Check for updates

УДК 004.422
https://doi.org/10.37661/1816-0301-2022-19-4-42-52

Оригинальная статья
Original Paper

Методика и программное средство для проведения аудита систем менеджмента информационной безопасности

В. А. Бойправ[1]✉, Л. Л. Утин[2]

[1]*Национальный центр современных искусств Республики Беларусь, ул. Некрасова, 3, Минск, 220040, Беларусь*
✉*E-mail: name_abs@rambler.ru*

[2]*Белорусский государственный университет информатики и радиоэлектроники, ул. П. Бровки, 6, Минск, 220013, Беларусь*

Аннотация

Цели. Исследование проводилось с целью классификации показателей безопасности информационных систем (ИС) и создания на основе полученных результатов методики усовершенствования ранее разработанного программного средства для проведения аудита систем менеджмента информационной безопасности в организациях Республики Беларусь.

Методы. В ходе разработки и усовершенствования программного средства с помощью метода системно-информационного анализа были определены подходы к его реализации с использованием следующих возможностей: организации анкетирования руководителей подразделений и служб, специалисты которых работают с ИС, предназначенными для обработки не отнесенной к государственным секретам информации, распространение и (или) предоставление которой ограничено; оценки уровня соответствия системы защиты информации ИС организации требованиям, установленным законодательством Республики Беларусь и другими национальными нормативными правовыми актами; систематизации рекомендаций по повышению уровня соответствия системы защиты информации ИС организации установленным требованиям.

Результаты. По результатам апробации разработанного и усовершенствованного программного средства установлено, что его использование позволяет на 20–30 % сократить финансирование затрат на реализацию процесса проведения аудита систем менеджмента информационной безопасности организации.

Заключение. Разработанное и усовершенствованное программное средство по сравнению с аналогами характеризуется пониженной стоимостью ввиду следующих его свойств: простоты запуска и настройки; независимости от типа операционной системы; возможности организации как локального, так и удаленного доступа к нему. Разработанное и усовершенствованное программное средство было апробировано в филиале «Междугородная связь» РУП «Белтелеком».

Ключевые слова: аудит системы менеджмента, информационная безопасность, информационная система, показатели безопасности, программное средство

© Бойправ В. А., Утин Л. Л., 2022

Для цитирования. Бойправ, В. А. Методика и программное средство для проведения аудита систем менеджмента информационной безопасности / В. А. Бойправ, Л. Л. Утин // Информатика. – 2022. − Т. 19, № 4. – С. 42–52. https://doi.org/10.37661/1816-0301-2022-19-4-42-52

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

Поступила в редакцию | Received 26.10.2022
Подписана в печать | Accepted 18.11.2022
Опубликована | Published 29.12.2022

Methodology and software development for auditing information security management systems

Vladimir A. Boiprav[1]✉, Leonid L. Utin[2]

[1]National Center for Contemporary Arts of the Republic of Belarus,
st. Nekrasova, 3, Minsk, 220040, Belarus
✉E-mail: name_abs@rambler.ru

[2]Belarusian State University of Informatics and Radioelectronics,
st. P. Brovki, 6, Minsk, 220013, Belarus

Abstract

Objectives. Classification of information systems (IS) security indicators and the creation of the method of improved software tool based on its results (in comparison with similar software tool developed earlier by the authors) for auditing information security management systems of organizations in the Republic of Belarus.

Methods. During the development and improvement of the software tool using the method of system-information analysis and the approaches to its implementation were identified based on following capabilities: organization of questionnaires of heads of departments and services whose specialists work with IS designed to information processing not classified as state secrets or IS with limited dissemination; assessment of the level of compliance of the organization's IS information protection system with the requirements established by the legislation of the Republic of Belarus and other national regulatory legal acts; systematization of recommendations for improving the level of compliance of the organization's IS protection system with the established requirements.

Results. Based on the results of the developed improved software tool approbation, it was found that the use of this tool makes it possible to reduce by 20–30 % the financing of costs for the implementation of the auditing the information security management systems of an organization.

Conclusion. The developed improved software tool, compared to analogues, is characterized by reduced cost due to the following properties: ease of launch and configuration; independence from the type of operating system; the possibility of organizing both local and remote access. The developed improved software tool was tested in the branch "Long-Distance Communication Branch" of RUE "Beletelecom".

