О базе данных мер обеспечения информационной безопасности, разработанной в соответствии с ИСО/МЭК 27002:2022

Д.С. Буренок, В.А. Воеводин

***Аннотация* — Приводятся сведения о базе данных, которая включает в себя совокупность мер обеспечения информационной безопасности и позволяет автоматизировать процесс построения системы управления информационной безопасностью (СУИБ). Обосновывается структура базы данных мер обеспечения информационной безопасности, с использованием которой возможно осуществить проектирование соответствующей СУИБ и разработку формальной онтологии предметной области. В основу решения заложены положения международного стандарта ИСО/МЭК 27002:2022 и результаты анализа атрибутов мер обеспечения информационной безопасности, которые содержатся в ИСО/МЭК 27002:2022. База данных выполнена в рамках реляционной модели данных и оснащена графическим интерфейсом для взаимодействия с пользователями. В качестве системы управления базой данных используется MS Access. Интерактивный функционал базы данных реализован на языке программирования VBA, а также с использованием встроенных элементов MS Access. Для построения запросов используется SQL-синтаксис. Новизна предложения заключается в применении двухуровневого графического интерфейса базы данных и реализации функционала по подбору мер обеспечения информационной безопасности согласно заданным фильтрам. Реализованное решение позволяет автоматизировать процесс построения СУИБ. Элементы решения зарегистрированы в качестве объекта интеллектуальной собственности в Роспатенте.**

***Ключевые слова* — проектирование системы управления информационной безопасностью, автоматизация, реляционная база данных, меры защиты.**

I. Введение

Обладатель информации в силу закона обязан «принимать меры по защите информации».

Государственное регулирование отношений в сфере защиты информации осуществляется путем установления требований к защите информации, а также ответственности за нарушение соответствующего законодательства РФ.

За неисполнение обязанностей к обладателю информации могут быть применены санкции от дисциплинарной ответственности и вплоть до уголовной.

Результаты анализа основных нормативных правовых документов, содержащих требования по защите информации, приведены в таблице 1.

Таблица 1 – Источники требований по защите информации

Источник требований	Обладатель информации
Указ Президента Российской Федерации от 01.05.2022 № 250	Органы государственной власти, системообразующие, стратегические российские компании
Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»	Субъекты критической информационной инфраструктуры, которым принадлежат значимые объекты критической информационной инфраструктуры
Постановление Правительства РФ от 06.07.2015 № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации»	Операторы государственных информационных систем
Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»	Операторы и обработчики персональных данных
Приказ ФСТЭК России от 14.03.2014 № 31	Лица, обеспечивающие эксплуатацию автоматизированных систем управления
Положения Банка России № 382-П, 716-П, 683-П, 747-П, 719-П, 757-П	Субъекты банковской деятельности

Для обеспечения защиты информации в организации выделяется соответствующий ресурс и строится система управления информационной безопасностью (далее – СУИБ). Основу СУИБ составляют взаимоувязанные единой целью меры обеспечения информационной

Статья получена 29 мая 2023.

Буренок Дмитрий Сергеевич, студент 1 курса магистратуры кафедры «Информационная безопасность» НИУ «МИЭТ», Москва (e-mail: corr.dmitry@yahoo.com)

Воеводин Владислав Александрович, к.т.н., доцент, доцент кафедры «Информационная безопасность» НИУ «МИЭТ», Москва (e-mail: vva541@mail.ru)

безопасности (далее – ИБ), для чего были разработаны и внедрены соответствующие национальные стандарты [1]. В настоящее время Техническим Комитетом № 362 ФСТЭК России ведется работа по внедрению гармонизированной версии международного стандарта ИСО/МЭК 27002 от 2022 года [2]. В указанном стандарте определен перечень основных мер по обеспечению ИБ. Однако выбор подходящих мер непосредственно по стандарту предполагает значительный объем ручного труда.

С целью автоматизации деятельности по выбору совокупности мер по обеспечению ИБ была разработана с использованием СУБД MS Access реляционная база данных [3], оснащенная графическим интерфейсом и функционалом фильтрации мер [4] по их атрибутам. В статье представлены структура, содержание и атрибуты базы данных, включая сведения о соответствии нормализованной форме представления данных, порядок формирования SQL-запросов для фильтрации мер обеспечения ИБ, а также приведены особенности графического интерфейса и организации наполнения базы данных в СУБД MS Access.

