УДК 004.056.5+004.89
DOI: 10.38028/ESI.2023.29.1.014

Оценка состояния комплексной системы защиты информации на основе онтологий

Наседкин Павел Николаевич, Аршинский Леонид Вадимович

Иркутский государственный университет путей сообщения,
Россия, Иркутск, *nasedkin_pn@irgups.ru*

Аннотация. Одной из проблем организации комплексной системы защиты информации (КСЗИ) является оценка функциональности системы в целом. Для решения подобных задач могут использоваться подходы на основе агрегированного оценивания. В настоящее время такие оценки строятся, как правило, с помощью взвешенных средних, что не позволяет моделировать ключевые компоненты системы, то есть такие, утрата которых ведёт к нефункциональности системы в целом или отдельных её подсистем. В работе на основе метода логико-аксиологического оценивания показан подход к агрегированному оцениванию подсистемы программно-технических решений КСЗИ предприятия. Необходимой частью такого оценивания является онтологическое моделирование системы с помощью лёгких онтологий, отражающих взаимосвязи между компонентами. Построены онтологии и дан пример расчёта для одной из подсистем.

Ключевые слова: информационная безопасность, комплексная система защиты информации, агрегированное оценивание, логико-аксиологический подход, присоединённый вывод

Цитирование: Наседкин П.Н. Оценка состояния комплексной системы защиты информации на основе онтологий / П.Н. Наседкин, Л.В. Аршинский // Информационные и математические технологии в науке и управлении. – 2023. – № 1(29). – С. 158-177. – DOI:10.38028/ESI.2023.29.1.014.

Введение. Считается, что одна из аксиом управления гласит: «Что невозможно измерить, тем невозможно управлять» (Дж. Уэлч) [1]. В полной мере это относится к управлению системами защиты информации. Тезис Уэлча можно ещё усилить, добавив: «Управление тем лучше, чем лучше формализация», то есть, хорошая формализация системы ведёт к более эффективному управлению ею.

Информационная безопасность – важнейшая область исследований в наше время, о чем свидетельствуют многочисленные публикации на эту тему [2-5]. В частности, последние исследования посвящены вопросам, связанным с «Большими данными», облачными технологиями и электронным обучением [2, 4, 5]. В работах [6, 7] исследованы различные средства информационной безопасности, включая фактографические системы и кибербезопасность сетей связи транспортных средств. Несмотря на то, что автоматизированным средствам информационной безопасности уделяется значительное внимание [8, 9], в этой области недостаточно внимания уделяется системному анализу и системному подходу. В работе [7] на базе принципов системного анализа и системного подхода [10-13] введены необходимые частные показатели, связанные с оценкой эффективности средств ИБ и фактографических информационных систем. В работе [15] и [16] показана возможность применения системного анализа в области информационной безопасности. Для этого в [17, 18, 19, 20], рассматриваются различные затраты и показатели. Стандарт ISO/IEC TR 27016 [20] является полезным инструментом для оценки эффективности средств информационной безопасности, особенно с точки зрения их экономической и стоимостной оценки.

Сегодня существуют разные подходы к формализации. Наиболее основательная из них – математическая, описывающая количественные взаимосвязи между компонентами системы, внешней средой, целями функционирования. Однако такое возможно только для относительно простых систем, или их фрагментов. В более сложных случаях, особенно характеризующихся случайностью протекающих процессов, хорошо подходят имитационное моделирование [21, 22] и его подвид – агентное [23-25], когда специальным образом имитируется поведение системы через поведение её фрагментов (например, агентов) и их ближнее взаи-

модействие, а поведение системы в целом изучается по поведению модели. Наконец, если система слабо структурирована и трудно формализуема, а это типично для многих управленческих задач, приходится использовать качественное моделирование, например, на основе знаний [26-28], а также агрегатное моделирование, характеризующее объект в целом на основе характеристик его частей [29].

Одним из видов знаниевого моделирования является моделирование с помощью онтологий [26, 27]. Однако описать структуру системы и отношения между её частями ещё недостаточно. Полезно знать, хотя бы в общих чертах, как изменение одних составляющих повлияет на другие. Этого можно достичь, если с каждым концептом онтологии связать, например, некоторое характеризующее его число, а с каждой дугой – своего рода передаточную функцию, преобразующую изменение объекта *A* во вклад в изменение связанного с ним объекта *B*. Для сложных предметных областей взаимовлияние трудно описать исчерпывающим количественным образом, однако можно применять приближённые схемы, использующие, в том числе, экспертные оценки. Например, в [30-32] онтологии использовались как часть метода оценки качества. Агрегат качества считался традиционным образом как среднее арифметическое или среднее геометрическое взвешенное [32]. Привлекая онтологии, можно агрегировать и другие показатели и по иным расчётным схемам.

В статье рассматривается логико-аксиологический подход к агрегированному оцениванию, оперирующий понятием ценности объекта (компонента) *A* для объекта *B* как мерой убыли функциональности *B* при утрате *A* [29, 33]. Причём ценность может быть такова, что утрата первого может повлечь утрату второго, независимо от состояния других, связанных с *B*, объектов. В целом, в основе логико-аксиологического подхода лежит структурирование предметной области с помощью лёгких онтологий с последующей расстановкой и обработкой числовых показателей – ценностей и характеризующих чисел в дугах и узлах структуры (концептах предметной области) и получением итогового показателя – агрегата – в ходе присоединённого логического вывода [33]. Важной особенностью данного метода является возможность избирательно вводить понятия ключевых компонентов системы, отказ которых ведёт к её полной нефункциональности. Существование подобных компонентов (функциональных элементов и подсистем) естественно для многих предметных областей, однако популярные методы агрегирования с помощью разного рода средних эту особенность фактически не учитывают. Возможность работы с ключевыми компонентами позволяет более последовательно учесть вклад значимых компонентов в общую функциональность системы. Например, при аддитивном агрегировании по среднему арифметическому взвешенному существует эффект ничтожного влияния оценок функциональных элементов сложной иерархизированной системы на итоговый показатель [34]. Здесь этого удаётся избежать.

В работе обсуждается вопрос агрегированного оценивания указанным методом состояния комплексной системы защиты информации (КСЗИ). КСЗИ является сложной иерархической системой, что делает во многом бессмысленными, например, аддитивные подходы к оцениванию. Применения логико-аксиологического подхода выглядит в этом смысле более перспективным. Его демонстрация для данной предметной области составляет цель и новизну работы. В связи с объёмностью КСЗИ в целом, оценку рассмотрим на примере базовой части – подсистемы программно-технических решений (ПТР) [35].

1. Онтологическое моделирование уровня программно-технических решений КСЗИ предприятия. Общая структура КСЗИ предприятия представлена на рис. 1. Её частью является уровень программно-технических решений – подсистема КСЗИ, структура которой представлена на рис. 2 [35, 36].

Рассмотрим структуру подсистемы ПТР (рис. 2), база знаний о ней позволяет в виде лёгких онтологий сформировать взаимосвязи между её компонентами, которые могут быть

использованы в процессе комплексной защиты информации на любом предприятии разного уровня зрелости по информационной безопасности.

Необходимо отметить, что термины «узлы» информационной системы и «компоненты» уровня ПТР имеют разные значения и используются для обозначения разных вещей в контексте информационных систем и подсистем средств защиты информации.

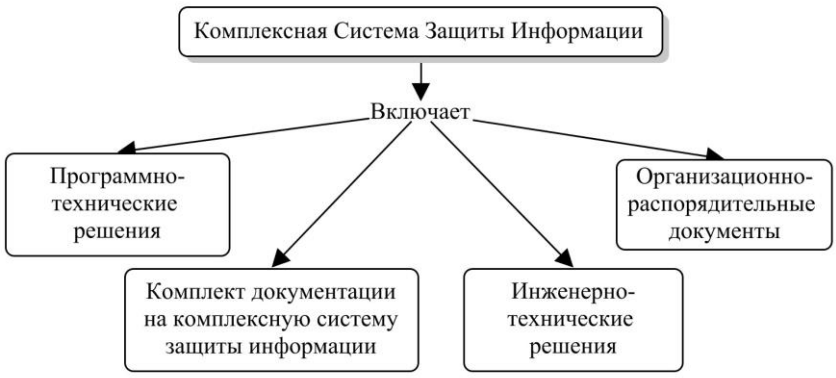

Рис. 1. Общая структура КСЗИ предприятия

В общем случае под «узлом» в информационной системе понимается любое устройство или компонент, подключенные к сети и имеющие уникальный сетевой адрес, например, компьютер, сервер или маршрутизатор. «Узлы» могут быть физическими устройствами, виртуальными машинами или программными приложениями.

С другой стороны, «компоненты» в подсистеме средств защиты информации означают отдельные части, составляющие единую систему, такие, как брандмауэры, системы обнаружения и предотвращения вторжений, антивирусное программное обеспечение, средства шифрования и механизмы контроля доступа. Эти компоненты работают вместе для защиты информационной системы от различных угроз и уязвимостей.

Таким образом, хотя и «узлы», и «компоненты» являются важными частями информационных систем и подсистем средств защиты информации, они обозначают разные вещи и играют разные роли в этих системах.

