УДК 004.9
DOI: 10.55648/1998-6920-2022-16-3-14-28

Интегральная модель оценки защищенности объектов информатизации в условиях деструктивного воздействия

В. В. Баранов[1]

В работе проведено обоснование необходимости создания информационной системы поддержки принятия решений при разработке систем защиты объектов информатизации, проведен анализ существующих систем в различных областях деятельности, определены требования к функционалу системы применительно к области защиты информации, рассмотрены методы разработки моделей функционирования защищенных информационных систем в условиях деструктивного воздействия на основе байесовских сетей, приведено описание функционирования типового модуля данной модели, рассмотрены структуры вероятностных моделей взаимосвязей уязвимостей, угроз безопасности информации, способов и сценариев их реализации, формирования мероприятий по защите объектов информатизации, формирования и оценки рисков инцидентов и ущерба от них, определены кластеры формирования типовых событий информационной безопасности, приведен методический аппарат для проведения расчетов совместного распределения вероятностей защитных и деструктивных событий, выявлены типовые цепочки взаимосвязей таких событий, разработан математический аппарат для расчета их вероятностей, приведено вербальное описание закономерностей их взаимного влияния, а также представлена методика перевода количественных вероятностных значений показателей защищенности объекта информатизации в качественные и подведены итоги проведенного исследования.

Ключевые слова: поддержка принятия решений, байесовская сеть, деструктивные воздействия, меры защиты информации, угрозы безопасности информации, стратегия управления, события информационной безопасности, анализ влияний, структурный анализ, системы защиты.

1. Введение

Наиболее сложным аспектом в процессе разработки систем защиты является полнота и качество оценки угроз безопасности информации, принятие обоснованного решения об их актуальности, а также выбор комплекса мер и средств защиты информации, эффективных в складывающейся обстановке.

Данный процесс строго регламентирован и основывается на требованиях организационно-правовых и методических документов [1–9]. Их структура представлена на рис. 1.

На этапе функционирования в условиях динамично меняющегося деструктивного воздействия система защиты требует непрерывного оперативного управления, своевременного и

1 Работа выполнена при финансовой поддержке гранта MTUSI, предоставленного Министерством финансов Российской Федерации из федерального бюджета в 2021 году (научный проект № 35/21-d) в рамках федерального проекта «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации».

обоснованного реагирования на возникающие новые риски и угрозы безопасности информации.

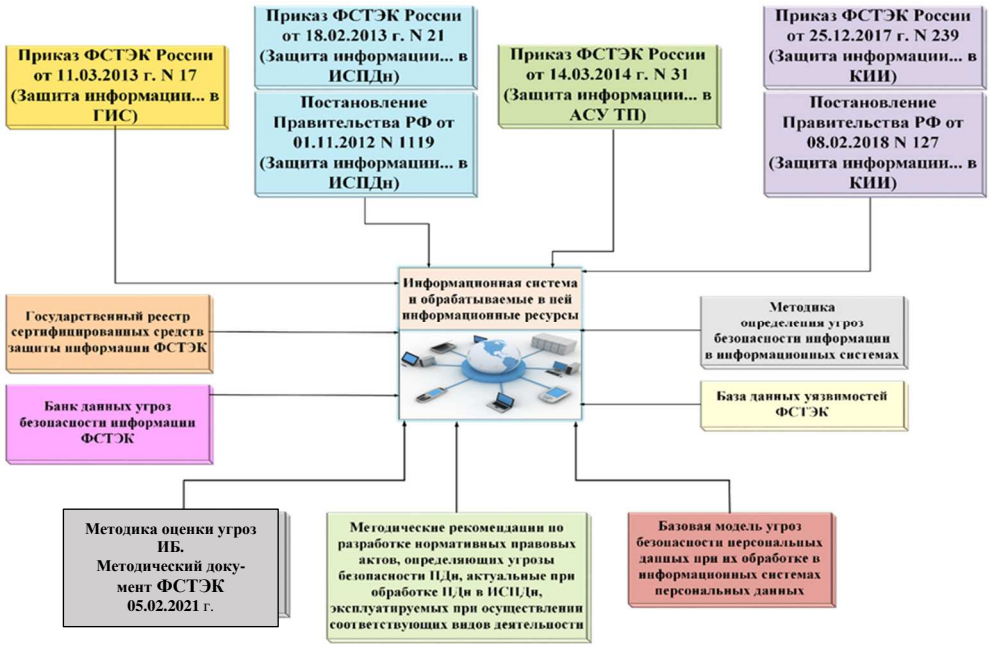

Рис. 1. Нормативно-правовое обеспечение формирования способов защиты информационных систем

Анализ содержания указанных организационно-руководящих методических документов показал, что данные задачи решаются методом экспертной оценки, что определяет субъективность принимаемых решений, качество которых зависит от полноты данных по складывающейся обстановке и подготовленности экспертов. В данном документе не рассматриваются методические подходы по оценке угроз безопасности информации, связанных с нарушением безопасности шифровальных (криптографических) средств защиты информации, а также угроз, связанных с техническими каналами утечки информации.

Это обстоятельство определяет необходимость создания новых и совершенствования существующих методических и инструментальных средств автоматизации процесса поддержки принятия экспертных решений в задачах разработки и оценки эффективности комплекса мер защиты информационных систем.

Анализ существующих автоматизированных информационных систем поддержки принятия решений (ИСППР) в различных областях деятельности позволяет выделить три их основных типа [10, 11].

Первый тип – это пассивные ИСППР, обрабатывающие данные и представляющие лицу, принимающему решение (ЛПР), структурированную информацию и отчеты. При этом конкретное решение принимается человеком.

Второй тип – это активные ИСППР. Данные системы формируют потенциальные решения на основе обработанной базы данных, а также предлагают возможные альтернативы действий.

К третьему типу относятся комбинированные ИСППР, которые предлагают вероятные решения и альтернативы, но при этом ЛПР может вносить уточнения, добавлять условия и отправлять проект на повторную обработку. В таких ситуациях прорабатываются различные модели, что позволяет принять оптимальное решение.

Исходя из существующего подхода к разработке способов защиты информационных ресурсов и подбору средств и мер защиты информации (рис. 2), наиболее подходящими для области информационной безопасности будут являться комбинированные ИСППР.