II. Структура, содержание и атрибуты мер обеспечения информационной безопасности согласно ИСО/МЭК 27002:2022

В обновленной версии международного стандарта [2] кардинально изменен подход к формированию СУИБ. В новой редакции проекта стандарта каждой мере обеспечения ИБ присвоены атрибуты, на основе которых можно спроектировать СУИБ, объективно удовлетворяющую заданным требованиям. Данная новация позволила автоматизировать сам процесс разработки СУИБ, разработать ее формальную онтологию.

Всего в [2] определено 93 меры обеспечения ИБ, разделенные на четыре группы:

– организационные меры;
– меры по безопасности персонала;
– физические меры безопасности;
– технические меры безопасности.

На рисунке 1 представлен пример описания меры обеспечения ИБ согласно [2].

5.2 Роли и обязанности в области информационной безопасности

Вид контроля	Свойства информационной безопасности	Концепции информационной безопасности	Операционные возможности	Сферы безопасности
#Превентивный	#Конфиденциальность #Целостность #Доступность	#Идентификация	#Высокоуровневое управление	#Управление и экосистема #Защита #Устойчивость

Мера обеспечения ИБ

Роли и обязанности в области информационной безопасности должны быть определены, распределены и закреплены в функциональных обязанностях в соответствии с потребностями организации.

Цель

Создать определенную, одобренную руководством и понятную для исполнителей организационную структуру для внедрения, эксплуатации и управления информационной безопасностью в организации.

Рисунок 1 – Пример описания меры обеспечения ИБ согласно ИСО/МЭК 27002:2022

Описание каждой меры представлено совокупностью следующих подразделов:

– название меры;
– цель меры;
– содержание меры;
– рекомендации по внедрению;
– другая информация.

Данный подход позволяет в принципе обеспечить создание формальной онтологии СУИБ.

Из рисунка 1 видно, что каждой мере поставлены в соответствие следующие атрибуты:

– группа;
– тип меры;
– свойства ИБ, на обеспечение которых она направлена;
– концепции ИБ, в которые она входит;
– операционные возможности, которые она реализует;
– области безопасности, к которым она относится.

Что также способствует разработке формальной онтологии СУИБ и автоматизации деятельности по разработке самой СУИБ в целом.

Возможные значения атрибутов мер обеспечения ИБ согласно [2] представлены в таблице 2.

Таблица 2 – Возможные значения атрибутов мер обеспечения ИБ согласно ИСО/МЭК 27002:2022

Атрибут	Возможные значения
Группы мер	– организационные меры; – меры по безопасности персонала; – физические меры безопасности; – технические меры безопасности.
Типы мер	– превентивный; – детективный; – корректирующий.
Свойства ИБ	– конфиденциальность; – целостность; – доступность.
Концепции ИБ	– идентификация; – защита; – обнаружение; – реагирование; – восстановление.
Операционные возможности	– высокоуровневое управление; – управление информационными активами; – защита информации; – безопасность персонала; – физическая безопасность; – безопасность систем и сети; – безопасность приложений; – безопасность конфигурации; – управление идентификацией и доступом; – управление угрозами и уязвимостями; – непрерывность; – безопасность при взаимодействии с поставщиками; – соответствие; – управление событиями информационной безопасности; – обеспечение информационной безопасности.
Области безопасности	– управление и экосистема; – защита; – отражение; – устойчивость.

III. Разработка базы данных мер обеспечения информационной безопасности

A. *Проектирование структуры реляционной базы данных*

На основе проведенного анализа структуры представления мер обеспечения ИБ из [2] были выделены основные сущности базы данных и их связи. Разработанная структура базы данных представлена на рисунке 2.