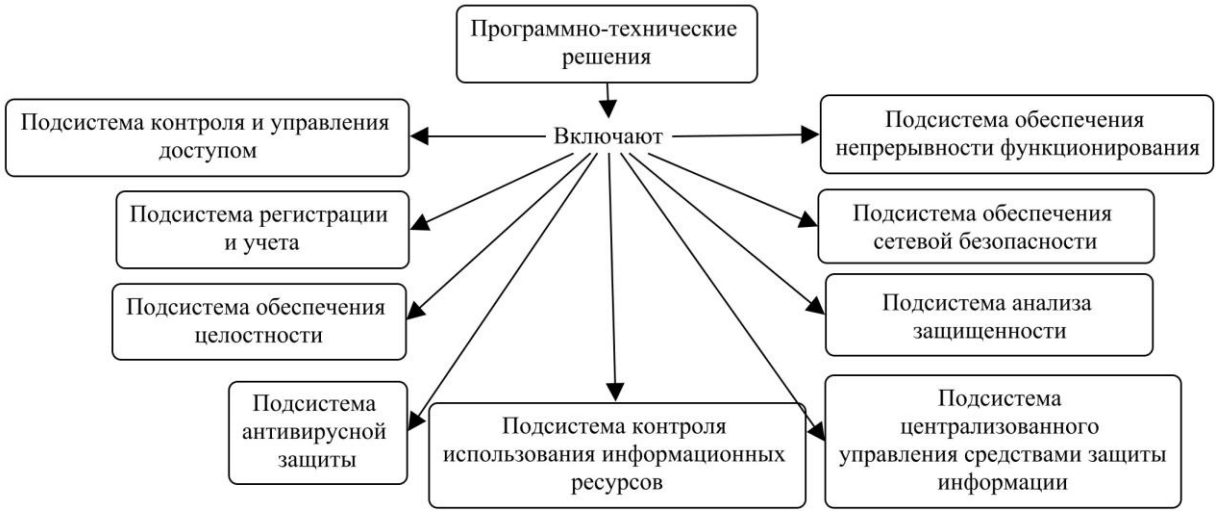

Рис. 2. Состав подсистемы программно-технических решений

Подсистема контроля и управления доступом описывается онтологией на рис. 3 [36, 37]. Здесь К1, … К15 – также сложные концепты, которые могут быть разбиты на составляющие, но ограничимся этим уровнем, рассматривая их здесь и далее в качестве своего рода функциональных элементов. Это:

- К1 – комплекс встроенных средств защиты серверов и автоматизированных рабочих машин (АРМ) под управлением операционных систем;
- К2 – комплекс антивирусной защиты;
- К3 – комплекс резервного копирования;
- К4 – комплекс защиты среды виртуализации;
- К5 – комплекс сбора, анализа и корреляции событий информационной безопасности (ИБ);
- К6 – комплекс встроенных средств активного сетевого оборудования (АСО);
- К7 – комплекс резервного копирования конфигурационных файлов АСО;
- К8 – комплекс межсетевого экранирования;
- К9 – комплекс обнаружения вторжений;
- К10 – комплекс встроенных средств защиты систем хранения данных;
- К11 – комплекс централизованного управления средствами защиты информации (СрЗИ);
- К12 – комплекс анализа защищенности;
- К13 – комплекс контроля целостности;
- К14 – комплекс встроенных средств защиты прикладного программного обеспечения (ППО);
- К15 – комплекс контроля использования информационных ресурсов.

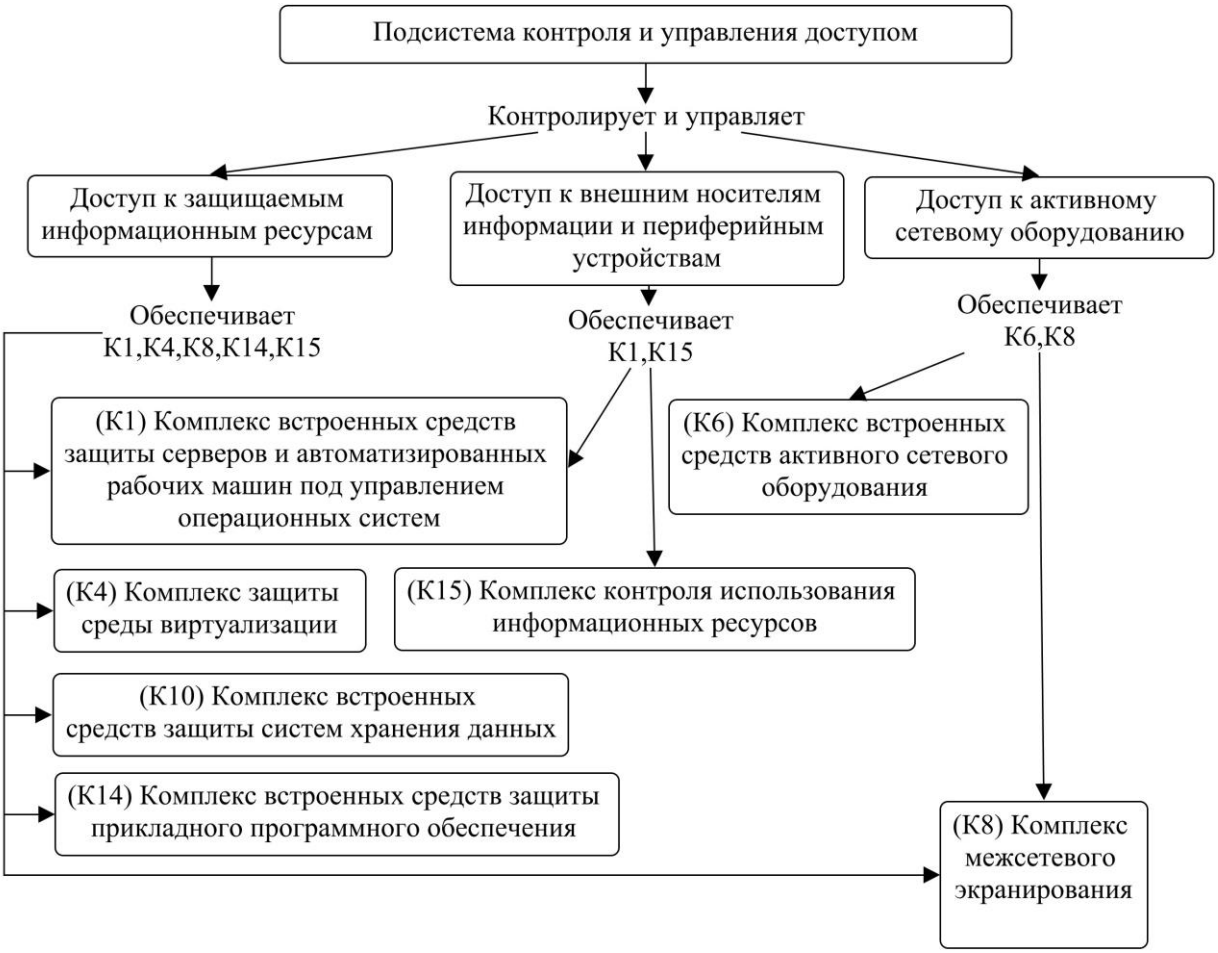

Рис. 3. Онтология подсистемы контроля и управления доступом комплекса ПТР

Подсистема контроля и управления доступом предназначена для задач [35-37]: идентификации; аутентификации; создания, активации, модификации, пересмотра (с установлен-

ной периодичностью), отключения (блокирования) и удаления учетных записей; обеспечения контроля за действиями пользователей и администраторов при доступе их к информационным активам предприятия.

В рамках данной подсистемы обеспечивается идентификация программ, томов, каталогов, файлов на АРМ и серверах.

Следующей идёт *подсистема регистрации и учёта* (рис. 4).

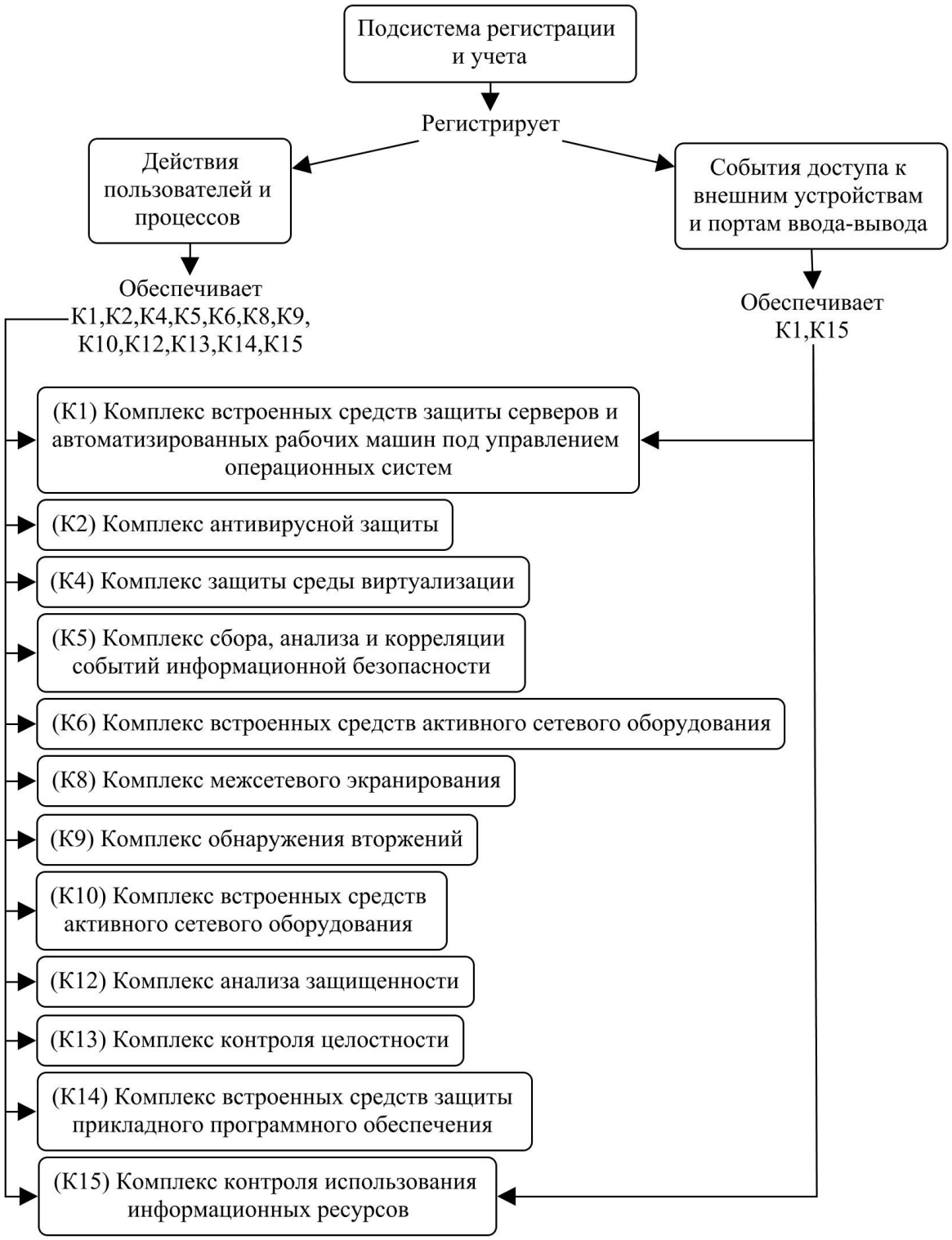

Рис. 4. Онтология подсистемы регистрации и учёта

В рамках подсистемы регистрации и учета выполняются следующие функции:

– Регистрация входа/выхода субъектов доступа (пользователей и процессов) к защищаемым информационным ресурсам (ИР), где ИР может относиться к любому источнику информации, который может быть использован для обучения, общения или принятия решений. Некоторые примеры того, что можно считать частью информационного ресурса, включают:
  - электронные документы (книги, статьи и т.п.);
  - электронный массив (базы данных и другие электронные источники информации);
  - веб-сайты;
  - аудио- и видеозаписи, включая подкасты и вебинары.

