ОРИГИНАЛЬНАЯ СТАТЬЯ

2021. № 2 (70). С. 182–189 *Современные технологии. Системный анализ. Моделирование*

DOI 10.26731/1813-9108.2021.2(70).182-189 **УДК** 004.056

Экспертная система оценки угроз безопасности информации: обоснование необходимости разработки, метод и сложности при реализации

Д. С. Милько ✉

Иркутский государственный университет путей сообщения, г. Иркутск, Российская Федерация

✉ dmitry.s.milko@gmail.com

Резюме

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 работе описана значимость проведения оценки угроз безопасности информации при разработке системы защиты информации объекта информатизации. Сравнение нового методического документа по оценке угроз безопасности информации, утвержденного Федеральной службой по техническому и экспортному контролю России в феврале 2021 г. с действовавшим ранее методическим документом показало увеличение трудоемкости процесса оценки актуальности угроз. В связи с этим в статье обоснована необходимость автоматизации процесса оценки угроз безопасности информации. Выделены факторы, которые влияют на увеличение трудоемкости процесса. Наглядно продемонстрирована динамика роста количества угроз безопасности информации в Банке данных угроз Федеральной службы по техническому и экспортному контролю России за время существования этого информационного ресурса. Указано юридическое обоснование возможности автоматизации процесса оценки угроз безопасности информации. В качестве метода автоматизации процесса оценки угроз безопасности выбран метод экспертных систем. Приведены преимущества и недостатки этого метода применительно к указанной задаче. Процесс оценки угроз безопасности информации выделен в формальное представление в виде логического выражения. На основе логического выражения и этапов проведения оценки угроз сформирована схема алгоритма работы экспертной системы. Описано функциональное назначение компонентов схемы. Определены вопросы для дальнейшей проработки при реализации программного комплекса автоматизации оценки угроз безопасности информации методом экспертной системы.

Ключевые слова

угрозы безопасности информации, модель угроз, метод экспертных систем, методический документ, программный комплекс, экспертная система

Для цитирования

Милько Д.С. Экспертная система оценки угроз безопасности информации: обоснование необходимости разработки, метод и сложности при реализации // Современные технологии. Системный анализ. Моделирование. – 2021. – № 2 (70). – С. 182–189. – DOI: 10.26731/1813-9108.2021.2(70).182-189

Информация о статье

поступила в редакцию: 04.05.2021, поступила после рецензирования: 21.05.2021, принята к публикации:03.06.2021

Threat modeling expert system: reasons for development, method and implementation troubles

D. S. Milko ✉

Irkutsk State Transport University, Irkutsk, the Russian Federation

✉ dmitry.s.milko@gmail.com

Abstract

The assessment of information security threats is necessary to develop a threat model. Also, the results of the assessment are needed to choose information protection measures. This paper describes the importance of assessing information security threats in the process of developing an information security system. A comparison of the new methodological document of the FSTEC of Russia (February 2021) with the previously valid methodological document showed an increase in the complexity of threat analysis. In this regard, the paper identifies the need to automate the process of assessing information security threats. It describes the factors that lead to an increase in the complexity of the procedure.The dynamics of the growth of the number of information security threats in the Threat Database of the FSTEC of Russia during its existence is brought into sharp focus. The legal justification of the possibility of automating the analysis of information security threats is indicated.The method of expert systems is selected and justified as a method of automating the process of assessing security threats. The paper provides advantages and disadvantages of the method of expert systems in relation to this problem. The process of assessing information security threats is separated into a formal representation as a logical formula. Based on the logical formula and threat assessment stages, a diagram of the algorithm is formed. The functional purpose of the diagram components is described. The issues for further study in the

implementation of the software package of automating the assessment of information security threats by the expert system method are identified.

Keywords
information security threats, threat model, method of expert systems, methodological document, software package, expert system

For citation
Milko D. S. Ekspertnaya sistema otsenki ugroz bezopasnosti informatsii: obosnovanie neobhodimosti razrabotki, metod i slozhnosti pri realizatsii [Threat modelling expert system: reasons for development, method and implementation troubles]. *Sovremennye tekhnologii. Sistemnyi analiz. Modelirovanie* [*Modern Technologies. System Analysis. Modeling*], 2021, No. 2 (70), pp. 182–189. – DOI: 10.26731/1813-9108.2021.2(70).182-189