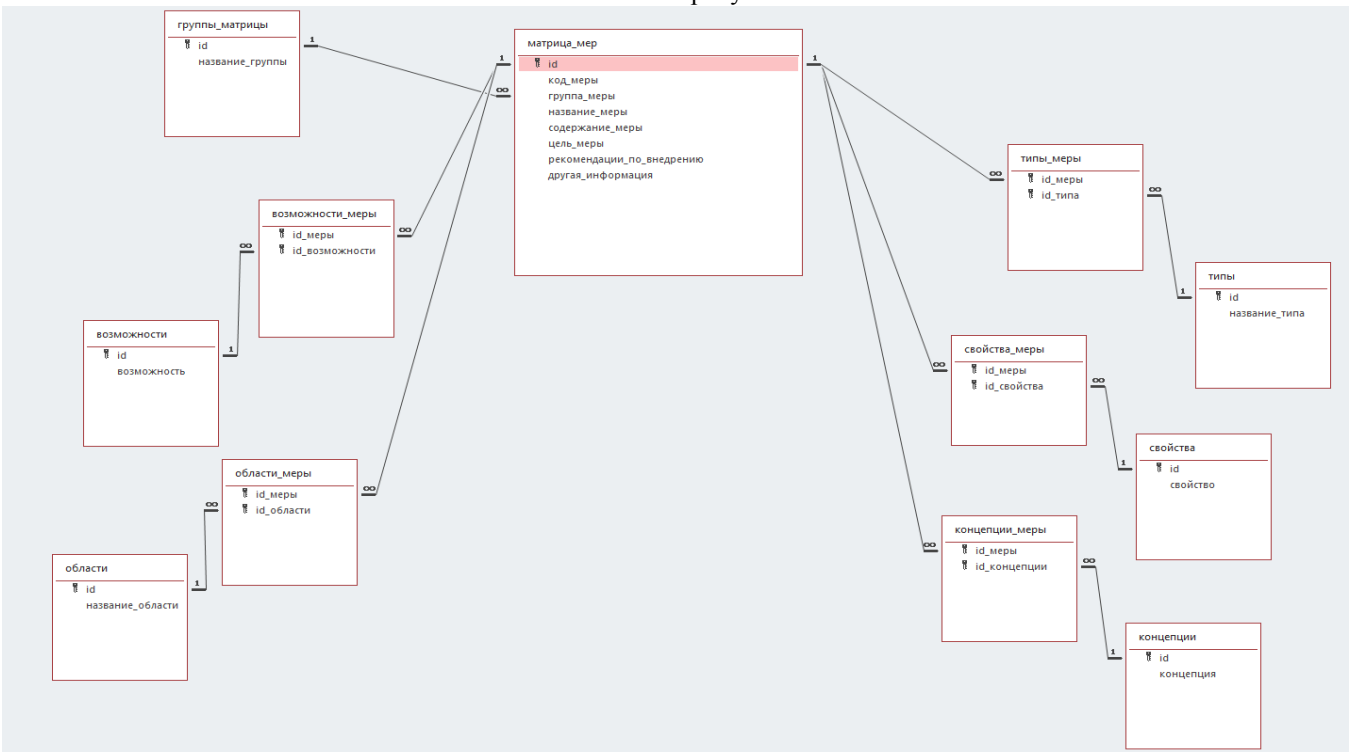


Рисунок 2 – Структура базы данных

Структура базы данных:

– укладывается в реляционную модель [5], в частности, в отдельные таблицы вынесены все допустимые значения атрибутов, а связи между таблицами атрибутов и мерами обеспечения ИБ реализованы по типу «*многие к многим*» через промежуточные таблицы;

– удовлетворяет требованиям первой нормальной формы (1NF), так как сохраняемые данные на пересечении строк и столбцов представлены скалярными значениями, все таблицы не содержат повторяющихся строк;

– удовлетворяет требованиям второй нормальной формы (2NF), так как во всех таблицах введен простой суррогатный (первичный) ключ и каждый столбец, не являющийся ключом, зависит от этого первичного ключа;

– удовлетворяет требованиям третьей нормальной формы (3NF), так как каждый столбец таблиц, не являющийся ключом, зависит только от первичного ключа (в таблицах отсутствуют транзитивные зависимости).

Неключевые столбцы не выполняют формально роль ключа в таблице, то есть они не предоставляют возможность получить данные из других столбцов. При этом обеспечивается возможность извлечения из них информации.

Следует отметить преимущества разработанной структуры базы данных по сравнению с нереляционными, а также ненормализованными реляционными базами данных. Ввиду нормализации база данных способствует устранению аномалий данных и гарантирует целостность данных. Немаловажными также является следующие факторы:

– простота конструирования SQL-запросов, все меры и соответствующие атрибуты могут быть получены прямым запросом к таблице «*матрица_мер*» и дополнительными запросами к таблицам, содержащим атрибуты выбранных мер, или на основе запросов объединения (JOIN);

– графические формы представления данных СУБД MS Access позволяют на полях основной формы отображать зависимую форму, тем самым снижая общее количество обособленных вкладок графического интерфейса и структурируя информацию, разработанная структура база данных позволяет задействовать указанный функционал подчиненных форм.

