УДК 004.056

Д.С. Милько, А.В. Данеев, А.Л. Горбылев

База знаний экспертной системы оценки угроз безопасности информации

Оценка угроз безопасности информации необходима для разработки соответствующей модели угроз. Результаты оценки угроз применяются для выбора и обоснования требуемых мер при построении систем защиты информации. В феврале 2021 г. 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.

Описан подход к автоматизации исключения неактуальных угроз безопасности информации путем разработки экспертной системы. Сформирована база знаний экспертной системы, описан подход к формированию базы знаний. Сформулированы ключевые понятия для экспертной системы оценки угроз, такие как область знаний, эксперт, пользователь. Приведена схема работы экспертной системы оценки угроз безопасности информации. Приведены практические результаты, полученные от внедрения разработанной базы знаний экспертной системы, на предприятии, занимающемся технической защитой конфиденциальной информации.

Приведено обоснование выбора экспертной системы в качестве метода автоматизации процедуры оценки угроз безопасности информации. Проведено сравнение экспертных систем с более современными технологиями автоматизации (искусственные нейронные сети).

Сделаны выводы об эффективности разработанной базы знаний, а также о необходимости разработки более удобного интерфейса и машины логического вывода.

Ключевые слова: угрозы безопасности информации, модель угроз, экспертная система, база знаний, банк данных угроз.

DOI: 10.21293/1818-0442-2021-25-1-61-69

Процедура разработки модели угроз безопасности информации, необходимая при построении систем защиты информации [1], усложнилась с введением ФСТЭК России в действие нового методического документа в феврале 2021 г. [2]. Внедрение в процедуру оценки угроз программного комплекса автоматизации позволит снизить временные, финансовые и иные издержки организаций на проведение оценки угроз [3]. В настоящий момент средства автоматизации оценки угроз безопасности информации отсутствуют, несмотря на законодательно предусмотренную возможность использования таких средств [4].

Экспертная система (ЭС) – это программный комплекс, который оперирует знаниями в определённой предметной области в целях решения проблем или выработки рекомендаций. ЭС имеют многочисленные применения: диагностика неисправностей в технических и биологических системах, планирование, проектирование, анализ сложных объектов, а также анализ наблюдательных данных [5].

Экспертные знания являются ключевым компонентом экспертной системы и формируются на основе надежной информации [6]. Эксперт структурирует знания таким образом, чтобы представить их в формальном виде. Полученное представление (база знаний) позволяет пользователям ЭС достичь результата, аналогичного экспертному, при условии, что ЭС будет работать по такому же алгоритму, что и эксперт-человек.

ЭС включает следующие основные функции:

– приобретение знаний;

– представление знаний;

– управление процессом поиска решений;

– разъяснение принятого решения.

Целью настоящей работы является разработка базы знаний ЭС оценки угроз безопасности информации. Задачи, решаемые в настоящей работе:

– обоснование выбора ЭС в качестве метода автоматизации процедуры оценки угроз;

– определение ключевых понятий, которые необходимы при разработке ЭС;

– разработка базы знаний ЭС оценки угроз безопасности информации;

– апробация базы знаний при приактической разработке модели угроз.

Результатом выполнения настоящей работы планируется представление знаний об угрозах безопасности в виде базы знаний. База знаний позволит пользователям использовать эти знания при наличии машины логического вывода. Источником знаний является Банк данных угроз (БДУ), ведение которого осуществляется ФСТЭК России [7].

В первом разделе настоящей работы обосновывается выбор ЭС в качестве метода оценки угроз безопасности информации. Во втором разделе определены ключевые понятия, используемые при разработке ЭС оценки угроз безопасности информации. Третий раздел включает описание процедуры разработки базы знаний ЭС. В четвертом разделе приведены результаты практического внедрения базы знаний ЭС на предприятии. Выводы о результатах разработки базы знаний ЭС приведены в заключении.

Обоснование выбранного метода

Как уже было заявлено ранее, в качестве метода для автоматизации оценки угроз безопасности информации была выбрана разработка соответствующей ЭС. Такой выбор обоснован совокупностью обстоятельств, указанных ниже.

В сфере информационной безопасности технологии искусственного интеллекта чаще всего находят применение с целями:

– предотвращения инцидентов информационной безопасности;

– противодействия атакам, связанным с социальной инженерией;

– исследования уязвимостей;

– противодействия сложным атакам;

– автоматизации служебных задач при противодействии атакам;

– внедрения функций безопасности в приложения [8, 9].

Центром компетенций Национальной технологической инициативы на базе Московского физико-технического института экспертные, рекомендательные, информационно-аналитические системы, автоматизация проектирования и управления выделены в одно из ключевых направлений, определяющих содержание технологии «Искусственный интеллект» [10].

Несмотря на актуальность задачи оценки угроз безопасности информации, технологии искусственного интеллекта для её решения ранее не применялись.

По масштабу решаемых задач технологии искусственного интеллекта принято разделять на сильные (способные решать универсальные задачи) и слабые (способные решать только узкоспециализированные задачи). К сильным технологиям искусственного интеллекта относятся искусственные нейронные сети (ИНС). К слабым технологиям искусственного интеллекта – ЭС [5].

Несмотря на все достоинства сильных технологий искусственного интеллекта, остается нерешенным вопрос прозрачности (объяснимости) ИНС. Разобраться в структуре связей современной ИНС человек не в состоянии. Для человека ИНС представляет собой «черный ящик», решениям которого приходится слепо доверять. В этом ИНС проигрывают прошлому поколению технологий искусственного интеллекта – ЭС. Поскольку ЭС основаны на системе жестких правил, они всегда способны объяснить своё решение, показать, какая именно цепочка правил была применена в каждом конкретном случае [5].

