УДК *004.056*

Д.С. Милько[1], П.Н. Наседкин[1]

[1]Иркутский государственный университет путей сообщения, г. Иркутск, Российская Федерация

ЭКСПЕРТНАЯ СИСТЕМА ОЦЕНКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ. ФОРМАЛЬНОЕ ПРЕДСТАВЛЕНИЕ ОБЪЕКТОВ ВОЗДЕЙСТВИЯ

Аннотация. *Оценка угроз безопасности информации необходима для разработки соответствующей модели угроз. Также результаты оценки угроз применяются для выбора и обоснования требуемых мер при построении системы защиты информации. В феврале 2021 года вступил в силу новый методический документ Федеральной службы по техническому и экспортному контролю Российской Федерации (ФСТЭК России), обязательный к исполнению всеми организациями, которые проводят оценку угроз безопасности информации.*

В работе описаны сложности, связанные с реализацией одного из этапов процесса проведения оценки угроз безопасности информации. Указанный этап заключается в проведении оценки актуальности объектов воздействия применительно к конкретной информационной системе. Определены два принципиально новых процесса для оценки актуальности объектов воздействия — введение идентификаторов для объектов воздействия и формализация представления объектов воздействия, позволяющие автоматизировать процесс проведения оценки актуальности объектов воздействия.

Также в работе отражены существующие сложности, связанные с терминологией в обязательном к применению источнике информации об угрозах безопасности — Банке данных угроз, ведение которого осуществляется ФСТЭК России.

Описана процедура выбора актуальных объектов воздействия в качестве одного из этапов алгоритма оценки угроз безопасности информации в целом.

Ключевые слова: *угрозы безопасности информации, модель угроз, экспертная система, банк данных угроз, идентификаторы.*

D.S. Milko[1], P.N. Nasedkin[1]

[1]Irkutsk State Transport University, Irkutsk, the Russian Federation

THREAT MODELING EXPERT SYSTEM. FORMAL REPRESENTATION OF IMPACT OBJECTS

Abstract. *An assessment of information security threats is necessary to develop an appropriate threat model. Also, the results of the threat assessment are used to select and justify the required measures when building an information protection system. In February 2021, a new methodological document of the Federal Service for Technical and Export Control of the Russian Federation (FSTEC of Russia) came into force, which is mandatory for all organizations that assess information security threats.*

The paper describes the difficulties associated with the implementation of one of the stages of the automated process of assessing threats to information security. This stage concerns the assessment of the relevance of the affected objects. Two approaches, which are fundamentally new for the objects of influence, are introduced - the introduction of identifiers for the objects of influence and the formalization of the representation of objects of influence, which allow automating the process of assessing the relevance of objects of influence.

The work also reflects the existing difficulties associated with the use of terminology in the source of information about threats to information security - the Threat Data Bank, which is maintained by the FSTEC of Russia.

An algorithm for selecting objects of influence as a part of the algorithm for assessing threats to information security in general is described.

In the conclusion, recommendations are given regarding the tightening of the rules for maintaining the FSTEC of Russia Threat Databank, namely: the introduction of identifiers of objects of influence, the introduction of more stringent rules for describing objects of influence, amending the terminology used in the FSTEC of Russia Threat Databank

Keywords: *information security threats, threat model, expert system, threat data bank, identifiers.*

Введение

Процедура разработки модели угроз безопасности информации, необходимая при построении систем защиты информации [1], усложнилась с введением Федеральной службой по техническому и экспортному контролю (ФСТЭК России) в действие нового методического документа в феврале 2021 года в пределах ее компетенции [2,3]. Внедрение в процедуру оценки угроз программного комплекса экспертной оценки позволит снизить временные, финансовые и иные издержки организаций на проведение оценки угроз [4]. Схема алгоритма проведения экспертной оценки угроз безопасности информации с применением программного комплекса представлена на рисунке 1.

Для разработки и внедрения указанного программного комплекса подлежит проработке ряд вопросов. В частности, экспертная система, в отличие от эксперта-человека, способна работать только с формальным описанием объектов воздействия, а не с терминами и определениями. Поэтому для реализации программного комплекса необходимо привести описание объектов воздействия в формальном виде. Проработка указанного вопроса позволит автоматизировать второй этап алгоритма, представленного на рисунке 1.

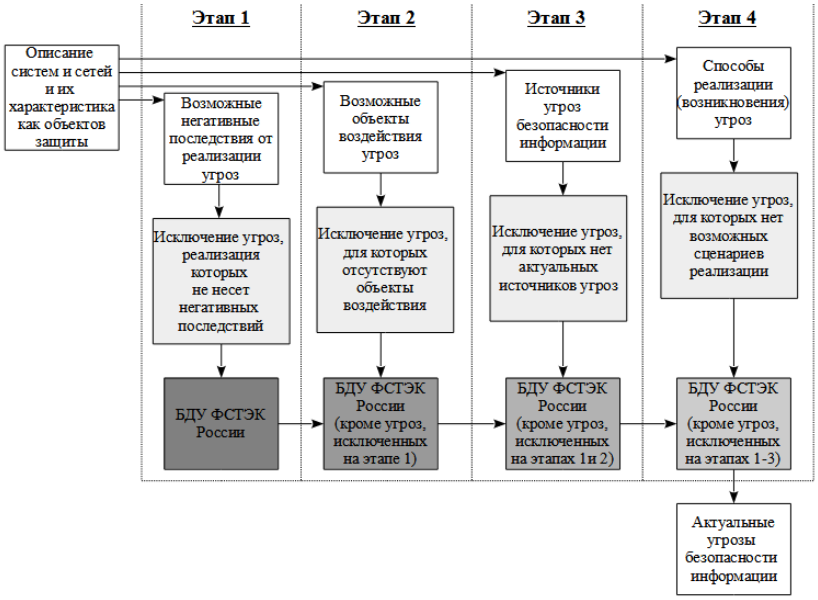

Рис. 1. Схема алгоритма работы экспертной системы оценки угроз безопасности информации.