B. *Наполнение базы данных*

Наполнение базы данных было осуществлено записями, составленными на основе результатов собственного семантического, контекстного и предметного перевода мер обеспечения ИБ и атрибутов указанных мер согласно [2].

При наполнении базы данных учитывалась спроектированная структура базы данных (раздел 3, пункт А), а также результаты анализа представления мер обеспечения ИБ согласно [2] (раздел 2).

Текстовым полям (столбцам таблиц, предназначенным для записи текста) в базе данных был

присвоен тип «*короткий текст*» или «*длинный текст*» в зависимости от изложенного в стандарте объема содержимого этих полей. Для столбцов, содержащих первичные ключи (*id*), применяется тип данных «*счетчик*». Для внешних ключей применяется тип данных «*числовой*». Для всех внешних ключей в СУБД MS Access был задействован функционал подстановок [6, с. 320] с целью повышения эргономичности и исключения ошибок при наполнении базы данных. Пример формата данных отображен на рисунке 3.

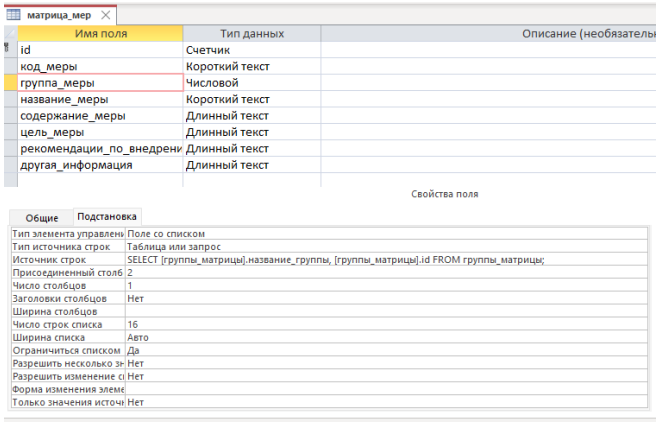


Рисунок 3 – Типы данных и подстановки для таблицы «*матрица_мер*»

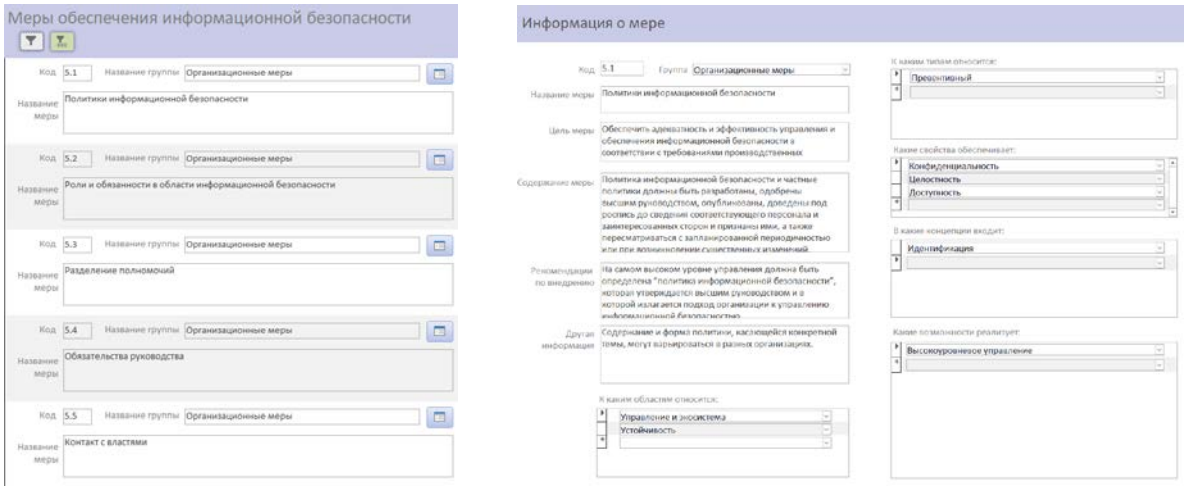
C. Графический интерфейс базы данных

Графический интерфейс базы данных реализован по типу оглавления книги: сначала пользователю предоставляется перечень всех мер обеспечения информационной безопасности без подробной детализации (рисунок 4, а), а после нажатия по соответствующей мере – детальная информация по выбранной мере (рисунок 4, б).