Article info
Received: 04.05.2021, Revised: 21.05.2021, Accepted: 03.06.2021

Введение

Разработка модели угроз безопасности информации является одним из обязательных этапов предпроектного обследования при построении систем защиты информации любого уровня сложности [1]. Разработка частной модели угроз безопасности информации проводится путем оценки актуальности угроз конкретного объекта информатизации. Оценка угроз безопасности информации, выполненная с учетом всех особенностей объекта, позволяет построить адекватную и эффективную систему защиты информации без избыточной траты активов организации (в том числе финансовых, людских и прочих [2]) на основе частной модели угроз [3], т. е. частная модель угроз безопасности информации позволяет построить систему защиты информации с выполнением критерия оптимальности (баланса) между защищенностью информации и затратами на реализацию системы защиты информации.

Особенностью оценки угроз безопасности информации является практическая направленность. В современных условиях кадровой необеспеченности задачу разработки моделей угроз безопасности информации приходится решать большому количеству сотрудников, занимающихся защитой информации – от уровня экспертов на крупных предприятиях до уровня техников и системных администраторов в небольших организациях. Существует большое количество организаций, сотрудники которых не являются специалистами в области информационной безопасности, но на них возложены обязанности по защите информации.

Для экспертов высокого уровня подготовленности задача оценки угроз решаема, хотя и не является тривиальной. Однако, с другой стороны, решение данной задачи для объектов информатизации со сложной архитектурой и нетипичными особенностями условий функционирования может быть очень трудоемкой и потребовать дополнительных ресурсов, в том числе информационных путем привлечения сторонних экспертов.

Для специалистов, не обладающих достаточной квалификацией, эта задача может быть не решаема в принципе. С учетом этого организации привлекают для оценки угроз сторонних экспертов на договорной основе [4, 5], что приводит к увеличению затрат финансовых активов организации на обеспечение информационной безопасности [2]. Кроме этого, сторонние эксперты также могут столкнуться со сложностями работы с незнакомым объектом информатизации. В частности, эксперты сторонней организации могут не получить достаточного объема сведений об особенностях условий функционирования объекта информатизации. В таком случае оценка угроз безопасности будет проведена не оптимально, баланс между защищенностью информации и затратами на реализацию системы защиты будет нарушен.

Оценка угроз безопасности информации и разработка модели угроз проводится в соответствии с методическими документами, разработанными и утвержденными Федеральной службой по техническому и экспортному контролю Российской Федерации (ФСТЭК России) [6] и Федеральной службой безопасности Российской Федерации [7] в пределах их компетенций. Трудоемкость оценки угроз безопасности информации выросла с введением ФСТЭК России в действие нового методического документа [8].

Перечисленные предпосылки стали поводом для рассмотрения возможности автоматизации процесса оценки угроз безопасности информации путем разработки программного комплекса.

В настоящей работе перечислены ключевые особенности нового методического документа, которые являются аргументами при обосновании необходимости автоматизации процесса оценки угроз безопасности информации; содержатся юридические основания для разработки такого программного комплекса; описан метод, в соответствии с которым будет разрабатываться программный комплекс; содержится формализованное представление процесса оценки угроз безопасности информации в виде логического выражения и высокоуровневой схемы работы программного комплекса; перечислены за-

дачи, требующие исследования и проработки, для реализации указанного программного комплекса.

Описание особенностей нового методического документа

В начале февраля 2021 г. ФСТЭК России был утвержден методический документ «Методика оценки угроз безопасности информации» [8]. Ключевое отличие нового методического документа от действовавшего ранее заключается в оценке сценариев реализации угроз безопасности информации, которая ранее не проводилась. Ранее существовавший в методических документах подход был основан на вероятностной математической модели и позволял произвести оценку актуальности угроз безопасности информации экспертным методом исходя, в большей степени, из субъективной составляющей [9]. Подход к оценке угроз безопасности в новом методическом документе основан на экспертной оценке возможных сценариев реализации угроз и в меньшей степени зависит от субъективной составляющей.

Предполагается, что эксперт должен провести анализ 10 тактик реализации угроз, которые включают в себя совокупность из 145 техник. Для определения возможных сценариев реализации угроз все тактики и техники должны быть сопоставлены со всеми 222 угрозами безопасности информации, которые содержатся на текущий момент в Банке данных угроз (БДУ) безопасности информации, ведение которого осуществляется ФСТЭК России [10]. Актуальной считается угроза безопасности информации, для которой имеется хотя бы один сценарий для ее реализации.