Результатом выполнения настоящей работы планируется получение структурированного и формализованного представления сведений об объектах воздействия, которые описаны в Банке данных угроз (БДУ), ведение которого осуществляется ФСТЭК России [5].

Настоящая статья состоит из введения, трех разделов и заключения. В первом разделе раскрыто понятие объектов воздействия, а также виды и типы их классификации, на основании которых предложена новая система идентификаторов, приведены основные преимущества, получаемые от введения идентификаторов. Во втором разделе описаны сложности существующего представления объектов воздействия в БДУ ФСТЭК России, связанные с применением существующих разделителей в описании объектов воздействия, а

также с терминологией, используемой в БДУ ФСТЭК России. В третьем разделе приведена модель реализации этапа оценки объектов воздействия с использованием новой системы идентификаторов в качестве одного из этапов процедуры оценки угроз безопасности с применением программного комплекса.

1. Идентификаторы объектов воздействия

Под объектами воздействия понимаются информационные ресурсы и компоненты систем и сетей, несанкционированный доступ к которым или воздействие на которые в ходе реализации (возникновения) угроз безопасности информации может привести к негативным последствиям [2]. Объекты воздействия имеют связь для информационного обмена с другими информационными ресурсами и компонентами систем и сетей, называемые интерфейсами. Объекты воздействия определяются путем инвентаризации ресурсов и группируются по следующим категориям [2]:

- информация (данные), содержащаяся в системах и сетях;
- программно-аппаратные средства обработки и хранения информации;
- программные средства;
- машинные носители информации;
- телекоммуникационное оборудование;
- средства защиты информации;
- привилегированные и непривилегированные пользователи систем и сетей, а также интерфейсы взаимодействия с ними;
- обеспечивающие системы.

Указанные категории объектов воздействия находятся во взаимосвязи между собой, которую можно изобразить графически (рисунок 2).

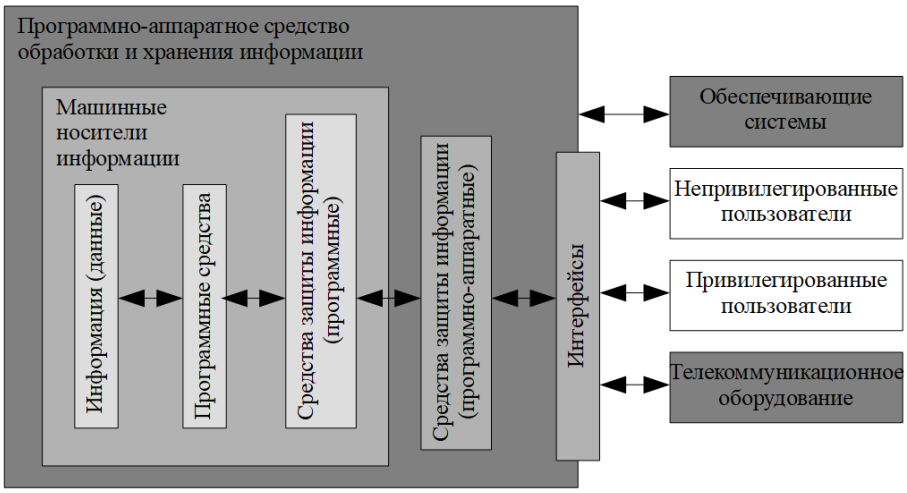

Рис. 2. Типовая структура связей объектов воздействия.

Актуальный методический документ ФСТЭК России также требует распределения объектов воздействия по пяти уровням архитектуры систем и сетей: аппаратный, системный, прикладной, уровень сетевой модели взаимодействия, а также уровень пользователей [2].

Комбинируя указанные выше категории объектов воздействия (рис. 2) и уровни архитектуры систем и сетей, для каждого подлежащего рассмотрению объекта воздействия предлагается присваивать идентификаторы следующего формата:

$$OB.X.Y.N, \quad (1)$$

где ОВ — постоянный префикс, обозначающий сокращение от «объект воздействия»;

X – указатель уровня архитектуры систем и сетей, к которому относится объект воздействия (1 — аппаратный; 2 — системный; 3 – прикладной; 4 - уровень сетевой модели взаимодействия; 5 - уровень пользователей);

Y – указатель группы информационных ресурсов и компонентов систем и сетей (1 - информация (данные), содержащаяся в системах и сетях; 2 - программно-аппаратные средства обработки и хранения информации; 3 - программные средства; 4 - машинные носители информации; 5 - телекоммуникационное оборудование; 6 - средства защиты информации; 7 - привилегированные и непривилегированные пользователи систем и сетей, а также интерфейсы взаимодействия с ними; 8 - обеспечивающие системы), для некоторых уровней архитектуры может отсутствовать;

N — порядковый номер объекта воздействия внутри указанных уровня архитектуры и группы информационных ресурсов.

