А.Ж. Абдеиов, А.А. Абдеиова

ИНТЕЛЛЕКТУАЛЬНЫЕ СЕРВИСЫ ПО УПРАВЛЕНИЮ ИНФОРМАЦИЕЙ И СОБЫТИЯМИ БЕЗОПАСНОСТИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ И СЕТЯХ

Учебное пособие

ЭВЕРО
Алматы, 2022

УДК 004.0 (075)
ББК 32.973. 202 я 73
А 13

Рецензенты:
д-р техн. наук, профессор *В.П. Разинкин*
канд. техн. наук, доцент *С.А. Зырянов*

Работа подготовлена на кафедре защиты информации для студентов IV курса АВТФ дневной формы обучения, обучающихся по направлению «Информационная безопасность» и специальности «Информационная безопасность автоматизированных систем»

Абденов А.Ж., А.А. Абденова
А13 Интеллектуальные сервисы по управлению информацией и событиями безопасности в компьютерных системах и сетях: Учебное пособие. – Алматы: Эверо, 2022. – 152 с.

Данноу учебное пособие составлено на основе материалов статей научно-методического характера относительно важных исследований в области информационной безопасности компьютерных инфраструктур. Значимым элементом, выполняющим реорганизации межкомпонентного взаимодействия относительно технологий управления информацией и событиями безопасности (Security Information and Event Managment, SIEM), является репозиторий. При этом репозиторий является существенным узлом в SIEM-системе, влияющим на эффективность подхода к построению, изменению модели данных, к организации хранилища данных, а также к их обработке в режиме почти реального времени. Материал основан на новых результатах в области информационной безопасности.

Для специалистов в области информационной безопасности компьютерных инфраструктур, а также студентов и аспирантов соответствующих специальностей.

УДК 004.0 (075)
ББК 32.973. 202 я 73

ISBN 978-601-327-530-7

ВВЕДЕНИЕ

В настоящее время ведущие страны мира вынуждены уделять особое внимание вопросам обеспечения безопасности информационных инфраструктур, включая критически важные инфраструктуры и объекты, к которым относятся крупные гидротехнические сооружения, сети атомных электростанций, вредные химические производства, транспортные узлы, аэродромы и другие. Интенсивное развитие и внедрение информационных и телекоммуникационных технологий приводит к появлению не только новых средств и способов обработки информаций, но и новых угроз информационной безопасности (НБ), уязвимостей, видов компьютерных атак.

В разделе 1 настоящего учебного пособия, приводятся общие положения по построению и функционированию SIEM-систем (Security Information and Event Management), реализующих технологию управления информацией и событиями безопасности, дается характеристика известных реализаций таких систем, а также обсуждаются особенности проекта MASSIF (Management of Security in formation and events in Service InFrastructure – Управление информацией и событиями безопасности в инфраструктурах услуг), рамочной программы Европейского Союза по созданию перспективных систем управления событиями и информационной безопасностью.

В разделе 2 предложено применение онтологического подхода для построения репозитория и логического вывода в системах управления информацией и событиями. Рассмотрена задача создания онтологических моделей и приведен пример ее решения для онтологии уязвимостей и анализа безопасности программно-аппаратных компонентов. Предложена и оценена архитектура репозитория с гибридным хранилищем (интегрирующее реляционное представление, XML, хранилище триплетов), обеспечивающим манипулирование данными о событиях безопасности через веб-сервисы в интересах функционирования SIEM-компонента моделирования атак и анализа безопасности.

В разделе 3 приводятся общие положения по построению и функционированию интеллектуальных сервисов защиты информации

в компьютерных системах и сетях, касающиеся понятийного аппарата, общей архитектуры системы интеллектуальных сервисов защиты, а также построения ее компонентов, реализующих базовые интеллектуальные сервисы защиты.

В разделе 4 дано систематизированное изложение математических методов и моделей анализа мер безопасностей, изучение который поможет студентам сформулировать практические навыки их разработки и применения к расчету рисков относительно исследуемых информационных систем. Управление рисками базируется на данных, которые должны фиксироваться, накопляться, анализироваться, храниться, обрабатываться для оценивания потенциального ущерба от ошибок пользователей и атак нарушителей на информационные ресурсы (ИР) в информационных систем (ИС) компании, выбора мер для его минимизации, расчета оценок предсказания и фильтрации всех возможных параметров и показателей, связанных с информационной безопасностью (ИБ). В частности, предложены методики, позволяющие получать оценки объективной вероятности в возможности наступления неблагоприятного события (НС), объективной стоимости ущерба от нарушений безопасности ИР в ИС компании, оценки предсказания и фильтрации величины ущерба, соответствующие количественным показателям НС. Все основные расчеты показателей ИБ в ИС проведены с использованием линейной дискретной стохастической стационарной модели в форме ПС и уравнений фильтра Калмана для получения более достоверных значений оценок состояния исследуемого объекта.

В разделе 5 обобщены системно-технические решения по применению онтологического подхода для построения на его основе SIEM-репозитория нового поколения с добавлением узла сервисного маркетингового компонента. Этот узел охватывает вопросы создания SIEM-репозитория с применением SOA-ориентированной гибридной архитектуры для его апробации и тестирования функциональных потребностей компонентов модуля, отвечающего в SIEM-системе за моделирование, анализ безопасности и дополнительные сервисные услуги. Рассмотрен практический опыт использования известных основных инструментов антикризисного управления в условиях сокращения доходов населения и падения спроса на платные дополнительные услуги, предоставляемые отдельными частными

лицами. Описаны известные мероприятия по выходу из кризисной ситуации. Дальнейшие исследования могут быть связаны с расширением предложенных услуг, а также с добавлением различных сервисов, которые обеспечат безопасность данных и метаданных, включая моделирование и анализ безопасности, верификацию политик безопасности и т. п.

В разделе 6 рассмотрены основные задачи, связанные с маркетинговой информацией в повседневной работе, которые позволяют проводить корректировки в бизнес-планах и документах конкретным предприятиям, подразделениям и т. д.

В разделе 7 рассматривается основные понятия, характер и содержание задач защиты в сервисных и критических инфраструктурах, которые целесообразно положить в основу построения системы мониторинга SIEM-системы, а также рассматриваются содержания этих основных понятий.

1. SIEM – СИСТЕМЫ ДЛЯ УПРАВЛЕНИЯ ИНФОРМАЦИЕЙ И СОБЫТИЯМИ БЕЗОПАСНОСТИ

Для успешной реализации мероприятий защиты информационных инфраструктур необходимо решить ряд задач, связанных с созданием системы мониторинга угроз безопасности. Системы мониторинга реализуют *апостериорный* подход к защите информации, главной целью создания которой – снижение внутреннего и внешнего воздействий на инфраструктурные объекты до минимального уровня риска и минимизация возникающего ущерба.

Одним из наиболее перспективных и эффективных направлений в создании систем мониторинга угроз безопасности в настоящее время считаются использованием SIEM–системы, обеспечивающей управление информацией и событиями безопасности. Исследования вопросов построения SIEM–систем для сервисных информационных инфраструктур проводятся в настоящее время в проектах MASSIF рамочных программ Европейского союза. В настоящем учебном пособии представлены основные взгляды на построение SIEM–системы и результатов, полученных специалистами в рамках указанного проекта.

1.1. ПОНЯТИЕ SIEM-СИСТЕМЫ

Учитывая характер и содержание задач защиты в сервисных и критических инфраструктурах, представляется целесообразным положить в основу построения системы мониторинга концепцию SIEM-системы [1]. Рассмотрим подробнее содержание этого понятия.

Основная цель построения и функционирования SIEM-систем – значительно повысить уровень информационной безопасности в информационной инфраструктуре за счет обеспечения возможности, манипулировать информацией о безопасности и осуществлять *проактивное управление* инцидентами и событиями безопасности в режиме близком к реальному времени.

Проактивный означает «действующий до того, как ситуация станет критической». Предполагается, что проактивное управление инцидентами и событиями безопасности основывается на автоматических механизмах, которые используют информацию об

«истории» анализируемых сетевых событий и прогнозе будущих событий, а также на автоматической подстройке параметров мониторинга событий к текущему состоянию защищаемой системы [2].

Для достижения такой цели SIEM-система должна успешно решать следующий комплекс задач:

- сбора, обработки и анализа событий безопасности, поступающих в систему из множества гетерогенных источников;
- обнаружение в режиме реального времени атак и нарушений критериев и политик безопасности;
- оперативная оценка защищенности информационных, телекоммуникационных и других критически важных ресурсов;
- анализ и управление рисками информационной безопасности;
- проведение расследований инцидентов;
- обнаружение расхождения критически важных ресурсов и бизнес-процессов с внутренней политикой безопасности и последующее приведение их в соответствие друг с другом;
- принятие эффективных решений по защите информации;
- формирование отчетных документов.

Для решения указанных задач, записи различных журналов аудита (logs), протоколирующие события SIEM-системы используют в информационной инфраструктуре понятия, называемые «событиями безопасности». Эти события отражают такие действия пользователей и программ, которые могут влиять на безопасность информации. Из общего множества событий безопасности SIEM-система должна находить такие, которые свидетельствуют об атаках или иных подобных воздействиях, причем традиционные методы поиска такой информации достаточно трудоемки.

1.2. АРХИТЕКТУРА SIEM СИСТЕМЫ

Как правило, SIEM-система имеет архитектуру **«агенты»-«хранилище данных»-«сервер приложений»**, которая разворачивается поверх защищаемой информационной инфраструктуры [3]. Агенты выполняют сбор событий безопасности, их первоначальную обработку и фильтрацию. Собранная и отфильтрованная информация

о событиях безопасности поступает в *хранилище данных*, или *репозиторий*, где она хранится во внутреннем формате представления для последующего использования и анализа сервером приложений. *Сервер приложений* реализует основные функции защиты информации. Он анализирует информацию, хранимую в репозитории, и преобразует ее для выработки предупреждений или управленческих решений по защите информации.

Таким образом, в SIEM-системе можно выделить три следующих архитектурных уровня ее построения: *сбор данных*, *управления данными*, *анализ данных* (рис. 1.1).

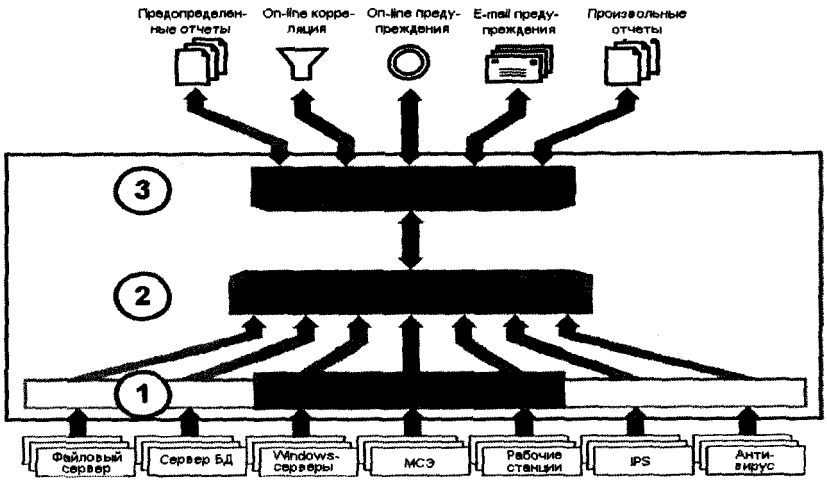

Рис. 1.1. Архитектура типовой SIEM-системы

На первом уровне сбор данных осуществляется от различного типа источников. К числу таковых относятся: файловые серверы, серверы баз данных, Windows-серверы, межсетевые экраны (МСЭ), рабочие станции, системы противодействия атакам (intrusion prevention systems (IPS)), антивирусные программы и т. п.

На втором уровне осуществляется управление данными о событиях безопасности, которые хранятся в репозитории. Данные, хранящиеся в репозитории, выдаются по запросам моделей анализа данных.

Результатами обработки информации в SIEM-системе, получаемыми *на третьем уровне*, являются отчеты в предопределенной и произвольной форме, оперативная (on-line) корреляция данных о событиях, а также предупреждения, вырабатываемые в режиме on-line и / или передаваемые по электронной почте.

1.3. ФУНКЦИОНИРОВАНИЕ SIEM-СИСТЕМЫ

SIEM-система сочетает функции двух других классов подсистем, относящихся к системам мониторинга и управления безопасностью информации: SIM (Security Information Management) и SEM (Security Event Management). Иными словами, SIEM-система реализует функции, одновременно свойственные SIM- и SEM-системам. К функциям SIM-системы относится сбор, хранение и анализ записей журналов, а также формирование необходимой отчетности. К функциям SEM-системы относится мониторинг событий безопасности в реальном времени, а также выявление уязвимости и реагирование на инциденты безопасности.

Указанные выше функции реализуются SIEM-системой на основе выполнения комплекса различных механизмов функционирования. В SIEM-системах первого поколения к их числу относились нормализация, фильтрация, классификация, агрегация, корреляция событий, а также генерация отчетов и предупреждений [3]. В перспективных SIEM-системах (т. е. нового поколения) к их числу следует добавить также анализ событий, инцидентов и их последствий, а также принятие решений и визуализацию информации. Примерное распределение указанных механизмов по уровням иерархии SIEM-системы показано на рис. 1.2.

Раскроем содержание основных механизмов функционирования SIEM-системы.

Нормализация означает приведение форматов записей журналов, собранных из различных источников, к единому внутреннему формату, который затем будет использоваться для их хранения и последующей обработки.

Фильтрация событий безопасности заключается в удалении избыточных событий из поступающих в систему потоков.

Классификация позволяет для атрибутов событий безопасности определить их принадлежность к определенным классам.

Агрегация объединяет события, сходные по определенным признакам.

Корреляция выявляет взаимосвязи между разнородными событиями, что позволяет обнаруживать атаки на инфраструктуры, а также нарушения критериев и политики безопасности.

Анализ событий, инцидентов и их последствий включает моделирование событий, атак и их последствий, анализ уязвимостей и защищенности системы, определение параметров нарушителей, оценку риска, прогнозирование событий и инцидентов.

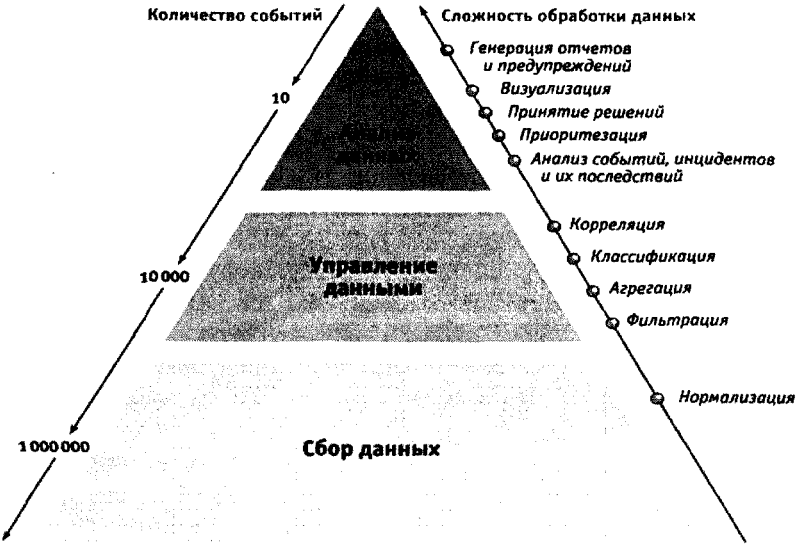

Рис. 1.2. Обобщенная иерархическая модель SIEM-системы

Генерация отчетов и предупреждений означает формирование, передачу, отображение и (или) печать результатов функционирования.

Принятие решений определяет выработку мер по реконфигурированию средств защиты с целью предотвращения атак или восстановления безопасности инфраструктуры.

Визуализация информаций предполагает представление в графическом виде данных, характеризующих результаты анализа событий безопасности и состояние защищаемой инфраструктуры и ее элементов.

Следует отметить, что при переходе к механизмам более высокого уровня количество обрабатываемых событий уменьшается, а сложность их обработки увеличивается.

Взаимосвязь механизмов функционирования SIEM-системы нового поколения показана на рис. 1.3. Как видим, в SIEM-системе выделяются пять основных функциональных подсистем: сбора данных, обработки, хранения, анализа, представления. Причем первые две функционируют в режиме on-line, остальные – в близком к нему.

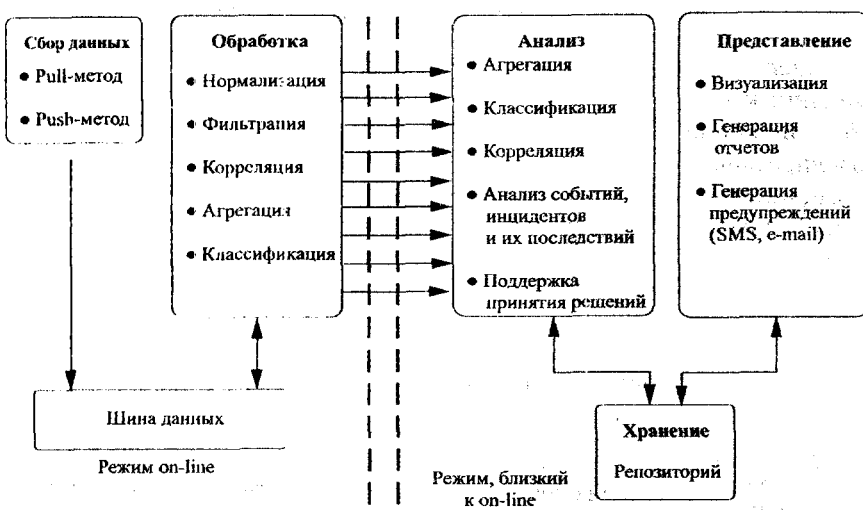

Рис. 1.3. Функциональная модель SIEM-системы

Приведем краткую характеристику этих подсистем:

Подсистема сбора данных. Для получения информации от источников используются два основных метода: Push («толкать») и Pull («тянуть»). Суть метода Push заключается в том, что источник сам

посылает данные записей своих журналов в SIEM-систему. В методе Pull система сама получает данные из журналов.

Подсистема обработки. Обработка информации включает в себя нормализацию, фильтрацию, корреляцию, агрегацию и классификацию.

Подсистема хранения. Отфильтрованные данные в нормализованном виде помещаются для хранения в репозиторий. Репозиторий может быть создан на основе реляционной СУБД (наиболее распространенное решение), XML-ориентированной СУБД и/или хранилища триплетов. *Хранилище триплетов* – это специально созданная база данных, оптимизированная для хранения и поиска триплетов, то есть утверждений вида «субъект–предикат–объект».

Подсистема анализа. Анализ данных включает в себя следующие функции: корреляцию данных, классификацию, агрегацию, и оценку событий, инцидентов и их последствий (в том числе посредством моделирования событий, атак и их последствий, анализа уязвимостей и защищенности системы, определения параметров нарушителей, оценки риска, прогнозирования событий и инцидентов), а также поддержку принятия решений. Анализ данных может основываться на качественных и количественных оценках. Количественная оценка более точная, но требует заметно большего времени, что не всегда допустимо. Чаще всего бывает, что система требует достаточно быстрого качественного анализа, задача которого заключается в распределении факторов риска по группам.

Подсистема представления. Представление включает в себя несколько функций: визуализацию, генерацию отчетов и генерацию предупреждений.

1.4. ОБЗОР СОВРЕМЕННЫХ SIEM-СИСТЕМ

В настоящий момент существует множество коммерческих SIEM-решений, которые имеют возможность собирать и идентифицировать события безопасности, а также выполнять корреляцию событий и инцидентов.

Компания Gartner ежегодно производит оценку разработанных SEIM-систем различных производителей. Согласно отчетам компании Gartner [4] в число лидеров вошли следующие SIEM-системы: ArcSight, RSA (EMC), Q1 Labs, IBM, Symantec, Log Logic и Novell. Приведем их краткую характеристику.

Компания Arc Sight разработала ряд SIEM-систем. Система Arc-SightExpress ориентирована на инфраструктуры среднего размера с предопределенными процедурами мониторинга и отчетности [5]. Система Arc Sight Logger осуществляет сбор данных как в структурированных, так и в неструктурированных форматах [6]. Структурированные данные собираются с помощью интерфейса, поддерживающего более 275 продуктов от 100 производителей. Неструктурированные данные собираются через Syslog или через доступ к log-файлам указанного устройства. Входная информация для данных систем представляется в специально разработанном едином формате CEF (Common Event Format) [7].

Подразделение RSA компании EMC распространяет приложение enVision, обеспечивающее одновременную реализацию функций SIM- и SEM-компонентов [8]. Для небольших инсталляций система включает функции сбора данных о событиях безопасности, управления ими и генерации отчетов. Для более крупных применений система может быть сконфигурирована для выполнения специальных функций сбора данных, манипулирования событиями, выполнения аналитических вычислений и имеет возможность горизонтального масштабирования.

Компания Q1 Labs разработала семейство SIEM-систем Qradar [9], которые обеспечивают управление записями журналов и событиями, отчетность и поведенческий анализ. Отличительной характеристикой SIEM-систем компании Q1 Labs является эффективная реализация функций сбора и обработки потоков сетевых данных о событиях безопасности.

Компания IBM предлагает комплексное решение в области SIEM-систем, которое называется Tivoli Security Information and Event Manager (TSIEM) [10]. TSIEM позволяет, с одной стороны, проводить аудит событий безопасности на соответствие внутренней политики и

различным международным стандартам, а с другой стороны, осуществлять обработку инцидентов, связанных с информационной безопасностью, и обнаруживать атаки и другие угрозы для элементов инфраструктуры.

В области представления и хранения событий TSIEM использует запатентованную методику W7 (Who, did What, When, Where, Where from, Where to and on What), в соответствии с которой все события трансформируются в единый формат, понятный администраторам безспасности, аудиторам и специалистам по управлению. Также TSIEM обладает развитыми возможностями по формированию отчетов и мониторингу активности пользователей.

Компания Symantec разработала систему Security Information Manager, особенностью которой является ее ориентация на конечных пользователей **Symantec** [11].

SIEM-продукты **компании LogLogic** обладают хорошими возможностями мониторинга активности баз данных [12]. Они ориентированы на широкий круг разработчиков, включая Oracle, SQL Server и Sybase. Их недостатком можно считать необходимость изменения интерфейса пользователя при интеграции системы LogLogic с другими приложениями по управлению событиями безопасности.