  В целом, все, что может быть использовано для сбора или передачи информации, может считаться частью информационного ресурса. Конкретные элементы, составляющие информационный ресурс, будут зависеть от контекста и цели, для которой он используется.
– Регистрация запуска и завершения программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов.
– Регистрация попыток доступа субъектов (пользователей и процессов) к защищаемым объектам доступа (файлам, каталогам).
– Регистрация событий вывода документов на печать.
– Регистрация событий доступа к внешним устройствам (внешние накопители информации), а также порты ввода-вывода на автоматизированных рабочих машинах.
– Регистрация событий информационной безопасности (ИБ) на активном сетевом оборудовании (коммутаторы, маршрутизаторы) и средствах защиты информации.
– Сбор, запись и хранение зарегистрированных событий безопасности в течение установленного времени хранения. Сбор событий ИБ должен осуществляться по протоколам (Syslog, MS Windows Event log, SSH/Telnet, СУБД с использованием ODBC, SNMP Trap, Checkpoint LEA/OPSEC, NetFlow и т.п.) с учетом функциональных возможностей источника событий):
  - обработка получаемых событий ИБ, включая: фильтрацию; нормализацию; агрегацию; категоризацию; приоритизацию; корреляцию; корреляцию событий ИБ, в т.ч.:
    - корреляцию событий ИБ на основе встроенной базы правил корреляции,
    - возможность создания собственных правил корреляции,
    - возможность использования в правилах корреляции перечня заведенных в подсистеме активов,
    - возможность использования справочников при формировании правил корреляции,
    - многоуровневую корреляцию, когда результаты срабатывания правил корреляции подаются на вход другому правилу корреляции;
  - возможность оптимизации правил корреляции с использованием новых данных об активах;
  - возможность управления задачами по сбору, обработке и корреляции событий, управления активами из единой консоли (web-интерфейса).

  Подсистема обеспечения целостности показана на рис. 5. В её задачи входят:
– контроль целостности исполняемых и конфигурационных файлов СрЗИ, операционных систем (ОС);
– контроль целостности ППО;

– контроль неизменности параметров встроенных средств защиты информации, ОС, АРМ и серверов, входящих в состав ИС и АСУ ТП.

Рис. 5. Онтология подсистемы обеспечения целостности

Подсистема антивирусной защиты показана на рис. 6.

В рамках подсистемы обеспечиваются:

– постоянная защита файловой системы АРМ и серверов под управлением различных версий ОС от вирусов, троянских программ и червей, как с использованием баз вирусных описаний, так и с помощью эвристического анализа;
– потоковая защита межсетевого трафика от вирусов и вредоносных программ.

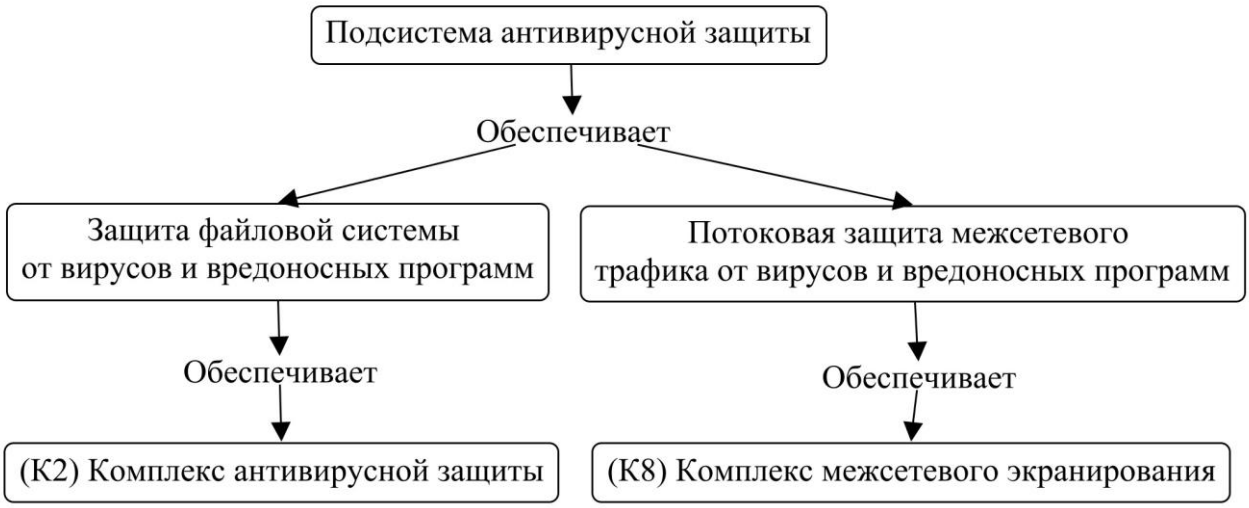

Рис. 6. Онтология подсистемы антивирусной защиты

На рис. 7 показана *подсистема контроля использования информационных ресурсов*. Несмотря на внешнюю простоту, она выполняет довольно много функций [35-37]:

– обнаружение несанкционированного хранения конфиденциальной информации в информационных ресурсах (файловые серверы, файловые хранилища, АРМ пользователей, БД);
– контроль каналов утечек защищаемой информации;
– аутентификация пользователей и формирования профилей доступа к ресурсам сети Интернет;

– расшифровка SSL (TLS) трафика средствами программного компонента на АРМ, который выполняет определенную задачу или набор задач от имени более крупной системы или приложения, часто распределенным или децентрализованным образом;
– контроль действий по отправке информации, когда программный компонент находится вне ЛВС предприятия;

Рис. 7. Онтология подсистемы контроля использования информационных ресурсов

– перехват и анализ трафика с возможностью блокировки сообщений, отправляемых с использованием корпоративной электронной почты (протокол SMTP). В контексте корпоративной электронной почты (протокол SMTP) это означает мониторинг электронных писем, отправленных и полученных сотрудниками с помощью системы электронной почты компании. Перехват и анализ трафика может включать различные методы, например, использование инструментов сетевого мониторинга, программного обеспечения для перехвата пакетов или специализированных аппаратных устройств. Эти инструменты могут перехватывать и анализировать содержание сообщений электронной почты, включая адреса отправителя и получателя, темы и текст сообщения. Кроме того, благодаря возможности блокировать сообщения, отправленные с помощью корпоративной электронной почты, система может предотвратить попадание определенных сообщений к адресатам. Эта функция обычно используется для предотвращения передачи вредоносного содержимого или конфиденциальной информации за пределы сети компании. В целом, перехват и анализ трафика с возможностью блокировки сообщений, отправляемых с использованием корпоративной электронной почты, может помочь организациям поддерживать безопасность и целостность своих систем электронной почты и предотвратить утечку данных или другие инциденты безопасности;
– перехват и анализ сообщений, отправляемых с использованием веб-сервисов (веб-почта, социальные сети, файловые Интернет-ресурсы, облачные хранилища и т.п.);
– перехват и анализ информации в системах мгновенных сообщений (ICQ, Skype, Jabber, Mail.ru);
– централизованное хранение истории инцидентов, исходных почтовых сообщений и перехваченных данных;

- автоматический разбор сообщения на составляющие на этапе приема сообщения с возможностью анализа сообщения по его атрибутам (заголовки, тело, вложения);
- создание, редактирование и удаление правил фильтрации, анализа и архивирования;
- детектирование заполненных форм – определение заполненных и незаполненных бланков документов с возможностью обнаружения в форме документа (бланке) информации, относящейся к защищаемой федеральным законом «О персональных данных» от 27.07.2006 № 152-ФЗ;
- возможность оперативного оповещения по электронной почте ответственных работников о зафиксированных событиях ИБ;
- перехват документов, отправляемых на печать (сетевые и локальные принтеры) и многое другое.

Следующей подсистемой является *подсистема централизованного управления средствами защиты информации* (СрЗИ), показанная на рис. 8.

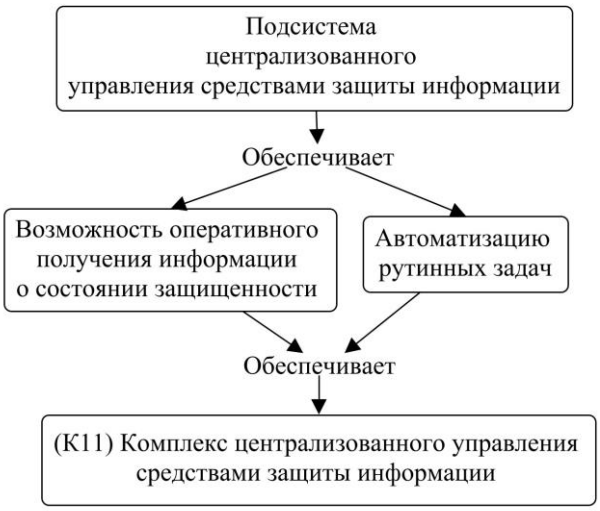

Рис. 8. Онтология подсистемы централизованного управления СрЗИ

С её помощью выполняются функции:

- обеспечение возможности оперативного получения информации о состоянии защищенности ИС и АСУ ТП;
- оперативного реагирования на инциденты ИБ;
- предоставление администраторам инструментов для выполнения функций контроля;
- управления по обеспечению ИБ и автоматизации рутинных задач.