Примеры распределения объектов воздействия относительно уровней архитектуры, а также указателей группы информационных ресурсов и компонентов систем и сетей приведены в таблице 1.

Таблица 1

Пример распределения объектов воздействия по уровням архитектуры и указателям групп информационных ресурсов и компонентов систем и сетей

X	Y	Примеры объектов воздействия
1 - аппаратный	1 - информация (данные), содержащаяся в системах и сетях	Низкоуровневые данные (биты), файловая система
	2 — программно-аппаратные средства обработки и хранения информации	Технические средства, серверы, автоматизированные рабочие места, программируемые логические контроллеры, распределенные системы контроля
	3 - программные средства	BIOS и микропрограммы
	4 - машинные носители информации	Жесткие магнитные диски, SSD-накопители, USB-flash накопители, оптические накопители, оперативная память
	5 - телекоммуникационное оборудование	Сетевая карта
	6 - средства защиты информации	Модуль доверенной загрузки
	7 - привилегированные и непривилегированные пользователи систем и сетей, а также интерфейсы взаимодействия с ними	Учетные записи пользователей для доступа к BIOS и микропрограммам, устройства ввода-вывода
	8 - обеспечивающие системы	Внутренний блок электропитания, внутренний блок охлаждения
2 - системный	1 - информация (данные), содержащаяся в системах и сетях	Реестр операционной системы
	3 - программные средства	Системное программное обеспечение, гипервизор
	4 - машинные носители информации	Логические разделы
	5 - телекоммуникационное оборудование	Сетевой идентификатор устройства
	6 - средства защиты информации	Операционная система в защищенном исполнении
	7 - привилегированные и непривилегированные пользователи систем и сетей, а также интерфейсы взаимодействия с ними	Учетные записи пользователей для доступа к операционной системе, интерфейс операционной системы
3 - прикладной	1 - информация (данные), содержащаяся в системах и сетях	Файл, каталог
	3 - программные средства	Прикладное программное обеспечение, управленческие системы, другие программные средства контроля
	4 - машинные носители информации	Виртуальный носитель информации, образ диска
	5 - телекоммуникационное оборудование	Сетевой порт
	6 - средства защиты информации	Антивирус, средство защиты информации от несанкционированного доступа
	7 - привилегированные и непривилегированные пользователи систем и сетей, а также интерфейсы взаимодействия с ними	Учетные записи пользователей для доступа к приложениям, интерфейс приложения
4 - уровень сетевой	1 - информация (данные), содержащаяся в системах и сетях	Биты, пакеты данных
	2 — программно-аппаратные средства обработки и хранения	Телекоммуникационное оборудование

модели взаимодействия	информации	
	3 - программные средства	Программное обеспечение телекоммуникационного оборудования
	4 - машинные носители информации	Внутренние накопители телекоммуникационного оборудования, оперативная память
	5 - телекоммуникационное оборудование	Маршрутизатор, коммутатор
	6 - средства защиты информации	Межсетевые экраны, системы обнаружения вторжений
	7 - привилегированные и непривилегированные пользователи систем и сетей, а также интерфейсы взаимодействия с ними	Сетевые учетные записи пользователей, консоли для взаимодействия с телекоммуникационным оборудованием
	8 - обеспечивающие системы	Климатическое оборудование, электропитание, заземление, каналы связи
5 - уровень пользователей	6 - средства защиты информации	Средства физической защиты
	7 - привилегированные и непривилегированные пользователи систем и сетей, а также интерфейсы взаимодействия с ними	Пользователи
	8 — обеспечивающие системы	Климатическое оборудование, система освещения, системы водоснабжения и водоотведения

Внедрение идентификаторов для объектов воздействия позволит реализовать несколько важных функций [6]:

- отличие объектов воздействия друг от друга, в том числе при автоматизированной обработке;
- однозначное распределение объектов воздействия по уровням архитектуры систем и сетей;
- однозначное распределение объектов воздействия по группам информационных ресурсов;
- упорядочивание объектов воздействия;
- установление связей между объектами воздействия по принципу «часть-целое»;
- однозначная проверка корректности.

2. Формализация представления объектов воздействия

Для определения объектов воздействия могут быть изучены открытые источники информации об угрозах (БДУ ФСТЭК России, CAPEC, ATT&CK, OWASP, STIX, WASC и др.), а также отраслевые (ведомственные, корпоративные) модели угроз безопасности информации [2]. При этом БДУ ФСТЭК России является обязательным для рассмотрения источником информации об угрозах.

В условиях решения реальных задач база знаний экспертной системы должна, как минимум, содержать актуальные сведения об объектах воздействия из обязательного источника информации об угрозах - БДУ ФСТЭК России. Таким образом, на предварительном этапе работы экспертная система должна получать актуальные сведения об объектах воздействия из БДУ ФСТЭК России.

БДУ ФСТЭК России предполагает выгрузку всех данных об угрозах путем обращения через веб-интерфейс по адресу https://bdu.fstec.ru/files/documents/thrlist.xlsx одним файлом формата Open XML (расширение *.xlsx). Данный файл содержит описание угроз в текстовом варианте в столбце «Е». Однако, представленные сведения недостаточно формализованы.