Компания Novell разработала приложение Novell Sentinel Log Manager [13], которое может собирать и обрабатывать данные от таких источников, как журналы Syslog и Windows, базы данных, протокол SNMP, Novell Audit, SDEE (Security Device Event Exchange), Check Point OPSEC и других.

Приложения основываются на шинной событийной архитектуре, которая обеспечивает достаточно высокую гибкость и масштабируемость для больших разработок и предпочтительна для инфраструктур, использующих другие продукты Novell в области управления доступом и идентификации.

Таким образом, по итогам отчета компании Garter наиболее успешным и прогрессирующим производителем SIEM-систем, считается компания Arc Sight. По сравнению с конкурентами у компании Arc Sight имеется самое большое число внедрений продуктов класса SIEM. В то же время организации, которым нужны

только основные функции управления событиями безопасности, могут использовать более простые и менее дорогие продукты, которые фокусируются на сборе данных и формировании базовой отчетности. При этом следует отметить, что программные продукты с открытым кодом традиционно являются также хорошим решением, не требующим больших затрат на программное обеспечение.

1.5. ЦЕЛИ И ЗАДАЧИ ПРОЕКТА MASSIF

Поскольку ни одна из существующих SIEM-систем не может считаться полностью пригодной для управления безопасностью, а их значимость и предполагаемый эффект от применения в различных инфраструктурах растут, необходимо разработать компоненты SIEM-систем нового поколения, которые будут способны эффективно функционировать в различных гетерогенных инфраструктурах. В настоящее время в рамках программ Европейского Союза, выполняется такой проект, получивший название MASSIF [14].

В проекте участвуют 12 организаций-партнеров: ATOS (Испания), CINI (Италия), EPSILON (Италия), FRANCE TELECOM (Франция), Институт безопасных информационных систем Фраунхофера (Германия), Лиссабонский университет (Португалия), Санкт-Петербургский институт информатики и автоматизации РАН, Лаборатория проблем компьютерной безопасности (Россия), Institut Telecom (Франция), ALIENVAULT (Испания), T-SYSTEMS (ЮАР), Мадридский политехнический университет (Испания), 6CURE (Франция).

Основная цель проекта MASSIF – достижение значимых результатов в области управления информацией и событиями безопасности. На базе многоуровневой корреляции событий безопасности MASSIF должен предоставить инновационные методы для обнаружения возникающих угроз и инициирования действий, направленных на восстановление безопасности до непосредственного возникновения возможных инцидентов.

SIEM-платформа уровня сервисов, разрабатываемая в проекте, затрагивает моделирование и формальную проверку безопасности, включая концепции вычислений, с большей степенью доверия архитектуру надежного и отказоустойчивого сбора событий,

поддерживаемую масштабируемой и производительной обработкой событий в контексте моделей атак.

В документах проекта отмечается, что разрабатываемые решения призваны преодолеть следующие недостатки, присущие современным SIEM-системам:

- ограничения на функции, накладываемые целевой инфраструктурой;
- неспособность согласованно интерпретировать инциденты и события на различных уровнях;
- неспособность обеспечить высокую степень надежности и отказоустойчивости в распределенной среде сбора данных о событиях;
- низкая масштабируемость.

Устранить эти недостатки предполагается за счет формирования рекомендаций в режиме, близком к реальному времени, а также применения проактивного управления инцидентами и событиями. SIEM-система нового поколения ориентируется на инфраструктуру сервисов, в которой обработка событий безопасности отличается интеллектуальностью, высокой масштабируемостью, многоуровневостью и многодоменностью. При этом должно быть реализовано упреждающее управление безопасностью, а также надежный и устойчивый сбор данных о событиях.

Учет современного состояния исследуемой области в проекте MASSIF обеспечивается:

- участием в проекте компании Alien Vault – разработчика ведущего SIEM-продукта OSSIM с открытым исходным кодом;
- интеграцией результатов проекта MASSIF в систему Prelude (являющуюся вторым по популярности SIEM-продуктом с открытым исходным кодом), которая будет выполнена Institut Telecom (Франция);
- развертыванием и использованием ряда коммерческих SIEM-продуктов.

Система OSSIM [15] является комплексным решением по управлению безопасностью, позволяющим обнаруживать и классифицировать компьютерные атаки на основе анализа, оценки рисков и корреляции событий в реальном времени.

Сенсоры, как низкоуровневые компоненты, обеспечивают интерфейс между отдельными устройствами безопасности и сервером управления. Они включают множество агентов сбора данных, а также набор мониторов и детекторов. База данных – SQL-ориентированная, она хранит всю информацию, необходимую для функционирования OSSIM. Сервер управления включает консоль, используемую для контроля над остальными компонентами, и сервер OSSIM, который обрабатывает данные, поступающие от сенсоров.

Система Prelude имеет функциональную структуру, во многом сходную с OSSIM [16]. Она включает в себя следующие основные компоненты: менеджера, коррелятор, базу данных, интерфейсную подсистему и подсистему управления событиями безопасности (Prelude Log Monitoring Lackey, Prelude-LML).

Для обработки данных от источников система Prelude использует формат IDMEF [17]. Менеджер получает события от сенсоров, сохраняет их в постоянной памяти и сопоставляет события с другими менеджерами или корреляторами. Корреляционная логика может расширяться пользователем. Интерфейсная подсистема Prewikka обеспечивает сопряжение с базами данных MySQL, PostgreSQL и SQLite3. Подсистема Prelude-LML позволяет использовать в качестве исходных данных записи журналов от различных устройств.

1.6. ПОСТРОЕНИЕ РЕПОЗИТОРИЯ SIEM-СИСТЕМЫ

Как было отмечено выше, центральным компонентом SIEM-системы является репозиторий, или информационное хранилище, в котором хранятся данные о событиях, правилах и инцидентах безопасности [18]. Поэтому задача построения репозитория – ключевая, особую значимость данная задача приобретает в критической информационной инфраструктуре, где учитываются не только традиционные события безопасности компьютерной инфраструктуры, но и параметры безопасности физического уровня.

Для разработки архитектуры репозитория SIEM-системы был проведен анализ стандартов в области управления событиями, таких как Secutity Content Automation Protocol (SCAP) [19], Common Base Event (CBE) [20] и Common Information Model (CIM) [21]. На их основе, как правило, разрабатываются реляционные модели данных

при создании программного обеспечения в области управления информацией и событями безопасности, а в качестве хранилище используются реляционные СУБД. Однако при использовании реляционной модели существуют различные трудности по выражению всех необходимых отношений между признаками предметной области. Модель получается перегруженной, и выборка данных занимает значительное время. Это обусловлено недостаточной гибкостью и низкой выразительностью языка запросов SQL, используемого в реляционных СУБД. Вторая проблема заключается в необходимости обновлять схему данных в соответствии с требованиями активно меняющейся предметной области. Для реляционных СУБД эта задача влечет за собой серьезные затраты ресурсов на больших объемах данных.

В качестве альтернативного решения по представлению данных в проекте MASSIF предлагается использовать *онтологический подход*. Суть его заключается в том, что вначале выделяется набор концептов (базовых понятий данной предметной области), затем между ними строятся связи, т. е. определяются отношения и взаимодействие базовых понятий. В самом простом случае онтология описывает только иерархию концептов, связанных отношениями категоризации. Концепты и отношения могут формулироваться с использованием дескрипционной логики, где термины словаря являются именами унарных и бинарных предикатов (соответственно концепты и отношения). Таким образом, онтология представляет собой базу знаний, описывающую факты, которые предполагаются всегда истинными в рамках определенного сообщества на основе общепринятого смысла используемого словаря.

Актуальность использования онтологий в SIEM-системах, где необходимо хранить разнородную и быстро изменяющуюся информацию, обусловлена также тем, что изменение модели данных требует значительно меньших усилий, чем в реляционных моделях. При проектировании SIEM-системы необходимо обеспечить наиболее общую и в то же время не перегруженную модель данных, которая будет адаптирована и конкретизирована для каждой области применения в процессе внедрения. Слабое связывание доменных онтологий и модульный подход к разработке значительно облегчают добавление, удаление и поддержку отдельных онтологий.

Кроме того, компоненты онтологий могут быть динамически объединены для удовлетворения требований конкретных приложений.

Еще одной причиной применения онтологического подхода служит тот факт, что используемый в нем математический аппарат позволяет строить более точные запросы и тем самым значительно ускорить время, затрачиваемое аналитическими модулями SIEM-системы на выборку информаций из репозитория.

В рамках решения задачи построения репозитория была разработана онтология для представления модели данных компонента моделирования атак Attack Modeling and Security Evaluation Component (AMSEC). За основу построения этой модели, используемой модулем, взят протокол SCAP.

Для построения репозитория предлагается метод, базирующийся на использовании сервис-ориентированной архитектуры (SOA). Основные принципы SOA, применяемые для построения репозитория: множественное использование сервисов, однородная безопасность, интеграция с процессом программирования, использование открытых стандартов, независимость от местоположения компонентов, высокая управляемость.

В соответствии с принципами SOA архитектура репозитория может быть разделена на три базовых уровня: уровень доступа к данным, уровень презентации данных и уровень реализации сервисов. Уровень доступа к данным интерпретирует запросы на поиск данных от клиентских приложений во внутренний язык, используемый СУБД. Уровень презентации данных охватывает все, что связано с взаимодействием с системой. Уровень реализации сервисов позволяет абстрагировать взаимодействие между двумя и более объектами, потоками и сервисами через промежуточный интерфейс API (англ. *application programming interface*) – набор готовых *классов*, *процедур*, *функций*, *структур* и *констант*, предоставляемых приложением (библиотекой, сервисом) или операционной системой для использования во внешних программных продуктах. Используется программистами при написании всевозможных приложений.

В предлагаемой архитектуре репозитория выделяются два типа баз данных: кратковременного хранения и длительного хранения. В базе данных кратковременного хранения содержится детальная информация обо всех событиях безопасности, поступивших в

репозиторий. В базе данных долговременного хранения содержатся обобщенные данные, а также формализованное представление на внутреннем языке правил инцидентов безопасности, которые используются для получения логического вывода. Вместе взятые, эти базы образуют слой хранения данных репозитория. Другой функциональный слой представляет собой набор различных услуг, которые выполняются по отношению к хранимым данным.

Для выбора программно-инструментальных средств построения репозитория был проведен анализ СУБД следующих классов: традиционного класса реляционных СУБД, XML-ориентированных СУБД (Base X, Apache X Indice и др.) и хранилищ триплетов (4 store, BigData, BigOwlim, TDB иVirtuoso). В результате был сделан выбор в пользу сервера программной системы Virtuoso, которая рационально сочетает в себе возможности всех трех классов СУБД.

Программный макет репозитория, выполненный с использованием Virtuoso, был протестирован для хранения и обработки данных, используемых в модуле анализа и моделирования атак на критически важную информационную инфраструктуру. Результаты тестирования подтвердили правомерность принятых решений по выбору и использованию методов и средств построения репозитория SIEM-системы.

ВЫВОДЫ ПО РАЗДЕЛУ 1

Обеспечение информационной безопасности предполагает применение новых подходов к построению средств и систем защиты информации, которые способны осуществлять проактивный мониторинг событий безопасности, данные о которых могут собираться от различных сенсоров и источников и на основании межуровневой корреляции полученной информации в режиме времени, близком к реальному, вырабатывать предупреждения и решения по обеспечению информационной безопасности.

В качестве системообразующей технологии, реализующей указанные функциональные возможности, представляется целесообразным применять технологию SIEM. Однако системы мониторинга безопасности для сервисных инфраструктур, созданные на ее основе, следует относить к SIEM-системам нового поколения,

разработке которых посвящен проект MASSIF. Сценарии применения SIEM-системы, определенные в MASSIF, в полной мере задают функциональные и реализационные требования к этой системе.

Разработка методов и моделей в области представления, сбора, хранения и обработки информации о событиях безопасности, позволяющих реализовать требования, предъявляемые к SIEM-системе нового поколения, стала актуальной научной задачей, имеющей большое государственное и народнохозяйственное значение и определяющей новые направления научных исследований в области информационной безопасности.

2. ПРИМЕНЕНИЕ ОНТОЛОГИЙ И ЛОГИЧЕСКОГО ВЫВОДА ДЛЯ УПРАВЛЕНИЯ ИНФОРМАЦИЕЙ И СОБЫТИЯМИ БЕЗОПАСНОСТИ

Ключевым элементом в технологии SIEM-системы является обеспечение согласованной загрузки из различных источников в централизованное хранилище (репозиторий) записей журналов безопасности, отображающих так называемые «события безопасности», а также их хранение, моделирование и анализ для обнаружения атак, построения прогнозов и выработки мер противодействия. Технология SIEM способствует принятию эффективных решений в области обеспечения безопасности на основе корреляции событий, интеллектуального анализа данных, логического вывода и визуализации данных. Использование SIEM-систем представляется важным для управления информационной безопасностью крупных распределенных компьютерных сетей, управления услугами и финансовыми сервисами мобильных компаний, а также для критически важных объектов инфраструктуры, таких, например, как крупные гидротехнические сооружения, электростанции и т. д. Успешный опыт использования технологии SIEM-систем в области компьютерной инфраструктуры приводит к идее ее использования в более широком классе, которые могут быть определены как инфраструктуры. Они включают в себя помимо компьютерных систем различные другие сервисы (финансовые, материальные и другие).

SIEM-системы, которые ориентированы на применение в сервисных инфраструктурах, можно рассматривать как SIEM-системы нового поколения. Они должны обладать следующими характеристиками: достаточной общностью для различных видов инфраструктур, последовательной интерпретацией инцидентов и событий на различных уровнях, высокой степенью надежности и долговечности хранения событий, высокой масштабируемостью.

Одним из наиболее важных компонентов SIEM-технологии, используемой в сервисных инфраструктурах, является репозиторий. В нем хранятся данные о событиях безопасности во внутреннем формате, которые извлекаются по запросам от других компонентов для выявления угроз безопасности, атак и разработки контрмер.

Преобразование данных, входящих в систему событий безопасности, во внутренний формат, осуществляется методами нормализации. Далее нормализованные данные подвергаются корреляционному анализу и логическому выводу, необходимому для обнаружения атак, их упреждения и прогнозирования поведения целевой инфраструктуры. В SIEM-системах нового поколения может также использоваться компонент моделирования и имитации атак, который обеспечивает построение на основе хранящейся в репозитории информации графов атак и контрмер [22].

Поскольку репозиторий и решения по их построению представляются специалистам ключевыми и первичными для SIEM-технологии нового поколения, в настоящем разделе рассмотрим основные системотехнические решения в SIEM-системах для сервисных инфраструктур. Эти решения включают в себя результаты анализа известных решений по построению хранилищ данных в SIEM-системах, обоснование онтологического подхода, как наиболее предпочтительного для внутреннего представления событий безопасности, предложения по созданию онтологических моделей для репозитория перспективных SIEM-систем и предложения по архитектуре репозитория SIEM-системы нового поколения. Рассматриваемые решения получены специалистами в рамках проекта MASSIF (Management of Security information and event Service Infrastructures), выполняемого совместно с рядом научных организаций Европейского сообщества.

2.1. ИЗВЕСТНЫЕ РЕШЕНИЯ ПО ПОСТРОЕНИЮ ХРАНИЛИЩ ДАННЫХ SIEM-СИСТЕМ

Для анализа были отобраны следующие наиболее известные SIEM–системы: Alien Vault OSSIM, Accel Ops, Qradar, Prelude, Arc Sight, IBM Tivoli, Novel Sentinel.

В системе **Alien Vault OSSIM** используется реляционное хранилище. В свободно распространяемой версии оно создается на базе СУБД MySQL. Репозиторий этой SIEM-системы включает определяемую пользователем базу знаний об инцидентах [23].

Система **Accel Ops** ориентирована, в первую очередь, на сбор записей журналов безопасности, генерируемых сетевыми и

защитными средствами сетей Cisco. Новые устройства интегрируются через XML-файлы. Записи классифицируются, коррелируются между собой и хранятся для последующих оперативных обработок. Репозиторий реализован на базе Postgre SQL и используется для анализа событий безопасности [24].

В качестве классической SIEM-системы была исследована система **QRadar** [9]. Эта система осуществляет сбор событий безопасности из разнородного множества источников, в качестве которых могут выступать аппаратные компоненты (сетевая инфраструктура, средства защиты, серверы) или программные средства (операционные системы и приложения). Система QRadar полностью хранит входной поток событий, что обеспечивает возможность детальных судебных расследований и развитую отчетность.

Система **Prelude** является характерным представителем открытых SIEM-систем. Она предназначена для сбора, нормализации, сортировки, агрегации, корреляции данных о событиях безопасности и формирования на их основе отчетности. Собранные данные хранятся в отдельном репозитории, для построения которого могут использоваться My SQL, Postgre SQL, SQL lite [25].

Система **Arc Sight Logger 4** осуществляет сбор данных в структурированном и неструктурированном формате [26]. Эта система реализует ролевой доступ и доступ через веб-интерфейс, а также интеллектуальный и интуитивный механизм поиска с помощью визуального мастера запросов.

Система **IBM Tivoli** [27] обеспечивает долговременное и компактное хранение данных о событиях безопасности. Собранные данные хранятся в базе данных, как текстовые объекты, содержащие информацию об инцидентах, управляющих действиях, правилах корреляции и т. д. Нормализованные события объединяются с данными, отображающими правила политики безопасности. Для представления данных используется специальная схема классификации "W7" (Who; When; What; Where; On What; Where To; and Where From), которую можно рассматривать как особый вид онтологического подхода.

Наконец, особенностью системы Novell Sentinel Log Manager является хранение всех данных в сжатом формате [28], доступ к которым может выполняться локально или удаленно. Это

обеспечивает высокую гибкость конфигурирования репозитория. Для управления данными используется Postgre SQL.

Из проведенного анализа следует, что, во-первых, для хранения событий в существующих SIEM-системах используются отдельные хранилища данных, во-вторых, все рассмотренные хранилища данных для управления данными, как правило, используют SQL. Наконец, в некоторых системах (имеется в виду IBM Tivoli) предприняты попытки реализовать онтологический подход.

Из анализа программного обеспечения (ПО) также следует, что для репозитория SIEM-системы нового поколения необходимо решить следующие задачи:

- разработка информационной модели, обладающую достаточной гибкостью, для представления информации о безопасности в самых различных доменах;
- разработка более эффективной архитектуры построения информационного хранилища, максимально полно реализующую возможности такой информационной модели.

Важность этих задач обусловлена следующим: во-первых, надо учитывать, что данные, хранящиеся в репозитории, собраны из различных источников в самых различных форматах, которые должны поддерживаться информационной моделью; во-вторых, данные из репозитория используются в различных компонентах обработки, моделирования и поддержки принятия решений в SIEM-системе. Следовательно, необходимо использовать язык, обладающий достаточной выразительностью для построения запросов к хранилищу, который будет удовлетворять потребностям всех компонентов SIEM-системы и позволять делать точные и корректные выборки. Кроме того, необходимо обеспечить обработку данных в режиме, близком к реальному времени. Репозиторий должен поддерживать высокоскоростную обработку данных, и модель данных должна быть разработана с учетом поддержки максимальной эффективности запросов и не содержать лишних связей. Наконец, поскольку область применения SIEM-систем, весьма широка, модель данных должна быть гибкой и расширяемой.

Для разрешения этих задач планируется внести в перспективную SIEM-систему следующие инновации. Во-первых, для построения

модели данных онтологический подход, который обеспечивает необходимую гибкость внутреннего представления данных и предоставляет возможность использовать системы логического вывода для получения точных выборок из хранилища. Во-вторых, применение гибридного подхода к реализации хранилища репозитории. Этот подход основан на совместном использовании реляционной СУБД, XML, а также хранилища триплетов, основанных на представлении данных в виде трех элементов – субъекта, предиката и объекта. Наконец, современная архитектура репозитория, построенная на основе сервис-ориентированной архитектуры (Service-Oriented Architecture, SOA). Для тестирования данной архитектуры был выбран компонент моделирования атак. Рассмотрим содержание и результаты решения указанных задач.

2.2. ОБОСНОВАНИЕ ОНТОЛОГИЧЕСКОГО ПОДХОДА К ВНУТРЕННЕМУ ПРЕДСТАВЛЕНИЮ ДАННЫХ

Анализируя подходы к представлению данных, специалисты по SIEM-системам рассмотрели наиболее перспективные и широко используемые стандарты по безопасности (событий, инцидентов, атак и т. д.). К ним относятся: протокол SCAP (Security Content Automation Protocol – протокол автоматизации управления данными безопасности – набор открытых стандартов) [29], **стандарт Common Base Event** (CBE) [30] и **стандарт Common Information Model** (CIM) [31].

Протокол SCAP разрабатывается компанией Mitre и Американским Национальным институтом по стандартизации и технологиям (NIST – National Institute of Standarts and Technology) [19]. SCAP является спецификацией, которая объединяет ряд стандартов для унифицированного управления данными по безопасности. SCAP позволяет составить список используемых в системе платформ и приложений, задать особенности их конфигурации, неблагоприятно влияющие на защищенность, специфицировать список уязвимостей, оценить неблагоприятное влияние конфигураций и уязвимостей, выявить наиболее критичные уязвимости (обнаружить присутствие уязвимостей и присвоить им оценки критичности). SCAP включает а себя следующие стандарты:

«Общие перечисление платформ» (CPE – Common Platform Enumeration) используется для описания программно-аппаратного обеспечения; «Общее перечисление конфигураций» (CCE – Common Configuration Enumeration) применяется для описания особенностей программно-аппаратной конфигурации, неблагоприятно влияющих на защищенность; «Общие уязвимости и дефекты» (CVE – Common Vulnerabilities and Exposures) используется для описания списка уязвимостей данных продуктов; «Система оценивания уязвимостей» (CVSS – Common Vulnerabilities Scoring System) необходимая для оценки неблагоприятного влияния конфигураций и уязвимостей, выявления наиболее критичных уязвимостей, на основе чего потом проводится исправление ошибок.

Стандарт Common Base Event (CBE) применяется для представления моделей событий. Он разрабатывается компанией IBM и поддерживается в ряде ее продуктов.

Стандарт Common Information Model (CIM) охватывает самую широкую область применения. В настоящий момент он активно развивается, содержит детально проработанное описание сетевой инфраструктуры, событий, инцидентов и множество других понятий.

На основе описанных выше стандартов, как правило, разрабатываются реляционные модели данных программного обеспечения в области управления информацией и событиями безопасности, а в качестве хранилища используются реляционные СУБД. Однако существуют определенные трудности в выражении всех необходимых отношений между сущностями предметной области. Модель получается перегруженной, и выборка данных занимает значительное время. Это обусловлено также недостаточной гибкостью и низкой выразительностью языка запросов SQL, используемого в реляционных СУБД.