Похожую топологию имеет онтология *подсистемы анализа защищённости* на рис. 9.

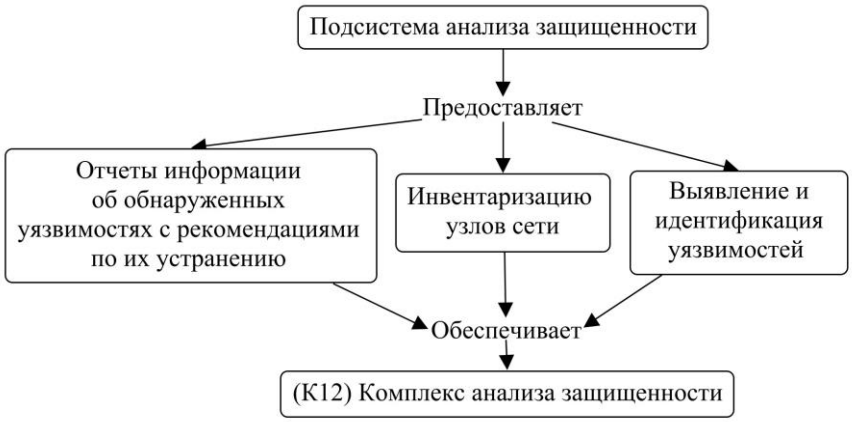

Рис. 9. Онтология подсистемы анализа защищённости

В рамках этой подсистемы (рис. 9) решаются задачи:

- обнаружение и учет защищаемых ресурсов;
- анализ защищенности компонентов ЛВС предприятия (ОС серверов ИС, АСУ ТП и СрЗИ, АСО, сетевые сервисы серверов ИС, АСУ ТП и СрЗИ, ППО);
- анализ защищенности информационных систем предприятия;
- сканирование узла ЛВС и принятие решений о соответствии или несоответствии узлов ИС и информационных систем в целом принятым на предприятии технических стандартов;
- регулярное централизованное обновление компонентов подсистемы;
- централизованное управление компонентами подсистемы и доступом пользователей к функциям подсистемы;
- генерация отчетов о результатах сканирования, а также доставка отчетов уполномоченным сотрудникам предприятия.

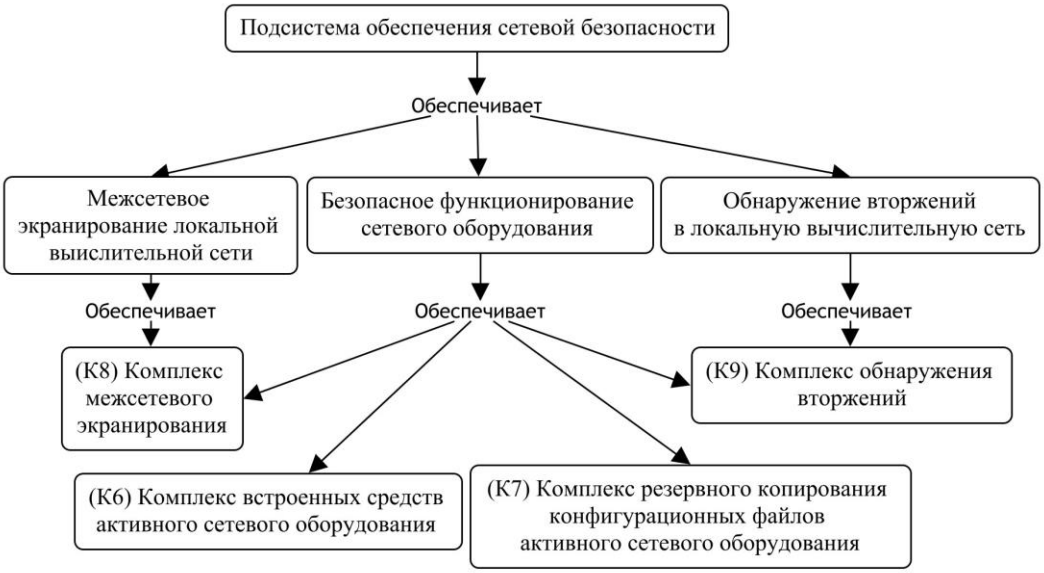

Рис. 10. Онтология подсистемы обеспечения сетевой безопасности

Последними двумя подсистемами комплекса ПТР являются *подсистема обеспечения сетевой безопасности* (рис. 10) и *подсистема обеспечения непрерывности функционирования* (рис. 11).

Первая (рис. 10) выполняет следующие функции:

- межсетевое экранирование и сегментирование ЛВС предприятия;
- обнаружение вторжений;
- централизованное управление подсистемой;
- интеграция с периметральной системой защиты информации предприятия.

Вторая (рис. 11) решает задачи:

- резервного копирования конфигурационных файлов СрЗИ и АСО и восстановления данных из резервных копий в случаях сбоев;
- хранения резервных копий;
- восстановления данных из резервных копий;
- реализации отказоустойчивой конфигурации межсетевого экрана (МЭ) и АСО.

Данная структура может быть положена в основу логико-аксиологического оценивания.

Рис. 11. Онтология подсистемы обеспечения непрерывности функционирования

2. Логико-аксиологическая оценка КСЗИ предприятия. Представленные онтологии позволяют оценить эффективность функционирования КСЗИ предприятия в разрезе комплекса ПТР. Поскольку состояние комплекса фактически определяется состояниями компонентов *K1-K15*, оценка должна выглядеть как агрегированный результат состояний этих элементов.

Известны множество подходов к агрегированию. Большинство так или иначе сводятся к некоторой функции характеризующих чисел $U(\chi_1,\ldots,\chi_n)$, где каждое характеризующее число (частный показатель) отражает состояние соответствующего компонента системы. Здесь полагаем, что $\forall i(\chi_i\in[0,1])$, где ноль означает полную неработоспособность (нефункциональность) компонента, а единица – что система полностью соответствует своему функциональному назначению. Значения из (0,1) отражают промежуточные степени такого соответствия. Для сложных иерархических систем, какой является рассматриваемая, компоненты – это функциональные элементы и образуемые ими подсистемы. Функциональными элементами здесь являются *K1-K15,* далее не углубляемся.

На практике характеризующие числа (частные показатели) $\chi_i=\chi(K_i)$ обычно задаются «аудиторами» – лицами, принимающими решения о состоянии функциональных (базовых) элементов системы. На их основе строится агрегированный показатель (агрегат), учитывающий значимость каждого компонента в системе.

Помимо значимости функциональных элементов, следует говорить и о значимости подсистем, из них образованных. Показатели значимости задаются экспертно, исходя из представлений о роли и месте того или иного компонента в общей функциональности системы.

Как следует из рис. 1-11, итоговый агрегат строится иерархически, согласно иерархии системы, причём некоторые компоненты входят более чем в одну подсистему, что также следует учитывать.

Чаще всего при агрегировании пользуются аддитивными функциями наподобие среднего арифметического взвешенного, где вес каждого слагаемого отражает значимость компонента. Однако аддитивность не позволяет учесть действительную роль компонентов в системе. Отказ или отсутствие некоторых из них может драматически снижать общую функциональность системы вплоть до её полного «обнуления». Среднее арифметическое не моделирует эту ситуацию в принципе. Другая популярная функция агрегирования – среднее геометрическое (среднее геометрическое взвешенное). Здесь, наоборот, нефункциональность каж-

дого компонента означает нефункциональность системы в целом, что также редко отвечает действительности. Примеры можно посмотреть в [33, 38, 39].

Для такого рода случаев в [40] был предложен логико-аксиологический подход к оцениванию, позволяющий более тонко учитывать роль и значимость компонентов. Он опирается на понятие ценности компонента-потомка (субкомпонента) для компонента-родителя (надкомпонента). Под ценностью понимается мера убыли функциональности надкомпонента при утрате его потомка. Ценность здесь играет роль «значимости». Количественно её можно рассматривать как величину уменьшения характеризующего числа надкомпонента при обнулении характеризующего числа потомка [29, 40]. Ценности могут задаваться экспертно.

Понятно, что такая модель не отражает всех особенностей системы, однако «физически» она может быть более адекватной, чем вышеозначенные способы. В известном смысле её можно рассматривать как промежуточную между грубой качественной моделью и точным описанием системы традиционными уравнениями.

Логико-аксиологическая модель строится как множество нечётких продукций вида:

$$\neg a_i \to \neg b\,, \tag{1}$$

где $\neg a_i$ – утверждение об утрате компонента-потомка, $\neg b$ – о результирующей нефункциональности компонента-родителя. Истинность продукции: $\|\neg a_i \to \neg b\|$ отражает степень снижения функциональности родителя при утрате потомка с точки зрения эксперта, то есть, роль и место *i*-го субкомпонента в этом фрагменте иерархии. Если $\|\neg a_i \to \neg b\| = 1$, утрата субкомпонента i влечёт утрату родительского компонента (*i*-й компонент ключевой). Если $\|\neg a_i \to \neg b\| = 0$, утрата потомка на надкомпонент не влияет (это возможно, к примеру, при холодном резервировании). Очевидно, что такая модель естественным образом реализуется с использованием технологии экспертных систем.