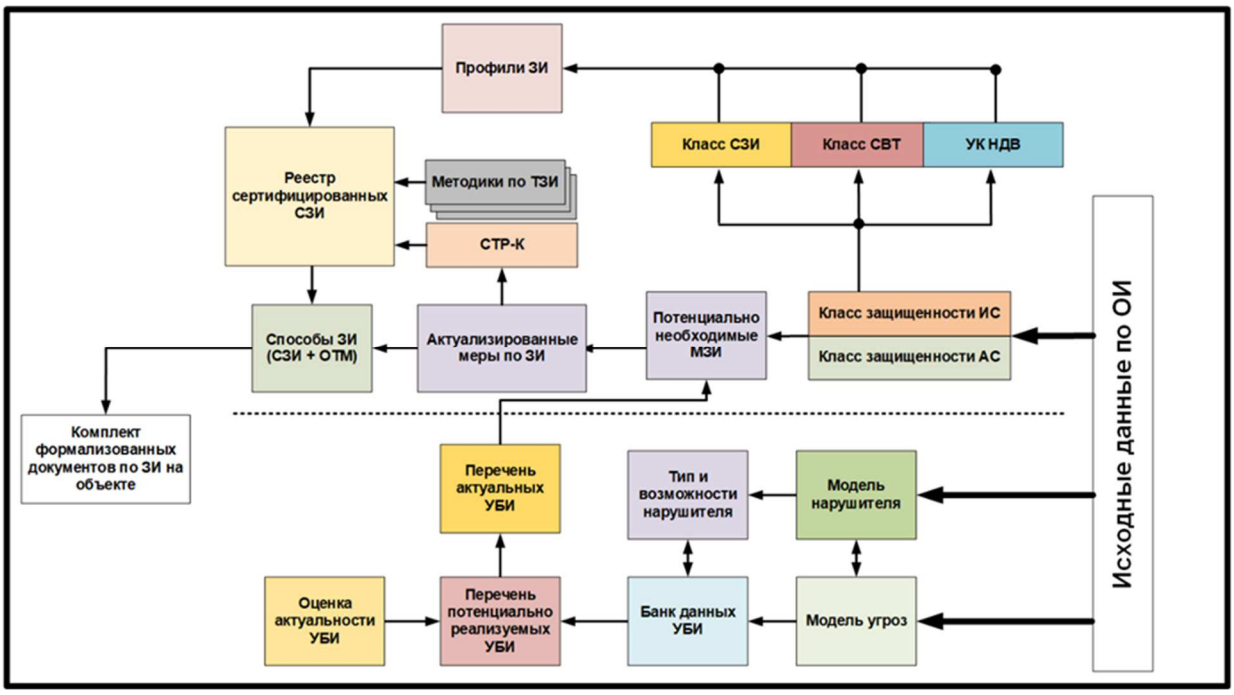

Рис. 2. Структурная схема процесса разработки способов защиты информационных ресурсов

Большинство существующих в настоящее время комбинированных ИСППР основаны на программных продуктах для работы с байесовскими сетями [12, 13, 14]. Их следует классифицировать прежде всего по способу использования. В случае, если основная задача исследователя – решить конкретную прикладную проблему, то необходимо выбрать готовый пакет, обладающий максимальными свойствами, необходимыми исследователю. В работе был проведен анализ ряда наиболее функционально адаптированных к области информационной безопасности программ.

BayesiaLab представляет собой комплексный инструмент для создания и использования байесовских сетей. С помощью пакета BayesiaLab можно определять, изучать, редактировать и анализировать байесовские сетевые модели. [15, 16, 17].

Программный продукт AgenaRisk можно применять для широкого круга проблем, связанных с неопределенностью. Пакет предназначен для моделирования проблем, связанных с использованием карт рисков – сочетание статистического моделирования и технологий BN. Это обеспечивает сочетание мощности, простоты использования и гибкости. AgenaRisk поддерживает как диагностические, так и интеллектуальные неопределенности. Сильной стороной AgenaRisk является возможность работы с различными типами моделей, обучение байесовской сети, применение различных типов распределений, а также графическая визуализация при анализе рисков [18, 19, 20].

Программный продукт Hugin и его ядро Hugin Development Environment состоят из трех основных компонентов.

Первый – Hugin GUI – это интерфейс для создания и модификации сетевых моделей и их реализации путем ввода фактов и отображения результирующих распределений вероятностей и ожидаемого использования. В режиме редактирования модуль позволяет определять узлы путем вставки узлов, их объединения, определения состояний и действий, таблиц условной вероятности и таблиц полезности.

Второй компонент – система принятия решений Hugin (HDE) – является ядром системы, которая выполняет вывод на основе данных, представленных байесовской сетью или диаграммой влияния. Система позволяет формировать и использовать базы знаний с применением объектно-ориентированных байесовских сетей. Она также позволяет использовать как дискретные, так и непрерывные переменные, прямое определение условного распределения

вероятностей, определять отношения вспомогательных функций с помощью математических и логических описаний [21, 22].

Анализ возможностей указанных программных продуктов позволил выделить их сильные стороны, необходимые для выполнения задачи поддержки принятия решений в области информационной безопасности. Такая информационная система должна обладать рядом перечисленных ниже функций.

Функция моделирования будет обеспечивать процесс разработки решений на основе построения вероятностных, ситуационных, аналитических, имитационных и других моделей.

Функция обработки баз данных (информационно-расчетная функция) обеспечивает принятие решений на основе цифровых хранилищ информации по конкретной организации, ее активам, информационной системе, классам нарушителей, угрозам безопасности информации, способам их реализации, уязвимостям, организационным и техническим мерам защиты информации и др.

Функция обработки баз знаний (аналитическая функция) реализует процесс принятия решений в условиях нечетких исходных данных на основе сценариев выполнения аналогичных задач с учетом статистических закономерностей, зависимостей и установленных методик и алгоритмов.

Функция обеспечения коммуникативности обеспечивает возможность взаимодействия нескольких должностных лиц, работающих над одной задачей.

Функция документирования обеспечивает процесс разработки комплекта документов по принятым решениям.

Реализация данной задачи может быть осуществлена путем разработки комплексной динамической модели функционирования защищенных информационных систем различного назначения в условиях деструктивного воздействия, позволяющей также моделировать процесс оперативного управления событиями информационной безопасности в условиях изменений воздействующих факторов.

2. Обсуждение

В основу данной модели предлагается заложить типовые модули, отражающие процесс функционирования защищаемой информационной системы в условиях деструктивного воздействия (рис. 3).

В составе модуля выделены четыре кластера:

1. Кластер формирования рисков угроз безопасности информации.
2. Кластер ликвидации рисков угрозы инцидента.
3. Кластер формирования рисков инцидента.
4. Кластер ликвидации последствий инцидента.