Другая проблема – это необходимость обновлять схему данных в соответствии с требованиями активно меняющейся предметной области. Для реляционных СУБД эта задача на больших объемах данных требует больших затрат временных ресурсов.

Одним из альтернативных решений по представлению данных в системах обработки информации сложной структуры считается **онтологический подход**. Используя средства дескрипционной логики, он позволяет значительно проще выразить сложные

отношения между сущностями. Суть этого подхода заключается в том, что вначале выделяется набор концептов (базовых понятий данной предметной области). Зятем строятся связи между ними, т. е. определяются отношения и взаимодействия базовых понятий. В самом простом случае онтология описывает только иерархию концептов-отношений, связанных отношениями категоризации. Концепты и отношения могут формулироваться с использованием дескрипционной логики, где термины словаря являются именами унарных и бинарных предикатов. Такие аксиомы используются для полноты выражения отношений между концептами и для того, чтобы ограничить их предполагаемую интерпретацию. Таким образом, онтология представляет собой базу знаний, описывающую факты, которые предполагаются всегда истинными в рамках определенного сообщества на основе общепринятого смысла используемого словаря.

Кроме того, изменение модели данных требует значительно меньших усилий, чем в реляционных моделях Таким образом, она является особенно актуальной в таких областях, где необходимо хранить разнородную быстро изменяемую информацию. Одной из таких областей является технология SIEM, так как для SIEM-системы необходима наиболее общая и неперегруженная модель данных, которая в то же время адаптирована и конкретизирована для каждой области применения. Поэтому использование онтологий представляется тем необходимым подходом, который позволяет создавать модель, способную гибко и быстро дополняться всеми необходимыми концептами в процессе работы SIEM-системы в конкретной области. Слабое связывание доменных онтологий и модульный подход к разработке облегчают добавление, удаление и поддержку отдельных онтологий. Кроме того, компоненты онтологии во время исполнения запросов могут быть динамически объединены для удовлетворения требований конкретных приложений.

Математический аппарат, положенный в основу онтологического подхода, позволяет строить более точные запросы на выборку и тем самым значительно ускорять время, затрачиваемое аналитическими модулями SIEM-системы на выборку информации из хранилища для ее последующего анализа. Такое преимущество особенно важно для области SIEM-систем, так как здесь имеется потребность выполнять глубокий и разнородный анализ информации. В качестве основы

построения онтологической модели данных также используются описанные выше стандарты. В рамках исследуемой задачи был рассмотрен ряд работ по выражению этих стандартов в онтологии. Например, работа [32] посвящена построению онтологий для стандартов протокола SCAP. В работе [33] рассматривается трансляция CIM в онтологии.

2.3. СОЗДАНИЕ ОНТОЛОГИЧЕСКИХ МОДЕЛЕЙ ДЛЯ SIEM-СИСТЕМЫ

Онтологическая модель описывает иерархию и связи между концептами. Разработанная онтология состоит из схемы данных, которая называется TBox (Terminology Box), и самих данных – ABox (Assertion Box). Описание уязвимости представляет собой некоторую последовательность программно-аппаратных компонентов, соединенных логическими операторами (AND, OR, NOTAND, NOTOR). В рассматриваемой онтологии такие связи будут выражены набором аксиом, что позволяет перенести в модель данных логику взаимосвязей концептов.

Следует отметить, что в реляционной модели список продуктов, приводящих к возникновению уязвимостей, хранится в виде строки, и при необходимости загружается весь список уязвимостей, который анализировался программно. Применение онтологического подхода с лежащей в его основе дескрипционной логикой позволяет решить задачу представления таких данных гораздо эффективнее, значительно уменьшить объем выборки и соответственно ускорить работу модуля AMSEC.

В дальнейшем планируется расширить разрабатываемую онтологическую модель для обеспечения возможности представления вырабатываемых контрмер, результатов оценки риска, модели нарушителя и других концептов, основываясь на протоколе SCAP.

2.4. АРХИТЕКТУРА РЕПОЗИТОРИЯ ПРИ ИСПОЛЬЗОВАНИИ ОНТОЛОГИЧЕСКОГО ПОДХОДА

Для хранения и манипулирования данными предлагается построение репозитория на принципах сервис-ориентированной архитектуры.

Доступ к данным осуществляется с использованием веб-сервисов. В качестве хранилища используется СУБД Virtuoso компании Open Link Software, которая поддерживает функциональность как реляционной СУБД, так и хранилища триплетов.

В общем случае к репозиторию предъявляются следующие функциональные требования:

- хранение данных;
- хранение метаданных;
- возможность корректировки метаданных;
- управление данными на разных уровнях детализации;
- последовательный доступ к данным, основанный на привилегиях;
- поддержка целостности и непротиворечивости данных;
- поддержка многоверсионного управления.

В целом репозиторий должен служить средством кроссплатформенной интеграции различных компонентов SIEM-системы.

В качестве основы предлагается выбрать сервис-ориентированную архитектуру (SOA). Она реализует множество веб-сервисов для доступа к данным в репозитории. Преимущества этой архитектуры – гибкость и слабая связанность компонентов, что обеспечивает высокую масштабируемость и расширяемость системы.

Архитектура SOA является концептом распределенной информационной среды, которая объединяет воедино различные программные модули и приложения, основанные на хорошо определенных интерфейсах, и обеспечивает их взаимодействие.

Основной принцип архитектуры SOA заключается в том, что элементы бизнес-процессов и элементы информационной инфраструктуры, их обеспечивающей, рассматриваются как компоненты, которые объединены и попеременно используются в

качестве «строительных блоков» для реализации корпоративных процессов.

На рисунке 2.1 показаны общая архитектура репозитория, основанного на SOA, и его взаимодействие с другими компонентами SIEM-системы.

В соответствии с основными принципами SOA архитектура репозитория SIEM-системы может быть разделена на три основных слоя: Память, Представление и Сервисы.

Память включает в себя различные виды хранилищ, такие как реляционное, триплетов и XML-ориентированное.

Представление охватывает все элементы, которые связаны взаимодействием пользователя с SIEM-системой. Этот механизм может быть реализован в виде командной строки или текстового меню, однако для него предпочтителен графический интерфейс, разработанный как тонкий клиент (Windows Swing API и другие) или основанный на HTML. Основной особенностью слоя **представление** является отображение информации и интерпретация входных пользовательских команд SIEM-системы с их конвертацией на соответствующие операции в контексте домена (бизнес-логики) и источника данных. Этот слой обеспечивает отображение данных, обработку событий, пользовательский интерфейс, сервисные HTTP-запросы, пакетное выполнение API типа «командная строка» и другие функции – набор готовых классов, процедур, функций, структур и констант, предоставляемых приложением (библиотекой, сервисом) или операционной системой для использования во внешних программных продуктах. Используется программистами при написании всевозможных приложений.

Слой **сервисы** является дополнительным слоем между слоями **представление** и **память**. Слой **Сервисы** позволяет абстрагировать взаимодействие между одним или многими бизнес-объектами, потоками и сервисами посредством промежуточного интерфейса API.

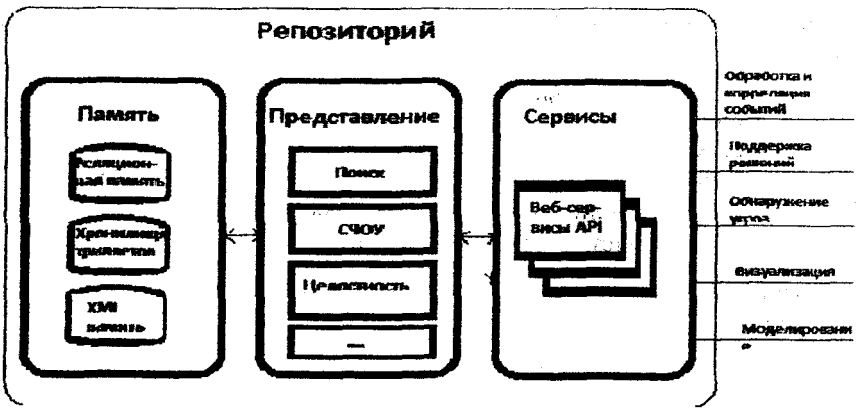

Рис. 2.1. Общая архитектура репозитория (СЧОУ обозначает базовые операции манипулирования данными: создание, чтение, обновление и удаление)

В дополнение к этим трем слоям должен быть предусмотрен слой доступа к данным. На этом слое сгенерированные запросы к репозиторию должны быть проверены на право доступа к таблицам и полям таблиц, к которым обращается запрос.

Для тестирования предлагаемых решений по внутреннему представлению данных и архитектуре репозитория был использован компонент SIEM-системы, осуществляющий моделирование и анализ безопасности (AMSEC). На этой стадии интеграции был реализован репозиторий, который взаимодействует с набором AMSEC-моделей

Результаты тестирования показали, что предложенный отологический подход к разработке модели данных позволяет выполнять загрузку и выборку AMSEC-данных более точно, требует меньших вычислительных затрат и, таким образом, улучшает производительность репозитория.

ВЫВОДЫ ПО 2 РАЗДЕЛУ

В настоящем разделе рассмотрены основные системно-технические решения по применению онтологического подхода для технологии SIEM-систем и построению на его основе репозитория нового поколения. Они охватывают вопросы создания онтологических моделей SIEM-репозитория, применения SOA-ориентированной гибридной архитектуры для построения репозитория и его апробации, а также тестирования для функциональных потребностей компонентов модуля AMSEC, отвечающего в SIEM-системе за моделирование и анализ безопасности.

Использование логического дедуктивного вывода, который является дополнительной функциональной возможностью для хранилища триплетов и обеспечивает управление онтологиями, позволяет проводить глубокий и всесторонний анализ событий безопасности с получением результата высокого качества.

Дальнейшие исследования связываются с расширением предложенной онтологии уязвимостей, а также с добавлением различных сервисов, которые обеспечивают безопасность данных, включая моделирование и анализ безопасности, верификацию политик безопасности и т. д.

Наконец, планируется изучение вопросов логического вывода, ориентированного на онтологический репозиторий, а также разработка механизмов визуализации данных.

3. ИНТЕЛЛЕКТУАЛЬНЫЕ СЕРВИСЫ ЗАЩИТЫ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ И СЕТЯХ

Одним из актуальных направлений обеспечения информационной безопасности (ИБ) в современных компьютерных системах и сетях (компьютерных инфраструктурах) является интеллектуализация сервисов защиты информации, которая предполагает широкое внедрение в системы защиты интеллектуальных методов, моделей, алгоритмов и средств обработки информации.

В первую очередь интеллектуальные сервисы осуществляют интегральную оценку состояния компьютерной инфраструктуры, управление механизмами безопасности и адаптацию политики безопасности и компонентов системы защиты информации. Будучи объединенными в **систему интеллектуальных сервисов защиты информации** (СИСЗИ), эти сервисы становятся тем необходимым средством, которое способно успешно противостоять современным угрозам компьютерной безопасности, различным видам атак на компьютерную инфраструктуру и в конечном итоге обеспечить необходимый уровень кибербезопасности защищаемой инфраструктуры в условиях киберпротивоборства.

В настоящем разделе рассмотрены основные вопросы, связанные с построением интеллектуальных сервисов защиты и их объединением в единый комплекс СИСЗИ, – специфическую систему, предназначенную для обеспечения кибербезопасности. На основе рассмотрения основных понятий в области интеллектуализации защиты информации представлены предложения по общей архитектуре СИСЗИ и реализации ряда входящих в ее состав интеллектуальных сервисов защиты, которые, по мнению специалистов, являются базовыми.

3.1. ОСНОВНЫЕ ПОНЯТИЯ ИНТЕЛЛЕКТУАЛИЗАЦИИ ЗАЩИТЫ ИНФОРМАЦИИ

Реализация принципов, методов, моделей и алгоритмов интеллектуализации защиты информации в компьютерной инфраструктуре переводит **традиционную** систему защиты

информации (СЗИ) на новый уровень, наделяя ее качественно новыми функциональными возможностями, необходимыми для эффективного решения задач обеспечения кибербезопасности. В результате можно говорить не о традиционной, а об *интеллектуальной* системе защиты информации (ИСЗИ).

Раскроем терминологический аппарат, который связан с новыми подсистемами, образующими ИСЗИ. Для подсистемы ИСЗИ, которая непосредственно осуществляет перевод традиционной СЗИ на интеллектуальный уровень, предлагается использовать термин «система интеллектуализации защиты информации» (СИЗИ). Тем самым подчеркивается значение понятия «интеллектуализация» как процесса, осуществляющего наращивание возможностей традиционной СЗИ за счет внедрения в нее интеллектуальных сервисов защиты. При этом СИЗИ следует воспринимать как интеллектуальную надстройку над традиционной системой защиты информации, которая не подменяет ее функциональные возможности, а дополняет их.

В то же время следует отметить, что СИЗИ является системой с управлением. Объектами управления в ней выступают отдельные интеллектуальные модели, методы, механизмы и средства, которые получили название «интеллектуальные сервисы защиты». Управление ими осуществляет система управления интеллектуальными сервисами защиты информации. В результате для СИЗИ, как для системы с управлением, на взгляд специалистов, вполне пригоден и другой термин, который уже был упомянут выше, а именно «система интеллектуальных сервисов защиты информации» (СИСЗИ).

Объекты и субъекты защиты для СИСЗИ остаются такими же, как в традиционной системе защиты. Первые – это информационные и телекоммуникационные ресурсы компьютерной инфраструктуры, а вторые, т. е. лица, осуществляющие управление безопасностью информации, – это администраторы безопасности.

Решения по защите информации принимаются на основе обработки данных о событиях безопасности. К ним относятся все данные об изменении состояния элементов защищаемой компьютерной инфраструктуры, формируемые программным или аппаратным способом, подлежащие хранению в электронном виде в специальных журналах в форме учетных записей (логов) или

поступающие непосредственно в модуль анализа и сбора информации по каналам связи. К событиям безопасности следует также отнести те из них, которые приводят к критическому изменению бизнес-процессов и параметров физических датчиков информации, задействованных в защищаемой инфраструктуре.

Источниками информации о событиях безопасности служат элементы защищаемой компьютерной инфраструктуры различных типов и производителей: серверы баз данных, серверы компьютерной сети, рабочие станции, межсетевые экраны, системы обнаружения атак, антивирусы, виртуальные сети, управляемые сетевые маршрутизаторы (коммутаторы) и другие средства. Кроме того, источниками являются прикладные приложения бизнес-процессов и физические датчики, контролирующие параметры защищаемой инфраструктуры.

Так как сбор, хранение и обработка данных о событиях безопасности лежат в основе функционирования СИСЗИ, то представляется целесообразным использовать для ее создания принципы и особенности построения систем управления информацией и событиями безопасности SEIM-систем.

В общих чертах особенности построения такого класса систем заключаются в следующем. Информация, содержащаяся в указанных источниках, подлежит сбору и последующей обработке в СИСЗИ. Результатом этой обработки становится выработка предупреждений или непосредственных решений по изменению выполняемой политики безопасности, в том числе по перенастройке или реконфигурации традиционных средств защиты.

Типовой метод обработки этой информации включает следующие процессы:

- сбор информации о событиях безопасности;
- приведение информации безопасности к единому внутреннему формату представления;
- хранение событий безопасности в информационном хранилище;
- выдача необходимых данных из хранилища по запросам аналитических модулей;
- анализ данных, полученных по запросам, в аналитических модулях и модулях моделирования для принятия решений;
- формирование решений (контрмер);

• визуализация событий безопасности, решений и формирование по ним отчетности;

• реагирование (выполнение контрмер).

На основе рассмотренных особенностей построения SIEM-систем далее предложена общая архитектура СИСЗИ [34].

3.2. ОБЩАЯ АРХИТЕКТУРА СИСТЕМЫ ИНТЕЛЛЕКТУАЛЬНЫХ СЕРВИСОВ ЗАЩИТЫ ИНФОРМАЦИИ

Поскольку СИСЗИ для современных компьютерных систем и сетей, как правило, функционирует в гетерогенной и крупномасштабной среде с различными уровнями критичности ресурсов, отличающимися возможными воздействиями компьютерных атак, она нуждается в корректных вычислительных моделях, адекватно отображающих ее характеристики. Поэтому архитектура СИСЗИ должна охватывать различные узлы и устройства компьютерной инфраструктуры с возможным соединением граничных узлов через ведомственные сети и сети общего пользования. Следует учитывать, что граничные узлы, предназначенные для сбора данных, как правило, защищены в меньшей степени, чем основные узлы, на которых обрабатываются данные, а телекоммуникационная среда может быть ненадежной. Основные узлы должны быть защищены в большей степени.

В общем случае архитектура СИСЗИ имеет несколько уровней: **уровень данных, уровень событий, прикладной уровень.** На уровне данных осуществляется сбор данных о событиях безопасности, их обобщение, нормализация и предварительная корреляция. Уровень событий отвечает за распространение информационных потоков событий безопасности между потребителями в реальном времени. При этом следует отметить, что восходящий информационный поток, идущий от уровня данных к прикладному уровню, более интенсивен, чем противоположный. На прикладном уровне осуществляется обработка событий безопасности, моделирование, поддержка решений и реагирование, визуализация, хранение событий в репозитории.

Данные о событиях безопасности формируются на уровне защищаемой инфраструктуры, подлежат предварительной обработке

на уровне данных, распространяются с помощью уровня событий к требуемым элементам прикладного уровня и в конечном итоге окончательно обрабатываются элементами прикладного уровня.

Структурная модель общей архитектуры СИСЗИ представлена в [38]. В структуре СИСЗИ выделяются три группы элементов: удаленные (граничные) сервисы и агенты, шина обмена данными и центральные (основные) сервисы и агенты.

Телекоммуникационная система, играющая роль шины обмена данными, соответствует модели «глобальной сети, состоящей из локальных сетей» (WAN-of-LANs) [35], которая в наибольшей степени подходит для отображения слабосвязанных компьютерных инфраструктур, охватывающих одинаковые или разнородные административные домены. В этом случае местные интрасети связаны между собой через сети общего пользования (Интернет). Одним из способов их соединения являются виртуальные частные сети, образующие защищенные каналы (туннели).

Функциональная модель общей архитектуры системы интеллектуальных сервисов защиты информации показывает распространение информационных потоков через уровни архитектуры и ее элементы. Информация собирается в граничных узлах и распространяется к основным прикладным сервисам.

Охарактеризуем основные интеллектуальные сервисы защиты [36].

Данные о событиях информационной безопасности (далее по тексту – *события*) формируются на уровне защищаемой компьютерной инфраструктуры с помощью различных источников данных и процедур трансляции событий.

Обмен событиями, приведенными к унифицированному виду, т. е. *унифицированными событиями*, осуществляется через *шину обмена данными*.

Сервисы *обработки событий* выполняют корреляцию релевантных событий, выделяемых из потока информации, и помещают их на хранение в репозиторий.

Репозиторий обеспечивает хранение событий и взаимодействие прикладных модулей.

Сервисы моделирования и анализа выполняют моделирование атак и поведения системы, оценивают угрозы, вычисляют метрики безопасности и вырабатывают рекомендации по усилению защиты.

Наконец, сервисы поддержки принятия решений и реагирования анализируют входящие события, модели угроз и предупреждения безопасности и вырабатывают контрмеры, приводящие к модификации политики безопасности, которая посылается обратно к граничным узлам и воздействуют, в том числе, на удаленные источники данных, агенты и модули предварительной обработки событий безопасности.

Рассмотрим архитектуру модулей, реализующих указанные интеллектуальные сервисы защиты, более детально.

3.3. СЕРВИСЫ ОБРАБОТКИ СОБЫТИЙ

Интеллектуальные сервисы обработки событий – важнейшие компоненты СИСЗИ. Основные функции, реализуемые данными сервисами: преобразование входных событий во внутренний универсальный формат, их корреляция и хранение в репозитории. Рассмотрим подробнее решения, которые предлагаются для реализации этих функций.

Процессы сбора данных о событиях безопасности должны поддерживать различные протоколы взаимодействия и иметь возможность настройки новых протоколов и входных форматов. Наиболее популярными протоколами передачи журнальных данных являются Syslog, FTP, ODBC и SNMP. Кроме того, важно не только поддерживать транспортный протокол, но и распознавать формат и семантику содержимого журнала. Для этих целей имеются форматы Syslog (*англ.* system log – **системный журнал**) – стандарт отправки и регистрации сообщений о происходящих в системе событиях (т. е. создания **логов**), использующийся в **компьютерных сетях**, SCAP (протокол автоматизации управления данными безопасности), CIM (Common Information Model - общая информационная модель) – открытый стандарт, определяющий представление управляемых элементов IT среды в виде совокупности объектов и их отношений, предназначенный обеспечить унифицированный способ управления такими объектами, вне зависимости от их поставщика или

производителя, предлагаемые различными поставщиками продуктов в области безопасности.

Простые форматы не обеспечивают удовлетворения требований поддержки структурированного представления информации, использования меток времени, поддержки иерархической структуры для представления информации и ряда других элементов.

Поэтому для построения СИСЗИ и в связи с развитием средств интеллектуального анализа данных необходимо обоснование подхода к построению формата, способного применяться в различных прикладных областях и быть достаточно выразительным и расширяемым.

На взгляд специалистов, наиболее перспективен онтологический подход к представлению данных. В нем используется специальное формализованное описание предметной области, основанное, как правило, на дескрипционной логике, получившее название онтологии.

В частности, онтологическая архитектура имеет слабосвязанное, модульное представление, устойчивое к быстрым изменениям и росту сложности. Основанные на такой архитектуре сервисы и приложения могут свободно объединять и расширять архитектурные компоненты во время своего выполнения в интересах контекста приложения. Такой подход весьма уместен для СИСЗИ, так как для этой системы необходима наиболее общая и неперегруженная модель данных, которая в то же время адаптирована и конкретизирована для различных областей применения.

Онтологический подход к построению сервисов сбора, преобразования и хранения информации позволяет реализовать в СИСЗИ системы логического вывода, основанные на онтологии [37]. Так, в настоящее время для этой цели широко используются языки OWL (Web Ontology Language) и SWRL (Semantic Web Rule Language).

Следующий этап обработки данных о событиях безопасности – корреляция событий, под которой понимается сопоставление различной информации об одинаковых событиях или явлениях, полученной от разных источников, с целью устранения имеющейся в них неопределенности и/или получения новой достоверной информации о безопасности. Процесс корреляции информации тесно связан с процессом получения новой информации на основе анализа

хранимых онтологий в условиях неполноты и противоречивости имеющихся данных.