Keywords: management system audit, information security, information system, security indicator, software tool

For citation. Boiprav V. A., Utin L. L. *Methodology and software development for auditing information security management systems*. Informatika [*Informatics*], 2022, vol. 19, no. 4, pp. 42−52 (In Russ.).
https://doi.org/10.37661/1816-0301-2022-19-4-42-52

Conflict of interest. The authors declare of no conflict of interest.

Введение. Обеспечение информационной безопасности в организациях должно осуществляться согласно Концепции информационной безопасности Республики Беларусь, утвержденной постановлением Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1. Одной из ключевых задач в достижении этой цели является проведение мониторинга, анализа и оценки состояния информационной безопасности, т. е. регулярный аудит систем менеджмента информационной безопасности (СМИБ).

Для сокращения временных и материальных затрат на проведение аудита СМИБ, а также для автоматизации этого процесса авторами настоящей статьи в 2018 г. было разработано программное средство [1], которое позволяет оценить уровень соответствия системы защиты информации (СЗИ) ИС организации требованиям, изложенным в приказе Оперативно-аналитического центра при Президенте Республики Беларусь от 30 августа 2013 г. № 62 «О некоторых вопросах технической и криптографической защиты информации», и систематизировать рекомендации по улучшению СЗИ. Данный приказ утратил значение в силу приказа Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66 «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449» с изменениями и дополнениями, утвержденными приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 12 ноября 2021 г. № 195, что сделало неактуальным ранее разработанное программное средство.

Цель исследования, результаты которого представлены в настоящей статье, состояла в классификации показателей безопасности ИС, утвержденных приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66, и создании на основе результатов такой классификации методики разработки усовершенствованного программного средства (по сравнению с программным средством, представленным в работе [1]) для проведения аудита СМИБ организаций Республики Беларусь.

Методика разработки программного средства. Усовершенствованное программное средство должно обеспечивать следующие возможности для аудитора СМИБ:

– проведение анкетирования руководителей подразделений и служб [2, 3], специалисты которых работают с ИС, предназначенными для обработки не отнесенной к государственным секретам информации, распространение и(или) предоставление которой ограничено (далее – руководители подразделений и служб);

– оценку уровня соответствия СЗИ ИС организации требованиям, изложенным в Положении о порядке технической и криптографической защиты информации в ИС, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, утвержденном приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66 с изменениями и дополнениями, утвержденными приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 12 ноября 2021 г. № 195 (далее – Положение);

– систематизацию рекомендаций по повышению уровня соответствия СЗИ ИС организации требованиям, изложенным в Положении.

Реализация возможности проведения анкетирования руководителей подразделений и служб. Контрольные листы, предназначенные для анкетирования руководителей подразделений и служб, должны включать в себя вопросы, сформулированные на основе представленного в Положении перечня требований к СЗИ, подлежащих включению в частное техническое задание или задание по безопасности на ИС. Эти требования, по сути, определяют показатели безопасности информации, обрабатываемой с помощью таких ИС.

Так как анкетирование руководителей подразделений и служб направлено на установление факта выполнения (невыполнения) изложенных в Положении требований, то количество вопросов, ответы на которые необходимо получить от указанной категории лиц, составляет более 50 (по количеству требований). В целях оптимизации и структурирования данного процесса в ходе разработки усовершенствованного программного средства была выполнена следующая последовательность действий:

1. Показатели безопасности условно разделены на два класса: общие и частные.

При этом были использованы следующие наименования общих показателей:

– «реализация организационных мер по защите информации» (показатель 1);

– «использование средств технической и криптографической защиты информации» (показатель 2);

– «обеспечение защиты информации в виртуальной инфраструктуре» (показатель 3);

– «обеспечение защиты информации, передаваемой по каналам связи» (показатель 4);

– «обеспечение защиты системы защиты информации» (показатель 5).

Каждый из общих показателей безопасности информации, обрабатываемой в ИС, соответствует определенному виду мероприятий по обеспечению безопасности информации, реализуемых в рамках такой системы.

Информация, обрабатываемая в ИС аудируемой организации, может характеризоваться как всеми, так и некоторыми из указанных общих показателей безопасности в зависимости от класса такой системы. В частности, в ИС классов 4-ин, 4-спец и 4-бг обрабатываемая информация характеризуется показателями 1, 2 и 5; классов 4-юл, 4-дсп – показателями 1, 2, 3, 5; классов 3-ин, 3-спец, 3-бг, 3-юл, 3-дсп – показателями 1–5.

2. Каждому из общих показателей безопасности поставлен в соответствие уникальный набор частных показателей безопасности. С помощью последних может быть установлена степень полноты выполнения требований, определяющих общие показатели безопасности информации, обрабатываемой в ИС аудируемой организации.