Во-первых, для столбца «Е» не установлен единый формат разделителя при перечислении нескольких объектов воздействия. Для большинства представленных угроз безопасности в качестве разделителя при перечислении нескольких объектов воздействия используется знак запятой («,»). Но для угроз с порядковыми идентификаторами от УБИ.218 до УБИ.222 (угрозы, связанные с технологиями машинного обучения и искусственного интеллекта) использован знак точки с запятой («;»), а для угрозы УБИ.180 (угроза отказа подсистемы обеспечения температурного режима) - знак запятой («,») совместно с буквой «и».

По причине отсутствия единого формата разделителя в указанном столбце для всех угроз безопасности информации использование функции «Текст по столбцам...», имеющейся в большинстве известных табличных редакторов, приводит к неудовлетворительному результату автоматической обработки (рисунки 3 и 4). Аналогичный результат будет получен при автоматическом обновлении сведений об объектах воздействия в базе знаний экспертной системы.

ID угрозы	Объекты воздействия
УБИ.056	Информационная система, иммигрированная в облако, облачная система
УБИ.080	Виртуальные устройства хранения, обработки и передачи данных
УБИ.089	Системное программное обеспечение, использующее реестр, реестр
УБИ.180	Технические средства воздушного кондиционирования, включая трубопроводные системы для циркуляции охлаждённого воздуха в ЦОД, программируемые логические контроллеры, распределённые системы контроля, управленческие системы и другие программные средства контроля

Рис. 3. Данные об объектах воздействия, представленные в БДУ ФСТЭК, для угроз УБИ.056, УБИ.080, УБИ.089, УБИ.180.

ID угрозы	Объект воздействия 1	Объект воздействия 2	Объект воздействия 3	Объект воздействия 4	Объект воздействия 5
УБИ.056	Информационная система	иммигрированная в облако	облачная система		
УБИ.080	Виртуальные устройства хранения	обработки и передачи данных			
УБИ.089	Системное программное обеспечение	использующее реестр	реестр		
УБИ.180	Технические средства воздушного кондиционирования	включая трубопроводные системы для циркуляции охлаждённого воздуха в ЦОД	программируемые логические контроллеры	распределённые системы контроля	управленческие системы и другие программные средства контроля

Рис. 4. Некорректные результаты работы функции «Текст по столбцам...» для угроз УБИ.056, УБИ.080, УБИ.089, УБИ.180.

Таким образом использование в качестве разделителя объектов воздействия знака запятой («,») некорректно, так как при описании объектов воздействия он должен быть использован при перечислении и введении причастных оборотов внутри описания одного объекта воздействия. Наилучший результат работы функции «Текст по столбцам...» получается после введения вместо знака запятой («,») знака точки с запятой («;») в качестве разделителя для всех объектов воздействия в БДУ ФСТЭК России (рисунки 5 и 6).

ID угрозы	Объекты воздействия
УБИ.056	Информационная система, иммигрированная в облако; облачная система
УБИ.080	Виртуальные устройства хранения, обработки и передачи данных
УБИ.089	Системное программное обеспечение, использующее реестр; реестр
УБИ.180	Технические средства воздушного кондиционирования, включая трубопроводные системы для циркуляции охлаждённого воздуха в ЦОД; программируемые логические контроллеры; распределённые системы контроля; управленческие системы; другие программные средства контроля

Рис. 5. Данные об объектах воздействия для угроз УБИ.056, УБИ.080, УБИ.089, УБИ.180, полученные после изменения разделителя на знак точки с запятой.

ID угрозы	Объект воздействия 1	Объект воздействия 2	Объект воздействия 3	Объект воздействия 4
УБИ.056	Информационная система, иммигрированная в облако	облачная система		
УБИ.080	Виртуальные устройства хранения, обработки и передачи данных			
УБИ.089	Системное программное обеспечение, использующее реестр	реестр		
УБИ.180	Технические средства воздушного кондиционирования, включая трубопроводные системы для циркуляции охлаждённого воздуха в ЦОД	программируемые логические контроллеры	распределённые системы контроля	управленческие системы и другие программные средства контроля

Рис. 6. Корректные результаты работы функции «Текст по столбцам...» для угроз УБИ.056, УБИ.080, УБИ.089, УБИ.180.

Во-вторых, требуется изменить ряд терминов, определяющих объекты воздействия в БДУ ФСТЭК России (рекомендации по внесению изменений приведены в таблице 2). На текущий момент одинаковые по существу объекты воздействия в столбце «Е» отличаются по своему текстовому описанию.

Таблица 2

Рекомендации по внесению изменений в текстовое описание объектов воздействия

№ п/п	Текстовые описания объекта воздействия, которые встречаются в БДУ ФСТЭК России	Возможная форма для замены существующего	Комментарий

