DOI: https://doi.org/10.15688/NBIT.jvolsu.2020.3.1

УДК 681.5:005.71
ББК 32.81

СНИЖЕНИЕ РИСКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СУБЪЕКТОВ ДЕЦЕНТРАЛИЗОВАННЫХ АВТОНОМНЫХ ОРГАНИЗАЦИЙ

Юлия Сагидулловна Бахрачева

Кандидат технических наук, доцент кафедры информационной безопасности,
Волгоградский государственный университет
bakhracheva@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Арина Романовна Алеева

Студент кафедры информационной безопасности,
Волгоградский государственный университет
bakhracheva@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. Целью данной работы является снижение риска информационной безопасности субъектов децентрализованных автономных организаций. Для этого была проведена разработка математической модели аудита информационной безопасности субъектов децентрализованных автономных организаций.

Ключевые слова: информационная безопасность, математическая модель, аудит информационной безопасности, децентрализованные автономные организации, Интернет.

© Бахрачева Ю.С., Алеева А.Р., 2020

Интернет быстро вступает в новую технологическую эру с появлением технологии блокчейн, дающая возможность обмениваться ценностями совершенно безопасно [3]. Данная технология является инструментом для появления децентрализованных автономных организаций.

Децентрализованные автономные организации (ДАО), использующие технологию распределенной бухгалтерской книги, могут потенциально улучшить корпоративное управление за счет автоматизации базовых правил. На сегодняшний день ДАО, как новый тип экономической организации, жизнеспособна и эффективна в теории, но требует от разработчиков особой тщательности в сфере безопасности от атак и случайных ошибок в коде [1; 2; 4].

Децентрализованные автономные организации состоят из субъектов, наделенных определенными правами. Действия субъектов могут привести к определенным последствиям, влияющих на стабильность ДАО. Данные организации должны отслеживать состояние системы. Для решения этого вопроса необходимо проводить аудит информационной безопасности, позволяющий дать количественную и качественную оценки состояния информационной безопасности.

Целью данной работы является снижение риска информационной безопасности субъектов децентрализованных автономных организаций. Для этого была проведена разработка математической модели аудита информационной безопасности субъектов децентрализованных автономных организаций.

Проект модели выполнен в соответствии с методологией функционального моделирования IDEF0, предназначенной для формализации и описания процесса проведения аудита информационной безопасности субъектов децентрализованных автономных организаций. Контекстная IDEF0 – диаграмма процесса проведения аудита представлена на рисунке 1.

На функциональный блок «Аудит информационной безопасности субъектов децентрализованных автономных организаций» воздействуют:

1) Входные данные – информация о децентрализованных автономных организациях.

2) Управляющая информация, в качестве которой выступают – список возможных угроз, существующие данные, математическая модель и меры предотвращения угроз.

3) Механизмами, необходимыми для повышения защищенности, являются программное средство и пользователь.

4) В результате данных воздействий на выходе функции результат – программный комплекс, способный проводить аудит ИБ субъектов ДАО.

При декомпозиции функционального блока выделены его составляющие:

1) Определение функционала планируемой ДАО.

2) Обрабатывание данных существующей ДАО.

3) Изъятие данных существующей ДАО.

4) Расчет показателя ИБ ДАО и оценки рисков.

5) Определение мер предотвращения угроз ИБ ДАО.

6) Снижение риска.