Моделирование в динамике складывающейся ситуации осуществляется, как описано ниже. Ввод исходных данных осуществляется по направлению деструктивных воздействий и направлению защитных мер.

Кластер рисков угроз безопасности информации формируется путем моделирования характеристик потенциальных возможностей нарушителя, который обладает неким функционалом показателей, соответствующих определенному классу $\{КлН_1 \ldots КлН_i\}$. Каждый из классов нарушителей способен с определенной вероятностью реализовать множество угроз безопасности информации (УБИ) определенными способами, составляющими для каждой УБИ множество $\{S_1 \ldots S_i\}$. Фрагмент матрицы потенциальных возможностей разных классов нарушителей по реализации УБИ представлен на рис. 4.

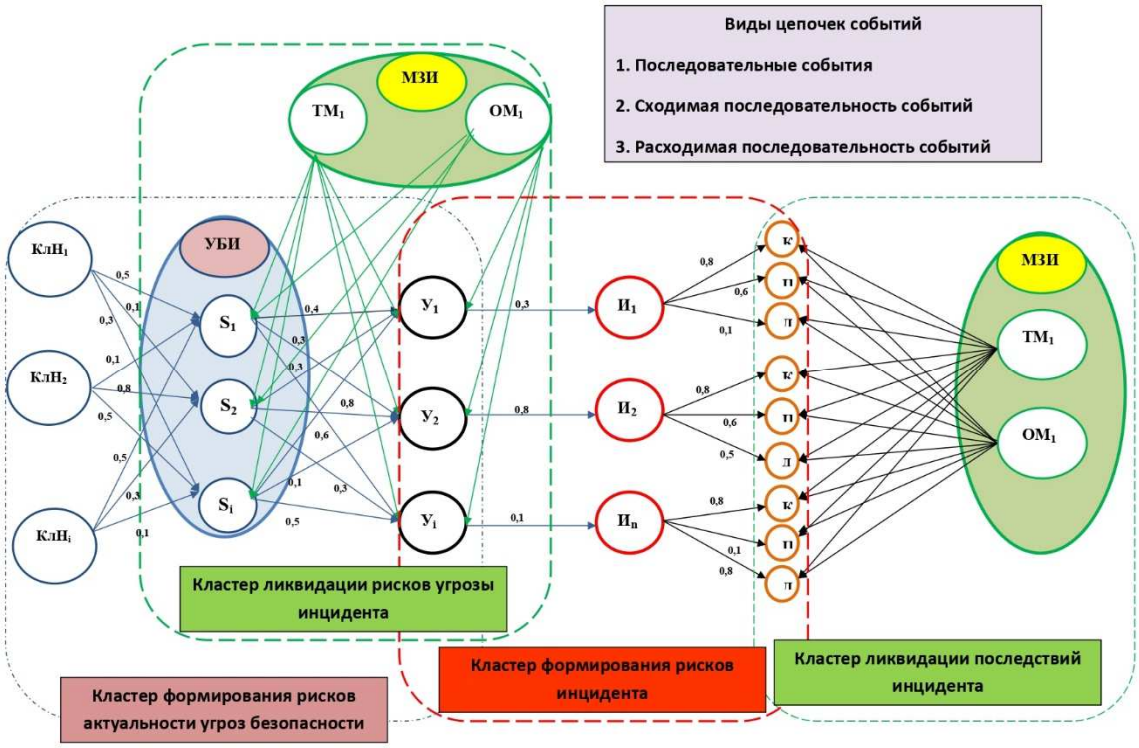

Рис. 3. Типовой модуль комплексной динамической модели функционирования защищенных информационных систем

УБИ реализуется через уязвимости, составляющие множество $\{Y_1 \ldots Y_i\}$. Исходные данные по типам, содержанию и характеру проявления УБИ и уязвимостей можно получить из банка на сайте ФСТЭК, перечней, разрабатываемых для каждого защищаемого объекта информатизации, и других баз данных.

		Нарушитель внутренний			Нарушитель внешний с высоким потенциалом		
		Нарушитель внутренний с высоким потенциалом	Нарушитель внутренний с средним потенциалом	Нарушитель внутренний с слабым потенциалом	Нарушитель внешний с высоким потенциалом	Нарушитель внешний с средним потенциалом	Нарушитель внешний с слабым потенциалом
24	Угроза изменения режимов работы аппаратных элементов	1					
25	Угроза изменения системных и глобальных переменных		1				
26	Угроза искажения XML-схемы		1			1	
27	Угроза искажения вводимой и выводимой на периферийные устройства информации			1	1		
28	Угроза использования альтернативных путей доступа к ресурсам			1			1
29	Угроза использования вычислительных ресурсов суперкомпьютера «паразитными» процессами			1			1
30	Угроза использования информации идентификации/аутентификации, заданной по умолчанию			1		1	
31	Угроза использования механизмов авторизации для повышения привилегий			1			1
32	Угроза использования поддельных цифровых подписей BIOS					1	
33	Угроза использования слабостей кодирования входных данных		1			1	
34	Угроза использования слабостей протоколов сетевого/локального обмена данными			1			1
35	Угроза использования слабых криптографических алгоритмов BIOS				1		
36	Угроза исследования механизмов работы программы		1			1	
37	Угроза исследования приложения через отчёты об ошибках		1			1	
38	Угроза исчерпания вычислительных ресурсов хранилища			1			

Рис. 4. Модель возможностей различных классов нарушителей по реализации УБИ (фрагмент)

Перечень возможных способов реализации каждой УБИ $\{S_1 \ldots S_i\}$ формируется из данных, полученных с сайта ФСТЭК, а также в ходе разработки такого перечня на объекте.

Каждый способ имеет свой сценарий (тактику) реализации (T_i) через существующие уязвимости.

Таким образом, представляется возможность составить вероятностную модель взаимных влияний УБИ, способов и сценариев их реализации. Фрагмент данной модели представлен на рис. 5.

Она представляет собой матрицу, у которой по горизонтали размещены наименование и описание УБИ, а по вертикали – уязвимости. Если угроза может быть реализована через одну или несколько уязвимостей, то в клетке на их пересечении указываются наименование и содержание способов ее реализации M_i, вероятность предпочтительности его выбора $P(M_i)$ и успешной реализации, а также сценарий (тактика) применения.

Вероятность выбора конкретного способа реализации УБИ будет зависеть от возможностей нарушителя, требуемых ресурсов, ценности защищаемых информационных ресурсов, инфраструктурных характеристик объекта, его системы защиты, а также имеющихся уязвимостей.