		текстового описания	
1.	Аппаратное обеспечение Аппаратное средство Аппаратное устройство Техническое средство	Технические средства или программно-аппаратные средства	В соответствии с терминологией ГОСТ Р ИСО/МЭК 9126-93 [7]
2.	Рабочая станция Средство вычислительной техники Стационарные и мобильные устройства (компьютеры и ноутбуки) (аппаратное устройство)	Программно-аппаратные средства обработки и хранения информации	В соответствии с терминологией Методики оценки угроз безопасности информации [2]
3.	Аутентификационные данные пользователя (программное обеспечение) Учетные данные пользователя Учётные данные пользователя	Данные об учетных записях	В соответствии с терминологией ГОСТ Р 57429-2017 [8], указать с буквой «е»
4.	Виртуальные диски Виртуальные устройства хранения Виртуальные устройства хранения данных Виртуальные устройства хранения обработки и передачи данных	Виртуальные накопители	В соответствии с терминологией ГОСТ Р 56938-2016 [9]
5.	Вычислительные узлы суперкомпьютера Вычислительный узел суперкомпьютера	Вычислительный узел суперкомпьютера	Указать в единственном числе
6.	Защищаемые данные Информационные ресурсы Информация	Защищаемая информация	В соответствии с терминологией ГОСТ Р 50922-2006 [10]
7.	Объект файловой системы Объекты файловой системы Файлы	Файлы и каталоги	В соответствии с терминологией ГОСТ Р 57429-2017 [8]
8.	Канал связи Каналы передачи данных суперкомпьютера Каналы связи Каналы связи (передачи) данных	Канал связи	
9.	Машинные носители информации Машинный носитель информации Носители информации Носитель информации	Машинный носитель информации	В соответствии с терминологией Методики оценки угроз безопасности информации [2], указать в единственном числе
10.	Мобильное устройство Мобильное устройство (аппаратное устройство) Мобильные устройства (аппаратное устройство)	Мобильное устройство	Указать в единственном числе
11.	Программное обеспечение Программное обеспечение (программы), запущенные на мобильном устройстве приложения (программное обеспечение)	Программные средства	В соответствии с терминологией Методики оценки угроз безопасности информации [2]
12.	Сетевое оборудование Телекоммуникационное устройство	Телекоммуникационное оборудование	В соответствии с терминологией Методики оценки угроз безопасности информации [2]
13.	Средства защиты информации Средство защиты информации Система управления доступом, встроенная в операционную систему компьютера (программное обеспечение)	Средство защиты информации	Указать в единственном числе, в соответствии с терминологией Методики оценки угроз безопасности информации [2]
14.	Технические средства воздушного кондиционирования, включая трубопроводные системы для циркуляции охлаждённого воздуха в ЦОД	Климатическое оборудование центра обработки данных	В соответствии с терминологией ГОСТ Р 54671-2011 [11]
15.	Информация, хранящаяся на компьютере во временных файлах (программное обеспечение)	Защищаемая информация, хранящаяся во временных файлах	В соответствии с терминологией Методики оценки угроз

			безопасности информации

Во избежание возникновения коллизий при дальнейшем присвоении уникальных идентификаторов необходимо привести к единому соответствию термины, определяющие объекты воздействия в БДУ ФСТЭК России. Сведения в разделе «Термины» [12] БДУ ФСТЭК России, касающиеся указанных объектов доступа отсутствуют.

Процедура формализации не требуется при проведении оценки угроз безопасности без использования средства автоматизации — эксперт самостоятельно способен разобраться с терминами в области защиты информации. В свою очередь, для разработки автоматизированного программного комплекса оценки угроз безопасности информации, проведение формализации объектов воздействия необходимо с целью корректного составления диалоговых окон с пользователем, не являющимся экспертом. Диалоговые окна, связанные с объектами воздействия, описаны в разделе 3 настоящей работы.

Процедуру формализации объектов воздействия при разработке экспертной системы возможно провести и самостоятельно, без привлечения разработчика БДУ ФСТЭК России. Однако, в таком случае указанная процедура должна будет проводиться регулярно вручную, с неизвестной периодичностью с целью отслеживания изменений в уже известных ФСТЭК России угрозах безопасности информации. Формализация объектов воздействия разработчиком БДУ ФСТЭК России позволит программному комплексу оценки угроз опрашивать указанный ресурс и автоматически безошибочно получать сведения об изменениях в нем.

3. Описание процедуры выбора актуальных объектов воздействия как части алгоритма работы экспертной системы

Условие актуальности угрозы безопасности информации, приведенное в методическом документе, можно представить в логическом виде:

$$A_i = [У_i \wedge O_i \wedge H_i \wedge C_i], \quad (2)$$

где i – индекс, соответствующий одной из 222 угроз безопасности информации в БДУ ФСТЭК России;

A_i – актуальность i-й угрозы;

$У_i$ – негативные последствия, связанные с ущербом от i-й угрозы;

O_i – объект воздействия i-й угрозы;

H_i – нарушитель (источник i-й угрозы);

C_i – способ реализации i-й угрозы.

В соответствии с (2), угроза безопасности информации возможна (актуальна), если реализация угрозы может привести к негативным последствиям, имеются объект, на который осуществляется воздействие, способы реализации угрозы и нарушитель (источник угрозы).

При работе второго этапа алгоритма пользователь через интерфейс программного комплекса должен сообщить системе сведения об имеющихся объектах воздействия (О), актуальных для объекта информатизации. Экспертная система должна сопоставить эти сведения с характеристиками угроз безопасности информации и исключить неактуальные угрозы безопасности.

Указанное условие выбора актуальных объектов воздействия можно также представить в логическом виде для каждой угрозы безопасности информации в БДУ ФСТЭК России:

$$O_i = [OB_i^1, OB_i^2, \dots, OB_i^N], \quad (3)$$

где i – индекс, соответствующий одной из 222 угроз безопасности информации в БДУ ФСТЭК России;

$OB_i^1 \dots OB_i^N$ — объекты воздействия для i-й угрозы с 1-го по N-й.