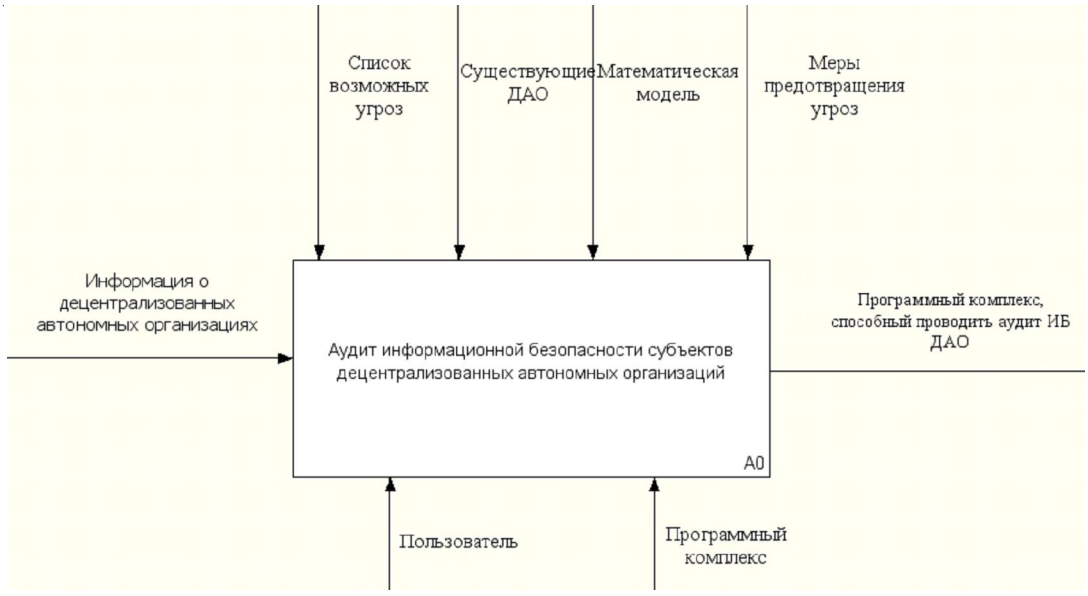

Рис. 1. Контекстная IDEF0 – процесса проведения аудита ИБ субъектов ДАО

На блок модуля «определение функционала планируемой ДАО» воздействуют:

1) Входные данные – информация о децентрализованных автономных организациях.

2) Управляющая информация – список возможных угроз.

3) Механизмами являются: программный комплекс и пользователь.

4) В результате данных воздействий на выходе функции результат – входные данные для расчета.

На блок «обрабатывание данных существующей ДАО» воздействуют:

1) Входные данные – заполнение полученными данными о существующей ДАО.

2) Управляющая информация – существующие ДАО.

3) Механизмом является программный комплекс.

4) В результате данных воздействий на выходе функции результат – входные данные для расчета.

На блок «изъятие данных существующей ДАО» воздействуют:

1) Входные данные – информация о децентрализованных автономных организациях.

2) Управляющая информация – существующие ДАО.

3) Механизмами являются: программный комплекс и пользователь.

4) В результате данных воздействий на выходе функции результат – заполнение полученными данными о существующей ДАО.

На блок «расчет показателя ИБ ДАО и оценки рисков» воздействуют:

1) Входные данные – входные данные для расчета.

2) Управляющая информация – математическая модель.

3) Механизмами являются: программный комплекс и пользователь.

4) В результате данных воздействий на выходе функции результат – результаты оценок рисков и показателя ИБ ДАО.

На блок «определение мер предотвращения угроз ИБ ДАО» воздействуют:

1) Входные данные – результаты оценок рисков и показателя ИБ ДАО.

2) Управляющая информация – список возможных угроз.

3) Механизмом является программный комплекс.

4) В результате данных воздействий на выходе функции результат – применение мер защиты.

На блок «снижение риска» воздействуют:

1) Входные данные – применение мер защиты.

2) Управляющая информация – меры предотвращения угроз.

3) Механизмами являются: программный комплекс и пользователь.

4) В результате данных воздействий на выходе функции результат – программный комплекс, способный проводить аудит ИБ ДАО.

Далее была проведена разработка архитектуры программного комплекса аудита информационной безопасности субъектов децентрализованных автономных организаций. На рисунке 2 представлена архитектура ДАО.

Основными компонентами разработанной архитектуры являются:

– Интерфейс пользователя.

– Модуль идентификации ДАО.

– Модуль функционирования смарт-контрактов.

– Модуль разделения капитала и силы голосования.

– Модуль реализации голосования.

– Обработка данных результатов функционирования.

К модулю обработки данных результатов функционирования дополняется модуль аудита ИБ ДАО, который в свою очередь имеет другую архитектуру (см. рис. 3).

Основными компонентами разработанной архитектуры являются:

– Пользовательский интерфейс.

– Модуль определения функционала планируемой ДАО.

– Модуль изъятия данных существующей ДАО.

– Модуль обработки данных, существующей ДАО.

– Модуль расчета показателя ИБ ДАО и оценки рисков.