Кроме этого, против более широкого применения ИНС в сфере информационной безопасности имеются юридические причины. Специалист в сфере информационной безопасности в России несет предусмотренную законом ответственность за принятые им решения. За неверно принятые решения при эксплуатации объектов критической информационной инфраструктуры, которые повлекли нарушения информационной безопасности, ч. 3 ст. 274.1 УК РФ [11] предусмотрена уголовная ответственность. За неверно принятые решения при эксплуатации иных информационных систем, которые повлекли нарушение информационной безопасности, ст. 13.12 КоАП РФ [12] предусмотрена административная ответственность. Кроме этого, за неверно принятые решения специалист по защите информации может быть привлечен к дисциплинарной или гражданско-правовой ответственности [13]. В связи с указанными обстоятельствами при нарушении информационной безопасности специалист должен суметь логически обосновать принятые им решения, чтобы избежать ответственности за неверно принятое решение. Достоверно логически обосновать решение, принятое «черным ящиком», не представляется возможным.

В отличие от сильных технологий искусственного интеллекта ЭС позволяют в определенной узкой области знаний проводить рассуждения по такому же принципу, как рассуждал бы эксперт-человек [6]. Использование ЭС является «прозрачным», и в случае наступления негативных последствий специалист будет способен достоверно логически обосновать решение, принятое системой.

С точки зрения программирования разработка ЭС относится к непроцедурному подходу решения задач. От эксперта-человека не требуется описание точных подробностей того, как должна быть решена задача. Основной объем работы заключается в том, чтобы указать что именно должно быть сделано, без прямого указания как ЭС должна это сделать. Кроме этого, процедурные методы не позволяют справляться с ситуациями неправильных, неполных или несогласованных данных [6].

К недостаткам ЭС относится неспособность обладать «глубинными знаниями» о моделируемых системах. Программирование ЭС осуществляется в большей степени с использованием «поверхностных знаний» [6].

Применительно к сфере информационной безопасности можно привести следующий пример, демонстрирующий указанный недостаток. ЭС не будет способна объяснить принятое ей решение при оценке угрозы безопасности информации на глубоком уровне. ЭС делает логический вывод на основе знаний о нарушителях, объектах воздействия и последствиях атаки, запрограммированных в нее экспертом-человеком. При этом ЭС ограничена только указанным объемом знаний. Такие знания являются поверхностными, так как не включают полноценного объяснения причинно-следственных связей между нарушителями, объектами воздействия и последствиях атаки. В частности, ЭС не способна вместить «глубинных знаний» о возможной мотивации нарушителя, физических принципах функционирования объектов воздействия или стоимости ущерба. Для применения метода ЭС в таком случае потребуется разработка отдельных систем для каждой из перечисленных задач. Однако практический опыт разработки моделей угроз безопасности информации показывает, что использование «глубинных знаний» в процессе исключении неактуальных угроз безопасности не требуется при условии использования БДУ ФСТЭК России.

Резюмируя, основным недостатком ЭС в сравнении с ИНС является узость предметной области. Несмотря на это, ЭС [6]:

– способны ускорять решение задач;
– обладают повышенной доступностью;
– обладают постоянством;
– способны снизить опасность негативных последствий;
– способны получать знания из многих источников;
– обладают повышенной надежностью;
– способствуют объяснению;
– имеют быстрый отклик.

По этим причинам использование ЭС является обоснованным компромиссом при необходимости автоматизации процедуры оценки угроз безопасности информации.

Определение ключевых компонентов экспертной системы оценки угроз безопасности информации

Для функционирования ЭС требуется наличие следующих компонентов: базы знаний, машины логического вывода, блока общения (рис. 1, 2) [5].

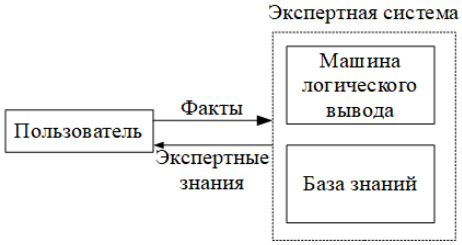

Рис. 1. Структура ЭС по Дж. Джарратано и Г. Райли [6]

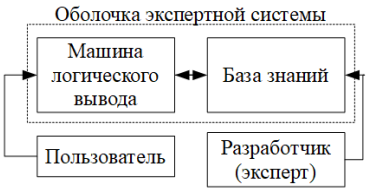

Рис. 2. Структура ЭС по П. Джексону [14]

Первым шагом в решении любой задачи с применением метода разработки ЭС является определение предметной области, в рамках которой необходимо найти решение (области знаний).

Первым шагом в решении любой задачи с применением метода разработки ЭС является определение предметной области, в рамках которой необходимо найти решение (области знаний).

В широком смысле предметной областью для работы эксперта-человека, который решает задачу оценки угроз, является информационная безопасность. В узком смысле областью знаний применительно к решаемой задаче является оценка угроз безопасности информации. Такой выбор области знаний соответствует критерию правильности выбора области знаний – в указанной области знаний эксперт-человек способен сформировать этапы решения задачи. Порядок процедуры оценки угроз безопасности информации может быть определен экспертом-человеком в соответствии с методическим документом ФСТЭК России. Для оценки угроз последовательно проводятся:

– определение негативных последствий от реализации угроз;
– определение возможных объектов воздействия;
– определение источников угроз;
– оценка способов реализации угроз;
– оценка актуальности угроз [2].

Когда определены этапы рассуждений, аналогичные действия вместо эксперта-человека могут быть выполнены пользователем, использующим ЭС. Система при решении задачи повторяет алгоритм, запрограммированный экспертом-человеком [6]. ЭС оценки угроз безопасности информации фактически эмулирует применение методического документа ФСТЭК России [2] экспертом-человеком.

Термином «эксперт-человек» или «эксперт» обозначается личность, обладающая экспертными знаниями в определенной области [6]. Для решения задачи оценки угроз безопасности на уровне эксперта необходимо широкое использование специализированных знаний в указанной сфере.