Расчёт агрегата для надкомпонента выполняется как набор элементов вывода:

$$\neg a_1, \neg a_1 \to \neg b \;\vdash\; \neg b : \|\neg b\|_1 = \|\neg a_1\| \bullet \|\neg a_1 \to \neg b\|;$$
$$\dots$$
$$\neg a_n, \neg a_n \to \neg b \;\vdash\; \neg b : \|\neg b\|_n = \|\neg a_n\| \bullet \|\neg a_n \to \neg b\|.$$

Через двоеточие указана схема расчёта истинности заключения на основе истинностей посылок. Символ $\bullet$ – треугольная (триангулированная) норма в инфиксной записи. Истинность $\|\neg a_i\|$ отражает степень снижения функциональности *i*-го субкомпонента. Если $\|\neg a_i\| = 0$ – субкомпонент «исправен», если $\|\neg a_i\| = 1$ – полностью неработоспособен или отсутствует.

Агрегирование на этом этапе выполняется как объединение свидетельств:

$$\|\neg b\| = \|\neg b\|_1 \oplus \dots \oplus \|\neg b\|_n,$$

где $\oplus$ – треугольная ко-норма в инфиксной записи. Именно при таком объединении не функционирующий ключевой субкомпонент обеспечивает нефункциональность надкомпонента, в который он входит. Объединяя эти шаги, схему вывода можно представить, как:

$$\begin{gathered}\neg a_1, \neg a_1 \to \neg b \;\vdash\; \neg b : \|\neg b\|_1 = \|\neg a_1\| \bullet \|\neg a_1 \to \neg b\|;\\ \dots\\ \neg a_n, \neg a_n \to \neg b \;\vdash\; \neg b : \|\neg b\|_n = \|\neg a_n\| \bullet \|\neg a_n \to \neg b\|;\\ \hline \neg b : \|\neg b\| = \|\neg b\|_1 \oplus \dots \oplus \|\neg b\|_n\,.\end{gathered} \tag{2}$$

Результат каждого агрегирования следует нормировать на величину $\| \neg b \|_{\max} = \| \neg a_1 \to \neg b \| \oplus ... \oplus \| \neg a_n \to \neg b \|$: отказ всех субкомпонентов приводит к отказу надкомпонента в целом.

Истинность утверждения b о функциональности надкомпонента вычисляем традиционным образом:

$$\| b \| = 1 - \| \neg b \|.$$

Вывод стартует от функциональных элементов – комплексов *K1-K15*. Значения истинности утверждений об их соответствии функциональному назначению (характеризующие числа компонентов) выставляются аудиторами.

Характеризующие числа надкомпонентов (истинности утверждений об их соответствии функциональному назначению) рассчитываются согласно (2). Эти надкомпоненты становятся субкомпонентами уже для своих надкомпонентов и участвуют в выводе на следующем уровне иерархии, и так далее, до характеризующего числа системы в целом – истинности утверждения о её соответствии целевому назначению.

Необходимо заметить, что описанный подход к оцениванию естественным образом ложится на технологию экспертных систем. Продукции вида (1) составляют базу знаний, а процедура (2) реализуется с помощью машины вывода. Это позволяет менять алгоритм расчёта без программирования, редактируя только базу знаний. Учитывая, что КСЗИ – динамическая система, которая может дополняться и изменяться, это позволяет гибко перестраивать расчёт при появлении или удалении тех или иных компонентов.

3. Пример расчёта. Приведём пример расчёта. За основу возьмём подсистему обеспечения сетевой безопасности (ПОСБ) (рис. 10). Она состоит из трёх подсистем: «Межсетевое экранирование ЛВС» (МСЭ); «Безопасное функционирование сетевого оборудования» (БФСО); «Обнаружение вторжений в ЛВС» (ОВ). С ними связаны продукции:

¬(*МСЭ отвечает своему функциональному назначению*)→ ¬(*ПОСБ отвечает своему функциональному назначению*);

¬(*БФСО отвечает своему функциональному назначению*)→ ¬(*ПОСБ отвечает своему функциональному назначению*);

¬(*ОВ отвечает своему функциональному назначению*)→ ¬(*ПОСБ отвечает своему функциональному назначению*).

С подсистемами второго уровня связаны продукции:

¬(*К8 отвечает своему функциональному назначению*)→ ¬(*МСЭ отвечает своему функциональному назначению*);

¬(*К8 отвечает своему функциональному назначению*)→ ¬(*БФСО отвечает своему функциональному назначению*);

¬(*К6 отвечает своему функциональному назначению*)→ ¬(*БФСО отвечает своему функциональному назначению*);

¬(*К7 отвечает своему функциональному назначению*)→ ¬(*БФСО отвечает своему функциональному назначению*);

¬(*К9 отвечает своему функциональному назначению*)→ ¬(*БФСО отвечает своему функциональному назначению*);

¬(*К9 отвечает своему функциональному назначению*)→ ¬(*ОВ отвечает своему функциональному назначению*).

Зададим истинности продукций (истинности задаются экспертами, здесь они условны):

||¬*МСЭ*→ ¬*ПОСБ*|| = 0.5;

||¬*БФСО*→ ¬*ПОСБ*|| = 0.6;

$$||\neg ОВ \rightarrow \neg ПОСБ|| = 0.7.$$
$$||\neg К8 \rightarrow \neg МСЭ|| = 1.0;$$
$$||\neg К8 \rightarrow \neg БФСО|| = 0.5;$$
$$||\neg К6 \rightarrow \neg БФСО|| = 0.6;$$
$$||\neg К7 \rightarrow \neg БФСО|| = 0.7;$$
$$||\neg К9 \rightarrow \neg БФСО|| = 0.8;$$
$$||\neg К9 \rightarrow \neg ОВ|| = 1.0.$$

Единичные значения связаны с тем, что соответствующий функциональный элемент единственный, а значит, его утрата повлечёт утрату соответствующей подсистемы. Остальные значения произвольны.

Пусть, далее, аудиторы выставили оценки функциональным элементам: $||К6|| = 0.6$, $||К7|| = 0.7$, $||К8|| = 0.8$, $||К9|| = 0.9$. Соответственно, для подсистемы *МСЭ* согласно (1) получаем:

$$\neg К8, \neg К8 \rightarrow \neg МСЭ \vdash \neg МСЭ: ||\neg МСЭ|| = ||\neg К8|| \bullet ||\neg К8 \rightarrow \neg МСЭ|| = 0.2.$$

Нормирование даёт ту же величину $||\neg МСЭ|| = 0.2$.

Субкомпонент у *МСЭ* единственный, агрегировать нечего. Здесь и далее для простоты в качестве *t* и *s*-норм взяты функции, соответственно, $x \bullet y = \min(x,y)$, $x \oplus y = \max(x,y)$.

Аналогично для ОВ:

$$\neg К9, \neg К9 \rightarrow \neg ОВ \vdash \neg ОВ: ||\neg ОВ|| = ||\neg К9|| \bullet ||\neg К9 \rightarrow \neg ОВ|| = 0.1.$$

Для *БФСО* агрегирование необходимо:

$$\neg К8, \neg К8 \rightarrow \neg БФСО \vdash \neg БФСО: ||\neg БФСО||_1 = ||\neg К8|| \bullet ||\neg К8 \rightarrow \neg БФСО|| = 0.2;$$
$$\neg К6, \neg К6 \rightarrow \neg БФСО \vdash \neg БФСО: ||\neg БФСО||_2 = ||\neg К6|| \bullet ||\neg К6 \rightarrow \neg БФСО|| = 0.4;$$
$$\neg К7, \neg К7 \rightarrow \neg БФСО \vdash \neg БФСО: ||\neg БФСО||_3 = ||\neg К7|| \bullet ||\neg К7 \rightarrow \neg БФСО|| = 0.3;$$
$$\underline{\neg К9, \neg К9 \rightarrow \neg БФСО \vdash \neg БФСО: ||\neg БФСО||_4 = ||\neg К9|| \bullet ||\neg К9 \rightarrow \neg БФСО|| = 0.1;}$$
$$||\neg БФСО|| = \max(0.2, 0.4, 0.3, 0.1) = 0.4.$$

Нормирование даёт $||\neg БФСО|| = 0.4/\max(0.5, 0.6, 0.7, 0.8) = 0.5$.

Наконец, для *ПОСБ* получаем:

$$\neg МСЭ, \neg МСЭ \rightarrow \neg ПОСБ \vdash \neg ПОСБ: ||\neg ПОСБ||_1 = ||\neg МСЭ|| \bullet ||\neg МСЭ \rightarrow \neg ПОСБ|| = 0.2;$$
$$\neg БФСО, \neg МСЭ \rightarrow \neg ПОСБ \vdash \neg ПОСБ: ||\neg ПОСБ||_2 = ||\neg БФСО|| \bullet ||\neg БФСО \rightarrow \neg ПОСБ|| = 0.5;$$
$$\underline{\neg ОВ, \neg МСЭ \rightarrow \neg ПОСБ \vdash \neg ПОСБ: ||\neg ПОСБ||_3 = ||\neg ОВ|| \bullet ||\neg ОВ \rightarrow \neg ПОСБ|| = 0.1;}$$
$$||\neg ПОСБ|| = \max(0.2, 0.5, 0.1) = 0.5$$

Или, после нормирования, $||\neg ПОСБ|| = 0.5/\max(0.5, 0.6, 0.7) \cong 0.7$.

Отсюда уже можно получить меру функциональности *ПОСБ* как $||ПОСБ|| = 1 - ||\neg ПОСБ||$, однако в силу нелинейности законов агрегирования (в общем случае) в расчёт вводится процедура калибровки функции агрегирования, обеспечивающая равномерное (линейное) изменение величины агрегата при равномерном же и одинаковом изменении характеризующих чисел функциональных элементов [41]. Окончательно получаем: $||ПОСБ|| = 0.74$, или 74 балла из 100.

Расчёт проведён с помощью программной системы «лАос 2.Х» [42].

Это и будет агрегированная оценка функциональности подсистемы обеспечения сетевой безопасности по введённым данным.