– Модуль определения мер предотвращения угроз ИБ.

Пользовательский интерфейс имеет графический вид и предназначен для ввода дан-

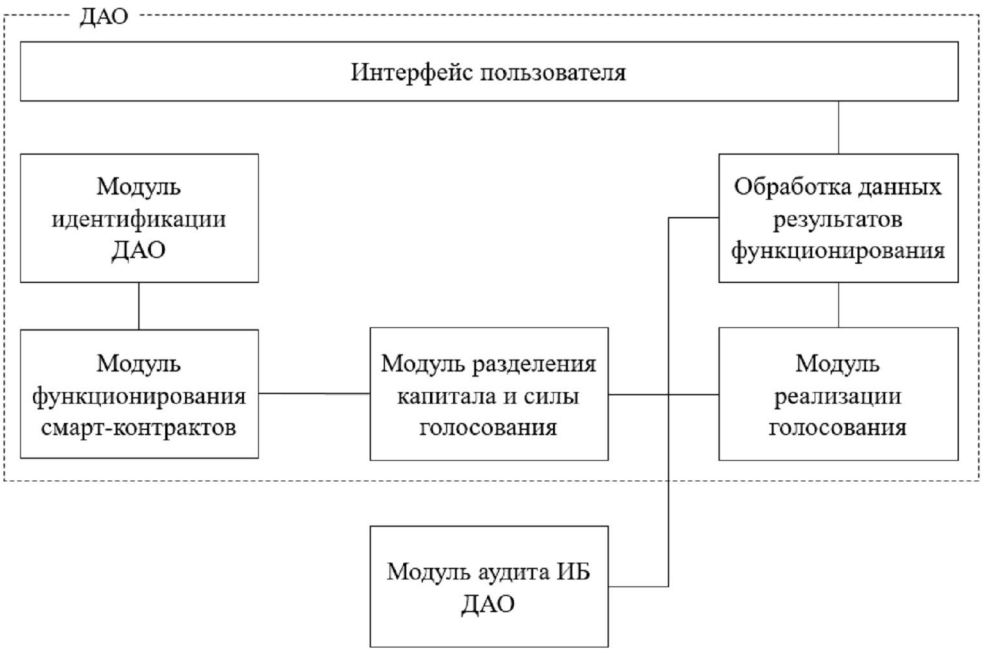

Рис. 2. Архитектура ДАО

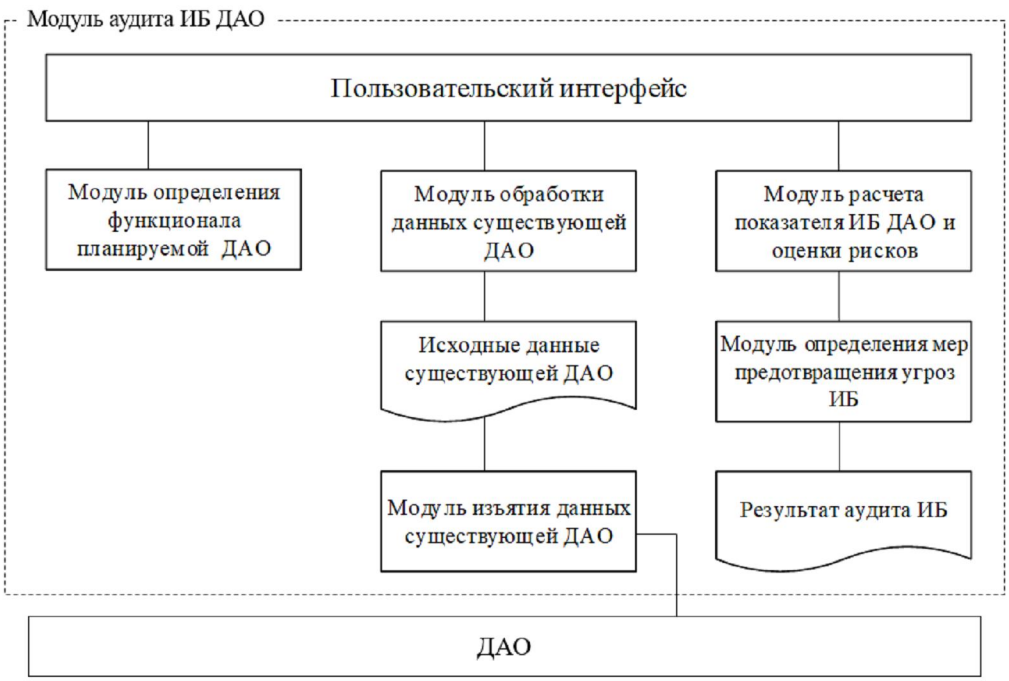

Рис. 3. Архитектура программного комплексааудита ИБ субъектов ДАО

ных, вывода результатов и организации взаимодействия пользователя с программой.