Корректность выбора эксперта-человека определяется Дж. Джарратано и Г. Райли следующим условием. Эксперт-человек должен решать поставленную задачу гораздо более эффективно, чем большинство людей. Более того, некоторые из задач человек без специализированных знаний не способен решить вообще [6].

В соответствии с рекомендациями по формированию экспертной группы [2] организовывать работу экспертной группы по оценке угроз рекомендуется специалисту по защите информации, имеющему стаж работ не менее трех лет и практический опыт оценки информационных рисков. Трудовые функции по анализу угроз безопасности и оценке рисков включены в профессиональные стандарты 06.033 «Специалист по защите информации в автоматизированных системах» и 06.030 «Специалист по защите информации в телекоммуникационных системах и сетях» [15, 16]. Другие профессиональные стандарты, включающие трудовые функции по оценке угроз безопасности информации, в Реестре профессиональных стандартов Минтруда России [17] не были найдены.

Обобщая вышеперечисленное, можно сказать, что специальными навыками по оценке угроз безопасности информации обладают специалисты по защите информации, имеющие стаж работы не менее трех лет. Указанное обстоятельство подтверждает корректность выбора специалиста по защите информации в качестве эксперта для разработки ЭС оценки угроз безопасности информации по Дж. Джарратано и Г. Райли [6].

В настоящий момент в соответствии с Доктриной информационной безопасности [18] состояние информационной безопасности России характеризуется недостаточным кадровым обеспечением. Проблема нехватки квалифицированных кадров в области информационной безопасности остается не решенной в течение длительного времени, что также

подтверждается в научных работах А.В. Царегородцева, Е.П. Цацкиной (2019), В.Н. Азарова, Ю.И. Гудкова (2015), А.А. Малюка (2011) [19–21].

В связи с нехваткой квалифицированных специалистов по защите информации одним из основных направлений, определенных Доктриной информационной безопасности, является осуществление опытных разработок в целях создания средств обеспечения информационной безопасности [18]. ЭС оценки угроз безопасности информации относится к средствам обеспечения информационной безопасности, способным снизить влияние проблемы кадрового обеспечения путем снижения трудозатрат эксперта-человека для решения задачи оценки угроз безопасности информации.

Пользователем же ЭС при исключении неактуальных угроз не обязательно должен быть эксперт со знаниями в сфере оценки угроз. Для использования ЭС достаточно обладать компетенциями пользователя. Рекомендации по формированию экспертной группы [2] позволяют включать в её состав специалистов, имеющих опыт работы не менее одного года по соответствующему направлению деятельности, в котором проводится оценка угроз безопасности информации. Такими пользователями могут являться специалисты в области информационных технологий, эксплуатации сетей связи, автоматизированных систем управления, риск-менеджеры и т.д. В частности, для оценки угроз, реализация которых может привести к финансовым рискам, также могут быть привлечены специалисты экономических подразделений.

Структура ЭС оценки угроз безопасности информации, полученная в результате сочетания структурных схем (см. рис. 1, 2) с учетом определения ключевых компонентов ЭС представлена на рис. 3.

Разработанная по такому принципу ЭС оценки угроз безопасности информации позволит предприятиям снизить затраты на проведение оценки угроз безопасности информации путем снижения затрат на привлечение специалиста по защите информации.

Разработка базы знаний экспертной системы оценки угроз безопасности

Условие актуальности угрозы безопасности информации в виде логического выражения

$$Ai = [Yi \wedge Oi \wedge Hi \wedge Ci], \quad (1)$$

где i – индекс, соответствующий одной из 222 угроз безопасности информации в БДУ ФСТЭК России; Ai – актуальность i-й угрозы; Yi – негативные последствия, связанные с ущербом от i-й угрозы; Oi – объект воздействия i-й угрозы; Hi – нарушитель (источник i-й угрозы); Ci – способ реализации i-й угрозы [4].

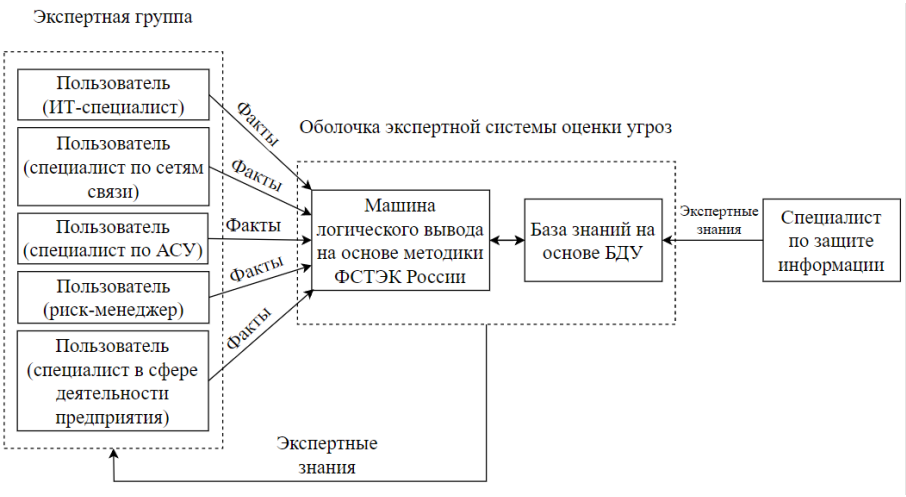

Рис. 3. Структура ЭС оценки угроз безопасности информации

Для автоматического исключения неактуальных угроз база знаний ЭС должна содержать знания:

– о возможных негативных последствиях (Yi);

– об объектах воздействия (Oi);

– о нарушителях (Hi).

ЭС с такой базой знаний позволит существенно сократить количество угроз, рассматриваемых далее аналитически.