Определив в модели критерии актуальности УБИ, способы и сценарии их реализации, мы получим соответствующую матрицу.

Кластер ликвидации рисков угроз инцидентов формируется путем ввода характеристик эффективности мер защиты информации (МЗИ), определенных в [1, 2, 3, 4] и состоящих из технических и организационных мер по локализации способов реализации УБИ и (или) ликвидации уязвимостей. Технические меры (ТМ) реализуются различными средствами защиты информации (СЗИ), а организационные меры (ОМ) – инженерно-техническими средствами и режимными мероприятиями, проводимыми на основе организационно-руководящих документов (ОРД).

Наименование угроз безопасности информации	Угроза физического выведения из строя средств хранения,	Угроза форматирования носителей	Угроза «форсированного веб-браузинга»	Угроза хищения средств хранения, обработки и (или)
Описание угрозы безопасности информации	Реализация данной угрозы возможна при условии получения нарушителем физического доступа к носителям информации (внешним, съёмным и внутренним накопителям), средствам обработки информации (процессору, контроллерам устройств и т.п.) и средствам ввода/вывода информации (клавиатура и т.п.)	Угроза заключается в возможности утраты хранящейся на форматируемом носителе информации, зачастую без возможности её восстановления, из-за преднамеренного или случайного выполнения процедуры форматирования носителя информации.	Угроза заключается в возможности получения нарушителем доступа к защищаемой информации, выполнения привилегированных операций или осуществления иных деструктивных воздействий на некорректно защищённые компоненты веб-приложений. Данная угроза обусловлена слабостями (или отсутствием) механизма проверки корректности вводимых данных на веб-серверах. Реализация данной угрозы возможна при условии успешной реализации «ручного ввода» в адресную строку веб-браузера определённых адресов веб-страниц и осуществления принудительного перехода по древу веб-сайта к страницам, ссылки на которые явно не указаны на веб-сайте	Реализация данной угрозы возможна при условии наличия у нарушителя физического доступа к носителям информации (внешним, съёмным и внутренним накопителям), средствам обработки информации (процессору, контроллерам устройств и т.п.) и средствам ввода/вывода информации
Интерфейсы				
внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными (взаимодействующими) системами или сетями (проводные, б/проводные, веб-интерфейсы, др.)				
внутренние сетевые интерфейсы, обеспечивающие взаимодействие (в том числе через промежуточные компоненты) с компонентами систем и сетей, имеющими				$У_1$ $У_3$ / S_2 S_3, S_5 / T_1 T_2, T_3
интерфейсы для пользователей (проводные, беспроводные, веб-интерфейсы, интерфейсы удаленного доступа и др.)	$У_1$ $У_3$ $У_7$ / S_2 S_3, S_5 S_1, S_4 / T_1 T_2, T_3 T_1, T_2	$У_1$ $У_3$ / S_2 S_3, S_5 / T_1 T_2, T_3	$У_2$ $У_3$ $У_1$ $У_1$ / S_2 S_1 S_1, S_4 S_2 / T_1 T_3, T_3, T_2 T_1	$У_1$ $У_3$ / S_2 S_3, S_3 / T_1 T_2, T_4

Рис. 5. Вероятностная модель взаимосвязей уязвимостей, УБИ, способов и сценариев их реализации (фрагмент)

Процесс формирования базы данных защитных мероприятий представлен на рис. 6 в виде модели. Она представляет собой матрицу, где по горизонтали представлены МЗИ в соответствии с ОРД ФСТЭК, а по вертикали – УБИ. В клетках на пересечении УБИ и противопоставленных им МЗИ указываются перечни реализующих их СЗИ и ОРД.

После актуализации УБИ в модели останутся только актуальные УБИ, способы и сценарии их реализации, а также необходимые для их закрытия СЗИ и ОРД.

Критерии защищенности определяются организационно-руководящими и методическими документами. Способы реализации МЗИ будут иметь вероятностную степень эффективности, зависящую от функционала характеристик ТМ, ОМ и функционала показателей способа

реализации УБИ, а также появления новых уязвимостей, УБИ, способов и сценариев их реализации.

Рис. 6. Модель формирования базы данных защитных мероприятий

Кластер формирования рисков инцидента моделируется с учетом вероятности нанесения ущерба конфиденциальности (К), целостности (Ц) и доступности (Д) защищаемым информационным ресурсам с определенной степенью вероятности. Для этого на основе матрицы формируется вероятностная модель зависимостей вида и степени ущерба от типа инцидента. В ней по горизонтали указываются параметры оценки ущерба по каждому виду информационного ресурса (К, Ц, Д) (рис. 7). По вертикали указываются наименование и содержание инцидента. На пересечении указывается вербальное описание ущерба и вероятность его нанесения в случае реализации инцидента.

Рис. 7. Вероятностная модель зависимостей вида и степени ущерба от типа инцидента

Кластер ликвидации последствий инцидента моделируется аналогично кластеру ликвидации рисков угроз реализации инцидентов с составлением соответствующей модели.

Данную модель целесообразно изобразить в виде байесовской сети, которая представляет совместное распределение вероятностей с использованием направленного ациклического графа, в котором каждое ребро является условной зависимостью, а каждый узел – отдельной случайной величиной, отражающей события информационной безопасности [23, 24, 25]. Это позволяет проводить обновление вероятностей отраженных в ней событий информационной безопасности всякий раз, когда становится доступной новая информация. Математической основой для этого является теорема Байеса, суть которой описывает следующая формула:

$$P(\mathrm{A}|\mathrm{B})\,P(\mathrm{B}) = P(\mathrm{B}|\mathrm{A})\,P(\mathrm{A}). \quad (1)$$

При корректно составленной модели и достоверной информации о событиях ИБ можно доказать, что заложенная в ней методика обеспечивает правильное вычисление обновленных вероятностей относительно аксиом классической вероятности.

Любой узел в различных кластерах сети может получать информацию, так как метод не различает логический вывод в направлении ребер или наоборот. Одновременный ввод информации в несколько узлов не повлияет на алгоритм.

В модели взаимные влияния деструктивных воздействий и МЗИ представлены в виде цепочек последовательных событий, сходимой и расходимой последовательностей событий.

События в последовательных цепочках могут быть однородные (деструктивные или защитные) и разнородные (деструктивные и защитные) (рис. 8).

Расчет совместного распределения вероятностей для последовательных как однородных, так и разнородных событий осуществляется по приведенным ниже формулам.