3. Разработаны восемь контрольных листов для анкетирования руководителей подразделений и служб.

Контрольный лист 1 включает в себя один вопрос и перечень вариантов ответов на него. По результатам ответов можно установить класс ИС, с которым работают организации электросвязи.

Контрольный лист 2 включает в себя пункты для выбора, по результатам которого можно выполнить следующие действия:

– установить, какие из мероприятий, соответствующих общим показателям безопасности информации, реализуются в рамках ИС аудируемой организации;

– сгенерировать на основе контрольных листов 3–7 пункты для выбора в виде перечня частных показателей безопасности информации, соответствующих выбранным общим показателям безопасности информации.

Содержание контрольного листа 2 зависит от ответа на вопрос из контрольного листа 1. Предложены три вида контрольного листа 2 (табл. 1). На рис. 1 представлен алгоритм проведения анкетирования с помощью контрольного листа 1, который отражает взаимосвязь между ответом на вопрос из контрольного листа 1 и выбором вида контрольного листа 2.

Разработанные авторами контрольные листы 3–8 включают в себя пункты для выбора, по результатам которого можно установить уровень соответствия ИС аудируемой организации требованиям, определяющим частные показатели безопасности информации, обрабатываемой с помощью этой системы. Содержание рассматриваемых контрольных листов представляет собой совокупность модулей, номенклатура которых зависит от выбранного ответа на вопрос из контрольного листа 1, т. е. от класса ИС, а также от номенклатуры выбранных пунктов в контрольном листе 2.

Обобщенный алгоритм проведения анкетирования, отражающий взаимосвязь между выбором пунктов из контрольного листа 2 и выбором модулей для формирования контрольных листов 3–8, показан на рис. 2, где используются следующие обозначения: N – номер вида контрольного листа $(N \in \{1, 2, 3\})$; M – номер пункта для выбора в контрольном листе $(M \in \{1, 2, 3\} \mid N = 1;\ M \in \{1, 2, 3, 4\} \mid N = 2;\ M \in \{1, 2, 3, 4, 5\} \mid N = 2)$; L – номер формируемого контрольного листа $(L \in \{3, 4, 5, 6, 7, 8\})$, который зависит от выбранного варианта ответа на вопрос из контрольного листа 1.

Таблица 1
Содержание трех видов контрольного листа 2
Table 1
Contents of the three kinds of checklist 2

Вид контрольного листа *Checklist kind*	Содержание *Content*
Вид 1	Выберите реализуемые на Вашем предприятии разновидности мероприятий по защите информации, обрабатываемой в информационной системе. Реализация организационных мер по защите информации (вариант 1.1). Использование средств технической и криптографической защиты информации (вариант 1.2). Обеспечение защиты системы защиты информации (вариант 1.3)
Вид 2	Выберите реализуемые на Вашем предприятии разновидности мероприятий по защите информации, обрабатываемой в информационной системе. Реализация организационных мер по защите информации (вариант 2.1). Использование средств технической и криптографической защиты информации (вариант 2.2). Обеспечение защиты информации в виртуальной инфраструктуре (вариант 2.3). Обеспечение защиты системы защиты информации (вариант 2.4)
Вид 3	Выберите реализуемые на Вашем предприятии разновидности мероприятий по защите информации, обрабатываемой в информационной системе. Реализация организационных мер по защите информации (вариант 3.1). Использование средств технической и криптографической защиты информации (вариант 3.2). Обеспечение защиты информации в виртуальной инфраструктуре (вариант 3.3). Обеспечение защиты информации, передаваемой по каналам связи (вариант 3.4). Обеспечение защиты системы защиты информации (вариант 3.5)