Для формирования базы знаний в ЭС выбрано представление в виде фреймов (ячеек), наполненных слотами с характеристиками (знаниями) об угрозах [6].

Входными данными ЭС являются факты, касающиеся характеристик защищаемого объекта. Выходными данными ЭС является перечень угроз безопасности информации с указанием сведений об актуальности или неактуальности каждой угрозы. Такие сведения в совокупности с обоснованием принятого решения являются экспертными знаниями о защищаемом объекте.

Негативные последствия от реализации угроз безопасности (Yi) представлены в БДУ ФСТЭК России в виде характеристик трех свойств безопасности информации – конфиденциальности, доступности и целостности. Существуют угрозы, способные нарушить все три свойства безопасности информации (например, УБИ.005). Также существуют угрозы, которые способны нарушить только одно свойство безопасности, например, конфиденциальность (УБИ.008), доступность (УБИ.013) или целостность (УБИ.011). Каждое из указанных свойств безопасности может быть представлено в базе знаний ЭС в виде отдельного слота с бинарной характеристикой.

Сведения об объектах воздействия (Oi) в БДУ ФСТЭК России представлены на естественном язы-

ке. В работе [4] был предложен подход по формализации путем присвоения каждому объекту воздействия уникального идентификатора (ID). В настоящей работе ранее предложенный подход был упрощен и доработан. Разделение объектов воздействия на кластеры осуществляется не по признаку уровня архитектуры, а по признаку отнесения к конкретным информационным технологиям. По указанному принципу были выработаны кластеры с идентификаторами, приведенные в табл. 1. Формат идентификатора определяет принадлежность к кластеру в целом (символ «0» в конце идентификатора) или непосредственно к объекту воздействия (все остальные идентификаторы).

Таблица 1

Идентификаторы объектов воздействия

ID	Объект воздействия
10	**Грид-система**
11	Ресурсные центры грид-системы
12	Узлы грид-системы
20	**BIOS/UEFI**
21	Микропрограммное и аппаратное обеспечение BIOS/UEFI
22	Микропрограммное обеспечение BIOS/UEFI
30	**Прочее (служебный параметр)**
31	Метаданные
32	Учетные данные пользователя
33	Реестр
34	База данных
35	Канал связи / Каналы связи / Каналы связи (передачи) данных
36	Ключевая система информационной инфраструктуры
37	Сетевой трафик
40	**Программное обеспечение / Программы**
41	Системное программное обеспечение
42	Прикладное программное обеспечение
43	Сетевое программное обеспечение
44	Микропрограммное обеспечение
45	Системное программное обеспечение, использующее реестр
46	Аутентификационные данные пользователя (программное обеспечение)
50	**Информационная система / Инфраструктура информационных систем**
51	Сетевой узел
52	Носитель информации / Носители информации / Машинный носитель информации / Машинные носители информации
53	Объекты файловой системы / Объект файловой системы / Файлы
54	Аппаратное обеспечение / Техническое средство / Аппаратное средство / Аппаратное устройство
55	Сервер
56	Рабочая станция / Средство вычислительной техники
57	Защищаемые данные / Информационные ресурсы
58	Сетевое оборудование / Телекоммуникационное устройство
59	Информация, хранящаяся на компьютере во временных файлах
60	**Система виртуализации**
61	Виртуальная машина
62	Образ виртуальной машины
63	Гипервизор
64	Виртуальные устройства
65	Виртуальные устройства хранения, обработки и передачи данных
66	Виртуальные устройства хранения данных
67	Виртуальные диски
68	Консоль управления гипервизором
70	**Облачная система**
71	Облачный сервер
72	Облачная инфраструктура
73	Информационная система, иммигрированная в облако
74	Консоль управления облачной инфраструктурой
75	Облачная инфраструктура, созданная с использованием технологий виртуализации
80	**Суперкомпьютер**
81	Вычислительные узлы суперкомпьютера / Вычислительный узел суперкомпьютера
82	Система хранения данных суперкомпьютера
83	Каналы передачи данных суперкомпьютера
84	Система разграничения доступа хранилища больших данных
90	**Средства защиты информации / Средство защиты информации**
91	Программно-аппаратные средства со встроенными функциями защиты
92	Система управления доступом, встроенная в операционную систему компьютера
100	**Большие данные**
101	Хранилище больших данных
102	Узлы хранилища больших данных
110	**Беспроводные системы**
111	Точка беспроводного доступа
120	**Система охлаждения**
121	Технические средства воздушного кондиционирования, включая трубопроводные системы для циркуляции охлаждённого воздуха в ЦОД
130	**АСУ ТП**
131	Программируемые логические контроллеры
132	Распределённые системы контроля
133	Управленческие системы и другие программные средства контроля
134	Программное обеспечение автоматизированной системы управления технологическими процессами
140	**Мобильное устройство / Мобильные устройства**
141	Мобильное устройство и запущенные на нем приложения
142	Данные пользователя мобильного устройства (аппаратное устройство)
150	**Машинное обучение / искусственный интеллект**
151	Программное обеспечение (программы), использующее машинное обучение / Программное обеспечение (программы), реализующие технологии искусственного интеллекта
152	Модели машинного обучения
153	Обучающие данные машинного обучения

Для угроз, содержащих сложное описание объектов воздействия, слоты должны быть представлены в нормальной форме (конъюнкция дизъюнкций). Для этого объекты воздействия были объединены логическими связками («и», «или», «не» и т.д.). Пример представления нормальной логической связки для угрозы УБИ.180:

$$ОВ.121 \wedge (ОВ.131 \vee ОВ.132 \vee ОВ.133), \quad (2)$$

где ОВ.121, ОВ.131, ОВ.132, и ОВ.133 – объекты воздействия «техническое средство воздушного кондиционирования, включая трубопроводные системы для циркуляции охлаждённого воздуха в ЦОД», «программируемые логические контроллеры», «рас-

пределённые системы контроля», «управленческие системы и другие программные средства контроля» соответственно.