Корреляция событий должна осуществляться в масштабируемом и адаптивном модуле управления корреляцией, который ориентирован на систему параллельной обработки сложных событий, способную объединять вычислительные мощности для громадного количества событий в секунду и регулировать количество выделенных ресурсов защищаемой компьютерной инфраструктуры.

Поведение этого модуля должно экстенсивно настраиваться через запросы, которые создаются из определяемых пользователем стандартных директив. Запросы определяют, каким образом следует абстрагировать, трансформировать, обобщать и коррелировать входные события.

Внутренняя архитектура модуля управления корреляцией и его взаимосвязь с другими компонентами показаны в [22].

Данный модуль характеризуется большим количеством обрабатываемых сущностей, организованных в последовательность подкластеров. Все обрабатываемые сущности подкластера вырабатывают одинаковую порцию запросов, называемую подзапросом, получая входную информацию от предыдущего подкластера и передавая выходные события на следующие подкластеры. Менеджер корреляции контролирует состояние каждой обрабатываемой сущности и определяет размер подкластера в соответствии с его текущей входной нагрузкой. Дополнение или удаление обрабатываемых сущностей требует от менеджера корреляции его взаимодействия с менеджером ресурсов, который содержит пул ожидающих сущностей, доступных для дальнейшей обработки. При этом менеджер корреляции может также перераспределять нагрузку между обрабатываемыми сущностями, непосредственно связанными с подкластером. Наконец, компилятор запросов получает стандартные директивы через входной интерфейс или через компонент моделирования и анализа, затем транслирует их в запросы, разделяет на подзапросы, каждый из которых затем отправляет в подкластер.

Данные о событиях безопасности, прошедшие преобразование форматов и корреляцию, помещаются в репозиторий. Репозиторий является средством кросс-платформенной интеграции различных

компонентов СИСЗИ [38]. В качестве основы для его реализации предлагается сервис-ориентированная архитектура (СОА), представляющая собой концепцию распределенной информационной среды, объединяющей модули программного обеспечения и приложений, основанные на хорошо определенных интерфейсах и взаимодействиях между ними.

Уровень хранилища включает в себя программно-инструментальные средства работы с базами данных различных видов. К их числу относятся реляционные СУБД, XML-СУБД и хранилища триплетов. Наиболее распространенным решением для построения баз данных репозитория на настоящий момент являются реляционные СУБД. Модель данных в реляционной СУБД можно представить диаграммой «сущность–связь». Репозиторий на основе XML-СУБД представляется в виде древовидноорганизованной файловой системы. Модель данных описывается с помощью XML-схемы. Триплет является тройкой «субъект–предикат–объект». Хранилище триплетов обеспечивает большую гибкость изменения модели данных, однако оно проигрывает реляционной СУБД по производительности. С учетом достоинств и недостатков перечисленных выше средств создания репозитория целесообразно использовать гибридное решение, поддерживающее все эти три вида хранилищ [39]. Гибридный подход к хранению данных о событиях безопасности сочетает в себя достоинства всех базовых моделей представления данных и обеспечивает, с одной стороны, задание моделей предметной области в виде онтологий, а с другой – использование в СИСЗИ логического вывода для выработки решений. Примером программно-инструментального средства, реализующего такой подход, служит система Virtuoso Universal Server компании Open Link [39].

Уровень web-сервисов делится на три основных слоя: слой доступа, слой реализации web-сервисов и слой представления.

Слой доступа является посредником между хранилищем и программной реализацией web-сервисов. Он интерпретирует универсальные запросы для извлечения данных, полученных от клиентских приложений в нотации языка используемой СУБД. Кроме того, на этом слое сгенерированные запросы к репозиторию проверяются на наличие прав доступа к таблицам и полям таблиц.

Слой реализации web-сервисов позволяет абстрагировать взаимодействие между одним или многими бизнес-объектами, потоками и сервисами посредством промежуточного интерфейса API.

Слой представления охватывает все элементы, которые связаны взаимодействием пользователя с СИСЗИ. Этот механизм может быть реализован в виде командной строки или текстового меню, однако для него предпочтителен графический интерфейс, разработанный как тонкий клиент (Windows, Swing API и др.) или основанный на HTML. Основной особенностью слоя представления является отображение информации и интерпретация входных пользовательских команд СИСЗИ с их конвертацией на соответствующие операции в контексте домена (бизнес-логики) и источника данных. Этот слой обеспечивает отображение данных, обработку событий, пользовательский интерфейс, сервисные HTTP-запросы, пакетное выполнение API типа «командная строка» и другие функции.

3.4. СЕРВИСЫ МОДЕЛИРОВАНИЯ И АНАЛИЗА

Предлагаемый подход к построению сервисов моделирования и анализа предполагает следующие действия:

- моделирование объекта защиты и поведения злоумышленника;
- генерацию общего графа атак;
- вычисление различных показателей безопасности;
- реализацию процедур анализа риска.

Интеллектуальные сервисы моделирования и анализа реализуются посредством двух модулей: прогностическим анализатором безопасности (ПАБ) и компонентом моделирования атак и поведения системы защиты (КМАПСЗ).

Модуль ПАБ обеспечивает расширенные возможности мониторинга безопасности в СИСЗИ. В частности, он поддерживает моделирование поведения компьютерной инфраструктуры в ближайшей перспективе и предсказывает возможные нарушения безопасности [40].

Так как качество проводимого анализа существенно зависит от процессов, а также от соответствующего описания событий безопасности, то до начала работы ПАБ все описания процессов,

целей и событий безопасности должны быть преобразованы в понятные модели, которые в дальнейшем будут использоваться для ведения в реальном времени непрерывного анализа и моделирования ситуаций ближайшей перспективы. Это выполняется в модулях моделирования событий безопасности и моделирования процессов, которые являются компонентами сборщика моделей. Данные модули взаимодействуют с репозиторием, содержащим модели атак, созданные КМАПСЗ, и модели, ранее созданные в сборщике моделей. Интерфейсы моделей событий безопасности и моделей процессов обеспечивают доступ к ним со стороны ПАБ. Модели, получившие интерпретацию, импортируются в ПАБ на фазе инициализации.

Модуль моделирования процессов ПАБ выявляет требования безопасности, спецификацию используемой имитационной модели и правил мониторинга. В репозитории СИСЗИ должны храниться высокоуровневые цели защиты, требования безопасности, правила спецификации и связи между ними. Эти связи необходимы для обеспечения корреляции вырабатываемых в ПАБ предупреждений с целями защиты и требованиями безопасности. Более того, описания ресурсов и форматы событий, которые хранятся в репозитории, необходимы для корреляции информации о защищаемых ресурсах с полученными событиями и предупреждениями, пересылаемыми в ПАБ через репозиторий.

Компонент КМАПСЗ обеспечивает дополнительные аналитические возможности СИСЗИ за счет реализации функций моделирования атак и поведения системы защиты, а также анализа защищенности расчета различных метрик безопасности [41]. Состав его входных данных:

- конфигурация защищаемой компьютерной сети (системы);
- политика безопасности для компьютерной сети (системы), определяемые множеством полномочий или правил доступа;
- формируемые предупреждения;
- внешние базы данных уязвимостей, атак, платформ и т. д.;
- профили возможных нарушителей (в виде множества характеристик нарушителя);
- требуемые значения метрик безопасности (в виде множества требований безопасности);
- зависимости сервисов.

Основные результаты работы КМАПСЗ:

- обнаруженные уязвимости;
- возможные маршруты (графы) атак и цели атак;
- «узкие места» в компьютерной безопасности;
- скорректированные деревья атак, основанные на изменениях, произошедших в сети;
- предсказания дальнейших шагов нарушителя, имеющие место в текущей ситуации;
- метрики безопасности, которые могут использоваться для оценки нарушителя, атак, контрмер, общего уровня безопасности компьютерной сети (системы) и ее компонентов;
- последствия атак и контрмер;
- предложения по повышению уровня безопасности.

КМАПСЗ работает в двух режимах:

1) проектирования (конфигурирования), когда выполняются проектирование и внутренний анализ исследуемой сети (системы), – этот режим не является режимом реального времени;

2) эксплуатации, когда компонент используется в реальном масштабе времени или близком к нему.

Рассмотрим порядок функционирования элементов КМАПСЗ. Загрузчик репозитория загружает базы данных об уязвимостях, атаках, конфигурации, «узких местах», платформах и контрмерах из внешних источников, посылая запросы во внешние базы данных для обновления и взаимодействуя с источниками данных.

Генератор спецификаций преобразует информацию о сетевых событиях, конфигурации и политике безопасности, полученную от других компонентов или от пользователя, во внутреннее представление.

Модуль моделирования нарушителя определяет индивидуальные характеристики нарушителей, их уровень квалификации, начальное местоположение (внутренний или внешний, возможная точка входа и т. д.), полномочия, уже осуществленные возможные действия (атаки), которые могут быть предсказаны на основе событий и предупреждений, и знания об анализируемой сети.

Генератор графов атак строит графы (деревья) атак путем моделирования последовательностей атакующих действий нарушителя в анализируемой компьютерной сети, используя

целей и событий безопасности должны быть преобразованы в понятные модели, которые в дальнейшем будут использоваться для ведения в реальном времени непрерывного анализа и моделирования ситуаций ближайшей перспективы. Это выполняется в модулях моделирования событий безопасности и моделирования процессов, которые являются компонентами сборщика моделей. Данные модули взаимодействуют с репозиторием, содержащим модели атак, созданные КМАПСЗ, и модели, ранее созданные в сборщике моделей. Интерфейсы моделей событий безопасности и моделей процессов обеспечивают доступ к ним со стороны ПАБ. Модели, получившие интерпретацию, импортируются в ПАБ на фазе инициализации.

Модуль моделирования процессов ПАБ выявляет требования безопасности, спецификацию используемой имитационной модели и правил мониторинга. В репозитории СИСЗИ должны храниться высокоуровневые цели защиты, требования безопасности, правила спецификации и связи между ними. Эти связи необходимы для обеспечения корреляции вырабатываемых в ПАБ предупреждений с целями защиты и требованиями безопасности. Более того, описания ресурсов и форматы событий, которые хранятся в репозитории, необходимы для корреляции информации о защищаемых ресурсах с полученными событиями и предупреждениями, пересылаемыми в ПАБ через репозиторий.

Компонент КМАПСЗ обеспечивает дополнительные аналитические возможности СИСЗИ за счет реализации функций моделирования атак и поведения системы защиты, а также анализа защищенности расчета различных метрик безопасности [41]. Состав его входных данных:

- конфигурация защищаемой компьютерной сети (системы);
- политика безопасности для компьютерной сети (системы), определяемые множеством полномочий или правил доступа;
- формируемые предупреждения;
- внешние базы данных уязвимостей, атак, платформ и т. д.;
- профили возможных нарушителей (в виде множества характеристик нарушителя);
- требуемые значения метрик безопасности (в виде множества требований безопасности);
- зависимости сервисов.

Основные результаты работы КМАПСЗ:

- обнаруженные уязвимости;
- возможные маршруты (графы) атак и цели атак;
- «узкие места» в компьютерной безопасности;
- скорректированные деревья атак, основанные на изменениях, происшедших в сети;
- предсказания дальнейших шагов нарушителя, имеющие место в текущей ситуации;
- метрики безопасности, которые могут использоваться для оценки нарушителя, атак, контрмер, общего уровня безопасности компьютерной сети (системы) и ее компонентов;
- последствия атак и контрмер;
- предложения по повышению уровня безопасности.

КМАПСЗ работает в двух режимах:

1) проектирования (конфигурирования), когда выполняются проектирование и внутренний анализ исследуемой сети (системы), – этот режим не является режимом реального времени;

2) эксплуатации, когда компонент используется в реальном масштабе времени или близком к нему.

Рассмотрим порядок функционирования элементов КМАПСЗ. Загрузчик репозитория загружает базы данных об уязвимостях, атаках, конфигурации, «узких местах», платформах и контрмерах из внешних источников, посылая запросы во внешние базы данных для обновления и взаимодействуя с источниками данных.

Генератор спецификаций преобразует информацию о сетевых событиях, конфигурации и политике безопасности, полученную от других компонентов или от пользователя, во внутреннее представление.

Модуль моделирования нарушителя определяет индивидуальные характеристики нарушителей, их уровень квалификации, начальное местоположение (внутренний или внешний, возможная точка входа и т. д.), полномочия, уже осуществленные возможные действия (атаки), которые могут быть предсказаны на основе событий и предупреждений, и знания об анализируемой сети.

Генератор графов атак строит графы (деревья) атак путем моделирования последовательностей атакующих действий нарушителя в анализируемой компьютерной сети, используя

информацию о различных типах возможных атак, зависимостях сервисов, конфигурации сети и использованной политике безопасности. Генератор графа атак может также строить трассы атак, учитывая уязвимости «нулевого дня» – неизвестные уязвимости, которые используются для компрометации ресурсов системы.

Анализатор безопасности служит для вычисления метрик безопасности и обеспечивает поддержку выбора решений (контрмер). Он позволяет имитировать многошаговые атаки и вычислять эффективность различных контрмер. Например, используя такие сложные объекты, как трасса (маршрут) атаки или совокупность трасс атак, реализующих определенную угрозу, анализатор безопасности вычисляет метрики безопасности этих объектов, чтобы оценить общий уровень безопасности и выработать рекомендации по минимизации угроз.

Генератор отчетов показывает уязвимости, которые обнаружены КМАПСЗ, представляет «узкие места», отображает значения метрик безопасности и генерирует рекомендации по повышению уровня безопасности, а также выделяет другую релевантную информацию безопасности.

3.5. СЕРВИСЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ И РЕАГИРОВАНИЯ

Для построения сервисов поддержки принятия решений и реагирования может быть использовано несколько методологических подходов. В [16] выделены фильтрующие методы, группирующие методы, а также процедуры, основанные на поиске.

Фильтрационные методы уменьшают набор эффективных вариантов выбора, отбрасывая наиболее «избыточные» точки. Пример применения подходов такого класса в контексте выбора средств защиты информации дан в [42], где используется структура данных «к-дерево» [43].

Группирующие методы могут быть применены к формированию групп одинаковых вариантов решений. Если задано определенное количество кластеров вариантов решений, то администратору безопасности дается представляющая точка из каждого кластера. Администратор может выбрать наиболее предпочтительное из

решений и проверить окрестности этой точки. Для этой цели можно использовать неиерархическую группировку «к-средних» [44].

Процедуры, основанные на поиске, начинаются с эффективного выбора и позволяют лицу, принимающему решения, «двигаться» в пространстве решений к более привлекательным альтернативам до того, как будет найдено «наилучшее» решение [45].

Компонентом СИСЗИ, реализующим указанные процедуры, является компонент поддержки принятия решений и реагирования (КППРР). Компонент КППРР предназначен для разработки и реализации инструментария администратора, основанного на модели организации OrBAC (Organization bazed Access Control Telecom Bretagne) [46]. Модель OrBAC в настоящее время является одним из наиболее распространенных формализмов описания политик безопасности. Такой подход к построению КППРР позволяет выполнять политику безопасности, используя различные структурные компоненты организации, и автоматически их конфигурировать.

С помощью КППРР администратор способен идентифицировать наличие конфликтов среди правил. Например, он не может обнаружить некорректное использование одной и той же политики безопасности в отношении различных внешних компонентов (LDAP и Apache), если конфигурирует их вручную. С другой стороны, при конфигурировании этих компонентов с помощью КППРР система автоматически обнаруживает наличие этих конфликтов и информирует о них перед тем, как использовать правила политики безопасности.

Политики безопасности динамически настраиваются с помощью контекста, что позволяет системе быстро реагировать на любые изменения (например, на попытки проникновения или нападения). При этом следует четко определять контекст и систему мониторинга, чтобы правильно выявлять изменения в контексте.

Все вновь сгенерированные правила безопасности могут быть одновременно применены ко всем компонентам защищаемой сети. Для этого новые правила распространяются КППРР автоматически, а остальные компоненты изменяют свою конфигурацию в соответствии с этими правилами.

КППРР позволяет идентифицировать предварительно установленные конфигурации и сохранять их в репозитории. На

основе знания политики безопасности данной организации КППРР способен их проверить и обнаружить конфликты. Каждый раз, когда администратор желает сконфигурировать новую политику, КППРР может проверить, во-первых, что эта политика не была создана ранее, во-вторых, что новая политика не создает каких-либо конфликтов с другими существующими политиками.

Модуль вычислений действует как сервер, который обеспечивает централизацию администрирования политики контроля доступа. Множество входящих в его состав агентов осуществляет конфигурирование политики компонентов, которые связаны с КППРР. Элементы политики поступают в КППРР из репозитория через интерфейс управления модулем вычислений. В модуле политик безопасности из отдельных элементов формируются текущие политики безопасности. сл

По командам, вырабатываемым модулем вычи ений и поступающим от API и GUI модуля визуализации, модуль выявления конфликтов и компиляции политик осуществляет верификацию политики и их преобразование (компиляцию) в требуемый формат.

Представленные в скомпилированном виде различные политики через модуль проверки и переработки политики, в котором они подвергаются окончательной обработке, подлежат передаче устройствам-потребителям через механизм распространения унифицированных событий, реализованный в шине обмена данными системы интеллектуальных сервисов защиты информации.

3.6. СЕРВИСЫ ВИЗУАЛИЗАЦИИ ИНФОРМАЦИИ О СОБЫТИЯХ БЕЗОПАСНОСТИ

В отличие от обработки данных, представленных в текстовой или табличной форме, визуализация предлагает более эффективный подход

к анализу информации. Визуализация информации в СИСЗИ – это процесс генерирования изображения на основе событий безопасности и результатов функционирования сервисов защиты. С помощью визуализации данных можно обобщать множество отдельных деталей таким образом, чтобы сделать доступным смысл того или иного события или совокупности событий. Визуализация также позволяет,

используя различные формы, цвета, размеры и взаимное расположение элементов, повысить оперативность восприятия больших объемов информации [47].

Известны следующие классы графов, которые можно использовать для построения сервисов визуализации информации в СИСЗИ [47]:

- простые диаграммы;
- диаграммы с накоплением;
- схемы полигонов;
- диаграммы рассеивания;
- графы параллельных координат;
- графы связей;
- карты;
- карты деревьев.

Каждый из этих графов имеет разные возможности и подчеркивает конкретные аспекты данных.

Для реализации этой функции в СИСЗИ предлагается использовать модуль визуализации: интерфейс пользователя, слой управляющих сервисов и слой графических элементов.

Выделение интерфейса пользователя в отдельный уровень позволяет поддерживать разработку различных видов графических интерфейсов, начиная от простой командной строки, заканчивая сложным многооконным интерфейсом с различными панелями управления.

Предполагается, что данные, которые необходимо представить графически, передаются соответствующему сервису, который возвращает готовый результат для отображения в форме приложения. Такой механизм взаимодействия дает возможность скрыть детали, например, кто инициировал процесс визуализации – пользователь или функциональный сервис. Это позволяет рассматривать слой управляющих сервисов как модуль управления.

Исходя из выполняемых функций, в слое управляющих сервисов можно выделить два основных компонента: контроллер графических элементов и менеджер сервисов.

Контроллер графических элементов предоставляет стандартный интерфейс по работе с потоками визуализации, который обеспечивает создание и остановку графического потока, реализуемого на уровне графических элементов. Менеджер сервисов обеспечивает

подключение интеллектуальных сервисов защиты, реализующих функциональность СИСЗИ. Такое решение позволяет вести разработку компонентов СИСЗИ различными организациями независимо друг от друга.

Уровень графических элементов включает библиотеку необходимых графических примитивов: графов, лепестковых диаграмм, гистограмм, карт деревьев, географических карт и т. д. Графические элементы реализуют обработку входных данных, их отображение и взаимодействие пользователя непосредственно с входными данными.

Предложенный подход позволяет для разработки графических элементов использовать различные технологии визуализации, например, Java3D, Flash, SVG и т. д.

ВЫВОДЫ ПО РАЗДЕЛУ 3

В разделе рассмотрены подхóды к построению нескольких базовых интеллектуальных сервисов защиты информации в компьютерных системах и сетях, к числу которых относятся сервисы обработки данных о событиях безопасности, моделирования и анализа, поддержки принятия решений и реагирования, а также визуализации безопасности. Предложенная общая архитектура СИСЗИ позволяет рассматривать ее как интеллектуальную надстройку над традиционной системой защиты информации.

Отличительной особенностью рассмотренных интеллектуальных сервисов защиты является их инвариантность относительно существующих и разрабатываемых типов программных атак, а также способность вырабатывать предупреждения и управляющие решения по безопасности информации в реальном или близком к реальному масштабу времени.

4. КОМПЛЕКСНАЯ МЕТОДИКА РАСЧЕТА ОБЪЕКТИВНЫХ ОЦЕНОК ОТНОСИТЕЛЬНО ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ ДЛЯ ПОВЫШЕНИЯ ДОСТОВЕРНОСТИ, ПРЕДЛАГАЕМЫХ ЭКСПЕРТНЫХ ОЦЕНОК

Разработка системы с интеллектуальными сервисами защиты конфиденциальной информации (КИ) требует успешной реализации различных мероприятий по защите информационных ресурсов (ИР) в компьютерных системах (КС). Эти мероприятия позволяют решить целый ряд задач, в частности, создать систему мониторинга угроз безопасности. Системы мониторинга реализуют текущий и апостериорный подходы к защите информации и их цель – снижение количества инцидентов воздействующих на ИР КС до минимального уровня риска и минимизация возникающего при этом ущерба. Инцидентом будем считать любое незаконное, неразрешенное, неблагоприятное события (НС), которые совершаются в информационных системах (ИС) компаний.

В настоящее время каждое предприятие широко использует различные вычислительные сети для продвижения услуг с интеллектуальными свойствами программных продуктов поиска клиентов, для заключения договоров и оплаты предоставленных сервисов и товаров. Сбором, обработкой, хранением деловой информации и ее обменом занимается любая компания. В процессе деятельности всевозможные данные, метаданные участвуют в бизнес-процессах (обрабатываются), находятся в стадии хранения в различных гибких и эффективных формах для дальнейшего быстрого запроса, использования и перемещения между участниками бизнеса как внутри компании, так и во внешней среде по отношению к партнерам, клиентам и т. п.

Предполагается, что активное управление статистической информацией о прошлом, настоящем и будущего относительно инцидентов и событий безопасности основывается на автоматических механизмах для автоматической подстройки параметров мониторинга событий к текущему состоянию защищаемой системы.