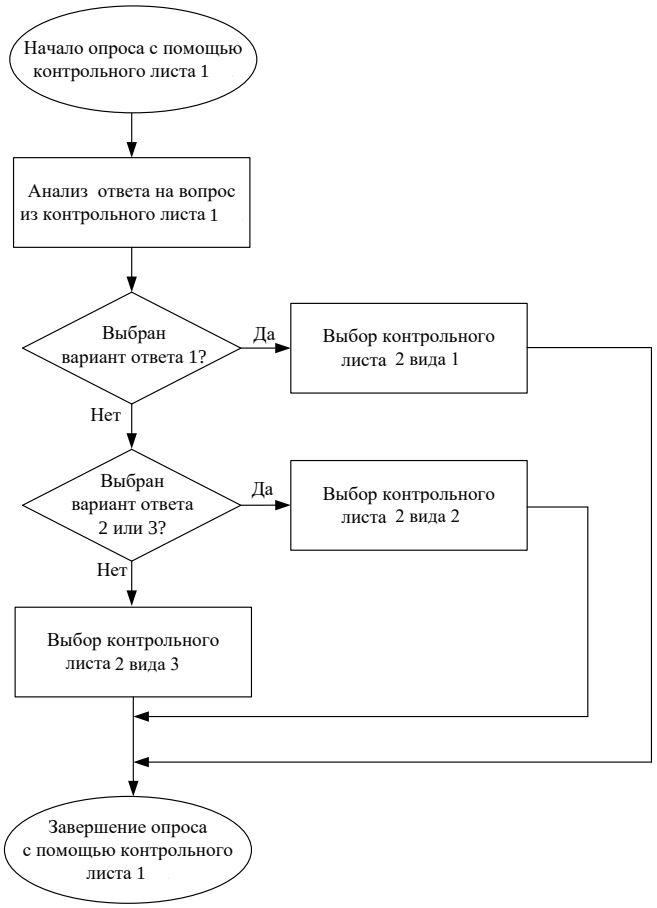

Рис. 1. Схема проведения анкетирования согласно контрольному листу 1
Fig. 1. Scheme of conducting a survey according to checklist 1