Нарушители (*Hi*) в БДУ ФСТЭК России классифицированы по потенциалу (низкий, средний и высокий) и возможности физического доступа к объекту атаки (внутренние и внешние). Комбинирование трех типов потенциала нарушителей и двух видов объектов атаки позволяет присвоить нарушителям уникальные числовые идентификаторы (ID).

Принцип формирования идентификаторов – позиционный (табл. 2). Для группы идентификаторов 11, 12, 13, 21, 22, 23, 31, 32 и 33 первое число (от 1 до 3) показывает потенциал внешнего нарушителя, а второе число — потенциал внутреннего нарушителя (от 1 до 3).

Таблица 2

Идентификаторы нарушителей информационной безопасности

ID	Типы нарушителей
11	Внешний нарушитель с низким потенциалом Внутренний нарушитель с низким потенциалом
12	Внешний нарушитель с низким потенциалом Внутренний нарушитель со средним потенциалом
13	Внешний нарушитель с низким потенциалом Внутренний нарушитель с высоким потенциалом
21	Внешний нарушитель со средним потенциалом Внутренний нарушитель с низким потенциалом
22	Внешний нарушитель со средним потенциалом Внутренний нарушитель со средним потенциалом
23	Внешний нарушитель со средним потенциалом Внутренний нарушитель с высоким потенциалом
31	Внешний нарушитель с высоким потенциалом Внутренний нарушитель с низким потенциалом
32	Внешний нарушитель с высоким потенциалом Внутренний нарушитель со средним потенциалом
33	Внешний нарушитель с высоким потенциалом Внутренний нарушитель с высоким потенциалом
41	Внешний нарушитель с низким потенциалом
42	Внешний нарушитель со средним потенциалом
43	Внешний нарушитель с высоким потенциалом
51	Внутренний нарушитель с низким потенциалом
52	Внутренний нарушитель со средним потенциалом
53	Внутренний нарушитель с высоким потенциалом
60	Прочие

В идентификаторах группы 4X первое число «4» соответствует исключению из рассмотрения внутреннего нарушителя, а второе число — потенциал внешнего нарушителя (от 1 до 3). Аналогично для идентификаторов группы 5X первое число «5» соответствует исключению из рассмотрения внешнего нарушителя, а второе число — потенциал внутреннего нарушителя (от 1 до 3). Идентификатор «60» позволяет выделить в отдельную группу угрозы, для которой антропогенные нарушители отсутствуют (например, УБИ.142).

ФСТЭК России периодически вносит изменения в БДУ. Для упрощения процедуры сравнения актуальности данных, представленных в базе знаний и в БДУ, введены два дополнительных слота. Первый слот содержит данные о дате добавления угрозы в БДУ ФСТЭК России. Второй слот содержит данные о дате изменения угрозы в БДУ ФСТЭК России.

На основании вышеперечисленных данных определена требуемая структура для представления знаний (рис. 4). Примеры фреймов, содержащих знания о ранее описанных угрозах, представлены на рис. 5 и 6.

```
deftemplate threat "List of TDB FSTEK of Russia"
        (slot id)
        (slot intruder)
        (slot victim)
        (slot confidentiality)
        (slot availability)
        (slot integrity)
        (slot create)
        (slot change)
        )
```

Рис. 4. Ввод формата представления знаний на языке CLIPS

```
(threat (id 8)
        (intruder 11)
        (victim (41|44|32))
        (confidentiality 1)
        (availability 0)
        (integrity 0)
        (create 20.03.2015)
        (change 15.11.2019)
        )
```

Рис. 5. Фрейм на языке CLIPS, содержащий знания об угрозе УБИ.008

```
(threat (id 180)
        (intruder 21)
        (victim (121&(131|132|133)))
        (confidentiality 0)
        (availability 0)
        (integrity 1)
        (create 18.08.2015)
        (change 11.02.2019)
        )
```

Рис. 6. Фрейм на языке CLIPS, содержащий знания об угрозе УБИ.180

Результаты разработки базы знаний экспертной системы

В результате работы получена база знаний ЭС для 222 угроз безопасности информации, содержащая данные о возможных негативных последствиях (*Yi*), об объектах воздействия (*Oi*), о нарушителях (*Hi*), а также данные о датах создания и изменения угрозы.

Для получения практических данных об эффективности разработанной базы знаний была произведена апробация в ООО по защите информации «Секрет-Сервис». Специалист по защите информации провел исключение неактуальных угроз безопасности для нескольких объектов информатизации. Исключение угроз производилось вручную, но в качестве источника информации об угрозах специалист использовал разработанную базу знаний, представленную в текстовом формате. В качестве интерфейса использовался текстовый редактор NotePad++ с возможностью поиска внутри файла. Результаты работы в описанном режиме представлены в табл. 3.

Информационная система персональных данных (ИСПДн) № 1 принадлежит государственному учреждению технической сферы деятельности. В ИСПДн содержатся персональные данные четвертого уровня защищенности. Для обработки персональных данных используется несколько автоматизиро-

ванных рабочих мест. ИСПДн № 2 аналогична по характеристикам ИСПДн № 1, но принадлежит высшему учебному заведению. Апробация базы знаний на аналогичных по характеристикам ИСПДн № 1 и № 2 показала совпадающие результаты работы.

Таблица 3

Сводные результаты апробации

Объект информатизации	Начальное количество угроз	Количество угроз, исключенных по причине			Общее количество угроз, исключенных из рассмотрения	Количество угроз после взаимодействия с базой знаний
		отсутствия негативных последствий от реализации угрозы	отсутствия объектов воздействия	отсутствия нарушителей определенных категорий		
ИСПДн № 1	222	0	102	22	124	98
ИСПДн № 2	222	0	102	22	124	98
МИС	222	0	67	71	138	84
ИСПДн № 3	222	0	101	22	123	99
ИСПДн № 4	222	0	154	10	164	58

Муниципальная информационная система (МИС) принадлежит муниципальному учреждению. Информационная система отнесена к третьему классу защищенности. Ресурсы МИС размещены на выделенном сервере без использования технологий виртуализации. В связи с указанными обстоятельствами общее количество угроз, исключенных из рассмотрения для МИС, больше, чем у ИСПДн № 1 и № 2.