Следует отметить, что количество угроз в БДУ ФСТЭК России регулярно увеличивается. Далее представлены данные о количестве угроз в БДУ ФСТЭК России, полученные с использованием онлайн-сервиса Internet Archive Wayback Machine (рис. 1) [11].

Таким образом, при перемножении количества техник и количества угроз в БДУ ФСТЭК России, получается внушительное число – 32 190 сценариев реализации угроз. При оценке угроз подлежат рассмотрению все варианты сценариев [9]. Дополнительно к БДУ ФСТЭК России необходимо учитывать отраслевые (ведомственные, корпоративные) модели угроз безопасности информации при их наличии [9].

Конечно, стоит отметить, что часть угроз безопасности информации должны быть исключены из рассмотрения еще до проработки сценариев реализации угроз. Причина исключения состоит в том, что в процессе оценки угроз учитываются структурно-функциональные характеристики объекта информатизации, а далее с учетом указанных характеристик часть угроз признается не актуальными по причине отсутствия той или иной информационной технологии на объекте информатизации [6, 7]. Например, далеко не каждый объект информатизации использует технологии больших данных, суперкомпьютеры, машинное обучение, беспроводные технологии и т. д. В случае, если какая-либо из технологий не используется на объекте информатизации, то все угрозы, связанные с данной технологией, исключаются.

Однако даже в случае исключения некоторого

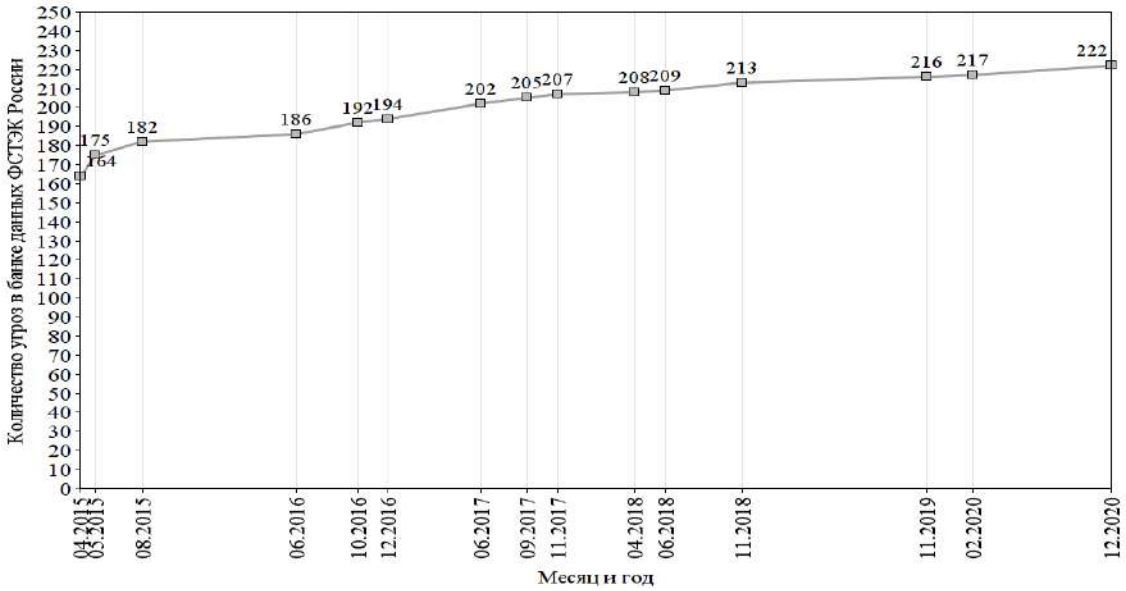

Рис. 1. График количества угроз безопасности информации в базе данных угроз Федеральной службы по техническому и экспортному надзору России за время его существования

Fig. 1. Graph of the number of information security threats in the Federal Service's threat database for technical and export supervision of Russia during its existence

количества угроз из рассмотрения, порядок числа рассматриваемых сценариев остается неизменным. Более того, в настоящий момент практически все объекты информатизации в России постоянно модернизируются [12]. В них регулярно внедряются новые информационные технологии, происходит их усложнение. Помимо этого, становится известно о новых угрозах безопасности информации и уязвимостях информационных технологий [13]. По этим причинам новый методический документ предусматривает периодическую повторную оценку угроз безопасности информации при эксплуатации объекта информатизации с целью постоянной доработки модели угроз и, как следствие, доработки системы защиты информации [9], т. е. даже в самом тривиальном случае, когда в организации имеется всего один объект информатизации, задача оценки угроз становится регулярной и требует периодических трудозатрат со стороны сотрудника, ответственного за обеспечение информационной безопасности. При увеличении количества объектов информатизации на предприятии время, затраченное сотрудником на проведение оценки угроз, будет увеличиваться. В предельном случае выделенные сотрудники должны постоянно работать только над оценкой угроз безопасности информации и доработкой модели.