Мы предполагаем, что одним из обсуждаемых вопросов в рамках проекта MASSIF должно быть наполнение и постоянное

совершенствование отдельных узлов SIEM-системы решением задач классификации инцидентов, прогнозированием, фильтрацией и оптимизацией использования средств защиты ИР в КС [48--52]. Основными исходными данными, которые используются SIEM-системой для решения указанных задач, являются записи различных журналов аудита (logs), протоколирующие события в информационной инфраструктуре, называемые «событиями безопасности». Данные по событиям отражают такие действия пользователей и программ, которые могут влиять на ИБ.

В перспективных SIEM-системах (т. е. в системах нового поколения) к числу функциональных возможностей узлов SIEM-системы следует добавить анализ событий, инцидентов и их последствий, принятие решений и визуализацию информации. Раскроем содержание некоторых механизмов наполнений узлов по уровням иерархии SIEM-системы: нормализация означает приведение записей журналов, собранных из различных источников, к единому внутреннему формату, который затем будет использоваться для их хранения и последующей обработки [47]; фильтрация событий безопасности заключается в корректировке текущих оценок состояния защищенности ИР в КС и расчете этих оценок на будущий интервал времени [51, 52, 53]; анализ событий, инцидентов и их последствий включает процедуры моделирования событий, атак и их последствий, оценка уязвимостей, риска, прогнозирование и фильтрацию оценок НС и инцидентов [54,55]; система поддержки принятия решений (СППР) определяет выработку мер по оптимизации и реконфигурированию средств защиты для предотвращения атак на КС; генерация отчетов и предупреждений означает формирование, передачу, отображение и (или) печать результатов функционирования.

В данном разделе будут предложены и раскрыты некоторые элементы наполнения отдельных узлов SIEM-системы алгоритмами решения задач расчета риска на основе объективных оценок, а также расчета оценок предсказания и фильтрации количества НС и величины ущерба ИР в КС.

Одновременно возникает проблема оценивания состояния возможных каналов утечки информации и соответствующей оценки ущерба, который может иметь место в случае утечки информации или при любом другом нарушении системы безопасности, а также

вероятности нанесения подобного ущерба. Для определения адекватности стоимости системы защиты следует сопоставить размеры ущерба и вероятность его нанесения с размерами затрат на обеспечение защиты. К сожалению, получить объективную реальную стоимость каждого ИР в ИС из-за множества неопределенностей, а также адекватный автоматизированный и автоматический контроль и учет ИС в вычислительных системах очень трудно. Поэтому часто применяют только экспертные оценки.

При решении практических задач защиты информации первостепенное значение имеет количественная оценка ее уязвимости (неспособность удержать атаку). Несанкционированный доступ (НСД) к информации в автоматизированной и автоматической системе (ААС) возможен не только непосредственным использованием информации в базах данных, но и многими другими путями. При этом основную опасность представляют преднамеренные действия злоумышленников. Воздействие случайных факторов само по себе не ведет к НСД, оно лишь способствует появлению каналов несанкционированного получения информации (КНПИ), которыми может воспользоваться злоумышленник.

Для целей защиты ИР в ИС предприятия будем рассматривать подходы управления рисками. При расчете рисков в ИС будем основываться не только на хорошо известных экспертных оценках, но и на объективных оценках вероятностей количества реализации НС. Будем также рассчитывать оценки предсказания величины ущерба от нарушений безопасности ИР.

Методическая оценка ущерба в ИС от реализации НС зависит от оценки риска вероятности НС в ИС. Оценка объективных вероятностей наступления НС – одна из важных задач в алгоритме расчета. Отметим также, что использование этих объективных оценок для повышения эффективности расчетов оценок риска в ИС предприятия является важной задачей в методике расчета потенциального ущерба от атак нарушителей.

4.1. АНАЛИЗ И КЛАССИФИКАЦИЯ ТЕРРИТОРИАЛЬНО И ПОТЕНЦИАЛЬНО ВОЗМОЖНЫХ НСД К ИНФОРМАЦИИ КОМПАНИЙ В РАЗЛИЧНЫХ ЗОНАХ

Известны следующие методы и способы совершения компьютерных преступлений: введение несанкционированных данных; манипулирование несанкционированными данными; незаконное использование файлов; создание несанкционированных файлов; преодоление внутренних контрольных механизмов; несанкционированное уничтожение и изменение данных на выходе; несанкционированное манипулирование компьютерными программами или документацией; несанкционированное манипулирование процессом обработки данных; манипулирование ошибками, отказами системы; несанкционированное использование паролей и кодов; несанкционированная передача и перехват сообщений по коммуникациям; кража компьютерного оборудования, программного обеспечения (ПО); умышленное нанесение вреда, уничтожение или порча оборудования, программного обеспечения или данных и т. д.

Территориально и потенциально возможные НСД к информации компании могут иметь место в разных зонах [55]:

1) внешней неконтролируемой зоне компании;
2) зоне контролируемой территории компании;
3) зоне помещений ААС;
4) зоне ресурсов ААС;
5) зоне баз данных.

При этом для НСД к получению информации необходимо одновременное наступление следующих событий:

- злоумышленник должен получить доступ в соответствующую зону;
- во время прохождения злоумышленника в зону в ней должен появиться соответствующий КНПИ;
- появившийся КНПИ должен быть доступен злоумышленнику соответствующей категории (здесь имеется в виду, что злоумышленник должен иметь соответствующий уровень образования, быть обеспечен необходимой техникой и средствами, а также владеть навыками, чтобы воспользоваться КНПИ);

• и КНИ в момент доступа к нему нарушителя должна находиться защищаемая информация.

4.1.1. ВНЕШНЯЯ НЕКОНТРОЛИРУЕМАЯ ЗОНА

Рассмотрим внешнюю неконтролируемую зону. При этом все компьютерные преступления можно условно разбить на три класса: перехват информации; несанкционированный доступ; «манипуляция данными».

Первый класс:

а) электромагнитный перехват, например, регистрация излучений, создаваемых процессором, принтером, монитором;

б) непосредственный перехват, например, прямое подключение к каналам передачи данных.

Второй класс:

а) незаконное подключение к линии законного пользователя;

б) вид преступления, который называется «абордаж», – это когда «компьютерные пираты» проникают в чужие информационные системы путем угадывания их кода.

Третий класс («манипуляция данными»):

а) вид преступления – подмена кода, например, вариантом подмены данных является изменение кода;

в) вид «троянский конь» – тайное введение в чужую программу таких команд, которые позволяют осуществить новые, не планируемые пользователем программные функции с сохранением прежней работоспособности;

г) компьютерные вирусы – действуют, например: по принципу, сотри все данные этой программы, перейди в следующую и сделай то же самое. Они обладают свойством переходить через коммуникационные сети из одной системы в другую, распространяясь как вирусное заболевание;

д) вид «логическая и временная бомбы» – действие ложно введенных команд на программы при определенных условиях и времени, и т. д.

Теперь составим список существенных видов НС, возникающих в ИС, которые приводят к снижению системной эффективности функционирования компьютерной системы. Пусть этот список

представляет собой множество видов НС $\{O_1, O_2, \ldots, O_m\}$. Выделим из этого множества существенное подмножество некоторых видов НС, приводящих к ощутимому нарушению безопасности ИР в КС. Это подмножество обозначим через $O = \{O_{i_1}, O_{i_2}, \ldots, O_{i_m}\}$, например, O_{i_1} – количество НС относительно нарушения запуска отдельных узлов КС; O_{i_2} – количество НС относительно неверного набора информации применительно к конкретному информационному процессу и обработке данных и т. д.

После построения подмножества O переходим к анализу свойств элементов подмножества на основе количественных показателей НС и соответственно величины ущерба, имевшей место в прошлом. Пусть $O = \{O_{i_1}, O_{i_2}, \ldots, O_{i_m}\}$ – множество всех существенных НС, приводящих к снижению системной эффективности КС. Математическое ожидание ущерба, вызываемого i-м НС за время ΔT (например, 1 месяц, 1 полугодие, 1 год и т. п.), можно представить формулой

$$e(O_i, \Delta T) = M[e(O_i) f_i], \; i = \overline{1,m}, \tag{4.1}$$

где $e(O_i)$ – случайная величина ущерба уже случившегося НС при единичном наступлении НС; f_i – случайная величина количества НС i-го вида за время ΔT; m – общее количество всех видов уже свершившихся НС.

Если НС не имеют последствия в том смысле, что ущерб от каждого НС независим, то

$$e(O_i, \Delta T) = M[e(O_i)] M[f_i], i = \overline{1,m}, \tag{4.2}$$

а ущерб для всего множества существенных НС будет определяться с помощью соотношения

$$E(O, \Delta T) = \sum_{i=1}^{m} M[e(O_i)] M[f_i]. \tag{4.3}$$

Алгоритм 1

Шаг 1.1. Для простоты будем рассматривать лишь один вид НС, например, зафиксируем конкретное значение $i = 1$. Далее количественные показатели НС, например, за μ лет сведем в табл. 4.1:

Шаг 1.2. Исходя из данных табл. 4.1, с помощью формулы (4.4) можно получить одну строку данных усредненных помесячных (поквартальных, полугодовых, годовых относительно редких реализаций НС) количественных значений НС по столбцам (табл. 4.2):

$$f_t^{\text{уср}} = \sum_{i=1}^{\mu} f_t^{(i)} / \mu, \quad t = \overline{1,12}. \tag{4.4}$$

Таблица 4.1

Количественные показатели НС, произошедших в течение последних μ лет по месяцам (или по нескольким кварталам, или нескольким полугодиям для редких реализаций НС)

Год	Месяц											
t	1	2	3	4	5	6	7	8	9	10	11	12
1	$f_1^{(1)}$	$f_2^{(1)}$	$f_3^{(1)}$	$f_4^{(1)}$	$f_5^{(1)}$	$f_6^{(1)}$	$f_7^{(1)}$	$f_{18}^{(1)}$	$f_9^{(1)}$	$f_{10}^{(1)}$	$f_{11}^{(1)}$	$f_{12}^{(1)}$
2	$f_1^{(2)}$	$f_2^{(2)}$	$f_3^{(2)}$	$f_4^{(2)}$	$f_5^{(2)}$	$f_6^{(2)}$	$f_7^{(2)}$	$f_{18}^{(2)}$	$f_9^{(2)}$	$f_{10}^{(2)}$	$f_{11}^{(2)}$	$f_{12}^{(2)}$
⋮	…	…	…	…	…	…	…	…	…	…	…	…
μ	$f_1^{(\mu)}$	$f_2^{(\mu)}$	$f_3^{(\mu)}$	$f_4^{(\mu)}$	$f_5^{(\mu)}$	$f_6^{(\mu)}$	$f_7^{(\mu)}$	$f_8^{(\mu)}$	$f_9^{(\mu)}$	$f_{10}^{(\mu)}$	$f_{11}^{(\mu)}$	$f_{12}^{(\mu)}$

Таблица 4.2

Усредненная строка количественных показателей произошедших НС

Год	Месяц											
t	1	2	3	4	5	6	7	8	9	10	11	12
$f_t^{\text{уср}}$	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}

Аналогичные таблицы желательно построить относительно других существенных видов НС, уже реализовавшихся суммарно в течение каждого, например, месяца.

Шаг 1.3. Применительно к усредненным данным (см. табл.4.2) можно построить дискретную линейную стохастическую стационарную модель в форме пространства состояний (ПС) [53, 54] (по методике, изложенной в [53]), следующего вида:

$$x(t+1) = ax(t) + bu(t) + w(t), \quad x(0) = \bar{x}_0, \tag{4.5}$$

$$f^{\text{уср}}(t+1) = x(t+1) + v(t+1), \quad t = \overline{0, N-1}. \tag{4.6}$$

где $x(t)$ – истинное количество НС, произошедших в течение месяца t (нескольких кварталов, нескольких полугодий, нескольких лет относительно реализации редких НС); $u(t)$ – внешнее наблюдаемое управляющее воздействие (на зафиксированный вид) НС в момент времени t; $w(t)$ – белое гауссовское ненаблюдаемое воздействие в момент времени t с нулевым математическим ожиданием и неизвестной дисперсией Q; $x(0)$ – количество НС в начальный момент времени $t = 0$ с математическим ожиданием $\bar{x}_0$ и неизвестной дисперсией $P(0)$; a, b – неизвестные коэффициенты в модели динамики (4.5); t – номер месяца в году (или нескольких кварталов, нескольких полугодий, нескольких лет); $N = 12$ – число месяцев в году; $f^{\text{уср}}(t)$ – наблюдаемое случайное количество НС в течении месяца t (данные из журнала наблюдений компании); $v(t)$ – белая гауссовская последовательность ошибок наблюдений относительно количества НС в течение каждого, например, месяца с нулевым математическим ожиданием и неизвестной дисперсией R.

На данном шаге требуется оценить все дисперсии, связанные с шумами; модели динамики $\hat{Q}$, величины начального состояния $\hat{P}(0)$; измерительной системы $\hat{R}$, по формулам, которые приведены в работе [56].

Шаг 1.4. Оценки коэффициентов в модели динамики (4.5) можно рассчитать на основе метода наименьших квадратов (МНК).

Шаг 1.5. Построенная модель (4.5), (4.6) позволит получить наиболее достоверные оценки количества НС (в режиме реального времени, с помощью уравнений фильтра Калмана), относительно каждого месяца в виде оценок фильтрации [54] за последующий месяц, например, ($\mu+1$), год. Полученные оценки фильтрации должны быть округлены до ближайшего целого.

Шаг 1.6. Оценки фильтрации позволят рассчитать объективные вероятностные оценки реализаций НС. Например, предлагается следующая процедура расчета вероятности конкретного вида НС. Пусть нас интересует вероятность появления НС, например, в каждом месяце предыдущего μ-го года. Для этого подсчитывается общее суммарное количество (для усредненного количества) НС оценок фильтрации в течение всего μ-года ($F^{(\mu)}$), затем фильтрационная оценка количества НС в течение каждого месяца ($f^{(\mu)}(t)$) делится на общую суммарную оценку фильтрационных оценок количества НС ($F^{(\mu)}$) в течение одного μ-года. В результате определяется объективная вероятность реализации конкретного вида НС в течение каждого месяца μ-года и всех 12 месяцев (табл. 4.3):

$$p^{(\mu)}(t) = f^{(\mu)}(t) / F^{(\mu)}, \quad t = \overline{1, 12}, \qquad (4.7)$$

Таблица 4.3

Объективные вероятности реализаций фиксированного вида НС в течение μ о года

Год	Месяц											
t	1	2	3	4	5	6	7	8	9	10	11	12
$p_t^{(\mu)}$	$p_1^{(\mu)}$	$p_2^{(\mu)}$	$p_3^{(\mu)}$	$p_4^{(\mu)}$	$p_5^{(\mu)}$	$p_6^{(\mu)}$	$p_7^{(\mu)}$	$p_8^{(\mu)}$	$p_9^{(\mu)}$	$p_{10}^{(\mu)}$	$p_{11}^{(\mu)}$	$p_{12}^{(\mu)}$

При этом для μ-го года будем иметь:

$$\sum_{t=1}^{12} p^{(\mu)}(t) = 1, \quad \mu = 4, 5, \ldots.$$

Работоспособность алгоритма 1 проиллюстрирована на тестовом примере в работе [56].

4.1.2. ОБЪЕКТИВНАЯ СТОИМОСТНАЯ ОЦЕНКА ПРЕДСКАЗАНИЯ ВЕЛИЧИНЫ УЩЕРБА ОТ НАРУШЕНИЙ БЕЗОПАСНОСТИ ИР

Алгоритм 2

Шаг 2.1. Пусть $O=\{O_i, i=\overline{1,m}\}$ – множество видов НС, приводящих к нарушению безопасности ИР. В разделе 4.1.1. данной работы была предложена процедура расчета оценки помесячной (или поквартальной, или полугодовой и т. д.) объективной вероятности количества нарушений определенного вида атаки на ИР в ИС компании. Предположим, что в отделе информационной безопасности (ИБ) компании имеется статистика относительно ежемесячной оценки ущерба, которая соответствует ежемесячному количеству нарушений ИБ конкретного i-го вида атаки, т. е. значениям данных табл. 4.1 соответствуют значения данных табл. 4.4.

В табл. 4.4 $\left\{S_t^{(i)},\ t=\overline{1,12}, i=\overline{1,\mu}\right\}$ – выходы, которые характеризуют ежемесячные (поквартальные, полугодовые) количества ущерба от НС в ИС условной компании в течение каждого i-го периода квантования.

Таблица 4.4

Количественные ежемесячные (или поквартальные, или полугодовые и т. д.) показатели ущерба от нарушений ИБ в зависимости от i-го вида атаки

Год	Месяц											
t	1	2	3	4	5	6	7	8	9	10	11	12
1	$S_1^{(1)}$	$S_2^{(1)}$	$S_3^{(1)}$	$S_4^{(1)}$	$S_5^{(1)}$	$S_6^{(1)}$	$S_7^{(1)}$	$S_8^{(1)}$	$S_9^{(1)}$	$S_{10}^{(1)}$	$S_{11}^{(1)}$	$S_{12}^{(1)}$
⋮	…	…	…	…	…	…	…	…	…	…	…	…
μ	$S_1^{(\mu)}$	$S_2^{(\mu)}$	$S_3^{(\mu)}$	$S_4^{(\mu)}$	$S_5^{(\mu)}$	$S_6^{(\mu)}$	$S_7^{(\mu)}$	$S_8^{(\mu)}$	$S_9^{(\mu)}$	$S_{10}^{(\mu)}$	$S_{11}^{(\mu)}$	$S_{12}^{(\mu)}$

Шаг 2.2. Заметим, что не всегда ежемесячные (поквартальные, полугодовые относительно нескольких лет) показатели ущерба прямо пропорциональны количеству произошедших НС. Тем не менее на основе данных табл. 4 можно построить линейную дискретную модель в форме ПС, которая будет соответствовать усредненным данным наблюдений по столбцам относительно данных табл. 4.4. Элементы строки усредненных вычисляются с помощью соотношения (см. табл. 4.5):

$$s_t^{(y)} = \left(\sum_{i=1}^{\mu} S_t^{(i)} \right) \Big/ \mu, \quad t = \overline{1,12}. \tag{4.8}$$

Таблица 4.5

Усредненная строка ежемесячных (поквартальных, полугодовых и т. д.) относительно некоторого временного интервала количественных показателей ущерба, нанесенного ИР предприятия

Ущерб	Месяц											
t	1	2	3	4	5	6	7	8	9	10	11	12
$s_t^{(y)}$	$s_1^{(y)}$	$s_2^{(y)}$	$s_3^{(y)}$	$s_4^{(y)}$	$s_5^{(y)}$	$s_6^{(y)}$	$s_7^{(y)}$	$s_8^{(y)}$	$s_9^{(y)}$	$s_{10}^{(y)}$	$s_{11}^{(y)}$	$s_{12}^{(y)}$

Шаг 2.3. На основе строки данных $\left\{ s_t^{(y)},\ t = \overline{1,12} \right\}$ по алгоритмам, описанным в работах [53, 54], можно построить линейную дискретную стохастическую стационарную модель в форме ПС вида

$$s(t+1) = \hat{c} s(t) + \hat{d} + w(t), \quad s(0) = s_0, \ t = \overline{0,11}, \tag{4.9}$$

$$s^{(y)}(t+1) = s(t+1) + v(t+1), \ t = \overline{0,11}. \tag{4.10}$$

При этом сначала на основе данных табл. 4.5 рассчитываются оценки дисперсий шумов модели вида (4.9), (4.10), а именно оценки дисперсий Q, R, $P(0)$ [12].

Шаг 2.4. Далее рассчитываем коэффициенты модели динамики (4.9) с помощью МНК [53, 54].

Шаг 2.5. Предположим, что мы располагаем данными наблюдений количественных показателей ущерба, нанесенных ИР компании в $(\mu+1)$ году (см. табл.4.6), и на основе уравнений фильтра Калмана [10] получаем строку оценок фильтрации (табл. 4.7).

Таблица 4.6

Ежемесячные (поквартальные, полугодовые относительно нескольких лет) количественные показатели ущерба от нарушений ИБ в зависимости от i-го вида атаки в $(\mu+1)$ году

Ущерб	Месяц											
t	1	2	3	4	5	6	7	8	9	10	11	12
$S_t^{(\mu)}$	$S_1^{(\mu)}$	$S_2^{(\mu)}$	$S_3^{(\mu)}$	$S_4^{(\mu)}$	$S_5^{(\mu)}$	$S_6^{(\mu)}$	$S_7^{(\mu)}$	$S_8^{(\mu)}$	$S_9^{(\mu)}$	$S_{10}^{(\mu)}$	$S_{11}^{(\mu)}$	$S_{12}^{(\mu)}$

Используя уравнения фильтра Калмана и данные табл. 4.6, получим последовательность оценок фильтрации $\{\hat{s}(t|t),\ t=\overline{1,12}\}$ относительно ежемесячных более достоверных количественных показателей нанесенного ущерба (табл. 4.7).

Таблица 4.7

Ежемесячные (или поквартальные, или полугодовые и т. д.) относительно нескольких лет) количественные показатели оценок фильтрации нанесенного ущерба в $(\mu+1)$-ом году

Ущерб	Месяц											
t	1	2	3	4	5	6	7	8	9	10	11	12
$\hat{s}(t\|t)$	s_1	s_2	s_3	s_4	s_5	s_6	s_7	s_8	s_9	s_{10}	s_{11}	s_{12}

Шаг 2.6. Используя округленные до ближайших целых чисел данные оценок фильтрации относительно количественных показателей свершившихся НС в течение μ-года по месяцам (или по кварталам, или полугодиям и т. д. относительно нескольких лет) и данные табл. 4.7 относительно оценок фильтрации как количественных показателей ущерба, нанесенного на ИР компании в

μ году, можно получить усредненный ущерб нанесенный от единичного случая свершившегося НС $\{e(t),\ t=\overline{1,12}\}$. Для этого необходимо данные табл. 4.7 разделить на соответствующие, округленные до целого, элементы строки данных количества реализации НС. Расчетные данные можно свести в табл. 4.8.

Таблица 4.8

Усредненный нанесенный ущерб от единичного случая свершившегося НС

Ущерб	Месяц											
t	1	2	3	4	5	6	7	8	9	10	11	12
$e(t)$	e_1	e_2	e_3	e_4	e_5	e_6	e_7	e_8	e_9	e_{10}	e_{11}	e_{12}

Шаг 2.7. Предсказывая количество НС ($f_i^{\text{пр}}$) i-го вида с помощью соответствующей модели в форме ПС и соответствующего усредненного ущерба от единичного случая свершившегося НС, по данным табл. 4.8 можно получить оценку предсказания величины ущерба, который будет нанесен компании в t-й месяц (или квартал, или полугодие и т. д. относительно нескольких лет) (μ+1) (текущего) года.