Для подсистемы ПТР (рис. 2) выполняется агрегирование по её подсистемам, куда входит и ПОСБ. Для КСЗИ в целом – такая же процедура агрегирования по всему комплексу соответствующих подсистем.

Заключение. Подытоживая, можно сделать следующие выводы.

1. Для определения степени соответствия системы своему функциональному назначению (с последующими управленческими решениями) могут использоваться агрегированные оценки, зависящие от состояния компонентов системы, в первую очередь – её функциональных элементов. Такой подход можно назвать агрегатным моделированием.

2. Агрегатное моделирование помогает получить числовые оценки функциональности системы в условиях, когда трудно или невозможно составить для неё полноценную математическую модель, описывающую её поведение.

3. Агрегатные модели могут быть разными. Наиболее популярными сегодня является агрегирование на основе взвешенного среднего, реже – среднего геометрического или гармонического. Однако такие модели неспособны полноценно отразить значимость каждого компонента системы для её функционирования, в частности, наличие отдельных ключевых компонентов, нефункциональность которых ведёт к нефункциональности системы в целом, а также компонентов, близких к таковым.

4. Одним из подходов, лишённых этого недостатка, является логико-аксиологический подход, естественным образом ложащийся на технологию экспертных систем и нечёткого вывода. Это позволяет, в частности, перенастраивать расчёт агрегата без программирования, путём простого редактирования базы знаний.

5. Первым шагом к использованию метода является онтологическое моделирование, описывающее компоненты системы и их структурные взаимосвязи. На втором шаге онтологическая модель превращается в продукционную базу знаний с нечёткими продукциями вида $\neg a_i \to \neg b$. Истинность продукции со значениями из интервала [0,1] показывает степень значимости компонента a_i для компонента b. Чем выше это значение, тем сильнее падает функциональность b при утрате a_i (выше ценность a_i для b). Ценность – это мера необходимости a_i для b.

6. Итоговый агрегат получается в ходе присоединённого логического вывода с дополнительными этапами нормировки и калибровки результатов, что продемонстрировано для подсистемы обеспечения сетевой безопасности КСЗИ предприятия.

7. Метод можно применить для КСЗИ в целом. Ценности в нём задаются экспертно или по иным соображениям. Итоговый агрегат получается путём аудиторского оценивания состояния функциональных элементов с последующим расчётом агрегата по описанной схеме. При этом для корректного сравнения различных КСЗИ ценности должны задаваться единообразно. Выбор функции агрегирования позволяет более тонко отразить особенности совместной работы компонентов. В примере представлен пессимативный подход, когда суммарная функциональность субкомпонентов определяется наихудшим из них.

Список источников

1. Цитаты Джона Уэлча. – URL: https://citaty.su/citaty-dzhona-uelcha.
2. Miloslavskaya N. Security intelligence centers for big data processing. 5th International conference on future internet of things and cloud Workshops (FiCloudW), Prague, Czech Republic, 2017, p. 7, 13, DOI:10.1109/FiCloudW.2017.68.
3. Miloslavskaya N. Security operations centers for information security incident management. Proceedings of the 4th international conference Future internet of things and cloud (FiCloud 2016). Vienna (Austria), 2016, p. 131-138, DOI: 10.1109/FiCloud.2016.26.
4. Melnikov D., Petrov V., Miloslavskaya N., Durakovskiy A., Kondratieva T. Cybertrust in E-learning environment based on network time synchronization. Proceedings of the 8th international conference on Computer supported education (CSEDU 2016), Rome (Italy), p. 402-407, DOI: 10.5220/0005874904020407.
5. Durakovskiy A.P., Melnikov D.A., Gorbatov V.S., Ivanenko V.G., Modestov A.A. Russian model of public keys and validation infrastructure as base of the cloud trust. Proceedings - 2016 IEEE 4th International conference on Future Internet of Things and Cloud, FiCloud 2016, p. 123-130, DOI: 10.1109/FiCloud.2016.25.

6. Кулик С.Д. Специальные средства для обеспечения информационной безопасности / С.Д. Кулик // Безопасность информационных технологий, 2015. – [S.l]. – Т. 22. – №. 2. – ISSN 2074-7136. – URL: https://bit.mephi.ru/ index.php /bit/article/view/114 (дата обращения: 20.02.2023).
7. Кулик С.Д. Обеспечение информационной безопасности и фактографические системы / С.Д. Кулик// Безопасность информационных технологий, 2015. – [S.l.]. – Т. 22. – №. 1. – ISSN 2074-7136. – URL: https://bit.mephi.ru/ index.php/bit/article/view/199 (дата обращения: 20.02.2023).
8. Зегжда П.Д. Применение рядов смежности для распознавания предфрактальных графов при оценке кибербезопасности VANET-сетей / П.Д. Зегжда, Д.В. Иванов, Д.А. Москвин, А.А. Иванов // Проблемы информационной безопасности. Компьютерные системы, 2018. – № 1. – С. 10-26.
9. Зегжда Д.П. Обеспечение киберустойчивости программно-конфигурируемых сетей на основе ситуационного управления / Д.П. Зегжда, Е.Ю. Павленко // Проблемы информационной безопасности. Компьютерные системы, 2018. – № 1. – С. 160-168.
10. Волкова В.Н. Системный анализ информационных комплексов / В.Н. Волкова. – СПб.: Лань, 2016. – С. 336.
11. Воронов М.В. Введение с системный анализ / М.В. Воронов. – Тирасполь: Полиграфист, 2011. – С. 224.
12. Артюхин Г.А. Теория систем и системный анализ. Практикум принятия решений / Г.А. Артюхин. – Казань: КГАСУ, 2016. – С. 165.
13. Ермак В.Д. Системы. Системные принципы. Системный подход / В.Д. Ермак // Соционика, 1997. – № 2. – URL: http://socionicasys.org/biblioteka/statji/sistemnij-podhod. (дата обращения: 20.02.2023).
14. Кулик С.Д. Последовательный анализ и нейронные сети в фактографических информационных системах / С.Д. Кулик //Нейрокомпьютеры: разработка, применение, 2018. – № 9. – С. 53-60.
15. Соколов А.В. Информационно-поисковые системы / / А.В Соколов. – М.: Радио и связь, 1981. – С. 152.
16. Кулик С.Д. Нейросетевые алгоритмы и автоматизированные фактографические информационные системы / С.Д. Кулик //Нейрокомпьютеры: разработка, применение, 2015. – № 12. – С. 58-65.
17. Безсонов Н.В. Методическое пособие для расчета экономического эффекта от использования изобретений и рационализаторских предложений (инструктивно-методические). – М.: ВНИИПИ, 1985. – 104 с.
18. Кулик С.Д. Исследование эффективности фактографического поиска в информационных системах / С.Д. Кулик. – Изд. Радиотехника, 2004. – №1326-В2004. – Библ. Указат. №9(391). – 251 с.
19. ISO/IEC TR 27016 Information technology - Security techniques - Information security management - Organizational economics (ISO/IEC TR 27016:2014).
20. Мирсанова О.А. К вопросу об оценке эффективности затрат на информационную безопасность / О.А. Мирсанова. – URL:https://www.academia.edu/18137465/ (дата обращения: 20.02.2023).
21. Лычкина Н.Н. Имитационное моделирование экономических процессов. Учебное пособие для слушателей программы eMBI / Н.Н. Лычкина. – М.: Академия АйТи, 2005. – 164 с.
22. Эленберг М.С. Имитационное моделирование: учеб пособие / М.С. Эленберг, Н.С. Цыганков. – Красноярск: Сиб. федер. ун-т, 2017. – 128 с.
23. Борщёв А. Практическое агентное моделирование и его место в арсенале аналитика / А. Борщёв // Exponenta PRO, 2004. #3-4(7-8). – С. 38-47.
24. Каталевский Д.Ю. Системная динамика и агентное моделирование: необходимость комбинированного подхода. – URL: https://www.anylogic.ru/upload/iblock/740/ 7408de9e68d2dd7a8f40eac1899f9cf4.pdf.
25. Улыбин А.В. Мультиагентный подход в имитационном моделировании / А.В. Улыбин, А.А. Арзамасцев // Вестник ТГУ, 2010. –Т. 15. –Вып.5. – С. 1470-1471.
26. Массель Л.В. Применение онтологического, когнитивного и событийного моделирования для анализа развития и последствий чрезвычайных ситуаций в энергетике / Л.В. Массель // Проблемы безопасности и чрезвычайных ситуаций, 2010. – №2. – С. 34-43.
27. Смирнов С.В. Онтологии как смысловые модели / С.В. Смирнов // Онтология проектирования, 2013. – № 2. – С.12-19.
28. Боярский К.К. Концептуальные модели в базах знаний // К.К. Боярский, Е.А. Каневский, Г.В. Лезин. – URL: https://cyberleninka.ru/article/n/kontseptualnye-modeli-v-bazah-znaniy/viewer.
29. Аршинский Л.В. Необходимость и достаточность при агрегировании на основе неубывающих функций / Л.В. Аршинский, В.Л. Аршинский // Онтология проектирования, 2022. – Т. 12. – №1. – С.93-105. DOI: 10.18287/2223-9537-2022-12-1-93-105.
30. Дорофеев Р.С. Совместное использование методологий квалиметрической экспертизы и онтологии для оценки качества технологий изготовления изделий / Р.С. Дорофеев, С.С. Сосинская // Информационные и математические технологии в науке и управлении: Сб. трудов XVI Байкальской всерос. конференции. Ч. 2. – Иркутск: ИСЭМ СО РАН, 2010. – С. 138-145.

