

Если ответ на вопрос «Нет» и, по мнению сотрудника, отнесенного к группе 1, нет необходимости в соблюдении требования к системе защиты информации, описанного в формулировке вопроса, то этому ответу присваивается 0,6 баллов.

Если ответ на вопрос «Нет» и, по мнению сотрудника, отнесенного к группе 2, нет необходимости в соблюдении требования к системе защиты информации, описанного в формулировке вопроса, то этому ответу присваивается 1 балл.

Если ответ на вопрос «Нет» и, по мнению сотрудника, отнесенного к группе 3, нет необходимости в соблюдении требования к системе защиты информации, описанного в формулировке вопроса, то этому ответу присваивается 0,4 балла.

Если ответ на вопрос «Нет» и, по мнению сотрудника, необходимо соблюдать требование к системе защиты информации, описанное в формулировке вопроса, то этому ответу присваивается 0 баллов.

Шаг 3. Обработка результатов, полученных на шаге 2. Она заключается в расчете коэффициента, который равен сумме присвоенных за каждый из ответов баллов, деленной на количество вопросов.

Шаг 4. Качественная оценка результатов анкетирования.

Если в результате расчета, выполненного в рамках шага 3, получен коэффициент, составляющий 0,5 или менее, то делается вывод о том, что уровень защищенности низкий. Величины коэффициента, принадлежащие диапазону от 0,5 до 0,8 или от 0,8 до 1, могут свидетельствовать соответственно о среднем или высоком уровне защищенности.

Блок-схема алгоритма функционирования разработанного программного средства представлена на рис. 1.

На рис. 2 представлено дерево хранилища приложений. Они созданы с помощью Redux. Данные о состоянии приложения хранятся в единой древовидной структуре. Вся необходимая информация о состоянии приложения содержится в одной структуре данных, состоящей из ассоциативных и обычных массивов. Преимуществом данной структуры является возможность отделения состояния приложения от его поведения.

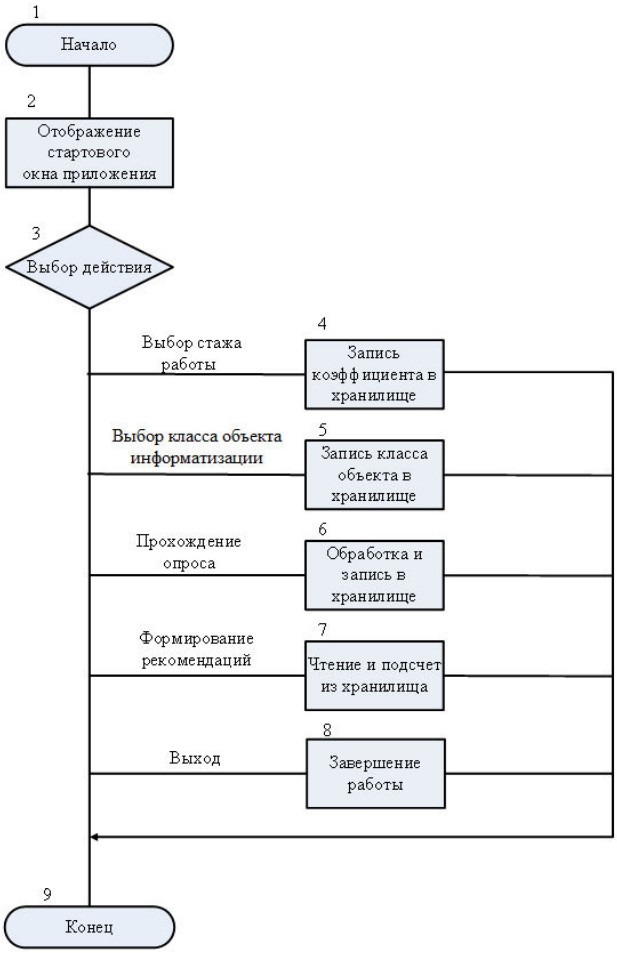

Рис. 1. Блок-схема алгоритма функционирования разработанного программного средства