Модуль определения функционала планируемой ДАО предназначен для ввода данных и организации взаимодействия пользователя с программой.

Модуль изъятия данных существующей ДАО позволяет извлекать и преобразовывать информацию из ДАО для ее дальнейшего использования в программном комплексе.

Исходные данные существующей ДАО содержат в себе данные о всех параметрах ДАО и их функционала.

Модуль обработки данных, существующей ДАО, позволяет обработать информацию

и автоматически заполнить поля данных программного комплекса.

Модуль расчета показателя ИБ ДАО и оценки рисков рассчитывает данные по угрозам для определения качественной или количественной оценки рисков, а также значение показателя ИБ ДАО.

Модуль определения мер предотвращения угроз ИБ предназначен для подбора меры предотвращения в соответствии с угрозой.

Результат аудита ИБ содержит отчет об выявленных угрозах, оценку рисков и меры предотвращения.

На основании разработанной архитектуры программного комплекса разработан пользовательский интерфейс (рис. 4).

Данный пользовательский интерфейс содержит в себе:

– Область выбора вида ДАО для проведения аудита.

– Область выбора функционала ДАО.

– Область заполнения доступных вкладок по функционалу ДАО.

– Кнопки «Выбрать файл», «Оценить риски и показатель ИБ ДАО» и «Сохранить и показать отчет» для взаимодействия с данными, введенными в различные области на данном интерфейсе.

На панели интерфейса имеется:

– Кнопки выбора вида ДАО для проведения аудита ИБ, которые позволяют выбрать вид ДАО для дальнейшей работы.

– Кнопка выбора файла с данными, существующей ДАО, позволяющая загрузить файл с информацией о ДАО.

– Кнопки выбора функционала в ДАО, в которых пользователь выбирает функционал ДАО в соответствии с параметрами ДАО.

– Кнопки выбранного функционала ДАО включают в себя доступный функционал, в каждой вкладке которого вводятся данные для дальнейших расчетов.

– Поля данных для заполнения в соответствии с ДАО позволяет заполнить поля для расчетов по формулам.

– Кнопка для проведения оценки риска рассчитывает оценки рисков, которые могут быть низкими, средними или высокими, также подбирает меры предотвращения.