В дополнение к занятости сотрудников-экспертов в области информационной безопасности следует отметить, что в методическом документе отмечена рекомендация о создании экспертной группы методом Дельфы [14] в интересах снижения субъективных факторов. В состав экспертной группы рекомендуется включать экспертов различной специализации – от специалистов в области информационных технологий до специалистов экономических (финансовых) подразделений [9]. Таким образом, для выполнения указанной рекомендации периодически должны быть задействованы уже несколько сотрудников организации, работающих над оценкой угроз безопасности информации и доработкой модели.

Охват типов объектов информатизации для нового методического документа также увеличился. Методика обязательна к применению для определения угроз безопасности информации в следующих системах:

– государственные (муниципальные) информационные системы;

– информационные системы персональных данных;

– значимые объекты критической информационной инфраструктуры Российской Федерации;

–информационные системы управления производством, используемые организациями оборонно-промышленного комплекса;

– автоматизированные системы управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды [9].

Таким образом, методический документ должен применяться на большинстве объектов информатизации на всех предприятиях на территории Российской Федерации.

Резюмируя особенности нового методического документа, далее будут перечислены факторы, определяющие увеличение трудоемкости оценки угроз безопасности информации в соответствии с новым методическим документом без использования средств автоматизации:

– большое число сочетаний угроз безопасности информации и сценариев их реализации;

– необходимость регулярного проведения повторной оценки угроз безопасности информации;

– привлечение экспертной группы для проведения оценки;

– большое количество объектов информатизации, для которых необходимо руководствоваться указанными методическими рекомендациями при проведении оценки.

Кроме этого, актуальной остается проблема недостаточного количества квалифицированных специалистов по защите информации на предприятиях, способных проводить оценку угроз безопасности информации для всех типов объектов информатизации [15]. Особенно остро эта проблема проявляется в регионах, удаленных от центральной части страны.

По совокупности указанных факторов можно сделать вывод о необходимости автоматизации оценки угроз безопасности информации с целью снижения издержек на ее проведение путем разработки соответствующего программного комплекса.

Правовые основания для автоматизации оценки угроз безопасности информации

Для обоснования возможности разработки программного комплекса автоматизации оценки угроз безопасности информации в методическом документе ФСТЭК России предусмотрены два тезиса: «при оценке угроз безопасности информации могут использоваться программные средства, позволяющие автоматизировать данную деятельность», «ведение модели угроз безопасности информации и поддержание ее в актуальном состоянии может осуществляться в электронном виде» [9].

Представленные тезисы позволяют сделать вывод о том, что для оценки угроз безопасности информации и разработки модели может быть официально использовано программное средство. Указанное программное средство позволит автоматизировать процесс оценки угроз безопасности информации и использовать в работе электронный вариант

модели угроз безопасности информации. Иные требования ФСТЭК России к программным средствам такого вида в настоящий момент отсутствуют.

Обоснование выбранного метода автоматизации оценки угроз безопасности информации

Для автоматизации процесса оценки угроз безопасности был выбран метод разработки экспертных систем. Для такого решения имеется ряд причин, которые связаны с преимуществами и недостатками указанного метода.

Во-первых, преимуществом экспертных систем является логический вывод. В результате работы экспертной системы на основании определенных фактов формируется логичное, оправданное заключение [16]. При реализации метода экспертных систем программный комплекс на основании известных фактов об угрозах безопасности информации формирует логически построенный вывод об актуальности угроз. В отличие от методов машинного обучения экспертная система способна объяснить свои рассуждения, которые привели к определенному заключению. Специалист по защите информации при необходимости должен уметь обосновать принятое решение по оценке угроз безопасности уполномоченным контролирующим органам. Экспертная система оценки угроз безопасности способна оказывать при этом существенную помощь [17, 18].

Во-вторых, экспертная система способна жестко повторять принятое решение независимо от внешних воздействий, т. е. по одним и тем же входным данным программный комплекс даст один и тот же отклик на выходе [16]. Экспертная система не подвержена субъективным факторам при принятии одинаковых решений через определенный период времени.