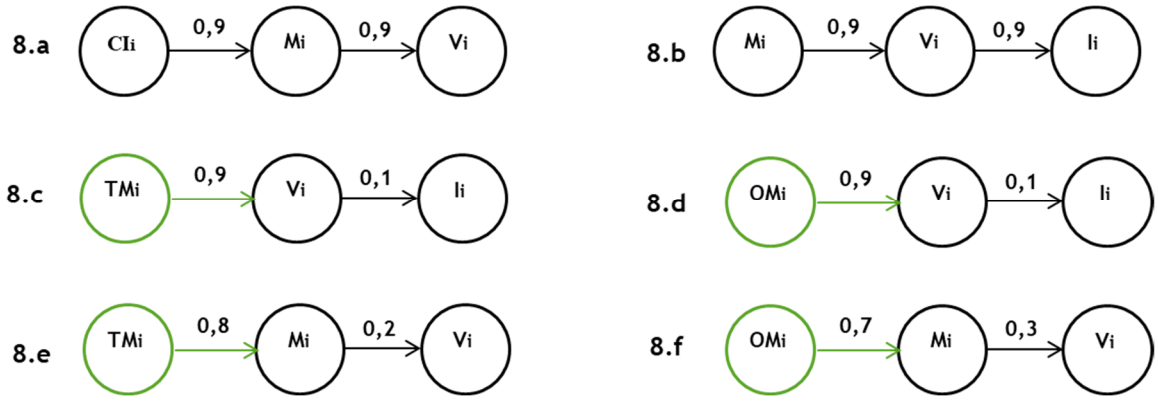

Рис. 8. Типы последовательных цепочек событий:
8 a, b – цепочки однородных (деструктивных) событий,
8 c, d, e, f – разнородные последовательности событий

Для варианта 8.a цепочки однородных (деструктивных) событий:

$$P(КлН_i, У_i \mid S_i) = \frac{P(КлН_i, S_i, У_i)}{P(S_i)} = \frac{P(КлН_i)(S_i|КлН_i)P(У_i|S_i)}{P(S_i)} = P(КлН_i \mid S_i)P(У_i \mid S_i). \quad (2)$$

Здесь априорная вероятность того, что нарушитель $КлН_i$ сможет реализовать УБИ способом S_i будет зависеть от апостериорной вероятности наличия незакрытой для данного способа уязвимости $У_i$.

Для варианта 8.c цепочки разнородных событий:

$$P(ТМ_i, И_i \mid У_i) = \frac{P(ТМ_i, У_i, И_i)}{P(У_i)} = \frac{P(ТМ_i)(У_i|ТМ_i)P(И_i|У_i)}{P(У_i)} = P(ТМ_i \mid У_i)P(И_i \mid У_i). \quad (3)$$

Здесь априорная вероятность эффективности технических мер будет зависеть от апостериорной вероятности наличия незакрытой уязвимости.

Аналогичным образом составляются формулы и устанавливаются вероятностные зависимости событий ИБ для других типов цепочек последовательных событий.

В модели также выявлено взаимное влияние деструктивных воздействий и МЗИ в виде цепочек сходимых событий (рис. 9).

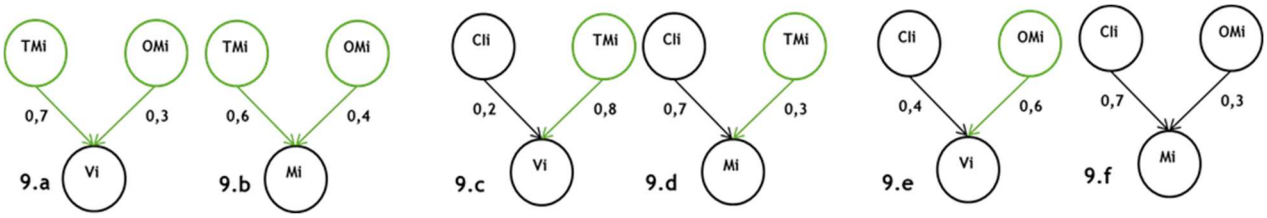

Рис. 9. Типы цепочек сходимых событий

Совместное распределение вероятностей для варианта 9.a сходимой последовательности событий ИБ рассчитывается по следующей формуле:

$$P(TM_i, OM_i, Y_i) = \sum_{y_i} P(TM_i)P(OM_i)P(Y_i \mid OM_i, TM_i) = P(OM_i \mid Y_i)P(TM_i \mid Y_i). \quad (4)$$

Для расходимых событий априорная вероятность существования уязвимости Y_i, будет зависеть от апостериорных вероятностей ее закрытия с помощью OM_i и TM_i.

Аналогичным образом составляются формулы и устанавливаются вероятностные зависимости событий ИБ для других типов цепочек расходимых событий.

Взаимное влияние деструктивных воздействий и МЗИ в виде цепочек расходимых событий представлено на рис. 10.

Рис. 10. Типы цепочек расходимых событий

Совместное распределение вероятностей для сходимой последовательности событий ИБ рассчитывается по следующей формуле:

$$P(S_i, Y_i \mid TM_i) = \frac{P(TM_i, S_i, Y_i)}{P(TM_i)} = P(S_i \mid TM_i)P(Y_i \mid TM_i). \quad (5)$$

Для расходимых событий априорная вероятность существования уязвимости Y_i и возможности реализации УБИ способом S_i будет зависеть от апостериорных вероятностей реализации OM_i и (или) TM_i.

Данный подход позволяет рассчитать зависимость априорной вероятности событий от вероятности событий, которые могут произойти, т.е. определить вероятностную зависимость деструктивных событий от защитных и наоборот.

Данная методика даёт возможность проведения универсальной оценки для событий информационной безопасности по количественным значениям подмножества переменных показателей МЗИ и деструктивного воздействия нарушителей, которая минимизирует вероятность ошибочного решения.

При принятии решения зачастую важна качественная оценка событий ИБ. Для перевода количественной оценки риска реализации инцидента ИБ в качественную применим нечетко-вероятностный метод [26].

Рассмотрим последовательность применения данного подхода для событий ИБ.

1. Зададим совместное распределение вероятностей событий ИБ $\{P(КлН_i,S_i,У_i)|P(ТМ_i,ОМ_i)\}$, где $P(ТМ_i,ОМ_i)$ – вероятная эффективность способа реализации МЗИ, $P(КлН_i,S_i,У_i)$ – вероятность риска реализации УБИ.

2. Проведем преобразование нечетких значений входных переменных $\{P(КлН_i,S_i,У_i)\}$ и $\{P(ТМ_i,ОМ_i)\}$ «Очень низкий (ОН)», «Низкий (Н)», «Средний (С)», «Высокий (В)», «Очень высокий (ОВ)» в числовые значения [27].