Таким логическим представлением можно описать все объекты воздействия всех угроз безопасности, представленных в БДУ ФСТЭК России. Например, условие актуальности по

наличию объектов воздействия для уже упомянутых угроз УБИ.056, УБИ.080, УБИ.089 и УБИ.180 (рисунок 6) можно представить в логическом виде следующим образом:

$$О_{056} = [ОВ_{056}^{1} \vee ОВ_{056}^{2}]; \quad (4)$$

$$О_{080} = [ОВ_{080}]; \quad (5)$$

$$О_{089} = [ОВ_{089}^{1} \vee ОВ_{089}^{2}]; \quad (6)$$

$$О_{180} = [ОВ_{180}^{1} \wedge (ОВ_{180}^{2} \vee ОВ_{180}^{3} \vee ОВ_{180}^{4} \vee ОВ_{180}^{5})]. \quad (7)$$

Представление (4) формально описывает, что угроза некачественного переноса инфраструктуры в облако (УБИ.056) актуальна для информационной системы, при условии что имеется информационная система, иммигрированная в облако ($ОВ_{056}^{1}$) или облачная система ($ОВ_{056}^{2}$). А представление (7) позволяет формально описать, что угроза отказа подсистемы обеспечения температурного режима (УБИ.180) актуальна для информационной системы, при условии что в информационной системе имеются техническое средство воздушного кондиционирования, включая трубопроводные системы для циркуляции охлаждённого воздуха в ЦОД ($ОВ_{180}^{1}$) и хотя бы один объект воздействия из перечисленных: программируемые логические контроллеры ($ОВ_{180}^{2}$); распределённые системы контроля ($ОВ_{180}^{3}$); управленческие системы ($ОВ_{180}^{4}$); другие программные средства контроля ($ОВ_{180}^{5}$).

А после введения единой системы идентификаторов, представленных в разделе 1, указанная запись об объектах воздействия угрозы УБИ.180 может быть представлена в базе знаний экспертной системы как:

$$О_{180} = [ОВ.4.8.1 \wedge (ОВ.1.2.1 \vee ОВ.1.2.2 \vee ОВ.3.3.1 \vee ОВ.3.3.2)], \quad (8)$$

где $О_{180}$ – индекс, соответствующий условию актуальности по наличию объектов воздействия для угрозы УБИ.180;

ОВ.4.8.1 — объект воздействия «техническое средство воздушного кондиционирования, включая трубопроводные системы для циркуляции охлаждённого воздуха в ЦОД»;

ОВ.1.2.1 — объект воздействия «программируемые логические контроллеры»;

ОВ.1.2.2 — объект воздействия «распределённые системы контроля»;

ОВ.3.3.1 — объект воздействия «управленческие системы»;

ОВ.3.3.2 — объект воздействия «другие программные средства контроля».

Полученный алгоритм второго этапа работы экспертной системы по оценке угроз безопасности информации описан ниже.

1) Подготовить базу знаний:

1.1) произвести проверку актуальности сведений, представленных в базе знаний экспертной системы, путем сверки с БДУ ФСТЭК России;

1.2) в случае появления изменений в БДУ ФСТЭК России, касающихся объектов воздействия, сделать запрос эксперту на формирование новых связей в базе знаний путем установления логических символов («и», «или», «не» и т. д.) для угроз, в которых произошло изменение сведений об объектах воздействия;

2) Опросить эксперта о наличии или отсутствии в информационной системе объектов воздействия;

3) Обработать данные, предоставленные экспертом на предыдущих этапах на основе сформированной базы знаний;

4) Исключить из перечня рассматриваемых угроз те, для которых не выполняются условия по наличию объектов воздействия.

Пример диалоговых окон экспертной системы, разработанных с использованием языка программирования «Python» и библиотеки «Tk» в среде операционной системы «Windows 10», представлен на рисунках 7-11.

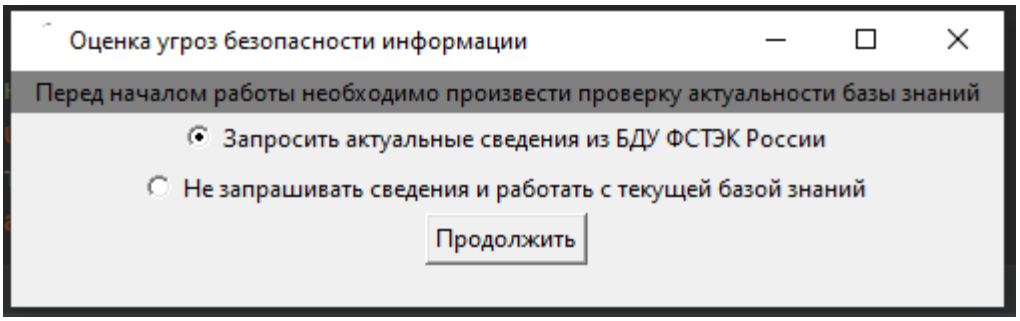

Рис. 7. Окно программы с запросом произвести проверку актуальности сведений, представленных в базе знаний экспертной системы, путем сверки с БДУ ФСТЭК России.