В-третьих, при использовании экспертных систем снижаются издержки, связанные с предоставлением экспертных знаний [16]. Экспертные знания в таком программном комплексе содержатся в базе знаний. При этом уровень квалификации пользователя экспертной системы может быть ниже уровня квалификации эксперта, который сформировал базу. Иными словами, при использовании программного комплекса для оценки угроз безопасности информации не обязательно привлечение высококвалифицированного специалиста.

В-четвертых, экспертная система позволяет использовать экспертные знания из многих источников [16]. С помощью программного комплекса могут быть собраны знания многих экспертов, которые не всегда могут быть привлечены к работе над оценкой угроз. Тем самым программный комплекс позволит снизить издержки, связанные с многократным привлечением членов экспертной группы без снижения объективности результатов оценки.

В-пятых, один из недостатков экспертных систем – узкая специализация. Одна экспертная система может быть использована только в одной определенной предметной области [16]. В данном случае предметная область определена однозначно как область информационной безопасности. По этой причине указанный недостаток экспертных систем не является препятствием для разработки программного комплекса выбранным методом.

Таким образом, с учетом анализа недостатков и преимуществ метода экспертных систем, можно сделать вывод о том, что именно экспертная система является подходящим вариантом для разработки программного комплекса оценки угроз безопасности информации.

Формализованное представление процесса оценки угроз безопасности информации

Для преобразования принципов, составляющих основу методического документа, в алгоритм работы экспертной системы необходимо формализовать представленный подход к оценке угроз безопасности информации в виде некоторой модели.

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

$$A_i = [У_i \wedge O_i \wedge H_i \wedge C_i], \quad (1)$$

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 (1), 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 этом у всех перечисленных в (1) сущностей имеется ряд свойств, которые необходимо учитывать при разработке экспертной системы. Указанные свойства описаны далее с указанием этапов оценки угроз безопасности информации.

На предварительном этапе пользователь должен провести инвентаризацию на объекте информатизации с целью получения входных данных для ввода в программный комплекс.

На первом этапе для определения возможных негативных последствий ($У$) программный комплекс должен задать пользователю ряд вопросов об объекте информатизации через интерфейс. Ответ на указанные вопросы позволит экспертной системе определить актуальные виды риска (ущерба) от $У1$ до $У3$.

На втором этапе пользователь через интерфейс программного комплекса должен сообщить сведения

о возможных объектах воздействия (*О*), актуальных для объекта информатизации. Экспертная система должна сопоставить эти сведения с характеристиками угроз безопасности информации.

На третьем этапе экспертная система должна задать пользователю вопросы об объекте информатизации, касающиеся актуальных видов нарушителей (источников угрозы, *Н*). Для выполнения третьего этапа экспертная система должна для каждого из видов нарушителей:

– установить соответствие с категорией нарушителя (внешний или внутренний);

– определить возможные цели реализации угрозы с учетом информации об объекте информатизации и субъективной оценки пользователя;

– установить соответствие целей реализации угрозы с видами ущерба, выбранными на первом этапе (от *У*1 до *У*3), и негативными последствиями.

В результате третьего этапа работы экспертной системы будут получены актуальные уровни возможностей нарушителей (от *Н*1 до *Н*4) и результаты оценки целей реализации угроз безопасности информации.

На четвертом этапе экспертная система должна сопоставить результаты работы первых трех этапов со всеми угрозами безопасности из БДУ ФСТЭК России.

Формализованное представление алгоритма работы экспертной системы по оценке угроз безопасности информации в соответствии с актуальным методическим документом ФСТЭК России [9] представлена в виде схемы (рис. 2).

На каждом этапе работы программного комплекса будут исключены те угрозы из БДУ ФСТЭК России, которые не могут быть реализованы на объекте информатизации по следующим причинам:

– реализация угрозы не приведет к негативным последствиям (ущербу) для организации;

– отсутствуют возможные объекты воздействия для реализации угрозы;

– отсутствуют нарушители безопасности информации, заинтересованные в реализации угрозы;

– отсутствуют возможные сценарии реализации угрозы безопасности информации;

Сведения, указанные в блоках белого цвета на схеме алгоритма работы экспертной системы, должны быть представлены в частной модели угроз безопасности информации.

Заключение

Разрабатываемый программный комплекс оценки угроз безопасности информации позволит снизить издержки организаций на проведение оценки угроз безопасности информации в соответствии с методическим документом ФСТЭК России [9].