3. Зададим правила преобразования нечетких значений оценки риска реализации инцидента ИБ в числовые значения из диапазона [0, 1] в виде матрицы нечетких правил оценки риска реализации инцидента ИБ (табл. 1).

Соотношение количественных и качественных оценок риска реализации инцидента представлено в табл. 2.

Таблица 1. Матрица нечетких правил оценки риска реализации инцидента информационной безопасности

		Вероятная эффективность способа реализации МЗИ при локализации *i*-ой УБИ				
		ОН	**Н**	**С**	**В**	**ОВ**
Вероятность риска реализации УБИ при реализации *i*-го способа МЗИ	**ОН**	Н	Н	Н	ОН	ОН
	Н	Н	Н	Н	Н	ОН
	С	С	С	С	Н	Н
	В	ОВ	В	С	Н	Н
	ОВ	ОВ	ОВ	В	С	Н

Таблица 2. Соотношение количественных и качественных оценок риска реализации инцидента

Значения количественной оценки риска реализации инцидента	Значения качественной оценки риска реализации инцидента
$0 \le P(S_i У_i \mid И_i) \le 0.2$	Очень низкая
$0.2 \le P(S_i У_i \mid И_i) \le 0.4$	Низкая
$0.4 \le P(S_i У_i \mid И_i) \le 0.6$	Средняя
$0.6 \le P(S_i У_i \mid И_i) \le 0.8$	Высокая
$0.8 \le P(S_i У_i \mid И_i) \le 1$	Очень высокая

3. Заключение

Предлагаемая методика позволяет проводить универсальную оценку событий информационной безопасности по количественным значениям подмножества переменных показателей защитных мероприятий и деструктивного воздействия нарушителей, что сводит к минимуму вероятность ошибочного решения [28, 29].

Представленная в работе модель является масштабируемой, а это значит, что она обладает свойствами универсальности как с точки зрения критериальных требований, так и

вероятностных показателей. На её основе можно реализовать нейро-байесовский подход и получить систему поддержки принятия решений на основе искусственного интеллекта [30].

Литература

1. Приказ ФСТЭК России «Об утверждении требований к защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» от 12.02.2013 № 17 [Электронный ресурс]. URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702-prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17 (дата обращения: 20.12.2021).
2. Приказ ФСТЭК России «Об утверждении состава и содержания организационных и технических мероприятий по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 18.02.2013 № 21 [Электронный ресурс]. URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21 (дата обращения: 20.12.2021).
3. Приказ ФСТЭК России «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и окружающей среды» от 14.03.2014 № 31 [Электронный ресурс]. URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/868-prikaz-fstek-rossii-ot-14-marta-2014-g-n-31 (дата обращения: 20.12.2021).
4. Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении требований к обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (с изменениями и дополнениями, 26 декабря 2019 г., № 60) [Электронный ресурс]. URL: https://fstec.ru/en/53-normotvorcheskaya/akty/prikazy/1592-prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239 (дата обращения: 20.12.2021).
5. Постановление Правительства Российской Федерации от 17.02.2018 № 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры» [Электронный ресурс]. URL: https://www.garant.ru/products/ipo/prime/doc/71783452 / (дата обращения: 20.12.2021).
6. Постановление Правительства Российской Федерации от 08.02.2018 № 127 «Об утверждении Правил категоризации объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» [Электронный ресурс ресурс]. URL: http://government.ru/docs/6339 / (дата обращения: 20.12.2021).
7. Постановление Правительства Российской Федерации от 01.10.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» [Электронный ресурс]. URL: https://www.garant.ru/products/ipo/prime/doc/72166260/ (дата обращения: 20.12.2021).
8. Методический документ. Утвержденная ФСТЭК России 5 февраля 2021 года «Методика оценки угроз информационной безопасности» [Электронный ресурс]. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2170-metodicheskij-dokument-utverzhden-fstek-rossii-5-fevralya-2021-g (дата обращения: 20.12.2021).
9. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России [Электронный ресурс]. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-

spetsialnye-normativnye-dokumenty/379-bazovaya-model-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-vypiska-fstek-rossii-2008-god (дата обращения: 20.12.2021).

10. *Джиарратано Д., Райли Г.* Экспертные системы: принципы разработки и программирования / изд. 4-е, перевод с англ. Изд. Уильямса. ISBN: 978-5-8459-1156-8, 2007. С. 115–201.
11. *Рассел С., Норвиг П.* Искусственный интеллект: современный подход / 2-е издание, перевод с англ. Изд. Уильямса, ISBN: 5-8459-0887-6, 2006. С. 345–428.
12. *Перл Д.* Байесовские сети. М.: Лаборатория когнитивных систем Калифорнийского университета, Лос-Анджелес, 2000. 102 с.
13. *Джаксен Ф.* Байесовские сети и графики принятия решений. Изд. Шпрингер, 2001. С. 54–120.
14. *Литвиненко Н. Г., Литвиненко А. Г., Мамырбаев О. Ж., Шаяхметова А. С.* Агенариск. Работа с байесовскими сетями. Алматы: Институт информационных и вычислительных технологий, 2019. 233 с.
15. *Конради С., Джуфф Л.* Байесовские сети и байесовская лаборатория. Практическое введение для исследователей.
16. Руководство пользователя BAYESIALAB. URL: https://library.bayesia.com/display/BlabC/BayesiAlab+Руководство пользователя+.
17. *Конради С., Джуфф Л.* Введение в байесовские сети и байесовскую лабораторию. URL: https://library.bayesia.com/download/attachments/10092794/BayesianNetworks Введение v16.pdf.
18. Расширенное моделирование с использованием AgenaRisk. URL: https://www.agenarisk.com.
19. Байесовская сетевая технология Agena. URL: https://www.agenarisk.com.
20. Начало работы с AgenaRisk. URL: https://www.agenarisk.com.
21. Эксперт Хугин. Построение байесовской сети. URL: https://www.hugin.com/wp-content/uploads/2016/05/Building-a-BN-Tutorial.pdf.
22. Эксперт Хугин. Технический документ. URL: http://download.hugin.com/webdocs/техническийдокумент/huginexpert-технический документ.pdf.
23. *Фентон Н., Нил М.* Оценка рисков и анализ решений с использованием байесовских сетей. ISBN 9781439809105.
24. *Басакер Р., Саати Т.* Конечные графы и сети. М.: Наука, 1974. С. 205–278.
25. *Свами М., Туласираман К.* Графики, сети и алгоритмы. М.: Мир, 1984. С. 55–146.
26. *Гавришев А. А.* Анализ программ моделирования нечетких систем // Дистанционное и виртуальное обучение. 2017. № 6. С. 76–83.
27. *Гавришев А. А.* Моделирование и количественный и качественный анализ широко распространенных систем защищенной связи // Прикладная информатика. 2018. Т. 13, № 5 (77). С. 84–122.
28. *Баранов В. В., Секретарев А. В., Игнатьева А. Р.* Автоматизация разработки методов защиты объектов информатизации // Материалы Всероссийской научно-практической конференции «Социотехнические и гуманитарные аспекты информационной безопасности», 2019. С. 21–30.
29. *Баранов В. В., Максимова Е. А., Лаута О. С.* Анализ модели информационной поддержки процессов и систем при реализации многоагентного интеллектуального взаимодействия // Устройства и системы. Управление, контроль, диагностика. 2019. № 4. С. 32–41.
30. *Баранов В. В., Максимова Е. А.* Прогнозирование разрушительных вредных воздействий на объекты критической информационной инфраструктуры // Коммуникации в компьютерных и информационных науках. 2021. 1395 CCIS. С. 88–99.