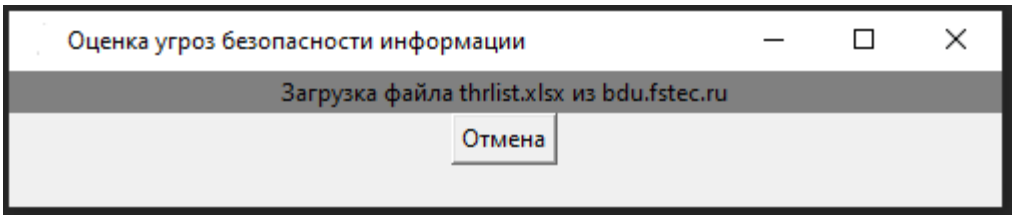

Рис. 8. Окно программы в процессе запроса сведений из БДУ ФСТЭК России.

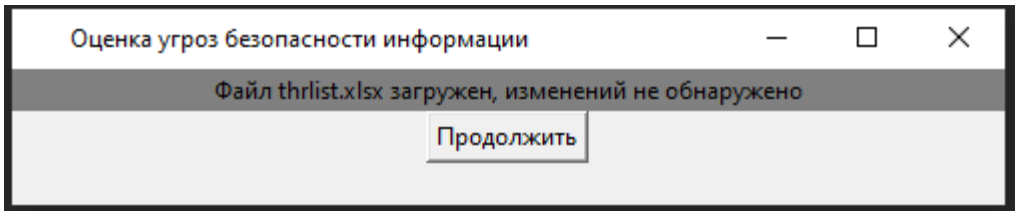

Рис. 9. Окно программы по окончании процедуры сверки сведений из базы знаний экспертной системы об объектах воздействия со сведениями в БДУ ФСТЭК России.

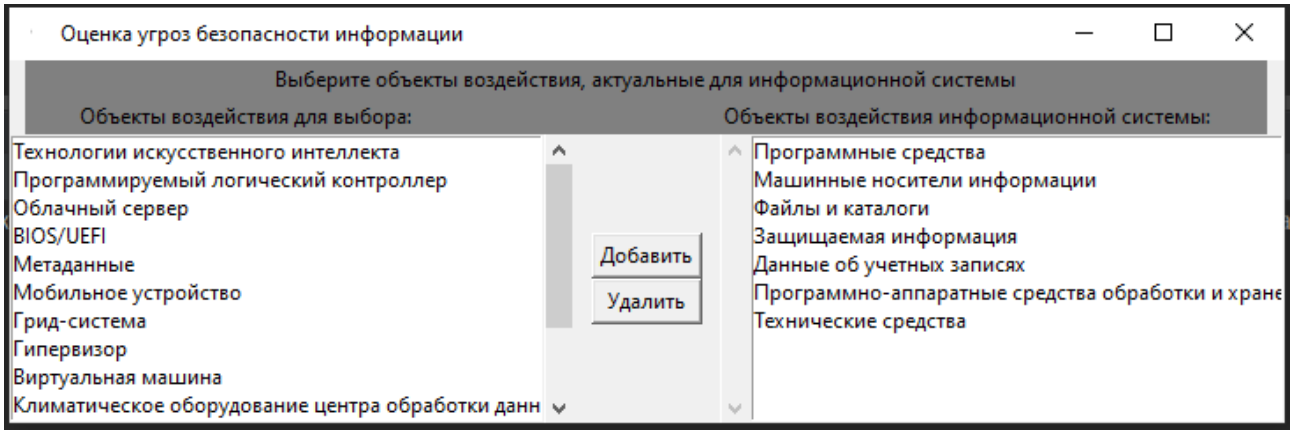

Рис. 10. Диалоговое окно опроса эксперта по информационной безопасности на предмет выбора возможных объектов воздействия.

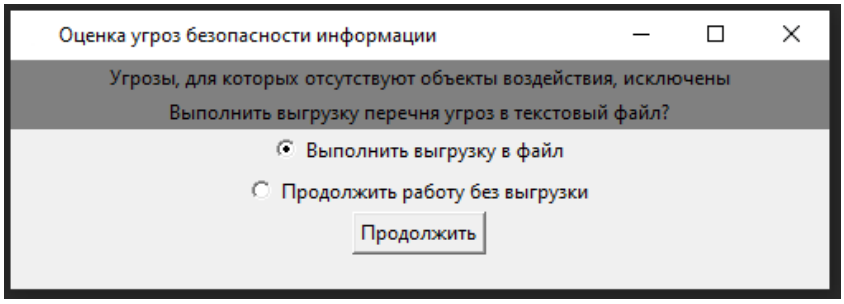

Рис. 11. Окно программы по окончании процедуры выбора актуальных объектов воздействия.

Заключение

В результате выполнения настоящей работы получены структура и описание формального представления сведений об объектах воздействия, представленных в БДУ ФСТЭК России.

Результаты работы позволят представить объекты воздействия в виде переменных, понятных для разрабатываемой экспертной системы оценки угроз безопасности информации. Тем самым станет возможным автоматически исключать из рассмотрения те угрозы безопасности, реализация которых невозможна ввиду отсутствия объектов воздействия.

Для дальнейшей разработки экспертной системы требуется введение более строгого регламента для внесения сведений в БДУ ФСТЭК России, а именно: введение идентификаторов объектов воздействия, введение более строгих правил описания объектов воздействия с использованием разделителей, внесение корректировок в используемую терминологию.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Конев А.А. Подход к построению модели угроз защищаемой информации // Доклады ТУСУР. 2012. №1-2 (25). С. 34–39.