31. Дорофеев Р.С. Методология и программная реализация совместного использования онтологии и квалиметрической экспертизы при оценке качества станков / Р.С. Дорофеев // Вестник ИрГТУ, 2013. – №3. – С. 16-23.
32. Сосинская, С.С. Разработка системы для расчёта рейтинга преподавателей на основе квалиметрического подхода и онтологии / С.С. Сосинская, Р.С. Дорофеев, А.С. Дорофеев // Онтология проектирования. – 2019. – Т.9. – №2(32). – С.214-224. – DOI: 10.18287/2223-9537-2019-9- 2-214-224.
33. Азгальдов Г.Г. Теория и практика оценки качества товаров (основы квалиметрии) / Г.Г. Азгальдов. – М.: Экономика, 1982. – 256 с.
34. Абрамова Н.А. О некоторых мифах в оценке качества программного обеспечения / Н.А. Абрамова // Надежность, 2004. – №1.– С.38-63.
35. Глухов Н.И. Разработка элементов комплексной системы защиты информации предприятия / Н.И. Глухов, П.Н. Наседкин // Информационные технологии и математическое моделирование в управлении сложными системами, 2021. – № 1 (9). – С. 35-42.
36. Наседкин, П.Н. Применение нечёткого присоединённого логического вывода в оценке эффективности функционирования комплексной системы защиты информации предприятий / П.Н. Наседкин, Л.В. Аршинский, Н.И. Глухов // Теоретические и прикладные вопросы реализации проектов в области информационной безопасности: Материалы межвузовской научно-теоретической конференции (в рамках Сибирского форума «Информационная безопасность – 2021»). – Новосибирск: Сибирский государственный университет телекоммуникаций и информатики, 2021. – С. 42-52.
37. Наседкин П.Н. Анализ востребованности компонентов уровня программно-технических решений КСЗИ предприятия с точки зрения обеспечения базовых требований по информационной безопасности / П.Н. Наседкин // Информационные технологии и математическое моделирование в управлении сложными системами, 2022. – № 2(14). – С. 50-64. – DOI 10.26731/2658-3704.2022.2(14).50-64.
38. ГОСТ 28195-89. Оценка качества программных средств. Общие положения / Межгосударственный стандарт. – М: ИПК Издательство стандартов, 2001. – 30 с.
39. ГОСТ 15467-79. Управление качеством продукции. Основные понятия термины и определения / Межгосударственный стандарт. – М: ИПК Издательство стандартов, 2002. – 22 с.
40. Аршинский Л.В. Логико-аксиологический подход к оценке состояния систем / Л.В. Аршинский // Современные технологии. Системный анализ. Моделирование, 2013. – № 3(39). – С. 140-146.
41. Аршинский Л.В. Методика экспертного оценивания качества функционирования производственно-экономических систем на основе знаниевых технологий / Л.В. Аршинский, В.Л. Аршинский, Х. Доржсурэн // Вестник Иркутского государственного технического университета, 2018. – Том 22. –№ 3. – С. 63-78.
42. Аршинский Л.В. Свидетельство об официальной регистрации программы для ЭВМ «лАос 2.Х». Зарегистрировано в Реестре программ для ЭВМ 02 ноября 2016 г. Свидетельство № 2016662218.

Наседкин Павел Николаевич. *Старший преподаватель, аспирант кафедры «Информационные системы и защита информации» Иркутского государственного университета путей сообщения, Author ID: 1066448; SPIN: 8365-9541, nasedkin_pn@irgups.ru, Россия, Иркутск, Чернышевского, 15.*

Аршинский Леонид Вадимович. *Д.т.н., доцент, профессор кафедры «Информационные системы и защита информации» Иркутского государственного университета путей сообщения, Author ID: 520252; SPIN: 9286-4084; ORCID: 0000-0001-5135-7921, larsh@mail.ru, Россия, Иркутск, Чернышевского, 15.*

UDC 004.056.5+004.89
DOI: 10.38028/ESI.2023.29.1.014

Assessment of the state of an integrated information security system based on ontologies

Pavel N. Nasedkin, Leonid V. Arshinskiy
Irkutsk State Transport University, Russia, Irkutsk, *nasedkin_pn@irgups.ru*

Abstract. One of the problems of organizing an information security system is to evaluate the functionality of the system as a whole. Approaches based on aggregated estimation can be used to solve such problems. Currently, such estimates are usually based on weighted averages, which does not allow modeling the concept of a key component of the system, that is, one whose loss leads to the non-functionality of the system as a whole or its individual subsystems. The paper shows an approach to the aggregated evaluation of the subsystem of software and technical solutions of the enterprise's integrated information security system based on the method of logical-axiological evaluation. A necessary part of such an assessment is the ontological modeling of the system by means of light ontologies reflecting the relationships between the components. Ontologies are constructed and an example of calculation for one of the subsystems is given.

Keywords: information security, integrated information security system, aggregated assessment, logical-axiological approach, attached inference

References

1. Citaty Johna Welcha [Quotes by John Welch]. Available at: https://citaty.su/citaty-dzhona-uelcha/.
2. Miloslavskaya N. Security intelligence centers for big data processing. 5th International conference on future internet of things and cloud Workshops (FiCloudW), Prague, Czech Republic, 2017, p. 7, 13, DOI:10.1109/FiCloudW.2017.68.
3. Miloslavskaya N. Security operations centers for information security incident management. Proceedings of the 4th international conference Future internet of things and cloud (FiCloud 2016). Vienna (Austria), 2016, p. 131-138, DOI: 10.1109/FiCloud.2016.26.
4. Melnikov D., Petrov V., Miloslavskaya N., Durakovskiy A., Kondratieva T. Cybertrust in E-learning environment based on network time synchronization. Proceedings of the 8th international conference on Computer supported education (CSEDU 2016), Rome (Italy), p. 402-407, DOI: 10.5220/0005874904020407.
5. Durakovskiy A.P., Melnikov D.A., Gorbatov V.S., Ivanenko V.G., Modestov A.A. Russian model of public keys and validation infrastructure as base of the cloud trust. Proceedings - 2016 IEEE 4th International conference on Future Internet of Things and Cloud, FiCloud 2016, p. 123-130, DOI: 10.1109/FiCloud.2016.25.
6. Kulik S.D. Spetsial'nyye sredstva dlya obespecheniya informatsionnoy bezopasnosti [Special tools for ensuring information security]. Bezopasnost' informatsionnykh tekhnologiy [Security of information technologies], 2015, [S.l], v. 22, no. 2, ISSN 2074-7136, available at: https://bit.mephi.ru/index.php/bit/article/view/114. (accessed: 02/20/2023).
7. Kulik S.D. Obespecheniye informatsionnoy bezopasnosti i faktograficheskiye sistemy [Ensuring Information Security and Factographic Systems]. Bezopasnost' informatsionnykh tekhnologiy[Security of information technologies], 2015, [S.l], v. 22, no. 1, ISSN 2074-7136, available at: https://bit.mephi.ru/index.php/bit/article/view/199 (accessed: 02/20/2023).
8. Zegzhda P.D., Ivanov D.V., Moskvin D.A., Ivanov A.A. Primeneniye ryadov smezhnosti dlya raspoznavaniya predfraktal'nykh grafov pri otsenke ki-berbezopasnosti VANET-setey [Appliance of contiguity sequences for recognition of self-similar graphs for assessing VANET networks cybersecurity]. Problemy informatsionnoy bezopasnosti. Komp'yuternyye sistemy [Information Security Problems. Computer Systems], 2018, no.1, pp. 10 - 26. (in Russian).
9. Zegzhda D.P., Pavlenko E.Y. Obespecheniye kiberustoychivosti programmno-konfiguriruyemykh setey na osnove situatsi-onnogo upravleniya [Situational management for cyber-sustainability of software-defined networks]. Problemy informatsionnoy bezopasnosti. Komp'yuternyye sistemy [Information Security Problems. Computer Systems], 2018, no.1, pp. 160 - 168. (in Russian).
10. Volkova V.N. Sistemnyy analiz informatsionnykh kompleksov[System analysis of information systems]. SPb., Lan', 2016. P. 336. (in Russian).
11. Voronov M.V. Vvedeniye s sistemnyy analiz [Introduction with system analysis]. Tiraspol, Poligrafist [Polygraphist], 2011, pp. 224. (in Russian).
12. Artyukhin G.A. Teoriya sistem i sistemnyy analiz. Praktikum prinyatiya resheniy [System theory and system analysis. Practical decision making]. Kazan': KGASU, 2016, pp. 165. (in Russian).