Статья поступила в редакцию 15.05.2022.

Баранов Владимир Витальевич
кандидат военных наук, доцент, заведующий кафедрой «Информационная безопасность» ФГБОУ ВО ЮРГПУ (НПИ) имени М. И. Платова (346428, Ростовская обл., Новочеркасск, ул. Просвещения, 132), e-mail: baranov.vv.2015@yandex.ru.

Models and methods for assessing the security of an informatization object

Baranov Vladimir
M.I. Platov South Russian State Polytechnic University, Novocherkassk, st. Troickaya 132, 346428, Russian Federation, baranov.vv.2015@yandex.ru.

The paper substantiates the need of creation an information decision support system in the development of systems for protecting informatization objects. Analyzes of existing systems in various fields of activity, the requirements for the functionality of the system in relation to the field of information protection, methods for developing models of functioning of protected information systems in a destructive environment impact on the basis of Bayesian networks are considered. The paper gives a description of a typical module functioning of this model. The structures of probabilistic models of the relationship of vulnerabilities, information security threats, methods and scenarios for their implementation, the formation of measures to protect informatization objects, the formation and assessment of the risks of incidents and their damage are considered. Clusters of typical information security events, methodological apparatus for calculating the joint distribution of the probabilities of protective and destructive events are determined. Finally, typical chains of interconnections of such events are identified. Mathematical apparatus for calculating their probabilities, a verbal description of the patterns of their mutual influence, and a method for converting quantitative probabilistic values of informatization object security indicators into qualitative ones are presented, and the results of the study are summarized.

Keywords: decision support; Bayesian network, destructive influences, information protection measures, information security threats, management strategy, information security events impact analysis, structural analysis, protection systems.

References

1. *Prikaz FSTEK Rossii "Ob utverzhdenii trebovanij k zashchite informacii, ne sostavlyayushchej gosudarstvennuyu tajnu, soderzhashchejsya v gosudarstvennyh informacionnyh sistemah" ot 12.02.2013 № 17* [Order of the FSTEC of Russia "On approval of requirements for the protection of information that does not constitute a state secret contained in state information systems" dated 12.02.2013 no. 17], available at: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702-prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17 (accessed 20.12.2021).
2. *Prikaz FSTEK Rossii "Ob utverzhdenii sostava i soderzhaniya organizacionnyh i tekhnicheskih meropriyatij po obespecheniyu bezopasnosti personal'nyh dannyh pri ih obrabotke v informacionnyh sistemah personal'nyh dannyh" ot 18.02.2013 № 21* [Order of the FSTEC of Russia "On 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" dated 02/18/2013 no. 21], available at: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21 (accessed 20.12.2021).
3. *Prikaz FSTEK Rossii "Ob utverzhdenii trebovanij k obespecheniyu zashchity informacii v avtomatizirovannyh sistemah upravleniya proizvodstvennymi i tekhnologicheskimi processami na kriticheski vazhnyh ob"ektah, potencial'no opasnyh ob"ektah, a takzhe ob"ektah, predstavlyayushchih povyshennuyu opasnost' dlya zhizni i zdorov'ya lyudej i okruzhayushchej sredy" ot 14.03.2014 № 31* [Order of the FSTEC of Russia "On approval of requirements for ensuring the protection of information in automated control systems for production and technological processes at critical facilities, potentially dangerous facilities, as well as facilities that pose an increased danger to human life and health and to the environment" dated 14.03.2014 no. 31], available at: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/868-prikaz-fstek-rossii-ot-14-marta-2014-g-n-31 (accessed 20.12.2021).