Работоспособность алгоритма 2 проиллюстрирована на тестовом примере в работе [56].

4.1.3. ГРУППЫ КОНТРОЛЕЙ БЕЗОПАСНОСТИ

Меры безопасности (контроли безопасности), применяемые в компании для защиты ИР ИС, можно подразделить на три основные группы: технические, операционные и управленческие [50]. Группы, в свою очередь, разбиваются на семейства. Перечислены эти меры безопасности в стандарте [57].

В группу *управленческих контролей* входят меры безопасности для ИС, которые направлены на управление рисками и ИБ ИС. Группа содержит пять семейств контролей [50, 57]. В группу *операционных контролей* входят меры безопасности для ИС, которые, прежде всего,

реализуются и корректируются людьми. В группу входят девять семейств контролей [50, 57]. В группу *технических контролей* входят меры безопасности для ИС, которые прежде всего реализуются через действия в аппаратных средствах, в программном обеспечении или микропрограммных компонентах системы. В группу входят четыре семейства контролей [50, 57].

Эксперты, которые проводят оценки, могут иметь различную профессиональную подготовку, например: техническую, финансовую, инженерную и управленческую, свое собственное индивидуальное восприятие, отношение и побуждение в определении ущерба от количества реализованных НС. Поэтому перед началом расчета величины риска и ИБ в ИС компании необходимо всем экспертам ознакомиться со всеми объективными оценками предсказания и фильтрации относительно ежемесячных (или поквартальных, или полугодовых относительно нескольких лет) количеств НС и ущерба от реализованных НС, которые позволят им наиболее реалистично предлагать собственные экспертные оценки.

Процедура оценки риска на основе экспертных оценок организована с помощью следующих шести этапов [50]: характеристика системы; идентификация угроз и уязвимостей; оценка вероятности; анализ последствия; определение риска и рекомендации по управлению.

Теперь рассмотрим методику расчета риска по предложенной выше методике.

4.2. МЕТОДИКА РАСЧЕТА ОБЪЕКТИВНЫХ ОЦЕНОК ПРЕДСКАЗАНИЯ КОЛИЧЕСТВА НС ДЛЯ ВНЕШНЕЙ НЕКОНТРОЛИРУЕМОЙ ЗОНЫ

Надо полагать, что в случае внешней неконтролируемой зоны количество НС относительно НСД в ИР КС даже в течение полугода составляет в пределах 0...5. Для того чтобы построить дискретную линейную стохастическую стационарную модель в форме ПС с двумя неизвестными коэффициентами, необходимо иметь в четыре-пять раз больше данных наблюдений, чем количество неизвестных коэффициентов. В связи с этим мы должны растянуть весь временной интервал квантования, относительно сбора достаточного количества

НС на 4...5 лет при условии, что объем выборки количества НС составляет не менее 8...10 ($N = 0$). При этих предположениях интервал времени между наблюдения будем брать не менее полугода.

Рассмотрим реализацию алгоритма 1 на численном примере.

1. Пусть одна реализация в виде временного ряда (ВР) наблюдений в течение 5 лет составляет $N = 10$. С целью повышения качества данных относительно анализа количественных показателей НС возьмем число ансамблей реализации равным, например, $k = 6$ и сведем эти данные в табл. 4.9 [58]. Все данные в табл. 4.9 смоделированы на основе использования равномерного закона распределения с использованием ограничений на количество НС до 5, а также с использованием процедуры округления до целого числа.

Таблица 4.9

Смоделированные шесть ВР с объемом выборки $N = 10$ в виде данных относительно количественных показателей НС

№ п/п (i)	Общее количество полугодий									
	1-й год		2-й год		3-й год		4-й год		5-й год	
	1	2	3	4	5	6	7	8	9	10
$y_1(i)$	3	2	4	2	2	4	2	2	5	0
$y_2(i)$	2	2	0	2	5	2	4	2	2	2
$y_3(i)$	2	2	4	3	4	5	2	4	4	4
$y_4(i)$	4	2	1	2	2	4	2	0	0	2
$y_5(i)$	2	2	1	4	1	2	1	1	2	1
$y_6(i)$	2	2	2	2	4	2	1	3	2	2

2. Для $k = 6$ ансамблевых реализаций рассчитаем усредненные величины количества НС по столбцам. Получим усредненный ВР, соответствующий количеству НС за каждое полугодие в течение 5 лет [58]. Данные сведены в табл. 4.10:

Таблица 4.10

Усредненный ВР, с объемом выборки $N=10$, характеризирующие количественные показатели НС

№ п/п (i)	Общее количество полугодий									
	1	2	3	4	5	6	7	8	9	10
	1-й год		2-й год		3-й год		4-й год		5-й год	
$\bar{y}(i)$	2.500 0	2.000 0	2.000 0	2.500 0	3.000 0	3.166 7	2.000 0	2.000 0	2.500 0	1.833 3

3. Строим дискретную линейную стохастическую стационарную модель в форме ПС на основе усредненных данных. Коэффициенты модели, рассчитанные с помощью МНК, приняли следующие значения: $a = 0.2233$; $b = 1.7958$ [10].

4. На основе рекуррентных формул, приведенных в работе [59], рассчитываем дисперсии шумов модели динамики Q, начального состояний $P(1)$ и шумов измерительной системы R на основе усредненных данных ВР $\{\bar{y}(i), \overline{1, N}\}$. После расчетов дисперсии принимают следующие значения:

$$Q = 0.0982;\ P(1) = 0.0982;\ R = 0.1013.$$

5. Расчетные переменные в пунктах 3 и 4 позволили на основе уравнений фильтра Калмана рассчитать оценки предсказаний и соответственно оценки фильтрации относительно, количества НС с интервалом упреждения на полгода, в течение предшествующего года.

Таблица 4.11

Рассчитанные оценки предсказания и соответствующие оценки фильтрации в предшествующем году

№ п/п (i)	Общее количество полугодий									
	1-й год		2-й год		3-й год		4-й год		5-й год	
	1	2	3	4	5	6	7	8	9	10

x(i+1)	2.5	2.354	2.282	2.274	2.33	2.391	2.417	2.289	2.274	2.329
x(i)	2.5	2.176	2.14	2.388	2.67	2.783	2.207	2.143	2.388	2.079
x(i)	2.5	2.000	2.000	2.500	3.00	3.167	2.000	2.000	2.500	1.833

На рисунке построены графики, отражающие изменения значений количества НС на основе значений ВР относительно реальных (z), предсказанных (*XP*) и фильтрационных оценок (*XF*)

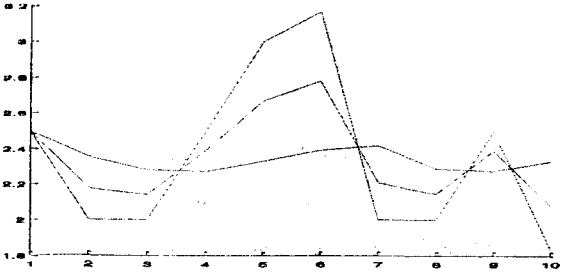

Рис. 4.1. Графики, построенные на основе реальных (*z*), предсказанных (XP) и фильтрационных оценок XF)

6. Рассчитываем оценки фильтрации, округленные до ближайшего целого. Результаты расчета сведены в табл. 4.12.

Таблица 4.12

Рассчитанные оценки предсказания и соответствующие оценки фильтрации в предшествующем году

№ п/п (*i*)	Общее количество полугодий									
	1-й год		2-й год		3-й год		4-й год		5-й год	
	1	2	3	4	5	6	7	8	9	10
V x(i|i)	2.5	2.176	2.14	2.388	2.67	2.783	2.207	2.143	2.388	2.079
x/c	3	2	2	2	3	3	2	2	2	2
p/f	0.13	0.087	0.087	0.087	0.13	0.13	0.087	0.087	0.087	0.087

В таблице *xfc* – n-вектор оценок фильтрации, округленных до ближайшего целого.

7. Рассчитаем объективные вероятностные оценки реализации НС предыдущего года на основе алгоритма 1, шаг 1.6 *pf* – n-вектор объективных полугодовых вероятностей (см. последнюю строку табл. 4.12).

8. Используем фильтрационные оценки для предсказания количества инцидентов на первое полугодие $(\mu+1)$-й реализации Для этого рассчитаем коэффициенты уравнения линейной аппроксимации μ-й реализации на основе фильтрационных оценок в виде ВР с объемом выборки $N=10$: XF = [2.5 2.1755 2.1396 2.3878 2.6674 2.7825 2.2067 2.1430 2.3882 2.0790]. В результате расчетов получим следующие оценки: $a = 0.2385$; $b = 1.7631$.

9. На основе уравнений фильтра Калмана получим следующую оценку предсказания: $XP^{(i+1)}(1) = 2.3541$. Далее на основе очередного наблюдения $z^{(i+1)}(1) = 5$ можно рассчитать оценку фильтрации $XF^{(i+1)}(1) = \quad = 3.6887$. Далее мы можем рассчитать оценку предсказания на следующее полугодие: $XP^{(i+1)}(2) = 2.6195$. На основе соответствующего наблюдения $z^{(i+1)}(2) = 2$ можем рассчитать оценку фильтрации $XF^{(i+1)}(2) = 2.307$ и т. д.

4.3. МЕТОДИКА РАСЧЕТА ОБЪЕКТИВНОЙ СТОИМОСТНОЙ ОЦЕНКИ ПРЕДСКАЗАНИЯ ВЕЛИЧИНЫ УЩЕРБА ОТ НАРУШЕНИЙ БЕЗОПАСНОСТИ ИР

Апробация алгоритма 2 на численном примере.

1. Пусть $O = \{O_i, i = \overline{1,m}\}$ – множество видов НС, приводящих к нарушению безопасности ИР, из которых выбираем один существенный вид. В разделе 4.1.1 была предложена процедура расчета оценки полугодовой объективной вероятности количества нарушений определенного вида атаки на ИР в ИС предприятия. Предположим, что в отделе ИБ компании имеется статистика

полугодовой усредненной оценки ущерба в зависимости от реализации единичного инцидента, т. е. значениям данных табл. 4.1 соответствуют значения данных табл. 4.4 при условии, что усредненный ущерб от реализации единичного ущерба составляет $x = 21$ у.е. Тогда табл. 4.4 будет соответствовать табл. 4.13.

Таблица 4.13

Смоделированные $k = 6$ ВР с объемом выборки $N = 10$ в виде данных количественных показателей ущерба соответствующие количеству НС из таблицы 4.9

№ п/п (i)	Общее количество полугодий									
	1-ый год		2-ой год		3-ий год		4-ый год		5-ый год	
	1	2	3	4	5	6	7	8	9	10
$s_1^{(y)}$	63	42	84	42	42	84	42	42	105	0
$s_2^{(y)}$	42	42	0	42	105	42	84	42	42	42
$s_3^{(y)}$	42	42	84	63	84	105	42	84	84	84
$s_4^{(y)}$	84	42	21	42	42	84	42	0	0	42
$s_5^{(y)}$	42	42	21	84	21	42	21	21	42	21
$s_6^{(y)}$	42	42	42	42	84	42	21	63	42	42

2. На основе данных $\left\{s_i^{(y)},\ i=\overline{1,10}\right\}$ (табл. 4.14) по алгоритмам, описанным в работах [53, 56], можно построить дискретную линейную стохастическую стационарную модель в форме ПС вида

$$s(t+1)=\hat{c}\cdot s(t)+\hat{d}\cdot+w(t),\quad s(0)=s_0,\quad t=\overline{0,11}, \tag{4.11}$$

$$s^y(t+1)=s(t+1)+v(t+1),\quad t=\overline{0,11}. \tag{4.12}$$

Таблица 4.14

Усредненная строка полугодовых за пять лет и шесть реализаций количественных показателей ущерба, нанесенного ИР предприятия, исходя из данных таблицы 4.13

t	1	2	3	4	5	6	7	8	9	10
$s_i^{(y)}$	70,83	42	42	70,83	63	66,5	42	42	70,83	42

Рассчитываем коэффициенты модели динамики (4.11): $\hat{c} = 0.1736, \hat{d} = 45.0051$.

3. На основе данных табл. 4.14 с объемом выборки $N = 10$ рассчитываются оценки дисперсий шумов модели вида (4.11), (4.12). Расчеты дали следующие оценки дисперсий: $Q = 88.4390$; $R = 56.7539$; $P(0) = 88.4390$.

4. Предположим, что мы располагаем исходными данными наблюдений количественных показателей ущерба, нанесенного ИР компании в $(\mu+1)$ году, и последовательно корректируем два полугодия с начальным условием в виде фильтрационной оценки $XF(1|1) = XF(1) = z(1) = 42$ на основе реальных наблюдений за два полугодия $z(2)$, $z(3)$ при помощи уравнений фильтра Калмана. В результате получаем последовательно сначала полугодовую оценку предсказания ущерба $XP(2|1) = 52.2963$ и с учетом реального наблюдения ущерба $z(2) = 45$ рассчитываем соответствующую оценку фильтрации ущерба $XF(2|2) = 47.8006$.

Для второго полугодия за начальное условие мы примем $XF(2|2) = 47.8006$. Используя это начальное условие, мы можем рассчитать оценку предсказания на второе полугодие $XP(3|2) = 53.3033$. Далее, получив на момент времени $t = 3$, наблюдение $z(3) = 54$, мы сможем рассчитать оценку фильтрации $XF(3|3) = 53.7326$, используя которую, мы можем корректировать оценку предсказания на основе объективного наблюдения.

5. Используя уравнения фильтра Калмана и данные табл. 4.15, получим последовательность оценок фильтрации $\{\hat{s}(t|t), t = \overline{1,12}\}$

относительно полугодовых более достоверных количественных показателей нанесенного ущерба (табл. 4.16).

Таблица 4.15

Полугодовые количественные показатели ущерба от нарушений ИБ в зависимости от i-го вида атаки в $(\mu+1)$ году

t	1	2	3	4	5	6	7	8	9	10	11	12
$S_t^{(\mu)}$	$S_1^{(\mu)}$	$S_2^{(\mu)}$	$S_3^{(\mu)}$	$S_4^{(\mu)}$	$S_5^{(\mu)}$	$S_6^{(\mu)}$	$S_7^{(\mu)}$	$S_8^{(\mu)}$	$S_9^{(\mu)}$	$S_{10}^{(\mu)}$	$S_{11}^{(\mu)}$	$S_{12}^{(\mu)}$

Таблица 4.16

Полугодовые количественные показатели оценок фильтрации нанесенного ущерба в $(\mu+1)$ году

t	1	2	3	4	5	6	7	8	9	10	11	12
$\hat{s}(t \mid t)$	s_1	s_2	s_3	s_4	s_5	s_6	s_7	s_8	s_9	s_{10}	s_{11}	s_{12}

6. Используя округленные до ближайших целых чисел данные оценок фильтрации количественных показателей свершившихся НС в течение $(\mu+1)$ года по месяцам, и данные табл. 4.7, можно получить усредненный ущерб, нанесенный от единичного случая свершившегося НС $\{e(t),\ t=\overline{1,12}\}$. Для этого необходимо данные табл. 4.7 разделить на соответствующие, округленные до целого элементы строки данных количества реализации НС (см. табл. 4.2). Расчетные данные можно свести в табл. 4.17.

Таблица 4.17

Усредненный нанесенный ущерб от единичного случая свершившегося НС

t	1	2	3	4	5	6	7	8	9	10	11	12
$e(t)$	e_1	e_2	e_3	e_4	e_5	e_6	e_7	e_8	e_9	e_{10}	e_{11}	e_{12}

7. Предсказывая количество НС $\left(f_i^{\text{пр}}\right)$ i-го вида с помощью соответствующей модели в форме ПС и соответствующего усредненного ущерба по данным табл. 4.17, можно получить оценку предсказания величины ущерба, который будет нанесен предприятию в t-е полугодие относительно $(\mu+2)$ реализации.

Работоспособность методики по алгоритму 2 проиллюстрирована на тестовом примере, а также в работе [59].

4.4. ЗОНЫ КОНТРОЛИРУЕМОЙ ТЕРРИТОРИИ, ПОМЕЩЕНИЙ ААС, РЕСУРСОВ ААС, БАЗ ДАННЫХ

В настоящем разделе рассмотрим все упомянутые выше зоны контролируемой территории, помещений ААС, ресурсов ААС, баз данных. Как уже говорилось выше, все компьютерные преступления можно условно разбить на три класса: перехват информации; несанкционированный доступ; «манипуляция данными». Все классы можно рассматривать поразделью.

Относительно оставшихся четырех зон, используя методику, описанную в разделах 4.1.1–4.1.3, можно на основе данных наблюдений, рассчитать оценки предсказаний и оценки фильтраций количества НС, а также соответствующие оценки ущербов, которые могут быть нанесены конкретным компаниям.

Теперь пусть на условной компании, для которой мы оцениваем риски, существует три ИС: ИС-1, ИС-2, ИС-3. Экспертами после ознакомления с результатами объективных оценок были обнаружены определенные уязвимости и угрозы, относящиеся к различным семействам контролей. (Исходные данные и численные расчеты отображены в работе [59]). Требуется провести расчеты экспертных оценок для усвоения описанной выше методики.

После ранжирования ИС по уровню риска в порядке убывания получили следующие расчетные данные (табл. 4.18).

Таблица 4.18

Ранги информационных систем

Информационная система	ИС-2	ИС-3	ИС-1
Уровень риска	0,224	0,217	0,213

Из табл. 4.18 видно, что ИС-2 получает самый высокий уровень риска. Значит, вероятность реализации угроз и ущерба для этой системы больше, чем для остальных систем. Поэтому руководителям организации в первую очередь необходимо обратить внимание на безопасность ИС-2.

4.5. АНАЛИЗ И КЛАССИФИКАЦИЯ ПОТЕНЦИАЛЬНО ВОЗМОЖНЫХ НСД К ИНФОРМАЦИИ В ЗОНЕ ИР ААС

Мы уже привыкли к постоянному поиску новых информации, использованию этих новых информации и наблюдению за активным развитием сети Интернет, как источника накопления данных преимущественно неструктурированной информации. Поэтому задача автоматизации процессов структурирования информации, формализации потоков знаний, формализации и оптимизации обработки неблагоприятных событий (НС), происходящих в компьютерной системе (КС), а также автоматизированной и автоматической обработки с использованием методов инженерии знаний, расчетов предсказания количества НС (инцидентов) и количества ущербов как последствие реализованных НС. Отметим, что почти все предприятия широко используют различные вычислительные сети для продвижения услуг с интеллектуальными свойствами относительно программных продуктов поиска клиентов для заключения договоров и оплаты предоставленных информационных продуктов, сервисов и товаров. При этом одним из подходов к формализации компактного представления информации, знаний, оперативного поиска необходимой информации в режиме реального времени (РРВ) является онтологический подход с элементами интегрированного представления [60]. Онтологически управляемая информационная система (ОУИС) состоит из информационных ресурсов (ИР), интеллектуальных пакетов прикладных программ (ИППП), баз данных, баз знаний, пользовательских интерфейсов. При этом ОУИС играет центральную роль влияя на пользовательские интерфейсы, ИР, ИППП, базы данных, базы знаний и т.п.

Систематизация, формализация экспоненциально возрастающих объемов разнородных данных, знаний, разнородных обучающих тренажеров электронного обучения широко использующиеся в разных целях. Формализация запросов пользователей, распознающих различные виды НС, целей, различные методики эффективного представления информации, методы их обработки, хранения, которые имеют большую актуальность в деятельности человека. Различные виды информации, области знаний требуют новые своеобразные

классификации, новые интеллектуальные и быстрые типы запросов в РРВ, новые типы задач по защите всевозможных видов ИР. Заметим, что ИР характеризуются различными уровнями структурированности, расплывчатостью, различными видами воздействующих на ИР шумов, различными способами формализации, описания и распознавания корпуса текстов инцидентов, запросов пользователей, формата ключевых слов, терминов, понятий. Увеличение объема информации, числа людей занятых в сфере интеллектуальной деятельности потребовали создания надежного средства сбора, обработки, хранения, передачи информации в различных форматах ее представления. Повышается актуальность вопроса перевода разнородных информаций в знания, с последующим применением их для принятия тех или иных управленческих решений [61].

Интеллектуальная защита информаций хранимых и накапливаемых в репозитории ОУИС приводит к постановке и решению задач разработки комплексных систем: связей информаций; баз знаний; указаний; ссылок; решаемых и обрабатываемых на основе автоматических и автоматизированных систем (ААС); компьютерно читаемых терминов; понятий; словарей; методик обработки ИР [62, 56]; предсказания, фильтрации количества реализованных НС (в различных территориальных зонах [64]); последствий реализованных НС в форме количества ущербов. Количественные оценки НС сильно зависят от: мотивации, квалификации, навыков, уровня знаний злоумышленников, типового автоматического и автоматизированного рабочего места, факторов условий эксплуатации ИР из ААС, органов зрения, слуха, усталости, эмоциональной напряженности, изменений в психике, снижении активности, загазованности, запыленности, освещенности, шума, вибрации, заболеваемости сердечно-сосудистой системы, заболеваемости опорно-двигательного аппарата и т.д.

4.5.1. Характеристика знаний и навыков злоумышленников

В настоящее время статус занимаемый злоумышленниками, характеризуются прежде всего знаниями, опытом на уровне сетевого и телекоммуникационного сертифицированного специалиста информационной безопасности (Certifed Information System Security Professional (CISSP)) [65]. В телекоммуникационных сетях есть хотя

бы один компьютер, имеющий прямое подключение к Интернету. Взлом такого компьютера ставит под угрозу безопасность всей сети, которая оперативно используется для моментального доступа к данным. При этом некоторые данные представляют собой информацию конфиденциального характера, а иногда и государственную тайну [50, 56, 66]. Злоумышленник - это специалист по взлому и тестированию защищенной интеллектуальной информационной системы (ИИС). Тестирование осуществляется на предмет: проникновения в содержание ИР, краж информации, модификации ИР и т. д. Такой специалист хорошо понимает базовые концепции построения компьютерных сетей, знает назначения и принципы работы основных сетевых протоколов, четко представляет себе назначения компонентов компьютерной сети и сетевых средств защиты, таких как: коммутатор, маршрутизатор, межсетевой экран, системы обнаружения и предотвращения вторжений и т. п. Взлом ИИС осуществляется для выявления уязвимостей ИР с целью нарушения запланированного функционирования алгоритма в ИИС. Злоумышленники также обладают знаниями и навыками как эксперт по информационной безопасности, обладающий навыками взлома ОУИС для выявления уязвимостей на уровнях "Белой шляпы" (White hat), "Серой шляпы" (Grey hat), "Черной шляпы" (Black hat) [65].