2. Методический документ ФСТЭК России от 05.02.2021 «Методика оценки угроз безопасности информации».

3. Указ Президента РФ от 16.08.2004 № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».

4. ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Дата введения 01.10.2009.

5. Банк данных угроз ФСТЭК России [Электронный ресурс]. URL: https://bdu.fstec.ru/threat (дата обращения 03.05.2021).

6. Серов А. В. Системы идентификаторов объектов и работа с ними // Вестник Сыктывкарского университета. Серия 1. Математика. Механика. Информатика. 2001. №4.

7. ГОСТ Р ИСО/МЭК 9126-93. Информационная технология. Оценка программной продукции. Характеристики качества и руководства по их применению. Дата введения 28.12.1993.

8. ГОСТ Р 57429-2017. Судебная компьютерно-техническая экспертиза. Термины и определения. Дата введения 01.09.2017.

9. ГОСТ Р 56938-2016. Защита информации при использовании технологий виртуализации. Общие положения. Дата введения 01.06.2017.

10. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. Дата введения 01.02.2008.

11. ГОСТ Р 54671-2011 (ЕН 14511-1:2011). Кондиционеры, агрегатированные охладители жидкости и тепловые насосы с компрессорами с электроприводом для обогрева и охлаждения помещений. Термины и определения. Дата введения 01.07.2012.

12. Термины - Банк данных угроз ФСТЭК России [Электронный ресурс]. URL: https://bdu.fstec.ru/terms (дата обращения 03.05.2021).

REFERENCES

1. Konev A.A. Podhod k postroeniyu modeli ugroz zashishaemoi informatsii [Approach to creation protected information model] // Doklady TUSUR [TUSUR reports]. 2012 No. 1-2 (25). pp. 34–39.
2. Methodological document of the FSTEC of Russia dated 05.02.2021 «Methodology for assessing information security threats».
3. Decree of the President of the Russian Federation No. 1085 of 16.08.2004 «Issues of the Federal Service for Technical and Export Control».
4. GOST R 53114-2008. Information security. Ensuring information security in the organization. Basic terms and definitions. Valid from 01.10.2009.
5. Bank Dannyh Ugroz FSTEC Rossii [Threat Data Bank of the FSTEC of Russia] [Electronic resource]. URL: https://bdu.fstec.ru/threat (accessed 03.05.2021).
6. Serov A. V. Sistemy identifikatorov objektov i rabota s nimi [Object identifier systems and work with them] // Vestnik Syktyvkarskogo universiteta [Syktyvkar University Bulletin]. Ep.1. Mathematics. Mechanics. Information Techniligy. 2001. No 4.
7. GOST R ISO/IEC 9126-93. Information technology. Software product evaluation. Qualitycharacteristics and guidelines for their use.Valid from 28.12.1993.
8. GOST R 57429-2017. Forensic information technology examination. Terms and definitions. Valid from 01.09.2017.
9. GOST R 56938-2016. Information protection. Information security with virtualization technology. General. Valid from 01.06.2017.
10. GOST R 50922-2006. Protection of information. Basic terms and definitions. Valid from 01.02.2008.
11. GOST R 54671-2011 (EH 14511-1:2011). Air conditioners, liquid chilling packages and heat pumps with electrically driven compressors for space heating and cooling. Terms and definitions. Valid from 01.07.2012.
12. Teminy - Bank Dannyh Ugroz FSTEC Rossii [Therms - Threat Data Bank of the FSTEC of Russia] [Electronic resource]. URL: https://bdu.fstec.ru/terms (accessed 03.05.2021).

Информация об авторах

Милько Дмитрий Сергеевич - аспирант кафедры «Информационные системы и защита информации», Иркутский государственный университет путей сообщений, г. Иркутск, e-mail: dmitry.s.milko@gmail.com

Наседкин Павел Николаевич - аспирант (ассистент) кафедры «Информационные системы и защита информации», Иркутский государственный университет путей сообщений, г. Иркутск, e-mail: nasedkin_pn@irgups.ru

Authors

Dmitry S. Milko — postgraduate of chair «Information systems and information security», Irkutsk State Transport University, Irkutsk, e-mail: dmitry.s.milko@gmail.com

Наседкин Павел Николаевич - postgraduate (assistant) of chair «Information systems and information security», Irkutsk State Transport University, Irkutsk, e-mail: nasedkin_pn@irgups.ru

Для цитирования

Милько Д.С. Экспертная система оценки угроз безопасности информации. Формальное представление объектов воздействия [Электронный ресурс] / Д.С. Милько, П.Н. Наседкин // Молодая наука Сибири: электрон. науч. журн. – 2021. – №2(12) – Режим доступа: http://mnv.irgups.ru/toma/212-2021, свободный. — Загл. с экрана. — Яз. рус., англ. (дата обращения: 23.06.2021)

For citation

Milko D.S., Nasedkin P.N. - Ekspertnaya sistema ocenki ugroz bezopasnosti informatsii. Formalnoe predtavlenie objektov vozdejstviya [Threat modeling expert system. Formal representation of impact objects]. *Molodaya nauka Sibiri: ehlektronnyj nauchnyj zhurnal* [Young science of Siberia: electronic scientific journal], 2021, no. 2. [Accessed 23/06/21]