Реализация представленного алгоритма в настоящий момент невозможна по причине ряда существующих сложностей, требующих проработки:

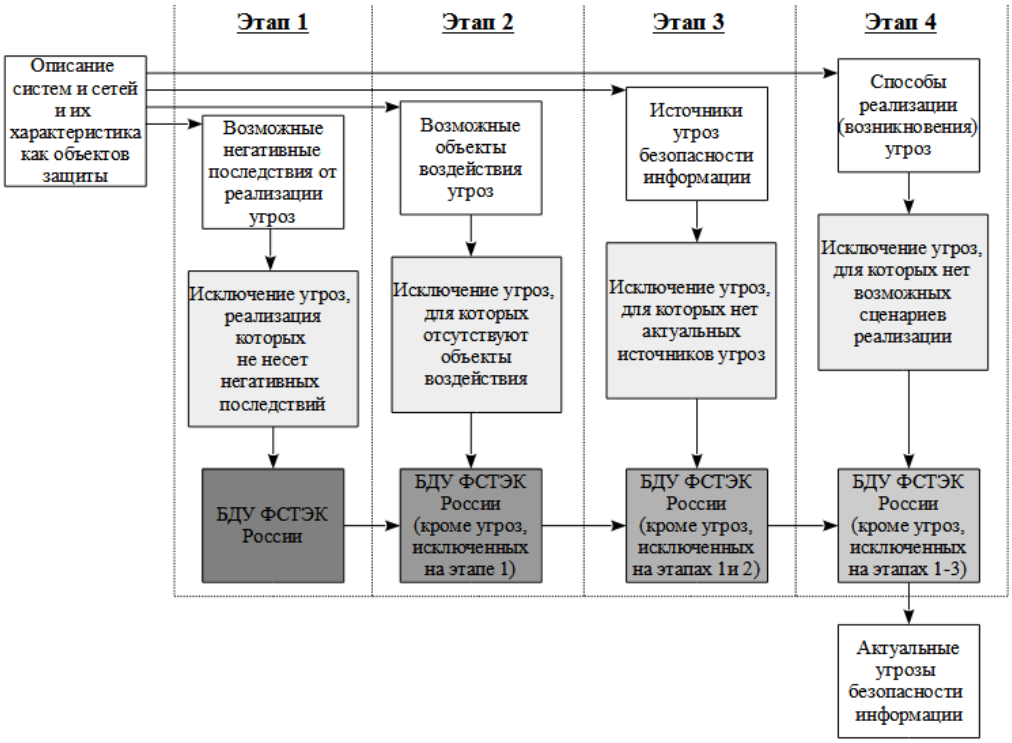

Рис. 2. Схема алгоритма работы экспертной системы оценки угроз безопасности информации
Fig. 2. Scheme of the algorithm of the expert system of the assessment of information security threats

– представленные в методическом документе возможные негативные последствия не охватывают всего множества предполагаемых негативных последствий от реализации угроз безопасности информации и требуют проработки;

– объекты воздействия, перечисленные в методическом документе, не в полной мере совпадают с объектами воздействия, указанными в описаниях угроз безопасности информации БДУ ФСТЭК России;

– представленный в методическом документе пример оценки целей реализации угроз безопасности информации необходимо дополнить другими видами объектов информатизации, кроме государственных информационных систем;

– существующий порядок представления потенциала (актуальных возможностей) нарушителей не позволяет однозначно сопоставить четыре уровня возможностей нарушителя в методическом документе [9] и три уровня потенциала нарушителей в БДУ ФСТЭК России.

Список литературы

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

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

3. Анищенко В.В., Криштофик А.М. Комплексная оценка угроз безопасности // Материалы конференции «Обеспечение безопасности информации в информационных системах», Минск, 11 ноября 2004 г. Минск, Академия управления, 2004, С. 33–36.

4. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

5. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при обработке в информационных системах персональных данных».

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

7. Указ Президента РФ от 11.08.2003 № 960 «Вопросы Федеральной службы безопасности Российской Федерации».

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

9. Методический документ ФСТЭК России от 14.02.2008 «Методика определения актуальности угроз безопасности персональных данных при их обработке в информационных системах персональных данных».

10. Банк данных угроз ФСТЭК России [Электронный ресурс]. URL: https://bdu.fstec.ru/threat (дата обращения 10.03.2021).