4. *Prikaz FSTEK Rossii ot 25.12.2017 № 239 "Ob utverzhdenii trebovanij k obespecheniyu bezopasnosti znachimyh ob"ektov kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii"* [Order of the FSTEC of Russia dated 25.12.2017 no. 239 "On Approval of requirements for ensuring the security of Significant Objects of Critical Information Infrastructure of the Russian Federation], available at: https://fstec.ru/en/53-normotvorcheskaya/akty/prikazy/1592-prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239 (accessed 20.12.2021).
5. *Postanovlenie Pravitel'stva Rossijskoj Federacii ot 17.02.2018 № 162 "Ob utverzhdenii Pravil osushchestvleniya gosudarstvennogo kontrolya v oblasti obespecheniya bezopasnosti znachimyh ob"ektov kriticheskoj informacionnoj infrastruktury"* [Resolution of the Government of the Russian Federation dated 17.02.2018 no. 162 "On approval of the Rules for the implementation of state control in the field of ensuring the security of significant objects of critical information infrastructure"], available at: https://www.garant.ru/products/ipo/prime/doc/ 71783452/ (accessed 20.12.2021).
6. *Postanovlenie Pravitel'stva Rossijskoj Federacii ot 08.02.2018 № 127 "Ob utverzhdenii Pravil kategorizacii ob"ektov kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii, a takzhe perechnya pokazatelej kriteriev znachimosti ob"ektov kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii i ih znachenij"* [Decree of the Government of the Russian Federation no. 127 dated 08.02.2018 "On approval of the Rules for categorizing objects of critical information infrastructure of the Russian Federation, as well as a list of indicators of criteria for the significance of objects of critical information infrastructure of the Russian Federation and their values"], available at: http://government.ru/docs/6339/ (accessed 20.12.2021).
7. *Postanovlenie Pravitel'stva Rossijskoj Federacii ot 01.10.2012 № 1119 "Ob utverzhdenii trebovanij k zashchite personal'nyh dannyh pri ih obrabotke v informacionnyh sistemah personal'nyh dannyh"* [Decree of the Government of the Russian Federation no. 1119 of 01.10.2012 "On approval of requirements for the protection of personal data during their processing in personal data information systems"], available at: https://www.garant.ru/products/ipo/prime/doc/72166260/ (accessed 20.12.2021).
8. *Metodicheskij dokument. Utverzhdennaya FSTEK Rossii 5 fevralya 2021 goda "Metodika ocenki ugroz informacionnoj bezopasnosti"* [Methodological document. Approved by the FSTEC of Russia on February 5, 2021, "Methodology for assessing threats to information security"], available at: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2170-metodicheskij-dokument-utverzhden-fstek-rossii-5-fevralya-2021-g (accessed 20.12.2021).
9. *Bazovaya model' ugroz bezopasnosti 2008 "Bazovaya model' ugroz bezopasnosti personal'nyh dannyh pri ih obrabotke v informacionnyh sistemah personal'nyh dannyh. FSTEK Rossii"* [Basic model of security threats 2008 "Basic model of threats to the security of personal data during their processing in personal data information systems. FSTEC of Russia"], available at: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/379-bazovaya-model-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-vypiska-fstek-rossii-2008-god (accessed 20.12.2021).
10. Giarratano D., Riley G. *Ekspertnye sistemy: principy razrabotki i programmirovaniya.* [Expert systems: principles of development and programming]. 4 nd edition, translated from English, Williams Publishing House, ISBN: 978-5-8459-1156-8, 2007, pp. 115-201.
11. Russell S., Norvig P. *Iskusstvennyj intellekt: sovremennyj podhod.* [Artificial Intelligence: a Modern approach]. 2 nd edition, translated from English, Williams Publishing House, ISBN: 5-8459-0887-6, 2006, pp. 345-428.
12. Pearl D. *Laboratoriya kognitivnyh sistem Kalifornijskogo universiteta, Los Angeles. Bajesovskie seti.* [Laboratory of Cognitive Systems of the University of California, Los Angeles. Bayesian networks]. Moscow, Mir, 2000, 102 p.
13. Jaxen F. *Bajesovskie seti i grafiki prinyatiya reshenij.* [Bayesian networks and decision graphs]. M, Springer, 2001, pp. 54-120.
14. Litvinenko N.G., Litvinenko A.G., Mamyrbayev O.J., Shayakhmetova A.S. *Agenarisk. Rabota s bajesovskimi setyami* [Agenarisk. Work with bayesian networks]. Almaty: Institut informacionnyh i vychislitel'nyh tekhnologij, 2019, 233 p.
15. Konradi S., Juff L. *Bajesovskie seti i Bajesovskaya laboratoriya, Prakticheskoe vvedenie dlya issledovatelej* [Bayesian networks and the Bayesian Laboratory, A practical introduction for researchers], available at: https://www.researchgate.net / publication/282362899 (accessed 20.12.2021).
16. BAYESIALAB User's Guide, available at: https://library.bayesia.com (accessed 20.12.2021).

17. Konradi S., Juff L. Introduction to Bayesian Networks and the Bayesian Laboratory, available at: https://library.bayesia.com/download/attachments/10092794/BayesianNetworks Introduction v16.pdf (accessed 20.12.2021).
18. Advanced modeling using AgenaRisk, available at: https://www.agenarisk.com (accessed 20.12.2021).
19. Agena Bayesian network technology, available at: https://www.agenarisk.com (accessed 20.12.2021).
20. Getting started with AgenaRisk, available at: https://www.agenarisk.com (accessed 20.12.2021).
21. Expert Hugin, Building a Bayesian network, available at: https://www.hugin.com/wp-content/uploads/2016/05/Building-a-BN-Tutorial.pdf (accessed 20.12.2021).
22. Expert Hugin, Technical Technical Document, available at: http://download.hugin.com / webdocs/technical document/huginexpert-technical document.pdf (accessed 20.12.2021).
23. Fenton N., Neil M. Risk assessment and decision analysis using Bayesian networks. *Queen Mary, University of London and Agena Ltd. CRC press*. ISBN: 9781439809105, ISBN 10: 1439809100.
24. Basaker R., Saati T. *Konechnye grafy i seti* [Finite graphs and networks]. Moscow, Nauka, 1974, pp. 205-278.
25. Swami M., Thulasiraman K. *Grafiki, seti i algoritmy* [Graphs, networks and algorithms]. Moscow, Mir, 1984, pp. 55-146.
26. Gavrishev A.A. *Analiz programm modelirovaniya nechetkih sistem.* [Analysis of fuzzy systems modeling programs]. *Distancionnoe i virtual'noe obuchenie*], 2017, no. 6, pp. 76-83.
27. Gavrishev A.A. Modelirovanie i kolichestvennyj i kachestvennyj analiz shiroko rasprostranennyh sistem zashchishchennoj svyazi. [Modeling and quantitative and qualitative analysis of widespread secure communication systems]. *Prikladnaya informatika*, 2018, vol. 13, no 5 (77), pp. 84-122.
28. Baranov V.V., Sekretarev A.V., Ignatieva A.R. Avtomatizaciya razrabotki metodov zashchity ob"ektov informatizacii [Automation of development of methods of protection of informatization objects]. *Vserossijskaya nauchno-prakticheskaya konferenciya. Sociotekhnicheskie i gumanitarnye aspekty informacionnoj bezopasnosti*, Pyatigorsk, Pyatigorskij gosudarstvennyj universitet, 10-13, April, 2019, pp. 21-30.
29. Baranov V.V., Maksimova E.A., Lauta O.S. Analiz modeli informacionnoj podderzhki processov i sistem pri realizacii mnogoagentnogo intellektual'nogo vzaimodejstviya [Analysis of the model of information support of processes and systems in the implementation of multi-agent intellectual interaction]. *Ustrojstva i sistemy. Upravlenie, kontrol', diagnostika,* 2019, no. 4, pp. 32-41.
30. Baranov V.V., Maksimova E.A. Prognozirovanie razrushitel'nyh vrednyh vozdejstvij na ob"ekty kriticheskoj informacionnoj infrastruktury [Forecasting destructive harmful effects on objects of critical information infrastructure]. *Kommunikacii v komp'yuternyh i informacionnyh naukah*, 2021, 1395 CCIS, pp. 88-99.