Дополнительно в базе данных для выбора подходящих мер был реализован функционал их фильтрации по атрибутам – рисунок 5. На рисунке 5 (а) представлено окно фильтрации, посредством которого устанавливаются параметры подбора, на рисунке 5 (б) – результаты фильтрации.

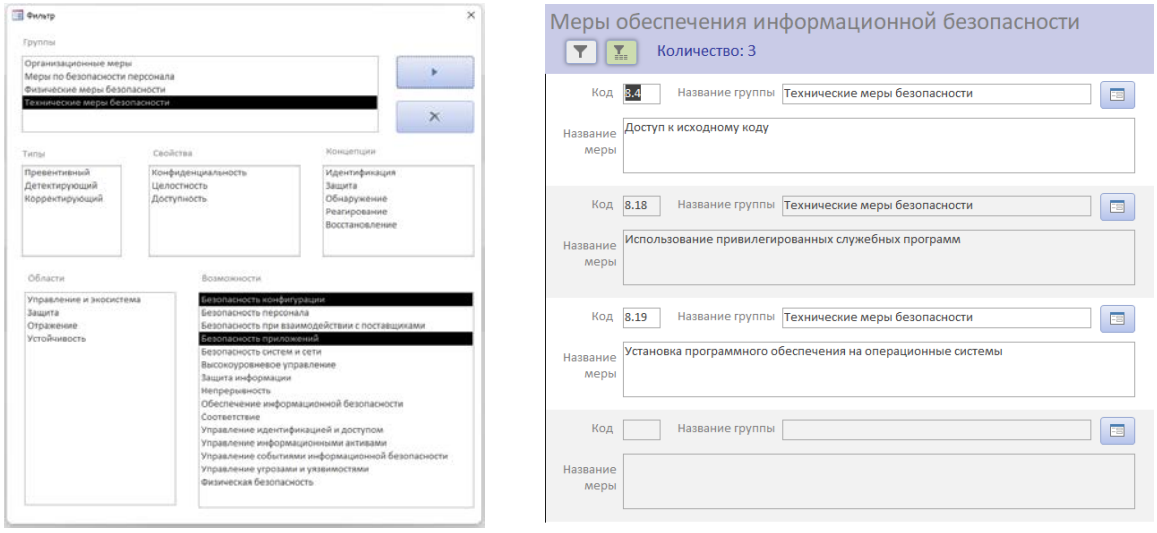
Используя фильтры, можно подобрать персонализированные меры обеспечения ИБ с учетом специфики проектируемой СУИБ и требованиям к ней.

Следует отметить, что элементы графического интерфейса были реализованы с использованием унифицированного функционала форм СУБД MS Access [6, с. 693]. В том числе, использовались элементы «*Форма*», «*Подчиненная форма*», «*Кнопка*», «*Надпись*», «*Поле*», «*Список*», «*Поле со списком*». Интерактивность графического интерфейса обеспечивается посредством встроенного механизма обработки событий СУБД MS Access и дополнительного кода, разработанного на VBA.



(а) (б)

Рисунок 4 – Графический интерфейс базы данных



(а) (б)

Рисунок 5 – Правило фильтрации мер обеспечения информационной безопасности

D. О функционале фильтрации мер

В качестве источника строк для формы, изображенной на рисунке 4 (а), выступает SQL-запрос, представленный в листинге 1.

Листинг 1 – SQL-запрос источника строк для основной формы «*Меры обеспечения информационной безопасности*»

```
Forms![Матрица мер].Form.RecordSource = "SELECT " & _
"матрица_мер.id, матрица_мер.код_меры, " & _
"матрица_мер.группа_меры, матрица_мер.название_меры, " & _
"группы_матрицы.название_группы FROM матрица_мер " & _
"INNER JOIN группы_матрицы ON " & _
"матрица_мер.группа_меры = группы_матрицы.id WHERE " & filter_str
```

При задании фильтров на основе формы из рисунка 5 (а) переменная «*filter_str*» динамически формируется с учетом выбранных в фильтре атрибутов мер обеспечения ИБ. Процесс формирования указанной переменной для атрибута «Возможности» представлен в листинге 2.