13. Ermak V.D. Sistemy. Sistemnyye printsipy. Sistemnyy podkhod [Systems. System principles. System Approach]. Sotsionika [Socionics], 1997, no. 2, URL: http://socionicasys.org/ biblioteka/ statji/sistemnij-podhod. (accessed: 02/20/2023). (in Russian).
14. Kulik S.D. Posledovatel'nyy analiz i neyronnyye seti v faktograficheskikh informatsionnykh sistemakh [Sequential analysis and neural networks in factographic information systems], Neyrokomp'yutery: razrabotka, primeneniye [Neurocomputers: development, application], 2018, no.9, pp.53-60 (in Russian).
15. Sokolov A.V. Informatsionno-poiskovyye sistemy [Information retrieval systems]. M.,Radio i svyaz' [Radio and communication], 1981, pp. 152 (in Russian).
16. Kulik S.D. Neyrosetevyye algoritmy i avtomatizirovannyye faktograficheskiye informatsionnyye sistemy[Neural network algorithms and automated factographic information systems]. Neyrokomp'yutery: razrabotka, primeneniye [Neurocomputers], 2015, no.12, pp. 58 - 65 (in Russian).
17. Bezsonov N.V. Metodicheskoye posobiye dlya rascheta ekonomicheskogo effekta ot ispol'zovaniya izobreteniy i ratsionalizatorskikh predlozheniy (instruktivno-metodicheskiye) [Methodological manual for calculating the economic effect of the use of inventions and rationalization proposals (instructive and methodical)]. M., VNIIPI, 1985, 104 p. (in Russian).
18. Kulik S.D. Issledovaniye effektivnosti faktograficheskogo poiska v informatsionnykh sistemakh [Research of the effectiveness of factographic search in information systems]. Izd. Radiotekhnika Ed. Radiotekhnika [Ed. Radio engineering], 2004, no. 1326-B2004, Bibl. Ukazat. №9 (391), M., VINITI, 251 p. (in Russian).
19. ISO/IEC TR 27016 Information technology - Security techniques - Information security management - Organizational economics (ISO/IEC TR 27016:2014).
20. Mirsanova O.A. K voprosu ob otsenke effektivnosti zatrat na informatsionnuyu bezopasnost' [On the issue of evaluating the effectiveness of information security costs], available at: https://www.academia.edu/18137465/ (accessed: 02/20/2023) (in Russian).
21. Lychkina N.N. Imitacionnoe modelirovanie ekonomicheskih processov. Uchebnoe posobie dlya slushatelej programmy eMBI [Simulation modeling of economic processes. Textbook for students of the eMBI program]. Moscow: Akademiya AjTi [IT Academy], 2005, 164 p.
22. Elenberg M.S., Tsygankov N.S. Imitacionnoe modelirovanie: ucheb posobie [Simulation modeling: textbook]. Krasnoyarsk: Sib. feder. un-t. [Siberian Federal University], 2017, 128 p.
23. Borshchyov A. Prakticheskoe agentnoe modelirovanie i ego mesto v arsenale analitika [Practical agent modeling and its place in the analyst's arsenal]. Exponenta PRO [Exponenta PRO], 2004, #3-4(7-8), pp. 38-47.
24. Katalevskij D.Yu. Sistemnaya dinamika i agentnoe modelirovanie: neobhodimost' kombinirovannogo podhoda [System dynamics and agent modeling: the need for a combined approach], available at: https://www.anylogic.ru/upload/iblock/740/ 7408de9e68d2dd7a8f40eac1899f9cf4.pdf.
25. Ulybin A.V., Arzamascev A.A. Mul'tiagentnyj podhod v imitacionnom modelirovanii [Multi–agent approach in simulation modeling]. Vestnik TGU [Tomsk State University Journal], 2010, vol. 15, issue 5, pp. 1470-1471.
26. Massel' L.V. Primenenie ontologicheskogo, kognitivnogo i sobytijnogo modelirovaniya dlya analiza razvitiya i posledstvij chrezvychajnyh situacij v energetike [Application of ontological, cognitive and event modeling for the analysis of the development and consequences of emergency situations in the energy sector]. Problemy bezopasnosti i chrezvychajnyh situacij [Safety and emergencies problems], 2010, no. 2, pp. 34-43.
27. Smirnov S.V. Ontologii kak smyslovye modeli [Ontologies as semantic models]. Ontologiya proektirovaniya [Ontology of designing], 2013, no. 2, pp.12-19.
28. Boyarskij K.K., Kanevskij E.A., Lezin G.V. Konceptual'nye modeli v bazah znanij [Conceptual models in knowledge bases], available at: https://cyberleninka.ru/article/n/kontseptualnye-modeli-v-bazah-znaniy/viewer
29. Arshinskiy L.V., Arshinsky V.L. Neobhodimost' i dostatochnost' pri agregirovanii na osnove neubyvayushchih funkcij [Necessity and sufficiency in aggregation based on non-decreasing functions]. Ontologiya proektirovaniya [Ontology of designing], 2022, vol. 12, no. 1, pp.93-105, DOI: 10.18287/2223-9537-2022-12-1-93-105.
30. Dorofeev R.S., Sosinskaya S.S. Sovmestnoe ispol'zovanie metodologij kvalimetricheskoj ekspertizy i ontologii dlya ocenki kachestva tekhnologij izgotovleniya izdelij [Joint use of methodologies of qualimetric expertise and ontology to assess the quality of manufacturing technologies]. Informacionnye i matematicheskie tekhnologii v nauke i upravlenii: Sb. trudov XVI Bajkal'skoj vseros. konferencii. Ch. 2 [Information and mathematical technologies in science and management: Proceedings of the XVI Baikal All-Russian Conference. Part 2]. Irkutsk: ISEM SO RAN [Melentiev Energy Systems Institute SB of the RAS], 2010, pp. 138-145.
31. Dorofeev R.S. Metodologiya i programmnaya realizaciya sovmestnogo ispol'zovaniya ontologii i kvalimetricheskoj ekspertizy pri ocenke kachestva stankov [Methodology and software implementation of shared use of ontologies and qualimetric examination when evaluating machine tool quality]. Vestnik Irkutskogo gosudarstvennogo tekhnicheskogo universiteta [Proceedings of Irkutsk State Technical University], 2013, no. 3, pp. 16-23.

32. Sosinskaya S.S., Dorofeev R.S., Dorofeev A.S. Razrabotka sistemy dlya raschyota rejtinga prepodavatelej na osnove kvalimetricheskogo podhoda i ontologii [Developing a system for estimation rating of teachers based on the qualimetric approach and ontology]. Ontologiya proektirovaniya [Ontology of designing], 2019, vol. 9, no. 2(32), pp.214-224, DOI: 10.18287/2223-9537-2019-9- 2-214-224.
33. Azgaldov G.G. Teoriya i praktika ocenki kachestva tovarov (osnovy kvalimetrii) [Theory and practice of assessing the quality of goods (fundation of qualimetry)]. Moscow, Ekonomika [Economy], 1982, 256 p.
34. Abramova N.A. O nekotoryh mifah v ocenke kachestva programmnogo obespecheniya [About some myths in software quality assessment]. Nadezhnost' [Dependability], 2004, no. 1, pp. 38-63
35. Gluhov N.I., Nasedkin P.N. Razrabotka elementov kompleksnoj sistemy zashchity informacii predpriyatiya [Development of elements of a complex information security system of the enterprise]. Informacionnye tekhnologii i matematicheskoe modelirovanie v upravlenii slozhnymi sistemami [Information technologies and mathematical modeling in the management of complex systems], 2021, no 1 (9), pp. 35-42.
36. Nasedkin P.N., Arshinskij L.V., Gluhov N.I. Primenenie nechyotkogo prisoedinyonnogo logicheskogo vyvoda v ocenke effektivnosti funkcionirovaniya kompleksnoj sistemy zashchity informacii predpriyatij [Application of fuzzy attached logical inference in the evaluation of the effectiveness of the integrated information security system of enterprises]. Teoreticheskie i prikladnye voprosy realizacii proektov v oblasti informacionnoj bezopasnosti. Materialy mezhvuzovskoj nauchno-teoreticheskoj konferencii (v ramkah Sibirskogo foruma «Informacionnaya bezopasnost' – 2021») [Theoretical and applied issues of implementation of projects in the field of information security: Materials of the interuniversity scientific and theoretical conference (within the framework of the Siberian Forum "Information Security-2021")], Novosibirsk, Sibirskij gosudarstvennyj universitet telekommunikacij i informatiki [Siberian State University of Telecommunications and Informatics], 2021, pp. 42-52.
37. Nasedkin P. N. Analiz vostrebovannosti komponentov urovnya programmno-tekhnicheskih reshenij KSZI predpriyatiya s tochki zreniya obespecheniya bazovyh trebovanij po informacionnoj bezopasnosti [Analysis of the demand for components of the level of software and technical solutions of the enterprise's KSZI from the point of view of ensuring basic requirements for information security]. Informacionnye tekhnologii i matematicheskoe modelirovanie v upravlenii slozhnymi sistemami [Information technologies and mathematical modeling in the management of complex systems], 2022, no 2(14), pp. 50-64, DOI 10.26731/2658-3704.2022.2(14).50-64.
38. GOST 28195-89. Ocenka kachestva programmnyh sredstv. Obshchie polozheniya. Mezhgosudarstvennyj standart [GOST 28195-89. Evaluation of the quality of software tools. General provisions. Interstate Standard]. Moscow, IPK Izdatelstvo standartov [IPK Publishing House of Standards], 2001, 30 p.
39. GOST 15467-79. Upravlenie kachestvom produkcii. Osnovnye ponyatiya terminy i opredeleniya. Mezhgosudarstvennyj standart [Product quality management. Basic concepts, terms and definitions. Interstate Standard]. Moscow, IPK Izdatelstvo standartov [IPK Publishing House of Standards], 2002, 22 p.
40. Arshinskiy L.V. Logiko-aksiologicheskij podhod k ocenke sostoyaniya sistem [Logic axiological approach to assessment of systems]. Sovremennye tekhnologii. Sistemnyj analiz. Modelirovanie [Modern technologies. System analysis. Modeling], 2013, no. 3(39), pp. 140-146.
41. Arshinsky L.V. Arshinsky V.L., Dorzhsuren H. Metodika ekspertnogo ocenivaniya kachestva funkcionirovaniya proizvodstvenno-ekonomicheskih sistem na osnove znanievyh tekhnologij [Knowledge technology-based method of expert estimation of productive-economic system operation quality]. Vestnik Irkutskogo gosudarstvennogo tekhnicheskogo universiteta [Proceedings of Irkutsk State Technical University], 2018, vol. 22, no. 3, pp. 63-78.
42. Arshinskiy L.V. Svidetelstvo ob oficialnoj registracii programmy dlya EVM «lAos 2.H». Zaregistrirovano v Reestre programm dlya EVM 02 noyabrya 2016 g. Svidetelstvo № 2016662218 [Certificate of official registration of the computer program "lAos 2.X". Registered in the Register of computer programs on November 02, 2016. Certificate no. 2016662218.]

Nasedkin Pavel Nikolaevich. *Senior lecturer, postgraduate student of the Department of Information Systems and Information Security at Irkutsk State Transport University, Author ID: 1066448; SPIN: 8365-9541, nasedkin_pn@irgups.ru.*

Arshinsky Leonid Vadimovich. *Doctor of Technical Sciences, Associate Professor, Professor of the Department Information Systems and Information Security of Irkutsk State Transport University, Author ID: 520252; SPIN: 9286-4084; ORCID: 0000-0001-5135-7921, larsh@mail.ru.*

Статья поступила в редакцию 10.03.2023; одобрена после рецензирования 11.03.2023; принята к публикации 24.03.2023.
The article was submitted 03/10/2023; approved after reviewing 03/11/2023; accepted for publication 03/24/2022.