ИСПДн № 3 принадлежит муниципальному учреждению сферы образования. Разница в характеристиках между ИСПДн № 3 и ранее рассмотренными ИСПДн № 1 и № 2 заключается только в использовании средств электронной подписи. Указанная разница в характеристиках послужила причиной разницы в результатах.

ИСПДн № 4 принадлежит силовой структуре. В ИСПДн содержатся персональные данные третьего уровня защищенности. Для обработки персональных данных используется несколько автоматизированных рабочих мест, не имеющих выхода в общедоступные сети. Можно наблюдать наглядную разницу в результатах работы по сравнению с ИСПДн № 1–3. Число исключенных угроз в четвертом столбце выросло по причине отсутствия сетевых подключений к общедоступным сетям передачи. Однако количество исключенных угроз в пятом столбце сократилось по причине более высокого потенциала нарушителя.

Нулевой результат в третьем столбце для всех объектов информатизации означает, что для них необходимо обеспечить конфиденциальность, доступность и целостность обрабатываемой информации. В случае если для некоторой системы не потребуется обеспечение конфиденциальности, количество угроз, исключенных из рассмотрения на этом этапе, перестанет быть нулевым. В частности, такой вариант возможен при необходимости защиты объекта информатизации с общедоступной информацией.

При использовании разработанной базы знаний среднее время оценки актуальности угроз по каждому из пяти указанных объектов информатизации составило 3,5 ч рабочего времени. Указанное время не включает в себя трудозатраты на составление описания объекта информатизации и оформление документации. Аналогичная работа по оценке угроз для других объектов информатизации с использованием непосредственного вывода табличного варианта БДУ ФСТЭК России ранее занимала у того же специалиста не менее 5 ч рабочего времени.

Стоит отметить, что указанное время оценки актуальности угроз достигнуто для базы знаний, представленной без графического интерфейса (исключительно в формате текстового файла). Представление базы знаний в графическом интерфейсе с использованием алгоритма принятия решения способно сократить время еще больше.

Заключение

ЭС могут решать сложные задачи в узкой предметной области «прозрачно», позволяя логически обосновать принятое решение. Задачи более широкой предметной области для экспертных систем недоступны, в них требуется применение более современных технологий искусственного интеллекта (ИНС). Однако при использовании ИНС становятся актуальными проблемы юридического характера.

Разработанная база знаний ЭС позволила специалисту по защите информации произвести исключение неактуальных угроз безопасности без использования БДУ ФСТЭК России. Для повышения эффективности требуется разработка машины логического вывода, которая будет автоматически делать экспертные выводы из базы знаний на основе фактов.

Экспертом отмечено снижение времени, требуемого на исключение неактуальных угроз. Причина снижения времени состоит в более ёмком представлении знаний по сравнению со стандартным выводом табличного файла из БДУ ФСТЭК России.

Взаимодействие эксперта с базой знаний в интерфейсе текстового редактора негативно влияет на эффективность работы. Требуется более удобный интерфейс для взаимодействия эксперта и знаний.

База знаний ЭС позволила эксперту получить одинаковый результат для аналогичных объектов информатизации. Это подтверждает постоянство выходных данных ЭС в зависимости от входных данных. Разница в выходных результатах при апробации для различающихся объектов информатизации доступна для понимания и объяснима.

При необходимости разработанную базу знаний ЭС можно гибко изменять (добавлять, модифицировать или удалять знания об угрозах).

Дальнейшими вопросами, требующими проработки, являются разработка и внедрение автоматического алгоритма принятия решений, а также разработка графического интерфейса взаимодействия с пользователем.

Литература

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

2. Методика оценки угроз безопасности информации. Методический документ ФСТЭК России от 05.02.2021 [Электронный ресурс]. – Режим доступа: https://fstec.ru/component/attachments/download/2919, свободный (дата обращения: 03.12.2021).

3. ГОСТ Р 53114–2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Дата введения 01.10.2009 [Электронный ресурс]. – Режим доступа: https://docs.cntd.ru/document/1200075565, свободный (дата обращения: 03.12.2021).

4. Милько Д.С. Экспертная система оценки угроз безопасности информации. Формальное представление объектов воздействия / Д.С. Милько, П.Н. Наседкин // Молодая наука Сибири: электрон. науч. журн. – 2021. – № 2 (12) [Электронный ресурс]. – Режим доступа: http://mnv.irgups.ru/toma/212-2021, свободный (дата обращения: 03.12.2021).

5. Технологии искусственного интеллекта [Электронный ресурс]. – Режим доступа: https://apr.moscow/content/data/6/11%20Технологии%20искусственного%20интеллекта.pdf, свободный (дата обращения: 03.12.2021).

6. Джарратано Дж. Экспертные системы: принципы разработки и программирование / Дж. Джарратано, Г. Райли. – М.: ИД «Вильямс», 2007. – 1152 с.

7. Банк данных угроз ФСТЭК России [Электронный ресурс]. – Режим доступа: https://bdu.fstec.ru, свободный (дата обращения: 03.12.2021).

8. Искусственный интеллект в ВПК [Электронный ресурс]. – Режим доступа: https://www.tadviser.ru/index.php/Статья:Искусственный_интеллект_в_ВПК, свободный (дата обращения: 03.12.2021).