Основная цель злоумышленников является получение доступа к определенной информации. Собрав информацию злоумышленник проникает на территории зон ИР ААС, где находятся ИР содержащие желаемую информацию. Злоумышленник с помощью психологических приемов старается спровоцировать сотрудника соответствующей организации раскрыть местонахождение ИР и определить уязвимости интересующего ИР. Уязвимость ИР при этом понимается как недостаток, позволяющий угрозе реализоваться (например, в работе [68] излагается информация с существенными различиями классификации и реестров уязвимостей ИР в ОУИС). Для взлома ОУИС нужна информация о возможностях программных решений, позволяющих найти пути для проникновения в конкретные ИР и узнать версию программного продукта. После того, как ИИС взломана у злоумышленника появляется канал к получению необходимой информации (КПНИ).

Еще одним из видов злонамеренных действий на ИИС является так называемые DoS, DDoS и DRDoS [62] атаки. Атаки типа "отказ в обслуживании", основанные на отражении и усилении трафика, остаются одной из наиболее актуальных проблем в сфере компьютерной безопасности. Эти виды атак связаны с отправкой или больших объемов трафика, или запросов из различных источников на целевые узлы ИИС [50, 62]. Этот вид атак приводит ИИС осуществлять обработку большого объема данных и выделять соответствующие ресурсы. Затем выполняется медленная передача данных и используются реестры компьютерной системы дольше, чем необходимо.

4.5.2. Постановка задачи. Анализ и классификация территориально, потенциально возможных несанкционированных доступов к информации в зонах ресурсов ААС

Территориально и потенциально возможные несанкционированные доступы (НСД) к информации могут иметь место в различных зонах ААС [64]. При этом для КНПИ необходимо одновременное наступление следующих событий: злоумышленник должен получить доступ в соответствующую зону; во время прохождения злоумышленника в зону, в ней должен появиться соответствующий КНПИ; проявившийся КНПИ должен быть доступен злоумышленнику соответствующей категории CISSP, а также навыками, чтобы очень быстро (в течении 1 минуты), воспользоваться КНПИ и в момент доступа к нему нарушителя должна находиться защищаемая информация.

Известно, что все компьютерные преступления можно условно разбить на три класса: перехват информации; несанкционированный доступ; «манипуляция данными». Это электромагнитный перехват, например: регистрация излучений, создаваемых процессором, принтером, монитором; непосредственный перехват, прямое подключение к каналам передачи данных. Это незаконное подключение к линии законного пользователя; вид преступления, который называется «абордаж» - это когда «компьютерные пираты» проникают в чужие ИИС путем угадывания их кода. Это

«Манипуляция данными или метаданными» которые характеризуются как вид преступления: вариант изменения кода для подмены данных или метаданных; вид «троянский конь» - тайное введение в чужую программу таких команд, которые позволяют осуществлять новые, не планируемые пользователем программные функции с сохранением прежней работоспособности; компьютерные вирусы, действующие по принципу, например, сотри все данные или метаданные этой программы, перейди в следующую и сделай то же самое. Они обладают свойством переходить через коммуникационные сети из одной системы в другую, распространяясь как вирусное заболевание и т.п.

Для последующих действий составим список видов НС, возникающих в ИИС и приводящих к снижению системной эффективности функционирования КС. Пусть этот список представляет собой множество видов НС $\{O_1, O_2, \ldots, O_m\}$. Выделим из этого множества некоторое существенное подмножество некоторых видов НС, приводящих к ощутимому нарушению безопасности ИР в КС. Это подмножество обозначим через $\tilde{O} = \{O_{i_1}, O_{i_2}, \ldots, O_{i_m}\}$, например, O_{i_1} – количество НС относительно нарушения запуска отдельных узлов КС; O_{i_2} – количество НС относительно неверного набора информации применительно к конкретному информационному процессу и обработке данных и т.п.

После построения подмножества $\tilde{O}$ переходим к анализу свойств элементов подмножества на основе количественных показателей НС и соответственно величины ущерба, имевшей место в прошлом. Математическое ожидание ущерба, вызываемого i-м НС за время ΔT (например, 1 месяц, 1 полугодие и т.п.), можно представить формулой:

$$e(O_i, \Delta T) = M[e(O_i) \cdot f_i], i = \overline{1,m},$$

где $e(O_i)$ – случайная величина ущерба уже случившегося НС при единичном наступлении НС; f_i – случайная величина количества,

заметно ощутимых, существенных, НС i-го вида за время ΔT; m – общее количество всех видов уже свершившихся НС.

Если НС не имеют последствия в том смысле, что ущерб от каждого НС независим, то

$$e(O_i, \Delta T) = M[e(O_i)] \cdot M[f_i], \quad i = \overline{1,m},$$

а ущерб для всего множества существенных НС будет определяться с помощью соотношения

$$E(\tilde{O}, \Delta T) = \sum_{i=1}^{m} M[e(O_i)] \cdot M[f_i].$$

На основе выше описанных условий характеристик функционирования ОУИС требуется разработать методику расчета объективных оценок количества реализованных НС и нанесенного ущерба от реализовавшихся НС, в отмеченных выше зонах.

4.5.3. Методика расчета взаимосвязанных объективных и экспертных оценок количества НС и нанесенного ущерба от реализовавшихся НС в зонах ААС

1. Для простоты будем рассматривать лишь один i-ый вид НС, например, зафиксируем конкретное значение i=1. Далее, сведем в таблицу количественные показатели НС, например, за μ лет.

2. Исходя из данных (см. п.4.5.1), с помощью формулы (4.13) можно получить одну строку данных усредненных помесячных (или полугодовых относительно редких реализаций НС) количественных значений НС по столбцам (строку данных в виде временного ряда):

$$f_i^{уср} = \sum_{i=1}^{\mu} f_i^{(i)} / \mu, \quad t = \overline{1,12}. \qquad (4.13)$$

3. Применительно к усредненным данным или метаданным (см. п.2) можно построить линейную стохастическую стационарную модель в форме пространства состояний (ПС) [51], по методике, изложенной в [56], следующего вида:

$$x(t+1) = a \cdot x(t) + b \cdot u(t) + w(t), \quad x(0) = x_0, \qquad (4.14)$$

$$f^{уср}(t+1) = x(t+1) + v(t+1), \quad t = \overline{0, N-1}. \qquad (4.15)$$

где $x(t)$ – истинное количество НС, произошедших в течение месяца t (нескольких полугодий и т.п.); $u(t)$ – внешнее наблюдаемое (внешнее управляющее воздействие) в момент времени t; $w(t)$ – белое гауссовское ненаблюдаемое воздействие в момент времени t с нулевым математическим ожиданием и неизвестной дисперсией Q; $x(0)$ – количество НС в начальный в момент времени $t=0$ с математическим ожиданием x_0 и неизвестной дисперсией $P(0)$; a, b – неизвестные коэффициенты, входящие в модель динамики (2); t – номер месяца в году (нескольких полугодий и т.п.); объем выборки $N = 12$ – число месяцев (или полугодий в течении интервала времени ΔT наблюдения); $f^{y\phi}(t)$ – наблюдаемое случайное количество реализации НС в течении времени ΔT наблюдения (например, данные из журнала наблюдений предприятия); $v(t)$ – белая гауссовская последовательность ошибок наблюдений относительно количества НС в течение каждого ΔT, например, месяца с нулевым математическим ожиданием и неизвестной дисперсией R.

На данном шаге методики требуется оценить все дисперсии шумовых аддитивных компонентов, входящих в модель (4.14), (4.15) связанные с шумами: измерительной системы $\hat{R}_1$; модели динамики $\hat{Q}_1$ и величины начального состояния $\hat{P}_1(0)$, рассчитываемые по рекуррентным формулам, которые изложены в работе [51].

4. Оценки коэффициентов, входящие в модель динамики (2) можно рассчитать на основе метода наименьших квадратов (МНК) [59].

5. Построенная модель в форме ПС (4.14), (4.15) позволит получить наиболее достоверные оценки количества НС в РРВ с помощью аппарата фильтра Калмана [71], относительно каждого месяца (или полугодия и т.п.) в виде оценок фильтрации за последующий, например, (μ+1) год. Полученные оценки фильтрации должны быть округлены до ближайшего целого.

6. Оценки фильтрации (п. 4.5) позволят рассчитать объективные вероятностные оценки реализаций НС. Например, предлагается

следующая процедура расчета вероятности для конкретного i-того вида НС.

Пусть нас интересует вероятность появления НС, например, в каждом месяце предыдущего μ-го года. Для этого подсчитывается общее суммарное количество (для усредненного количества) НС оценок фильтрации в течение всего μ-года ($F^{(\mu)}$), а затем фильтрационная оценка количества НС в течении каждого месяца ($f^{(\mu)}(t)$) делится на общую годовую суммарную оценку фильтрационных оценок количества НС ($F^{(\mu)}$) в течении одного μ-года, которая определяется по формуле:

$$p^{(\mu)}(t) = f^{(\mu)}(t) / F^{(\mu)}, \quad t = \overline{1,12}, \tag{4.16}$$

где $p_t^{(\mu)} = p^{(\mu)}(t)$ – объективная вероятность реализаций конкретного i-того вида фильтрационного количества НС в течение каждого месяца μ-года для всех 12 месяцев. При этом для μ-го года будем иметь следующее соотношение: $\sum_{t=1}^{12} p^{(\mu)}(t) = 1, \quad \mu = 1, 2, 3, \ldots.$

После расчетов количества НС в КС сразу возникает потребность расчета количественной величины ущерба, которая может характеризовать истинную картину последствий реализации НС. Поэтому с помощью адаптации алгоритма описанного выше, относительно количества НС, можно осуществить расчет величины ущерба. Подобный вариант алгоритма описан и апробирован в деталях в работе [56], относительно контролируемой зоны предприятия [55].

Меры безопасности (контроли безопасности), применяемые для организации защиты ИР в ОУИС предприятия, можно поделить на три основные группы [50]: технические, операционные и управленческие. Группы в свою очередь разбиваются на семейства. Перечислены эти меры безопасности в стандарте, которые описаны в работе [57].

Эксперты, которые проводят оценку защищенности ОУИС предприятия, могут приходить с различной профессиональной

подготовкой, например: технической, финансовой, инженерной и управленческой, со своими собственными индивидуальными восприятиями, отношениями и побуждениями в определении ущерба от количества реализованных НС. Поэтому перед началом расчета величины риска ИБ в ОУИС предприятия на основе экспертных оценок, всем экспертам необходимо ознакомиться со всеми объективными оценками предсказания и фильтрации относительно ежемесячных (или полугодовых и т.п.) количеств НС и ущерба от реализованных НС. Ознакомление с объективными оценками позволят экспертам наиболее реалистично предлагать и рассчитывать экспертные оценки.

Процедура оценки риска на основе экспертных оценок организована, детально описана и апробирована на реальных данных, с помощью следующих шести этапов в работе [10]: характеристика системы; идентификация угроз и уязвимостей; оценка вероятности; анализ последствия; определение риска; рекомендации по управлению.

4.6. ОЦЕНКИ УЯЗВИМОСТИ ИНФОРМАЦИИ, ОБРАБАТЫВАЕМОЙ В ААС

С учетом описанной методики расчета количества НС и соответствующих оценок наносимого ИР в ИС ущерба можно вывести формулу для оценки уязвимости информации, обрабатываемой в ААС. Для этого можно ввести, например [55], следующие показатели: $P_{ikl}^{(d)}$ – вероятность доступа злоумышленника k-й категории в l-ю зону; $P_{ijl}^{(k)}$ – вероятность наличия (проявления) j-го КНПИ в l-ой зоне i-го компонента ААС; $P_{ijkl}^{(n)}$ вероятность доступа нарушителя k-й категории к j-му КНПИ в l-й зоне i-го компонента ААС при условии доступа нарушителя в l-зону; $P_{ijl}^{(n)}$ – вероятность доступа нарушителя k-й категории к j-му КНПИ в l-й зоне i-го компонента ААС при условии доступа нарушителя в l-ю зону;

$$P_{ijkl} = P_{ikl}^{(d)} P_{ijl}^{(k)} P_{ijkl}^{(n)} P_{ijl}^{(n)}, \qquad (4.17)$$

– вероятность НСД в одном компоненте ААС одним злоумышленником одной категории по одному КНПИ назовем базовым показателем уязвимости информации (с точки зрения НСД). С учетом (4.16) выражение для базового показателя будем иметь вид:

$$P_{ijk}^{(b)} = 1 - \prod_{l=1}^{5} [P_{ijkl}] = 1 - \prod_{l=1}^{5} \left[P_{ikl}^{(d)} P_{ijl}^{(k)} P_{ijkl}^{(n)} P_{ijl}^{(n)} \right]. \qquad (4.17)$$

Рассчитанные таким образом базовые показатели уязвимости сами по себе имеют ограниченное практическое значение. Для решения задач, связанных с разработкой и эксплуатацией систем защиты информации, применяют обобщенные показатели уязвимости, обобщенные по какому-либо индексу (i, j, k) или по их комбинации. Например,

$\{K^*\}$-интересующее нас подмножеество из множества потенциально возможных нарушителей, или $\{l^*\}$, $\{J^*\}$ – подмножество компонентов ААС и КНПИ. Тогда в общем случае общий показатель уязвимости будет определяться как:

$$P_{(I^*)(J^*)(K^*)} = 1 - \prod_{\forall i} \left[1 - P_{ijkl}^{(b)} \right] \prod_{\forall j} \left[1 - P_{ijkl}^{(b)} \right] \prod_{\forall k} \left[1 - P_{ijkl}^{(b)} \right]. \qquad (4.18)$$

Необходимо также рассмотреть метод расчёта показателя уязвимости с учетом интервала времени, на котором оценивается уязвимость. При этом следует учитывать, что чем больше интервал времени, тем больше возможностей у нарушителя для злоумышленных действий и тем больше вероятность изменения состояния АС. Можно определить такие временные интервалы (не сводимые к точке), на которых процессы, связанные с нарушением защищенности, были бы однородными. Назовем эти интервалы малыми. Такой малый интервал, в свою очередь, может быть разделён на очень малые интервалы, уязвимость информации на каждом из которых определяется независимо от других. Зависимость на каждом из выделенных интервалов будет одинакова в силу однородности происходящих процессов уязвимости. Тогда через P_t^m обозначим

интересующий нас показатель уязвимости в точке (на очень малом интервале), а через тот же P – показатель на малом интервале. Получим следующую формулу:

$$P = 1 - \prod_{i=1}^{n_1} \left[1 - P_t^m \right],$$

где t – переменный индекс очень малых интервалов, на который поделен малый интервал; n_t – общее число очень малых интервалов. Такой подход справедлив, если на всем рассматриваемом интервале условия для нарушения защищенности информации остаются неизменными. В реальных ААС эти условия могут изменяться.

ВЫВОДЫ ПО РАЗДЕЛУ 4

Современная практика прикладных технических или экономических исследований свидетельствует, что для достижения успеха относительно безопасности ИР в ИС компании исследователь должен хорошо ориентироваться в трех областях: 1) технической и экономической теории; 2) математическом моделировании, т. е. искусстве формализации постановки задачи, которое заключается в умении перевести задачу с языка проблемно ориентированного на язык абстрактных математических схем моделей; 3) соответствующем ПО. Поэтому в настоящем разделе было дано систематизированное изложение математических методов и моделей анализа мер безопасностей, представлены теоретические подходы, а также формирование практических навыков, расчета рисков нанесения ущерба исследуемым информационным системам.

Управление рисками базируется на данных, которые должны фиксироваться, накопляться, анализироваться, храниться, обрабатываться для оценивания потенциального ущерба от ошибок пользователей и атак нарушителей на ИР в ИС компании, выбора мер для его минимизации, расчета оценок предсказания и фильтрации всех возможных параметров и показателей, связанных с ИБ. В частности, были предложены методики, позволяющие получать объективные оценки вероятности наступления НС, объективной оценки стоимости

ущерба от нарушений безопасности ИР в ИС компании, оценки предсказания и фильтрации величины ущерба, соответствующие количественным показателям НС. В основных расчетах показателей ИБ в ИС были использованы возможности линейной дискретной стохастической стационарной модели в форме ПС и уравнений фильтра Калмана для получения более достоверных значений оценок состояния исследуемого объекта.

Увеличение объема информации в репозитории SIAM-систем, а также числа людей занятых в сфере интеллектуальной деятельности потребовали создания надежных средств сбора, обработки, хранения, передачи информации в различных форматах ее представления. Поэтому в работе обращено особое внимание проблеме структуре построения системы оперативного, быстрого поиска необходимой информации, в режиме почти реального времени, удовлетворяющей свойствам полноты, точности, достоверности на основе использования онтологического подхода в ИИС.

В данной работе для целей защиты ИР в ИИС предприятия рассмотрен подход управления рисками. При расчете рисков в ИИС предложен алгоритм, который основывается не только на хорошо апробированных методиках расчета экспертных оценках, но и на методике расчета объективных оценках вероятностей количества реализаций НС и соответствующих объективных оценках ущербов как следствие реализованных НС в ИИС.

Для более четкого прояснения картины определения уязвимостей информационных ресурсов в ИИС предприятия предложена обобщенная формула, которая основана на различных вероятностных показателях доступа злоумышленника к информационным ресурсам в ААС.

В данном разделе для целей эффективной защиты ИР в ОУИС предприятия предложены подходы расчетов и управления рисками с помощью взаимосвязанных объективных и экспертных оценок. Поэтому при расчете рисков были осуществлены расчеты оценок количества инцидентов НС и величин ущербов от нарушений безопасности ИР на основе количественных и качественных оценок вероятностей реализации НС, угроз в семействах контролей безопасности [51, 56].

5. МАРКЕТИНГОВЫЕ ИНФОРМАЦИОННЫЕ УСЛУГИ В SIEM-СИСТЕМАХ

Наличие уязвимостей в компьютерных системах, разнообразие видов компьютерных атак, их непредсказуемый характер, территориальная и временная распределенность средств защиты сетевой инфраструктуры – все это приводит к тому, что в настоящее время для компьютерных сетей и систем все более важное значение приобретают технологии проактивной защиты информации, осуществляющих непрерывный мониторинг и управление безопасностью информации. В основе таких технологий лежит своевременный оперативный сбор данных и метаданных о событиях безопасности, фиксируемых в записях журналов аудита компьютерной инфраструктуры, их хранение в специализированном хранилище и последующая обработка, включающая процедуры классификации, корреляции, моделирования, выработки предупреждений и решений по противодействию атакам, а также другие наиболее эффективные оперативные процедуры восстановления и надежного сохранения безопасности информации. Поэтому другим названием для информационной системы (ИС), реализующей мониторинг и управление безопасностью информации, является SIEM-система [60].

Для хранения и манипулирования данными и метаданными предлагается построение репозитория на принципах сервис-ориентированной архитектуры (СОА или SOA, SOA – service-oriented architecture). При этом предполагается эффективное генерирование данных и метаданных непосредственно создателями ресурсов для быстрого поиска информации в Интернете. Доступ к данным и к метаданным осуществляется с использованием веб-сервисов. В частности, в качестве хранилища можно использовать СУБД Virtuoso компании Open Link Software, которая поддерживает функциональность как реляционной СУБД, так и хранилища триплетов.

В разделе 2.4 были описаны функциональные требования, которые предъявляются к репозитории.

В качестве основы предлагается выбрать сервис-ориентированную архитектуру– модульный подход к разработке программного

обеспечения, основанный на использовании распределённых, слабо связанных (*англ.* loose coupling – слабая связь) заменяемых компонентов, оснащённых стандартизированными интерфейсами для взаимодействия по стандартизированным протоколам). Программные комплексы, разработанные в соответствии с сервис-ориентированной архитектурой, обычно реализуются как набор веб-служб, взаимодействующих по протоколу SOAP (от англ. Simple Object Access Protocol – простой протокол доступа к объектам). SOAP – протокол обмена структурированными сообщениями в распределенной вычислительной среде. Архитектура SOA является инновационной идеей для распределенной информационной среды, которая объединяет различные программные модули и приложения, основанные на хорошо определенных интерфейсах, обеспечивает их взаимодействие.

5.1. ОБОБЩЕННАЯ АРХИТЕКТУРА РЕПОЗИТОРИЯ ПРИ ИСПОЛЬЗОВАНИИ ОНТОЛОГИЧЕСКОГО ПОДХОДА С МАРКЕТИНГОВЫМ КОМПОНЕНТОМ

В соответствии с основными принципами SOA, архитектура репозитория SIEM-системы может быть разделена на три основных слоя: Память, Представление и Сервисы [61] (рис. 5.1).

Все компоненты репозитории были описаны в разделе 2.4.

5.2. МАРКЕТИНГОВЫЕ ИНФОРМАЦИОННЫЕ УЗЛЫ В SIEM-СИСТЕМАХ

Маркетинг занимается проблемами удовлетворения потребностей пользователей в определенных продуктах и услугах. Назначение маркетинговых информационных систем (МИС), создаваемых и реализуемых во многих организациях, заключаются в поддержке принятий решений. За последние 35 лет в рамках PIMS (Profit Impact of Market Strategy – воздействие стратегии маркетинга на получение прибыли) многими компаниями и организациями в сфере бизнеса были разработаны принципы и методы стратегии бизнеса, опирающиеся на использование базы данных и метаданных (БДМ).

БД и БДМ заказчиков с 60-х гг. XX века претерпели существенные изменения, пройдя путь развития от контактных перечней как основы для коммуникаций пользователей с потребностями в пакетах прикладных программ и услуг (ППП и У), в продуктах и прочих услугах до важных и современных инструментов развития бизнеса. Центр тяжести в использовании БДМ сместился в сторону установления более непосредственных контактов с потребителями. Эти БДМ постепенно превратились в центральное звено в отношениях компаний с потребителями и другими компаниями, причем можно было наблюдать стремление организаций к интенсификации этих связей. Потребности МИС, на удовлетворение которых направлены компоненты SIEM-системы, непосредственно вытекают из проблем корректного функционирования МИС, которые приходится решать участникам рынка.