11. Internet Archive Wayback Machine [Электронный ресурс]. URL: https://archive.org/web/ (дата обращения 10.03.2021).

12. Цифровая экономика. Динамика и перспективы развития ИТ-отрасли. Экспресс-информация ИСИЭЗ НИУ ВШЭ [Электронный ресурс]. URL: https://issek.hse.ru/mirror/pubs/share/371960649.pdf (дата обращения 10.03.2021).

13. Муханова А., Ревнивых А.В., Федотов А.М. Классификация угроз и уязвимостей информационной безопасности в корпоративных системах // Вестник Новосиб. гос. ун-та. Серия: Информационные технологии. 2013. Т. 11, вып. № 2. С. 55–72.

14. Миков Д.А. Анализ методов и средств, используемых на различных этапах оценки рисков информационной безопасности // Вопросы кибербезопасности. 2014. № 4 (7). С. 49–54.

15. Малюк А.А. Кадровое обеспечение информационной безопасности // Государственная служба. 2011. № 5. С. 75–79.

16. Джарратано Д., Райли Г. Экспертные системы: принципы разработки и программирование. Изд. 4-е, Вильяме, 2006.

17. Данеев А.В., Жигалов Н.Ю., Шварц-Зиндер С.Н. Использование систем интеллектуальной поддержки принятия решений при проведении диагностических пожарно-технических экспертиз: монография. Иркутск: ФГОУ ВПО ВСИ МВД России, 2009. 144 с.

18. Данеев А.В., Воробьев А.А., Куменко А.Е., Лебедев Д.М., Мастин А.Б. Методика формирования комплекса средств управления сложной организационно-технической системой. Вестник Бурятского государственного университета. 2010. № 9. С. 263-268.

References

1. Konev A.A. Podkhod k postroeniyu modeli ugroz zashchishchaemoi informatsii [An approach to the creation of a protected information model]. *Doklady TUSUR* [*TUSUR reports*], 2012. No. 1-2 (25). Pp. 34–39.

2. GOST R 53114-2008. Zashchita informatsii. Obespechenie informatsionnoi bezopasnosti v organizatsii. Osnovnye terminy i opredeleniya. Data vvedeniya 01.10.2009. [GOST R 53114-2008. Information security. Ensuring information security in the organization. Basic terms and definitions. Valid from October 01, 2009].

3. Anishchenko V.V., Krishtofik A.M. Kompleksnaya otsenka ugroz bezopasnosti [Comprehensive security threat assessment]. *Materialy konferentsii «Obespecheniye bezopasnosti informatsii v informatsionnykh sistemakh». Minsk, 11 noyabrya 2004 g.* [*Materials of the conference "Ensuring information security in information systems", Minsk, November 11, 2004*]. Minsk, Akademiya upravleniya Publ., 2004. Pp.33–36.

4. Prikaz FSTEK Rossii ot 11.02.2013 No. 17 «Ob utverzhdenii Trebovanii o zashchite informatsii, ne sostavlyayushchei gosudarstvennuyu tainu, soderzhashcheisya v gosudarstvennykh informatsionnykh sistemakh». [Order of the FSTEC of Russia

No. 17 dated February 11, 2013 «On the approval of the Requirements for the protection of information that does not constitute a state secret contained in state information systems»].

5. Prikaz FSTEK Rossii ot 18.02.2013 No. 21 «Ob utverzhdenii Sostava i soderzhaniya organizatsionnykh i tekhnicheskikh mer po obespecheniyu bezopasnosti personal'nykh dannykh pri obrabotke v informatsionnykh sistemakh personal'nykh dannykh» [Order of the FSTEC of Russia No. 21 dated February 18, 2013 «On the approval of the Composition and content of organizational and technical measures to ensure the security of personal data during their processing in personal data information systems»].

6. Ukaz Prezidenta RF ot 16.08.2004 No. 1085 «Voprosy Federal'noi sluzhby po tekhnicheskomu i eksportnomu kontrolyu». [The Decree of the President of the Russian Federation No. 1085 dated August 16, 2004 «Issues of the Federal Service for Technical and Export Control»].

7. Ukaz Prezidenta RF ot 11.08.2003 No. 960 «Voprosy Federal'noi sluzhby bezopasnosti Rossiiskoi Federatsii». [The Decree of the President of the Russian Federation of 11.08.2003 No. 960 «Questions of the Federal Security Service of the Russian Federation»].

8. Metodicheskii dokument FSTEK Rossii ot 05.02.2021 «Metodika otsenki ugroz bezopasnosti informatsii» [The methodological document of the FSTEC of Russia dated February 05, 2021 «Methodology for assessing information security threats»].