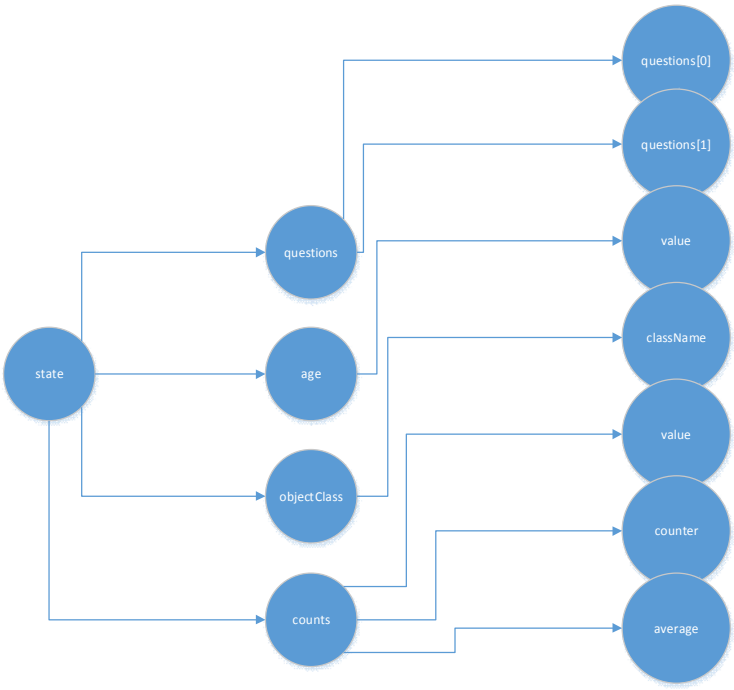

Рис. 2. Дерево хранилища приложения

Инструкция по использованию разработанного программного средства

Перед началом использования программного средства необходимо выполнить установку node. Для этого следует зайти на сайт nodejs.org, далее – на страницу загрузки Node.js. Для установки nodejs для операционной системы Mac OS необходимо выполнить следующие действия:

– открыть терминальное окно;

– ввести команду brew install node;

– дождаться сообщения об успешной установке.

При установке следует принимать стандартные настройки.

После установки следует проверить текущую версию программного обеспечения. Для этого необходимо выполнить команду node –v, и в окне будет выведена информация о версии программного продукта.

Перед запуском программного средства необходимо установить зависимости. Для этого следует выполнить команду npm install. При отсутствии ошибок установки в консольном окне появится соответствующая информация. Для запуска установленного программного средства необходимо ввести команду npm run webpack-dev. В результате выполнения этой команды в консольном окне появится соответствующая информация (рис. 3).

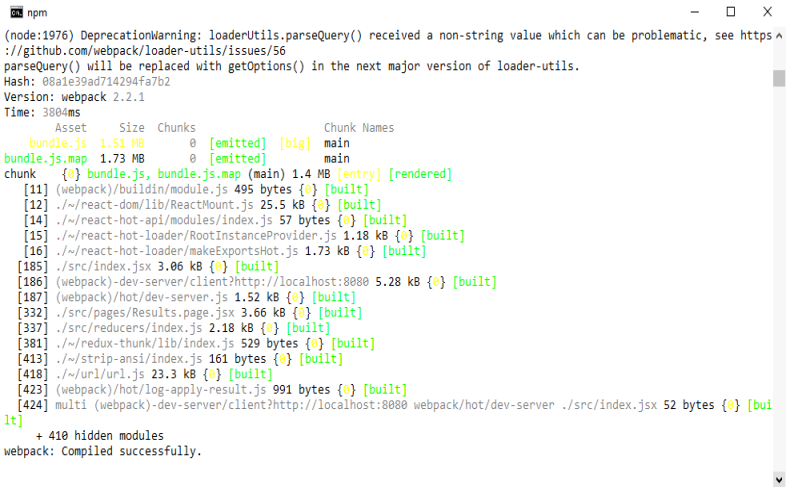

Рис. 3. Окно терминала операционной системы Mac OS (информации о запуске программы)

После выполнения команды npm run webpack-dev программное средство станет доступным для использования с целью анкетирования. Его следует открыть в браузере по адресу localhost:8080, где находится его главная страница (рис. 4).