9. Artificial Intelligence for Cyber-Security: A Double-Edge Sword [Электронный ресурс]. – Режим доступа: https://medium.com/sciforce/artificial-intelligence-for-cyber-security-a-double-edge-sword-6724e7a31425, свободный (дата обращения: 03.12.2021).

10. Центр компетенций НТИ по направлению «Искусственный интеллект» [Электронный ресурс]. – Режим доступа: https://nti2035.ru/technology/competence_centers/mipt.php, свободный (дата обращения: 03.12.2021).

11. Уголовный кодекс РФ [Электронный ресурс]. – Режим доступа: http://pravo.gov.ru/proxy/ips/?docbody&nd=102041891, свободный (дата обращения: 03.12.2021).

12. Кодекс РФ об административных правонарушениях [Электронный ресурс]. – Режим доступа: http://pravo.gov.ru/proxy/ips/?docbody&nd=102074277, свободный (дата обращения: 03.12.2021).

13. Федеральный закон от 08.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [Электронный ресурс]. – Режим доступа: http://pravo.gov.ru/proxy/ips/?docbody&nd=102108264, свободный (дата обращения: 03.12.2021).

14. Джексон П. Введение в экспертные системы / П. Джексон. – М.: ИД «Вильямс», 2001. – 623 с.

15. Профессиональный стандарт Специалист по защите информации в автоматизированных системах [Электронный ресурс]. – Режим доступа: https://profstandart.rosmintrud.ru/obshchiy-informatsionnyy-blok/natsionalnyy-reestr-professionalnykh-standartov/reestr-professionalnykh-standartov/index.php?ELEMENT_ID=60419, свободный (дата обращения: 03.12.2021).

16. Профессиональный стандарт. Специалист по защите информации в телекоммуникационных системах и сетях [Электронный ресурс]. – Режим доступа: https://profstandart.rosmintrud.ru/obshchiy-informatsionnyy-blok/natsionalnyy-reestr-professionalnykh-standartov/reestr-professionalnykh-standartov/index.php?ELEMENT_ID=62853, свободный (дата обращения: 03.12.2021).

17. Реестр профессиональных стандартов [Электронный ресурс]. – Режим доступа: https://profstandart.rosmintrud.ru, свободный (дата обращения: 03.12.2021).

18. Доктрина информационной безопасности Российской Федерации [Электронный ресурс]. – Режим доступа: http://publication.pravo.gov.ru/Document/View/0001201612060002, свободный (дата обращения: 03.12.2021).

19. Царегородцев А.В. Влияние информационного общества на подготовку обучающихся в сфере информационной безопасности / А.В. Царегородцев, Е.П. Цацкина // Вестник Моск. гос. лингв. ун-та. Образование и педагогические науки. – 2019. – № 4(833) [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/ vliyanie-informatsionnogo-obschestva-na-podgotovku-obuchayuschihsya-v-sfere-informatsionnoy-bezopasnosti, свободный (дата обращения: 03.12.2021).

20. Азаров В.Н. Некоторые проблемы инженерной подготовки в области информационных технологий и пути их решения / В.Н. Азаров, Ю.И. Гудков // Вестник ИрГТУ (Иркутск). – 2015. – № 3 (98) [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/nekotoryye-problemy-inzhenernoy-podgotovki-v-oblasti-informatsionnyh-tehnologiy-i-puti-ih-resheniya, свободный (дата обращения: 03.12.2021).

21. Малюк А.А. Кадровое обеспечение информационной безопасности // Государственная служба (Москва). – 2011. – № 5. [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/kadrovoe-obespechenie-informatsionnoy-bezopasnosti, свободный (дата обращения: 03.12.2021).

Милько Дмитрий Сергеевич
Аспирант каф. «Информационнные системы и защита информации» (ИСиЗИ) Иркутского государственного ун-та путей сообщения (ИрГУПС)
Чернышевского ул., д. 15, г. Иркутск, Россия, 664074
Тел.: +7 (395-2) 638-359
ORCID: 0000-0002-6259-6749
Эл. почта: dmitry.s.milko@gmail.com

Данеев Алексей Васильевич
Д-р техн. наук, проф. каф. ИСиЗИ ИрГУПС
Чернышевского ул., д. 15, г. Иркутск, Россия, 664074
ORCID: 0000-0003-4288-824X
Тел.: +7 (395-2) 638-359
Эл. почта: daneev@mail.ru

Горбылев Александр Леонидович
Аспирант Иркутского национального исследовательского технического ун-та (ИрНИТУ)
Лермонтова ул., д. 83, г. Иркутск, Россия, 664074
Тел.: +7 (395-2) 405-510
Эл. почта: gal@irksecret.ru

Milko D.S., Daneev A.V., Gorbylev A.L.

Knowledge base of the expert system for cyber security threat modeling

The appraisal of cyber security threats is necessary to create of the cyber security threat model. The results of appraisal shall

apply for choosing information security measures. In February 2021, the new methodical document issued by the Russian Federal Service for export control of engineering technologies has gone into effect, and is obligatory to follow by all organizations.

The paper presents the approach to ensure the automation of irrelevant cyber security threats ejection. The automation is done by developing the expert system. The knowledge base of expert system is created, and the methodology for its creating is described in the paper. The key terms for the expert system are worded. The flow chart of expert system is shown. The experimental results of knowledge base launching in manual mode are given.

A part of the paper is devoted to a justification for choosing the expert system as an automatization method. The expert systems are compared to a «smarter» artificial intelligence method (artificial neural networks).

As a result, the conclusions about efficiency of produced knowledge base are provided and the necessity of creating a more user-friendly interface and rule engine is made evident.

Keywords: cyber security threats, cyber security threats model, expert system, knowledge base, threat database.

DOI: 10.21293/1818-0442-2021-25-1-61-69

References

1. Konev A.A. [Approach to creation protected information model]. *Proceedings of TUSUR University*, 2012, no. 1-2 (25), P. 34–39 (in Russ.).