Листинг 2 – Формирование переменной «*filter_str*» для фильтрации по атрибуту «*Возможности*»

```
For Each itm In Forms![Фильтр].Возможности.ItemsSelected
    selected_possibilities_count = selected_possibilities_count + 1
    selected_possibilities = selected_possibilities & "," &_
                             Forms![Фильтр].Возможности.Column(0, itm)
Next
selected_possibilities = Mid(selected_possibilities, 2)

filter_possibilities = "SELECT возможности_меры.id_меры " &_
    "FROM возможности_меры WHERE " &_
    "возможности_меры.id_возможности " &_
    "in (" & selected_possibilities & ") GROUP BY " &_
    "возможности_меры.id_меры HAVING " &_
    "COUNT(возможности_меры.id_возможности) = " &_
    "selected_possibilities_count"

filter_str = "1 = 1 "
If selected_possibilities_count > 0 Then
    filter_str = filter_str & "AND матрица_мер.id in (" &_
                              filter_possibilities & ") "
End If
```

IV. Рекомендации по применению разработанной базы данных

Согласно [7], жизненный цикл СУИБ состоит из четырех основных этапов:

– разработка (модернизация) элементов СУИБ;

– внедрение и применение элементов СУИБ;

– мониторинг и анализ реализованных элементов СУИБ;

– поддержание и совершенствование СУИБ.

В общем случае вышеуказанные этапы соответствуют методологии PDCA (цикл Деминга-Шухарта), их взаимосвязь представлена на рисунке 6.

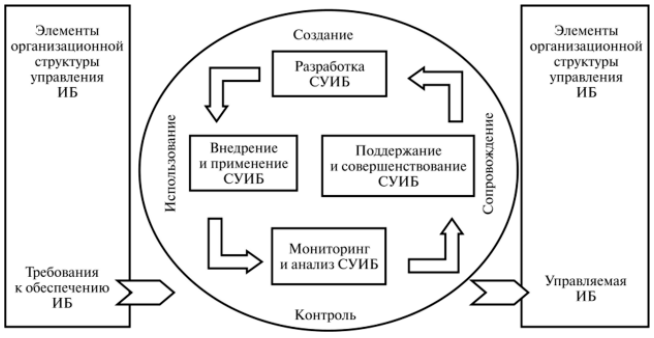


Рисунок 6 – Жизненный цикл СУИБ

На этапе разработки (модернизации) СУИБ формируется соответствующее техническое задание, устанавливающее требования к СУИБ (ее элементам). Указанные требования должны быть отображены на атрибуты и содержание планируемых к внедрению мер обеспечения ИБ. С практической точки зрения это означает, что требования технического задания выступают в качестве источника информации при выставлении параметров фильтров в базе данных мер обеспечения ИБ.

На этапе внедрения и применения элементов СУИБ разработанная база данных используется в качестве руководства по внедрению и применению выбранных мер, обеспечивающих функционирование СУИБ. Информация используется, преимущественно, из

столбца «*рекомендации_по_внедрению*» таблицы «*матрица_мер*».

На этапе мониторинга и анализа практический интерес представляют такие атрибуты меры обеспечения ИБ, как цель меры и содержание меры, на соответствие которым осуществляется контроль.

На этапе поддержания и совершенствования СУИБ осуществляется сравнительный анализ внедренных мер обеспечения ИБ по отношению к тем мерам, предположительное внедрение которых в будущем позволит обеспечить результативность. С практической точки зрения это означает, что лицо, принимающее решение, может использовать базу данных, запущенную в двух окнах одновременно, тем самым наглядно сопоставляя внедренные и планируемые к внедрению меры обеспечения ИБ. Также с использованием базы данных возможно подобрать меры обеспечения ИБ, схожие с характеристиками заданной меры, для чего требуется установить атрибуты этой меры в качестве параметры фильтрации, тогда в графическом интерфейсе будут отображены найденные вхождения схожих мер обеспечения ИБ. Лицу, принимающему решение, будет необходимо осуществить технико-экономический анализ в отношении найденных схожих мер и принять решение о целесообразности замены ими уже внедренных мер обеспечения ИБ.

V. Заключение

Таким образом, разработанная база данных позволяет обеспечить автоматизацию процесса подбора мер обеспечения ИБ для построения СУИБ. Об основных концептуальных предпосылках применения автоматизации при проектировании СУИБ и о функционале базы данных был выполнен доклад [8]. Предлагаемые технологические решения зарегистрированы в качестве объектов интеллектуальной собственности в Роспатенте [3, 4].