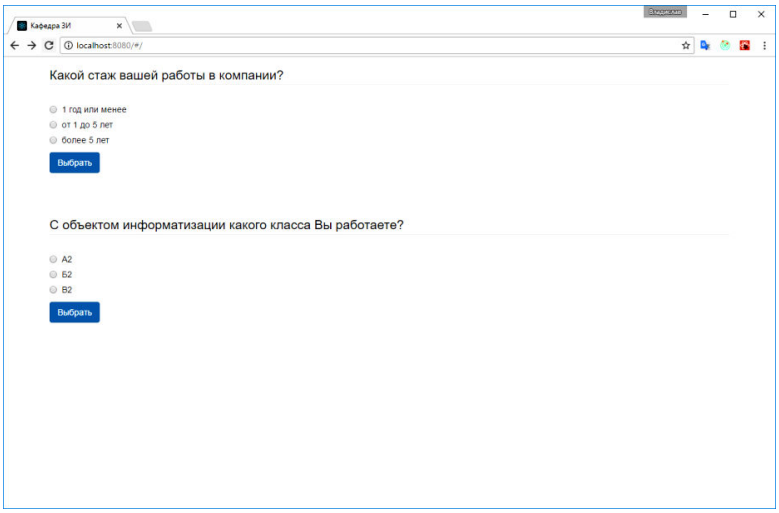

Рис. 4. Внешний вид главной страницы программного средства

Перечень анкетных вопросов формируется после того, как сотрудник укажет стаж своей работы в аудируемой организации и класс объекта информатизации, который он эксплуатирует в ходе выполнения своих должностных обязанностей (рис. 5).

После прохождения опроса пользователь должен нажать кнопку «Закончить», после чего происходит переход на страницу, на которой представлены сведения об уровне защиты информации и рекомендации по его повышению.

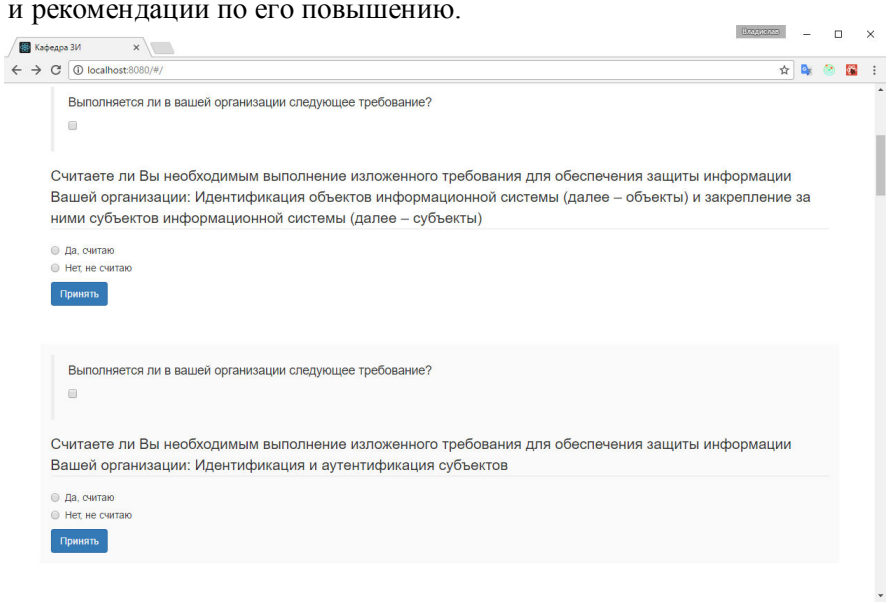

Рис. 5. Внешний вид страницы с перечнем вопросов

Заключение

Разработанное программное средство характеризуются более низкой стоимостью по сравнению с аналогами ввиду следующих его свойств:

1. Простота запуска и настройки.
2. Независимость от типа операционной системы.
3. Возможность получения доступа как через локальную сеть, так и посредством туннельного подключения VPN.

Указанные свойства избавляют аудитора или сотрудников аудируемой организации от необходимости выполнения ручной установки, а руководителя этой организации – от необходимости предоставления отдельного помещения для проведения аудита и закупки дополнительного оборудования для этих целей. В разработанном программном средстве имеется возможность редактирования вопросов для проведения аудита и изменения значения весового коэффициента, зависящего от стажа работы сотрудника. Предусмотрена возможность изменения графического интерфейса программного обеспечения, вне зависимости от устройства, на котором происходит анкетирование сотрудников в аудируемого предприятия.

Применение разработанного программного средства позволяет существенно сократить время и материальные затраты на проведение аудита.

Список литературы

1. Бойправ В.А., Утин Л.Л., Ковалев В.В. Особенности анкетирования сотрудников организаций электросвязи при проведении аудита системы менеджмента защиты информации // Тез. докл. XV Белорус.-рос. науч.-техн. конф. «Технические средства защиты информации». Минск, 6 июня 2017 г. С. 13–14.
2. Бойправ В.А., Утин Л.Л. Методика обработки результатов аудита системы менеджмента защиты информации организаций электросвязи // Материалы XXII междунар. науч.-техн. конф. «Современные средства связи». Минск, 19–20 окт. 2017 г. С. 276–277.

References

1. Bojprav V.A., Utin L.L., Kovalev V.V. Osobennosti anketirovanija sotrudnikov organizacij jelektrosvjazi pri provedenii audita sistemy menedzhmenta zashhity informacii // Tez. dokl. XV Belorus.-ros. nauch.-tehn. konf. «Tehnicheskie sredstva zashhity informacii». Minsk, 6 ijunja 2017 g. S. 13–14.
2. Bojprav V.A., Utin L.L. Metodika obrabotki rezul'tatov audita sistemy menedzhmenta zashhity informacii organizacij jelektrosvjazi // Materialy XXII mezhdunar. nauch.-tehn. konf. «Sovremennye sredstva svjazi». Minsk, 19–20 okt. 2017 g. S. 276–277.

Сведения об авторах

Бойправ В.А., аспирант кафедры защиты информации Белорусского государственного университета информатики и радиоэлектроники.

Ковалев В.В., разработчик программного обеспечения ИООО «ЭПАМ Системз».

Утин Л.Л., к.т.н., доцент, начальник кафедры связи Белорусского государственного университета информатики и радиоэлектроники.

Information about the authors

Boiprav V.A., PG student of information security department of Belarusian state university of informatics and radioelectronics.

Kovalev V.V., software developer of «EPAM Systems».

Utin L.L., PhD, Associate Professor, head of the communications department of the Belarusian state university of informatics and radioelectronics.

Адрес для корреспонденции

220013, Республика Беларусь,
Минск, ул. П. Бровки, 6,
Белорусский государственный
университет информатики и радиоэлектроники
тел. +375-33-602-78-88;
e-mail: name_abs@rambler.ru
Бойправ Владимир Андреевич

Address for correspondence

220013, Republic of Belarus,
Minsk, P. Brovka st., 6,
Belarusian state university
of informatics and radioelectronics
tel. +375-33-602-78-88;
e-mail: name_abs@rambler.ru
Boiprav Vladimir Andreevich