2. [Methodology for assessing cyber security threats]. FSTEC of Russia Methodical document (in Russ.). Available at: https://fstec.ru/component/attachments/download/2919, free (Accessed: December 3, 2021) (in Russ.).

3. [GOST R 53114-2008. Information security. Ensuring information security in the organization. Basic terms and definitions]. Available at: https://docs.cntd.ru/document/1200075565, free (Accessed: December 3, 2021) (in Russ.).

4. Milko D.S., Nasedkin P.N. [Threat modeling expert system. Formal representation of impact objects]. *Young Science of Siberia: Electronic Scientific Journal*, 2021, no. 2 (12). Available at: http://mnv.irgups.ru/toma/212-2021, free (Accessed: December 3, 2021) (in Russ.).

5. [Artifical intellect technologies] (in Russ.). Available at: https://apr.moscow/content/data/6/11%20Технологии%20искусственного%20интеллекта.pdf, free (Accessed: December 3, 2021) (in Russ.).

6. Giarratano Joseph C., Riley Gary D. Expert Systems. Principles and Programming. Moscow, Williams Publ., 2007, 1152 p. (in Russ.).

7. [FSTEC of Russia Threats Database]. Available at: https://bdu.fstec.ru, free (Accessed: December 3, 2021) (in Russ.).

8. [Artifical Intellect in Defence]. Available at: ttps://www.tadviser.ru/index.php/Статья:Искусственный_интеллект_в_ВПК, free (Accessed: December 3, 2021) (in Russ.).

9. Artificial Intelligence for Cyber-Security: A Double-Edge Sword. Available at: https://medium.com/sciforce/ artificial-intelligence-for-cyber-security-a-double-edge-sword-6724e7a31425, free (Accessed: December 3, 2021).

10. [«Artificial Intelligence» NTI Competence Center]. Available at: https://nti2035.ru/technology/competence_centers/mipt.php, free (Accessed: December 3, 2021) (in Russ.).

11. [Criminal Code of Russia]. Available at: http://pravo.gov.ru/proxy/ips/?docbody&nd=102041891, free (Accessed: December 3, 2021) (in Russ.).

12. [Administrative Violations Code of Russia]. Available at: http://pravo.gov.ru/proxy/ips/?docbody&nd=102074277, free (Accessed: December 3, 2021) (in Russ.).

13. [Federal Law No. 149 of 8 July 2006 on the Information, Information Technologies and Information Security]. Available at: http://pravo.gov.ru/proxy/ips/?docbody&nd=102108264, free (Accessed: December 3, 2021) (in Russ.).

14. Jackson Peter. Introduction to Expert Systems. Moscow, Williams Publ., 2001. 623 p. (in Russ.).

15. [Professional Standard. Information Security Specialist in Automated Systems]. Available at: https://profstandart.rosmintrud.ru/obshchiy-informatsionnyy-blok/natsionalnyy-reestr-professionalnykh-standartov/reestr-professionalnykh-standartov/index.php?ELEMENT_ID=60419, free (Accessed: December 3, 2021) (in Russ.).

16. [Professional Standard. Information Security Specialist in Telecommunication Systems and Networks]. Available at: https://profstandart.rosmintrud.ru/obshchiy-informatsionnyy-blok/natsionalnyy-reestr-professionalnykh-standartov/reestr-professionalnykh-standartov/index.php?ELEMENT_ID=62853, free (Accessed: December 3, 2021) (in Russ.).

17. [Registry of occupational standards]. Available at: https://profstandart.rosmintrud.ru, free (Accessed: December 3, 2021) (in Russ.).

18. [Information Security Doxy of Russia]. Available at: http://publication.pravo.gov.ru/Document/View/0001201612060002, free. (Accessed: December 3, 2021) (in Russ.).

19. Tsaregorodcev A.V., Tsatskina E.P. [The impact of the information society on the training of information security students]. *Bulletin of the Moscow State Linguistic University. Education and Pedagogical Sciences*, 2019, no. 4 (833). Available at: https://cyberleninka.ru/article/n/vliyanie-informatsionnogo-obschestva-na-podgotovku-obuchayuschihsya-v-sfere-informatsionnoy-bezopasnosti, free. (Accessed: December 3, 2021) (in Russ.).

20. Azarov A.N., Gudkov Yu.I. [Some problems of engineering training in the field of information technology and ways to solve them]. *Bulletin of ISTU (Irkutsk)*, 2015, no. 3 (98). Available at: https://cyberleninka.ru/article/n/nekotorye-problemy-inzhenernoy-podgotovki-v-oblasti-informatsionnyh-tehnologiy-i-puti-ih-resheniya, free. (Accessed: December 3, 2021) (in Russ.).

21. Malyuk A.A. [Information security staffing]. *Public Service (Moscow)*, 2011, no. 5. Available at: https://cyberleninka.ru/article/n/kadrovoe-obespechenie-informatsionnoy-bezopasnosti, free. (Accessed: December 3, 2021) (in Russ.).

Dmitry S. Milko
Postgraduate student, Department of Information Systems and Information Security (ISIS),
Irkutsk State Transport University (ISTU)
15, Chernyshevskogo st., Irkutsk, Russia, 664074
ORCID: 0000-0002-6259-6749
Phone: +7 (395-2) 63-83-59
Email: dmitry.s.milko@gmail.com

Alexey V. Daneev
Doctor of Science in Engineering, Professor,
Department of ISIS, ISTU
15, Chernyshevskogo st., Irkutsk, Russia, 664074
ORCID: 0000-0003-4288-824X
Phone: +7 (395-2) 63-83-59
Email: daneev@mail.ru

Alexander L. Gorbylev
Posgraduate student,
Irkutsk National Research Technical University
83, Lermontova st., Irkutsk, Russia, 664074
Phone: +7 (395-2) 40-55-10
Email: gal@irksecret.ru