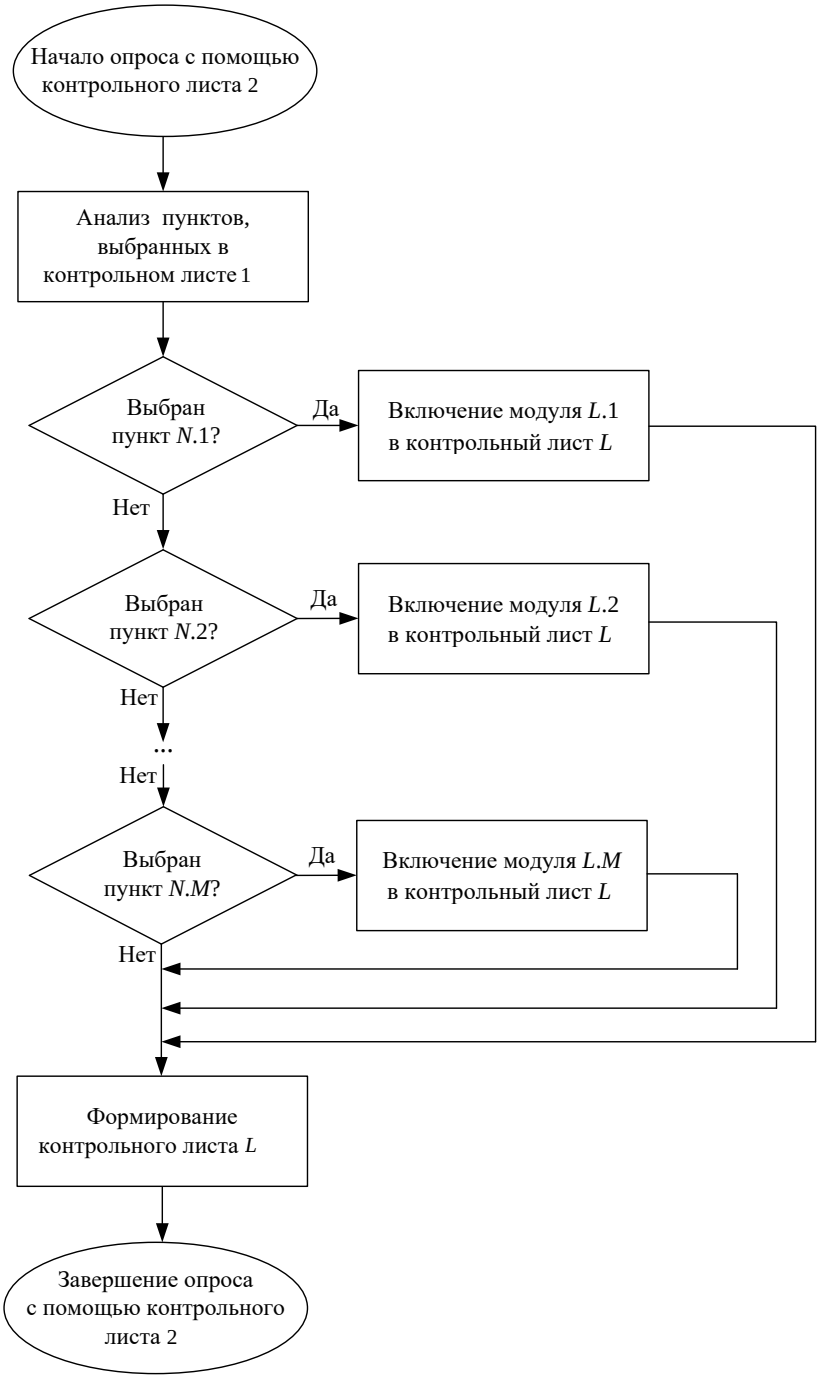

Рис. 2. Обобщенный алгоритм проведения анкетирования с помощью контрольного листа 2

Fig. 2. Generalized algorithm for the questionnaire conducting using checklist 2

Таким образом, если в качестве ответа на вопрос из контрольного листа 1 выбран вариант 1, то ему соответствует контрольный лист 3. Если в качестве ответа на вопрос из контрольного листа 1 выбран один из вариантов 2–6, то номер формируемого контрольного листа будет соответственно 4, 5, 6, 7 или 8.

Реализация возможности оценки уровня соответствия СЗИ ИС организации требованиям, изложенным в Положении. В ходе разработки усовершенствованного программного средства авторами предложено ранжировать по пяти уровням соответствие СЗИ ИС требованиям:

– полное несоответствие;
– низкий уровень соответствия;
– средний уровень соответствия;
– высокий уровень соответствия;
– полное соответствие.

Уровни соответствия СЗИ ИС вышеизложенным требованиям устанавливаются по каждому из общих показателей безопасности системы. Например, СЗИ ИС может характеризоваться средним уровнем соответствия требованиям Положения в части реализации организационных мер по защите информации, но при этом полностью не соответствовать требованиям в части реализации технической и криптографической защиты информации, защиты информации в виртуальной инфраструктуре, защиты информации, передаваемой по каналам связи, защиты СЗИ.

Уровень соответствия СЗИ ИС общему показателю безопасности зависит от количества выбранных анкетируемым сотрудником частных показателей безопасности, на которых основаны контрольные листы 3–8.

Взаимосвязь между уровнем соответствия общего показателя безопасности СЗИ ИС и количеством выбранных анкетируемым сотрудником частных показателей безопасности представлена в табл. 2, где *MAX* – количество частных показателей безопасности, на основе которых составлен контрольный лист для анкетирования и которые соответствуют определенному общему показателю безопасности; *MV* – медианное значение среди множества значений, отражающих количество частных показателей безопасности, на основе которых составлены все контрольные листы для анкетирования и каждый из которых соответствует определенному общему показателю безопасности.

Таблица 2
Уровни соответствия общих показателей безопасности СЗИ ИС количеству выбранных анкетируемым сотрудником частных показателей безопасности (*PM*)

Table 2
Compliance degrees of the general security indicators of the information security system of the IS to the number of private security indicators (PM) selected by the surveyed employee

Уровень соответствия *Compliance degree*	Значение *PM* *PM value*
Полное несоответствие	0
Низкий	$\begin{cases} 0 < PM < \dfrac{MAX - 1}{2}, \text{ если } MAX \text{ – нечетное число и } MAX \le MV; \\ 0 < PM < \dfrac{MAX}{2}, \text{ если } MAX \text{ – четное число;} \\ 0 < PM < \dfrac{MAX + 1}{2}, \text{ если } MAX \text{ – нечетное число и } MAX > MV \end{cases}$
Средний	$\begin{cases} \dfrac{MAX - 1}{2}, \text{ если } MAX \text{ – нечетное число и } MAX \le MV; \\ \dfrac{MAX}{2}, \text{ если } MAX \text{ – четное число;} \\ \dfrac{MAX + 1}{2}, \text{ если } MAX \text{ – нечетное число и } MAX > MV \end{cases}$
Высокий	$\begin{cases} MAX - 1, \text{ если } MAX \le MV; \\ MAX - 2, \text{ если } MAX > MV \end{cases}$
Полное соответствие	*MAX*

Значение *MV* определяется на основе совокупности следующих условий:

$$\begin{cases} MV \in \{GV_1, GV_2, ..., GV_m, ..., GV_r\}; \\ MV = GV_m; \\ m = \dfrac{r}{2}, \text{ если } r - \text{четное число}; \\ m = \dfrac{r+1}{2}, \text{ если } r - \text{нечетное число}, \end{cases}$$

где $GV_1, GV_2, ..., GV_m, ..., GV_r$ – проранжированные по возрастанию значения количества частных показателей безопасности, каждый из которых соответствует определенному общему показателю безопасности; GV_m – значение, которое является медианным в множестве $GV_1, GV_2, ..., GV_m, ..., GV_r$; m – порядковый номер значения, которое является медианным в множестве $GV_1, GV_2, ..., GV_m, ..., GV_r$; r – суммарное количество общих показателей безопасности в множестве $GV_1, GV_2, ..., GV_m, ..., GV_r$.