Библиография

[1] ГОСТ Р ИСО/МЭК 27002-2021. Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности. – М.: Стандартинформ, 2021. – 74 с.

[2] ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection — Information security controls. Available at: https://www.iso.org/ru/standard/75652.html

[3] Буренок Д. С., Воеводин В. А. База данных мер обеспечения информационной безопасности согласно ИСО/МЭК 27002 // Роспатент. Свидетельство о государственной регистрации базы данных № 2023620576 от 14 марта 2023 г.

[4] Буренок Д. С., Воеводин В. А. Программа многокритериального подбора мер обеспечения информационной безопасности согласно ИСО/МЭК 27002 // Роспатент. Свидетельство о государственной регистрации программы для ЭВМ № 2023619749 от 15 мая 2023 г.

[5] Рубанов В. В. Способы отображения объектов в реляционных базах данных // Труды ИСП РАН. 2002. № 3. С. 139-164.

[6] J. Korol, *Microsoft Access 2019 Programming by Example with VBA, XML, and ASP*. Mercury Learning and Information, 1106 p., 2019. ISBN: 1683924037.

[7] ГОСТ Р ИСО/МЭК 27001-2021. Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. – М.: Стандартинформ, 2022. – 28 с.

[8] Буренок Д.С. База данных мер обеспечения информационной безопасности согласно ИСО/МЭК 27002 // 30-я Всероссийская межвузовская научно-техническая конференция студентов и аспирантов “Микроэлектроника и информатика -2023”, 20 – 21 апреля 2023 года, г. Зеленоград.

On the information security controls database developed in accordance with ISO/IEC 27002:2022

D.S. Burenok, V.A. Voevodin

***Abstract* — The article describes a database containing a set of information security controls to automate the process of implementing an information security management system (ISMS). Author justifies the structure of the database of information security controls, using which it is possible to carry out the design of an appropriate ISMS and design a formal ontology of the subject area. The solution is based on the clauses of the international standard ISO/IEC 27002:2022 and the results of analysis of the attributes of information security measures specified in ISO/IEC 27002:2022. The database is designed within a relational data model and provided with a graphical interface for user interaction. MS Access is used as the database management system. Interactive functionality of the database is implemented in the VBA programming language, as well as using built-in MS Access elements. SQL syntax is used to generate queries. The novelty of the database involves the use of a two-level graphical interface and the implementation of features to select information security controls based on the specified filters. The proposed solution allows to automate the process of building an ISMS. Parts of the solution were registered as intellectual property objects in Russian patent and trademark office (Rospatent).**

***Keywords*—information security management system design, automation, relational database, security controls.**

REFERENCES

[1] GOST R ISO/IEC 27002-2021. Information technology — Security techniques — Code of practice for information security controls. – Standardinform publ., 2021. Available at: https://protect.gost.ru/v.aspx?control=8&id=230363

[2] ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection — Information security controls. Available at: https://www.iso.org/ru/standard/75652.html

[3] D. S. Burenok and V. A. Voevodin, "The information security controls database in accordance with ISO/IEC 27002:2022" RF certificate of state registration of a database, no. 2023620576, 2023.

[4] D. S. Burenok and V. A. Voevodin, "The program for multi-criteria selection of information security controls in accordance with ISO/IEC 27002" RF certificate of state registration of a computer program, no. 2023619749, 2023.

[5] V. V Rubanov, Sposoby otobrazheniya ob"ektov v relyatsionnykh bazakh dannykh. Trudy ISP RAN, no. 3, 2002, pp. 139-164.

[6] J. Korol, *Microsoft Access 2019 Programming by Example with VBA, XML, and ASP*. Mercury Learning and Information, 2019. ISBN: 1683924037.

[7] GOST R ISO/IEC 27001-2021. Information technology — Security techniques — Information security management systems — Requirements. – Standardinform publ., 2022. Available at: https://protect.gost.ru/v.aspx?control=8&id=231601

[8] D. S. Burenok. The information security controls database in accordance with ISO/IEC 27002:2022// 30-ya Vserossiiskaya mezhvuzovskaya nauchno-tekhnicheskaya konferentsiya studentov i aspirantov “Mikroelektronika i informatika-2023”, 20 – 21 apr., 2023, Zelenograd.