9. Metodicheskii dokument FSTEK Rossii ot 14.02.2008 «Metodika opredeleniya aktual'nosti ugroz bezopasnosti personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh» [The methodological document of the FSTEC of Russia dated February 14, 2008 «Methodology for determining the relevance of threats to the security of personal data during their processing in personal data information systems»].

10. Bank Dannykh Ugroz FSTEC Rossii [Threat Data Bank of the FSTEC of Russia] [Electronic media]. URL: https://bdu.fstec.ru/threat (Accessed: March 10, 2021).

11. Internet Archive Wayback Machine [Electronic media]. URL: https://archive.org/web/ (Accessed: March 10, 2021).

12. Tsifrovaya ekonomika. Dinamika i perspektivy razvitiya IT-otrasli. Express-informatsiya ISIEZ NIU VSE [Digital economy. Dynamics and prospects of the IT industry development. Express information of the HSE ISSEK] [Electronic media]. URL: https://issek.hse.ru/mirror/pubs/share/371960649.pdf (Accessed: March 10, 2021).

13. Mukhanova A., Revnivykh A.V., Fedotov A.M. Klassifikatsiya ugroz i uyazvimostei informatsionnoi bezopasnosti v korporativnykh sistemakh [Classification of threats and vulnerabilities of information security in corporate systems]. *Vestnik Novosibirskogo gosudarstvennogo universiteta. Seriya: Informatsionniye technologii* [*The bulletin of Novosibirsk State University. Series: Information Technologies*], 2013. Vol. 11. No. 2. Pp. 55–72.

14. Mikov D.A. Analiz metodov i sredstv, ispol'zuemykh na razlichnykh etapakh otsenki riskov informatsionnoi bezopasnosti [Analysis of methods and tools used at various stages of information security risk assessment]. *Voprosy kiberbezopasnosti* [*Cybersecurity issues*], 2014. No. 4 (7). Pp. 49–54.

15. Malyuk A.A. Kadrovoe obespechenie informatsionnoi bezopasnosti [Personnel support of information security]. *Gosudarstvennaya sluzhba* [*Public service*], 2011. No. 5. Pp. 75–79.

16. Giarratano J., Riley G. Expert systems: principles and programming. Fourth edition. Course Technology, 2004. 288 p. (Russ. ed.: Dzharratano D., Raili G. Ekspertnye sistemy: printsipy razrabotki i programmirovanie. Izd. 4-e, Vil'yams Publ., 2006.).

17. Daneev A.V., Zhigalov N.Yu., Shvartz-Zinder S.N. Ispolzovanie sistem intellektualnoi podderzhki prinyatiya reshenii pri provedenii diagnosticheskikh pozharno-technicheskikh ekspertiz: monografiya [The use of intellectual decision support systems in conducting diagnostic fire and technical examinations: a monograph]. Irkutsk: The East Siberian Institute of the Ministry of Internal Affairs of Russia Publ., 2009. 144 p.

18. Daneev A.V., Vorob'ev A. A., Kumenko A. E., Lebedev D. M., Mastin A. B. Metodika formirovaniya kompleksa sredstv upravleniya slozhnoi organizatsionno-tekhnicheskoi sistemoi [Methods of forming a complex of management tools for a complex organizational and technical system]. *Vestnik Buryatskogo gosudarstvennogo universiteta* [*The bulletin of Buryat State University*], 2010. No. 9. Pp. 263-268.

Информация об авторах

Милько Дмитрий Сергеевич – аспирант кафедры информационных систем и защиты информации, Иркутский государственный университет путей сообщений, г. Иркутск, e-mail: dmitry.s.milko@gmail.com

Information about the authors

Dmitrii S. Mil'ko – Ph.D. student at the Subdepartment of Information Systems and Information Security, Irkutsk State Transport University, Irkutsk, e-mail: dmitry.s.milko@gmail.com

DOI 10.26731/1813-9108.2021.2(70).189-199 **УДК** 73.31.75 + 73.01.77 + 625.096

Системный анализ травматизма с участием детей на российских автомобильных дорогах

В. С. Асламова[1]✉, А. А. Минко[1], А. А. Асламов[2], Е. А. Асламова[3]

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

[2] *Ангарский государственный технический университет, г. Ангарск, Российская Федерация*

[3] *Сибирский федеральный университет, г. Красноярск, Российская Федерация*

✉ aslamovav@yandex.ru