Для разработки программного средства использован язык программирования JavaScript.

Результаты исследования. Разработанное и усовершенствованное программное средство представляет собой совокупность файлов формата html, в связи с чем (в отличие от аналогов [4–8]) оно не требует установки и может быть запущено и использовано на всех рабочих станциях, оснащенных интернет-браузером.

На рис. 3–7 показаны фрагменты диалоговых окон файлов программного средства.

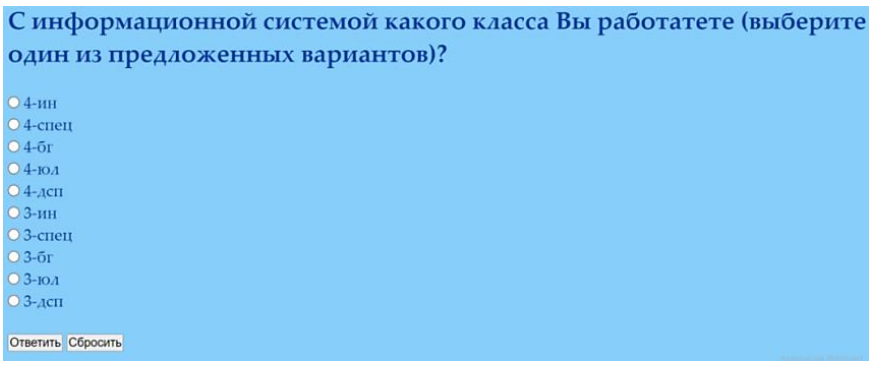

Рис. 3. Фрагмент диалогового окна программного средства для выбора класса ИС

Fig. 3. Fragment of the dialog box of the software tool for selecting the IP class

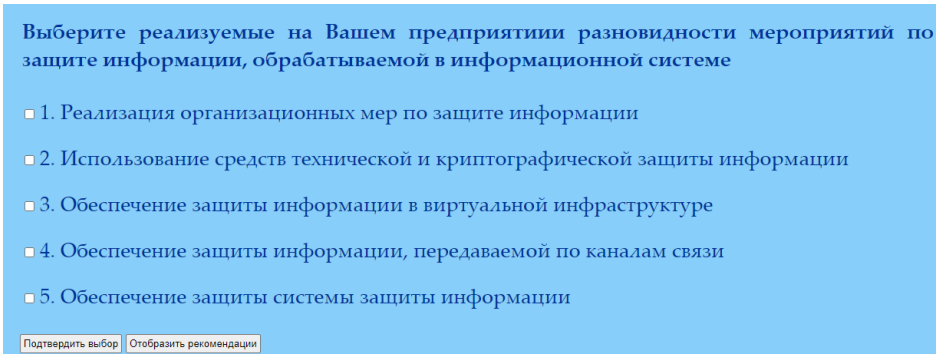

Рис. 4. Фрагмент диалогового окна программного средства для выбора реализуемых на предприятии разновидностей мероприятий по защите информации

Fig. 4. Fragment of the dialog box of the selection tool types of information security measures implemented at the enterprise