– Кнопка для создания отчета по аудиту ИБ формирует документ, в котором будет

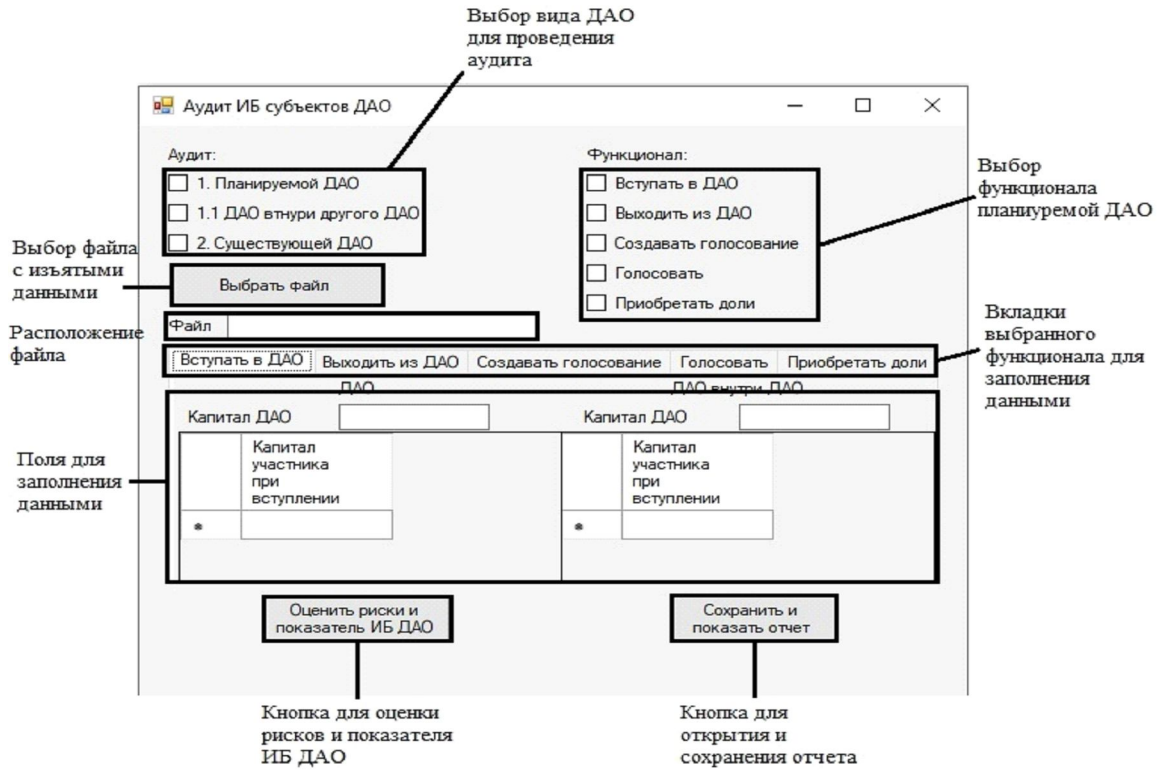

Рис. 4. Пользовательский интерфейс программного комплекса аудита ИБ субъектов ДАО

перечень выявленных угроз, оценка рисков, показатель ИБ ДАО и меры предотвращения.

Далее были проведены экспериментальные исследования работы разработанного программного комплекса. Было показано, что остаточный риск уменьшился на 2,5, а процент снижения риска уменьшился на 42,8 %.

СПИСОК ЛИТЕРАТУРЫ

1. Antonopoulos, A. M. Mastering Bitcoin: Unlocking Digital Cryptocurrencies / A. M. Antonopoulos. – Sebastopol, CA, USA : O'Reilly Media, 2014. – 270 p.

2. Ethereum white paper / V. Buterin [et al.] // GitHub repository. – 2013. – Vol. 1. – P. 22–23.

3. Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system / S. Nakamoto. – Manubot, 2019. – Electronic text data. – Mode of access: https://git.dhimmel.com/bitcoin-whitepaper/ (date of access: 27.09.2020).

4. Theory and praxis of DAOs. How can DAOs be conceptualized and classified? – 2019. – Electronic text data. – Mode of access: https://research.binance.com/analysis/dao-theory (date of access: 26.09.2020).

REFERENCES

1. Antonopoulos A.M. *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. Sebastopol, CA, USA, O'Reilly Media, 2014. 270 p.

2. Buterin V. et al. Ethereum white paper. *GitHub repository*, 2013, vol. 1, pp. 22-23.

3. Nakamoto S. *Bitcoin: A peer-to-peer electronic cash system*. Manubot, 2019. URL: https://git.dhimmel.com/bitcoin-whitepaper/ (accessed 27 September 2020).

4. *Theory and praxis of DAOs. How can DAOs be conceptualized and classified?* 2019. URL: https://research.binance.com/analysis/dao-theory (accessed 26 September 2020).

REDUCING THE RISK OF INFORMATION SECURITY OF SUBJECTS OF DECENTRALIZED AUTONOMOUS ORGANIZATIONS

Yulia S. Bahracheva

Candidate of Sciences (Engineering), Associate Professor, Department of Information Security,
Volgograd State University
bakhracheva@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Arina R. Aleeva

Student, Department of Information Security,
Volgograd State University
bakhracheva@volsu.ru 100
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Abstract. The purpose of this work is to reduce the risk of information security of subjects of decentralized autonomous organizations. For this purpose, a mathematical model of the audit of information security of subjects of decentralized autonomous organizations was developed.

Key words: information security, mathematical model, information security audit, decentralized autonomous organizations, Internet.