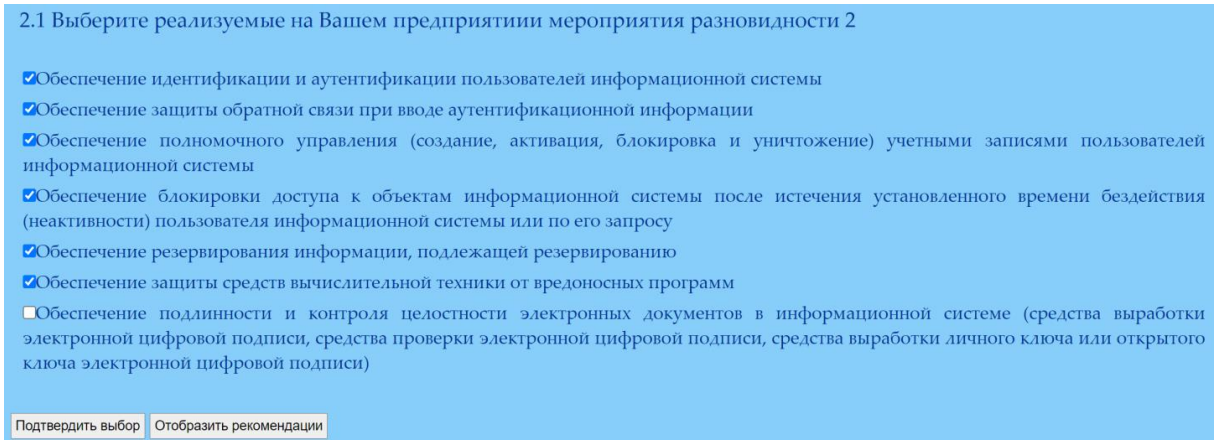

Рис. 5. Фрагмент диалогового окна программного средства после выбора реализуемых на предприятии разновидностей мероприятий по защите информации и нажатия на кнопку «Подтвердить выбор»

Fig. 5. A fragment of the dialog box of the software tool after selecting the types of information protection measures implemented at the enterprise and clicking on the "Confirm selection" button

Низкая степень соответствия требованиям приказа ОАЦ № 66 в части реализации организационных мер по защите информации
Полное несоответствие требованиям приказа ОАЦ № 66 в части реализации технической и криптографической защиты информации
Полное несоответствие требованиям приказа ОАЦ № 66 в части реализации защиты информации в виртуальной инфраструктуре
Полное несоответствие требованиям приказа ОАЦ № 66 в части реализации защиты информации, передаваемой по каналам связи
Полное несоответствие требованиям приказа ОАЦ № 66 в части реализации защиты системы защиты информации

Рис. 6. Текст диалогового окна программного средства после нажатия на кнопку «Подтвердить выбор» при условии сделанного выбора пунктов

Fig. 6. The text of the dialog box of the software tool after clicking on the "Confirm selection" button, provided that the items were selected

Для поддержания соответствия в части реализации организационных мер по защите информации необходимо: *обновление программного обеспечения объектов информационной системы и контроля за своевременность такого обновления*
Для поддержания соответствия в части реализации технической и криптографической защиты информации необходимо: *обеспечение подлинности и контроля целостности электронных документов в информационной системе (средства выработки электронной цифровой подписи, средства проверки электронной цифровой подписи, средства выработки личного ключа или открытого ключа электронной цифровой подписи)*
Для обеспечения соответствия в части реализации защиты системы защиты информации необходимо: *обеспечение изменения атрибутов безопасности сетевого оборудования, системного программного обеспечения и средств защиты информации, установленных по умолчанию*

Рис. 7. Текст диалогового окна программного средства после нажатия на кнопку «Отобразить рекомендации»

Fig. 7. The text of the dialog box of the tool after clicking on the button "Display recommendations"

В разработанном и усовершенствованном программном средстве предусмотрена возможность редактирования вопросов, что создает условия для его использования при проведении аудита СЗИ ИС любых организаций независимо от вида их деятельности, формы собственности и ведомственной подчиненности.

Заключение. Разработанное и усовершенствованное программное средство характеризуется пониженной (по сравнению с аналогами) стоимостью ввиду простоты запуска и настройки, независимости от типа операционной системы, а также возможности организации как локального, так и удаленного доступа к нему. 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. Применение разработанного программного средства позволит существенно сократить время и материальные затраты на проведение аудита.

Представленное в настоящей статье программное средство было апробировано в филиале «Междугородная связь» РУП «Белтелеком». Установлено, что использование этого средства позволяет сократить на 20–30 % финансирование затрат на реализацию процесса проведения аудита СМИБ организации.

Программное средство зарегистрировано в установленном порядке на государственном предприятии «Национальный центр интеллектуальной собственности» (свидетельство о регистрации № 1447 от 14.10.2021).

Вклад авторов. *В. А. Бойправ* создал методику разработки и усовершенствования программного средства, выполнил его практическую реализацию. *Л. Л. Утин* предложил подходы по оптимизации процесса практической реализации программного средства.

Список использованных источников

1. Бойправ, В. А. Программное средство для проведения аудита системы защиты информации организации / В. А. Бойправ, В. В. Ковалев, Л. Л. Утин // Доклады БГУИР. – 2018. – № 5(115). – С. 44–49.

2. Pandey, S. K. A comparative study of risk assessment methodologies for information systems / S. K. Pandey, K. Mustafa // Bulletin of Electrical Engineering and Informatics. – 2012. – Vol. 1, no. 2. – P. 111–122.

3. Сагитова, В. В. Применение метода экспертных оценок для автоматизации аудита информационных систем персональных данных / В. В. Сагитова, В. И. Васильев // Вестник УГАТУ. – 2017. – Т. 21, № 3(73). – С. 105–112.

4. Якимова, З. В. Динамика уровня вовлеченности персонала в зависимости от стажа работы в организации / З. В. Якимова, А. С. Пушкина // АНИ: экономика и управление. – 2018. – № 1(22). – С. 283–286.

5. Information security risk assessment / I. Kuzminykh [et al.] // Encyclopedia. – 2021. – Vol. 1(3). – P. 602–617.

6. Nest, D. P. van der. The use of generalised audit software by internal audit functions in a developing country: a maturity level assessment / D. P. van der Nest, L. Smidt, D. Lubbe // Risk Governance and Control: Financial Markets & Institutions. – 2017. – Vol. 7(4–2). – P. 189–202.

7. Lehmann C. M. Integrating generalized audit software and teaching fraud detection in information systems auditing courses / C. M. Lehmann // J. of Forensic & Investigative Accounting. – 2012. – Vol. 4, iss. 1. – P. 319–368.

8. SECURQUAL: An instrument for evaluating the effectiveness of enterprise information security programs / P. J. Steinbart [et al.] // J. of Information Systems. – 2015. – Vol. 30(1). – P. 71–92.

References

1. Boiprav V. A., Kovalev V. V., Utin L. L. Software for audit of information protection system of the organization. Doklady Belorusskogo gosudarstvennogo universiteta informatiki i radioèlektroniki [*Reports of the Belarusian State University of Informatics and Radioelectronics*], 2018, № 5(115), pp. 44–49 (In Russ.).

2. Pandey S. K., Mustafa K. A comparative study of risk assessment methodologies for information systems. *Bulletin of Electrical Engineering and Informatics*, 2012, vol. 1, no. 2, pp. 111–122.

3. Sagitova V. V., Vasil'ev V. I. *Application of the method of expert assessments to automate the audit of personal data information systems*. Vestnik Ufimskogo gosudarstvennogo aviacionnogo tehnicheskogo universiteta [*Bulletin of the Ufa State Aviation Technical University*], 2017, vol. 21, no. 3(73), pp. 105–112 (In Russ.).

4. Yakimova Z. V., Pushkina A. S. *Dynamics of the level of personnel involvement depending on the length of service in the organization*. Azimut nauchnyh issledovanij: jekonomika i upravlenie [*Azimuth of Scientific Research: Economics and Management*], 2018, no. 1(22), pp. 283–286 (In Russ.).

5. Kuzminykh I., Ghita B., Sokolov V., Bakhshi T. Information security risk assessment. *Encyclopedia*, 2021, vol. 1(3), pp. 602–617.

6. Nest D. P. van der, Smidt L., Lubbe D. The use of generalised audit software by internal audit functions in a developing country: a maturity level assessment. *Risk Governance and Control: Financial Markets & Institutions*, 2017, vol. 7(4–2), pp. 189–202.

7. Lehmann C. M. Integrating generalized audit software and teaching fraud detection in information systems auditing courses. *Journal of Forensic & Investigative Accounting*, 2012, vol. 4, iss. 1, pp. 319–368.

8. Steinbart P. J., Gal G., Dilla W. N., Raschke R. L. SECURQUAL: An instrument for evaluating the effectiveness of enterprise information security programs. *Journal of Information Systems*, 2015, vol. 30(1), pp. 71–92.

Информация об авторах

Бойправ Владимир Андреевич, заместитель директора по общим вопросам, Национальный центр современных искусств Республики Беларусь.
E-mail: name_abs@rambler.ru

Утин Леонид Львович, кандидат технических наук, доцент, заместитель начальника военного факультета по учебной и научной работе – первый заместитель начальника, Белорусский государственный университет информатики и радиоэлектроники.
E-mail: utin@bsuir.by

Information about the authors

Vladimir A. Boiprav, Deputy Director for General Affairs, National Center for Contemporary Arts of the Republic of Belarus.
E-mail: name_abs@rambler.ru

Leonid L. Utin, Ph. D. (Eng.), Associate Professor, Deputy Head of the Military Faculty for Educational and Scientific Work – First Deputy Head, Belarusian State University of Informatics and Radioelectronics.
E-mail: utin@bsuir.by