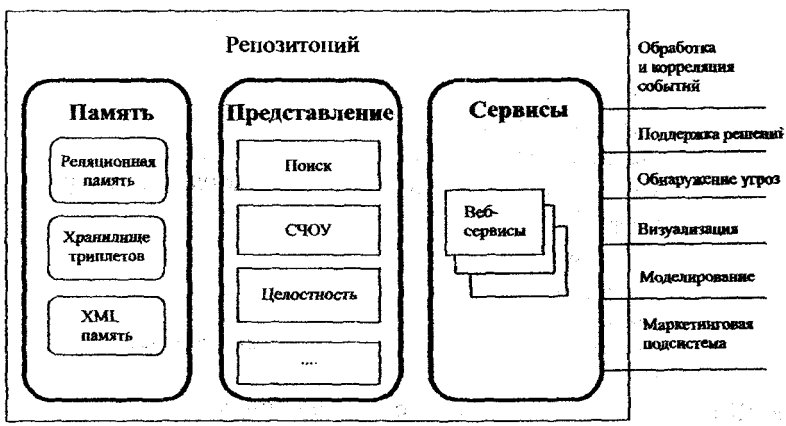

Рис. 5 1. Обобщенная архитектура репозитория с учетом дополнительного маркетингового компонента

Основные вопросы маркетинга постоянно расширяются.

КТО: наши потребители?
наши потенциальные потребители?
наши конкуренты?

ЧТО: какие новые или существующие ППТиУ мы должны развивать?
на какие новые или существующие рынки мы должны выходить?

ГДЕ: мы должны развиваться?
наши потребители?
мы должны сбывать наши ППТиУ?
наши конкуренты?

КОГДА: мы должны выходить на рынок с новыми продуктами, ППТиУ?
мы должны открыть для себя новые рынки или уйти с существующих?

КАК: мы должны способствовать продвижению на рынок продуктов и ППТиУ?
мы должны распространять наши продукты и ППТиУ?
мы должны реагировать на ожидания и реакцию потребителей и других компаний?
мы должны строить свои взаимоотношения с конкурентами и другими компаниями?
мы должны максимизировать оборот?
мы можем поддержать нашу деятельность и оценить новые возможности?

ПОЧЕМУ: потребители покупают наши продукты и услуги?
мы должны создавать новые продукты, ППТиУ и развивать новые услуги? Мы должны сохранять свое присутствие на данном рынке (в данном бизнесе)?

Основной упор при маркетинговом анализе делается на локализацию рынков, выявление и описание групп потребителей, изучение процесса продажи. Очевидно, что для решения любого из вопросов, перечисленных выше, необходимо располагать определенной оперативной информацией. Например, для ответа на

вопрос: «Где наши потребители?» нужны данные, собранные на двух уровнях:

• среди уже имеющихся потребителей. Имеются в виду данные и метаданные, составляющие так называемый профиль потребителей: возраст, семейное положение, расстояние до магазина, покупательские привычки, возможности и пр.;

• среди потенциальных потребителей, для выявления которых могут быть использованы указанные выше основные вопросы. Сопоставляя эти вопросы с внешними демографическими данными и метаданными, такими как данные переписи, а также данные и метаданные, собираемые организациями, которые заняты исследованиями рынка, можно выявить еще не охваченные группы потребителей возможностей и услуг, запросы которых собираются и концентрируются в репозиториях SIEM-систем. Для определения интересов потребителей SIEM-систем можно прибегнуть к таким приемам, как интервью непосредственно в местах совершения покупок и в перерывах конференций и симпозиумов. Все это поможет выявлять дополнительные группы потребителей.

5.3. ТИПЫ МИС КАК КОМПОНЕНТА SIEM-СИСТЕМ

МИС, как и прочие ИС, можно разделить на четыре основных типа.

• **Системы обработки транзакций** (транза́кция – минимальная логически осмысленная операция, которая имеет смысл и может быть совершена только полностью) и оперативных данных и метаданных, которые предназначены для обработки основных операций конкретного предприятия, организаций, рядовых пользователей и т. д. Примером таких систем могут служить системы учета запасов (например, новых ППЦиУ и продуктов на рынке) и сделок купли-продажи.

• **Управленческие МИС** нередко используют данные и меданные, получаемые из системы первого типа, но на выходе они могут предоставлять пользователям некоторые итоговые и аналитические данные и метаданные. Типичным примером могут служить определенным образом структурированные обзоры,

предназначенные для информирования руководителей и поддержки принятия решений. Так, в регулярных (еженедельных или ежемесячных) отчетах об объемах различных продаж ППП и У, продуктов и товаров предусматриваются дополнительные сведения по продажам ниже среднего уровня.

• **Интеллектуальные системы поддержки принятия решений** (ИСППР) предназначены для оказания помощи управленческому персоналу в принятии стратегических решений в нетипичных ситуациях [62]. В таких системах, функционирующих на основе БД систем второго типа, предусмотрены средства построения и анализа взаимозависимостей между важнейшими факторами данной среды. Примером подобных систем может служить использование географических ИСППР для планирования локальной сети розничной торговли различных ППП и У.

• **Исполнительные ИСППР** – предназначены в помощь руководителям верхнего звена SIEM-систем при получении и использовании информации, необходимой для стратегического управления. Основное внимание в этих системах уделяется предоставлению информации в ситуациях, когда для принятия решений необходимо привлекать данные или метаданные из большого числа разнообразных источников - (речь, как правило, идет об информации, в высшей степени неструктурированной). Например, по желанию какого-то менеджера может понадобиться сравнить показатели прошлогодних продаж ППП и У с аналогичными показателями фирмы-конкурента. Для этой цели необходимо будет получить доступ к отчетам компаний, аналитическим выводам и рекомендациям, содержащимся во внешних финансовых БД и решениях научных конференций и симпозиумов, а затем сравнить их с данными отчетов своей организации за предыдущие годы. Система должна выдать необходимую информацию в форме графиков, сопоставляющих объем купли-продаж фирмы-конкурента с собственными показателями организации.

Все перечисленные системы поддерживают процесс принятия решений в вопросах, касающихся оперативного, тактического и стратегического управления. Например, для управления запасами ППП и У необходимы детальные подробные данные, для

удовлетворения основного принципа SIEM-систем для выдачи рекомендации по проблеме с возникшим инцидентом в компьютерной системе, например, конкретному рядовому пользователю в режиме почти реального времени (в течение 2...5 мин). Эффективный результат здесь может быть достигнут с помощью системы складирования / поставки / рекламирования различных видов ППП и У. С другой стороны, для стратегического планирования требуется значительно менее детализированная, но с элементами научного характера прогнозных показателей информация, привлекаемая из гораздо более широкого круга источников, которая могла бы помочь в определении и оценке альтернативных каналов сбыта и распределении «складов» и торговых точек обслуживания пользователей, полученная на основе оперативных расчетов с помощью вычислительной техники [63].

Многие авторы учебных пособий, учебников и научных статей [64–67] указывают на необходимость учитывать при построении МИС четыре основополагающих для маркетинга фактора: продукт, цена, обработка данных, место и условия сбыта. Маркетинговая среда состоит из микросреды, и макросреды: микросреда, или ближайшее окружение фирмы, включает поставщиков, посредников, конкурентов и клиентуру; макросреда фирмы, или общее окружение фирмы, включает демографические, экономические, политические, природно-географические, научно-технические и культурно-исторические факторы.

В таблице 5.1 видна взаимосвязь этих факторов с системами переработки данных и метаданных.

Существует три способа сбора первичных данных и метаданных, а именно наблюдение, эксперимент, опрос. В основу любой системы анализа маркетинговой информации положен статистический банк и банк моделей. Статистический банк – совокупность современных методик статистической обработки информации, позволяющих наиболее полно вскрыть взаимозависимости данных и метаданных. Банк моделей – набор математических моделей, способствующих принятию более оптимальных и эффективных маркетинговых решений по деятельности SEIM-систем.

Таблица 5.1

Основные факторы, учитываемые при маркетинге и их взаимосвязь

Продукт	Цена	Обработка данных	Условия сбыта
Сорт Характеристики Выбор Расфасовка Качество Услуги Фирменный стиль Гарантия Рентабельность	Кредит Скидки Способы платежа Розничная цена	Сбор данных и метаданных Анализ данных и метаданных Представление данных и метаданных	Географический охват Место Реклама

Как видно из таблицы 5.1, система обработки данных и метаданных интегрирована в систему маркетинговых показателей и должна занимать в ней центральное место. Следует, однако, учитывать, что в зависимости от характера рынка ППТиУ сами показатели могут изменяться и варьироваться.

5.4. НОВЫЕ СОВРЕМЕННЫЕ ТРЕБОВАНИЯ К МИС

По мере того как специализированная организация со своей SIEM-системой будет больше уделять внимания вопросам стратегического управления и более аналитически подходить к изучению рынка ППТиУ, будет наблюдаться все большее сближение таких (прежде разрозненных) направлений, как маркетинговый анализ, планирование бизнеса и менеджмента. Все это потребует создания надежных и эффективных МИС, способных хранить и перерабатывать обширную информацию о рынке ППТиУ. В ближайшие годы при проектировании МИС потребуется принимать во внимание следующие условия:

• изменения рыночной среды, превращение ее в более агрессивную, что требует от участников более полной информированности;

• дальнейшая интеграция МИС путем объединения различных БД, например, для розничной торговли ППП и У может понадобиться интеграция данных и метаданных по таким областям, как организация торговли ППП и У, планирование и обновление запасов ППП и У, исследования рынка ППП и У, с внешними данными;

• изменения в области автоматизированных и автоматических интеллектуальных МИС и информационных технологий (создание разветвленных компьютерных сетей, появление более комфортабельных систем, осознание стратегического значения МИС в SHIM-систем);

• возможности получения больших объемов данных и метаданных из электронных касс оплаты и электронных систем перевода средств из касс оплаты (EPOS – electronic point of sates systems и EFTROS – electronic funds transfer at the point of sales), которые могут помочь создавать детальное представление о поведении клиентов при совершении заказов и покупок ППП и У, это может потребовать существенного увеличения аналитических возможностей современных МИС;

• появление новых методов маркетинга и продаж ППП и У. Электронный обмен данными и метаданными при электронной выписке счетов уже совершил революцию в операциях купли-продажи ППП и У. Заочные покупки (teleshopping) и различные способы прямого маркетинга также могут приводить к двум разнонаправленным процессам: с одной стороны, уходу потребителей с существующего рынка, а с другой – появлению (за счет появления новой информации) новых розничных торговцев.

5.5. АРХИТЕКТУРА МИС

Некоторые компании разрабатывают и внедряют интеллектуальные маркетинговые информационные системы, позволяющие менеджерам постоянно быть в курсе всех деталей,

касающихся потребителей и активных производителей ПППиУ для SIEM-систем.

МИС – это постоянно действующая система взаимосвязи людей, оборудования, средств защиты ИР и методических приемов, предназначенная для сбора, классификации, анализа, оценки и распространения своевременной и достоверной информации, необходимой для интеллектуальной системы поддержки и принятия маркетинговых решений (ИСППМР) [65] (рис. 5.2).

Для выполнения задач сбора информации, их анализа, планирования, прогнозирования [56], и контроля планов (левая область рис. 5.2) менеджеры SIEM-системы нуждаются в информации об изменениях в рыночной среде относительно ПППиУ (правая область рис. 5.2).

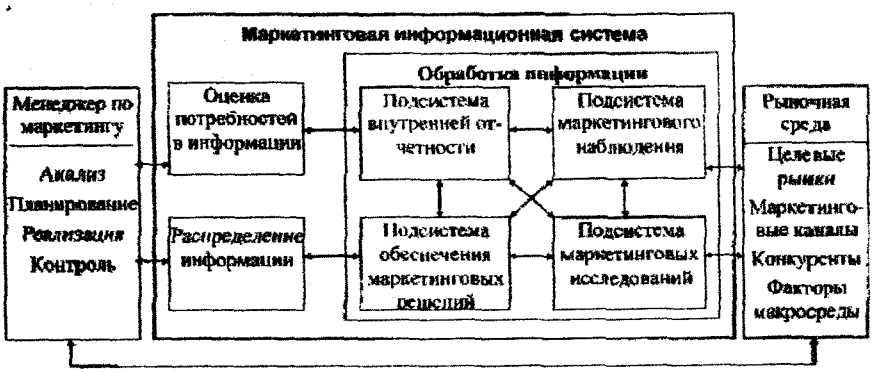

Рис. 5.2. Система маркетинговой информации

В правом прямоугольнике – составляющие маркетинговой среды, за которыми должны вести наблюдение управляющие по маркетингу. Информацию собирают и анализируют с помощью четырех вспомогательных подсистем, составляющих систему маркетинговой информации: подсистемы внутренней отчетности, подсистемы сбора текущей внешней маркетинговой информации (маркетингового наблюдения), подсистемы маркетинговых исследований и подсистемы обеспечения интеллектуальной поддержки принятия маркетинговых решений. Поток информации, поступающей к управляющим по маркетингу, помогает им в проведении анализа, планировании и

расчете оценок предсказаний, претворении в жизнь и контроле за исполнением маркетинговых мероприятий. Обратный поток в сторону рынка ППППиУ, продуктов – принятые управляющими решения и прочие коммуникации.

Основой МИС является подсистема внутренней отчетности, в документах которой отражаются сведения о заказах, продажах, ценах, списах, дебиторской и кредиторской задолженности и т. п. Система внутренней отчетности позволяет сохранить эти данные и/или метаданные и преобразовать в удобную для работы форму, а также рекомендации, выдаваемые заинтересованным лицам в режиме почти реального времени. В результате становится возможным анализировать эффективность и прибыльность конкретных ППППиУ, товаров и других услуг, каналов распределения, потребителей, динамики объемов продаж ППППиУ, что позволяет выявлять перспективные возможности и насущные проблемы SIEM-системы (как предприятия), которая выдает быстрые рекомендации в режиме почти реального времени для разрешения проблем с возникшими инцидентом или инцидентами.

В то время как подсистема внутренней отчетности содержит и предоставляет данные и метаданные о том, что уже произошло, подсистема маркетингового наблюдения предоставляет сведения о ситуации на рынке ППППиУ в данный момент. Маркетинговое наблюдение определяется как постоянная деятельность по сбору текущей информации об изменении внешней среды маркетинга, необходимая для разработки и для корректировки маркетинговых планов. Подсистема наблюдения за внешней средой включает в себя отслеживание изменений в законодательстве, в экономическом состоянии страны/региона и уровне доходов граждан; изменений в технологии эффективного «лечения» неисправностей [62] в КС пользователей, предприятий и организаций, появлении новых технологий и новых конкурентных ППППиУ и т. п.

Третьей основной составляющей МИС являются маркетинговые исследования, которые в отличие от маркетингового наблюдения предполагают подготовку и проведение различных обследований, анализ полученных данных и метаданных по конкретной маркетинговой задаче, стоящей перед SIEM-системой. Другими словами, маркетинговые исследования проводятся не постоянно, а

периодически, по мере появления определенных заказов на устранение компьютерных инцидентов и нефункциональности ИС. Разрешение проблем компьютерных инцидентов и выдача эффективных рекомендаций должны разрешаться в режиме почти реального времени.

По результатам маркетинговых исследований, проводимых самостоятельно либо по заказу рядовых владельцев ПК, отдельных предприятий и организаций специальные исследовательские отделы SIEM-системы будут решать конкретные проблемы (определять целесообразность разработки или закупки нового ППП и У, или предоставлять адреса и названия ППП и У на рынке, а также принимать решения по выбору места открытия новой торговой точки, для предоставления возможности «заказчикам» приобрести ППП и У).

В МИС также входит система обеспечения маркетинговых решений (COMP), которая представляет собой взаимосвязанный набор данных или метаданных, инструментов и методик, с помощью которого SIEM-система анализирует и интерпретирует внутреннюю и внешнюю информацию. Принцип работы COMP состоит в следующем: имеющаяся информация в виде данных и метаданных обрабатывается с помощью подходящей к конкретному случаю компьютерной модели, входящей в состав COMP, после чего результаты анализа используются для определения оптимального для данного случая порядка действий, осуществление которых порождает новые изменения макро- и микросреды.

Таким образом, роль МИС состоит в определении потребностей в информации для маркетингового анализа и управления, ее получении и своевременном предоставлении соответствующим менеджерам. МИС включает в себя некий набор правил, определяющих, какую информацию нужно собирать, с какой периодичностью, в какой форме и кому ее нужно передавать.

5.6. АНТИКРИЗИСНОЕ ИСПОЛЬЗОВАНИЕ ИНСТРУМЕНТОВ МАРКЕТИНГА

Трудно давать оптимистические прогнозы в период нестабильной экономической ситуации, когда люди не только задумываются о

пересмотре долгосрочных планов, но и начинают отказываться от затрат, которые ранее были регулярными.

Прежде чем приступать к рассмотрению антикризисных инструментов маркетинга в любой индустрии, необходимо разобраться, что же такое индустрия по устранению компьютерных инцидентов. Инцидент ИБ – одно или серия нежелательных или неожиданных событий в системе ИБ, которые могут скомпрометировать деловые операции и поставить под угрозу защиту информации.

На сегодня наиболее эффективными антикризисными инструментами управления по устранению компьютерных инцидентов являются инструменты маркетинга, которые позволяют создать новые возможности для предприятия, организации, частных лиц и т. п. Прежде всего инструменты маркетинга направлены на разработку сильных и устойчивых конкурентных преимуществ. К ним можно отнести [62, 64]:

• товарную политику: товар в виде ППППиУ, ассортимент, товарный знак, бренд, упаковка, дополнительные услуги или удобство при продаже ППППиУ, реклама, гарантия, сервисное обслуживание;

• ценовую политику: ценообразование, скидки, акционные цены, бонусные программы, ценовая стратегия;

• сбытовую политику: каналы сбыта, товародвижение (опт, розница, прямые продажи, интернет-магазины); процесс сбыта, дистрибьюция или трейд-маркетинг; материальная обработка, логистика (складирование, транспортировка, управление запасами, грузопереработка); маркетинговая логистика (управление заказами, условия контракта: условия оплаты, доставки, размер минимальной оплаты);

• коммуникационную политику: реклама, PR (Public Relations – коммуникативная активность компании, направленная на формирование гармоничных отношений с обществом, установление и поддержание результативных отношений с полезными аудиториями, изучение общественного мнения и реагирование на него); создание имиджа и общественного мнения (PR, relations); стимулирование сбыта, личные продажи, прямой маркетинг (инструментами прямого

маркетинга могут быть персональные продажи и деятельность торговых представителей) [66, с. 134].

Одним из важных инструментов маркетинга в антикризисный период является лояльность. Единственного определения лояльности нет, одни подразумевают под этим термином прежде всего эмоциональные отношения покупателей к бренду, другие считают, что смысл кроется в повторной покупке товара. Авторы настоящей работы придерживаются определения, что лояльность – это построение долгосрочных отношений, при которых клиент позитивно относится к товару, бренду или услугам и становится постоянным клиентом. Лояльность также позволяет понять с правильной стороны потребности клиента и разобрать сервисы обслуживания, в которых он нуждается [66, с. 75]. Многие руководители предприятий, организаций часто не уделяют должного внимания этому инструменту, а низкий уровень лояльности на предприятии, снижает показатели эффективности экономической деятельности на 20, 21,..., 25 процентов.

Для расчета показателя лояльности компания SAS (аббревиатура от Statistical Analysis System, который со временем стал использоваться в качестве имени собственного для обозначения как самой компании, так и её продуктов, давно уже вышедших за рамки только приложений для статистического анализа). Компания Customer Retention предложила ряд методов и решений:

- точный учет клиентов предприятия, у которых за рабочим столом стоит персональный ноутбук;
- анализ основных факторов, влияющих на решение производственных задач, взаимосвязь с различными клиентами;
- анализ поведений клиентов.

Специалисты советуют также присваивать своим клиентам определенные баллы лояльности с использованием аналитических процессов. Эти процессы позволят получить информацию на основе личных данных, а также сведения о личным счете, хозяйстве. Такая информация может быть использована при разработке стратегии устранения возникших инцидентов.

Еще один способ завоевать доверие клиентов, обращающихся в компанию, которая предоставляет услуги по устранению

инцидентов, – это выдача на год членских карт, дающих привилегированный статус, а также определенные льготы и бонусы, недоступные непостоянным клиентам.

Программа лояльности – это форма маркетинговых мероприятий, направленная на создание долгосрочных отношений с клиентами и превращение их в постоянных потребителей. Программа лояльности направлена на увеличение удовлетворенности клиентов.

Статистика показывает, что программы лояльности с использованием членских карт приводят к увеличению оборотов на 10 %.

Таким образом, можно сделать вывод, что лояльность создает запас доверия для компании, обслуживающий свою SIEM-систему, которая дает конкурентное преимущество, которое необходимо всем пользователям компьютерных вычислительных систем в любое время и даже во время кризиса.

Важным инструментом считаются также индивидуальные продажи услуг по разрешению любых проблем с компьютерными инцидентами, и их значимость возрастает с каждым годом.

Индивидуальная продажа – это непосредственная презентация услуг или идея предоставления рядовому пользователю компьютерных программ по разрешению компьютерных инцидентов.

Красивая запоминающая наружная реклама по устранению инцидентов непременно заинтересует прохожих. При этом информация должна быть легко воспринимаемой, привлекательной, читабельной.

Каждой фирме, обслуживающей SIEM-систему, нужно думать о будущих изменениях и кризисах, пока есть возможность все хорошо взвесить, пока кризис не даст о себе знать. На помощь приходит антикризисный план, как инструмент превентивного маркетинга и антикризисного управления. Целью антикризисного плана является определение негативных последствий кризиса или его предотвращение.

Статистика показывает [66], что 57 % руководителей отрицают наличие антикризисного плана на предприятия, но интересен тот факт, что из них 53 % руководителей уже ранее сталкивались с кризисом, и по их словам «выкарабкивались» из него не просто.

Процесс разработки антикризисного плана предполагает определение целей, выбор стратегии, оценку слабых мест компании, конкретные действия по предупреждению и выводу ее из кризиса, а также четко закрепляет полномочия за каждым сотрудником. Клиентоориентированный бизнес (каким являются услуги, предоставляемые SIEM-системой) сегодня, чтобы удержать (а желательно расширить!) количество своих клиентов, должен кардинально пересмотреть принципы работы, обращая особое внимание на эффективное управление продажами услуг и политику гибкого ценообразования. Кризис – самое подходящее время для этого [67].

Говоря об оптимизации предоставляемых услуг SIEM-системой в нестабильный период в работе [67] выделяется три основных направления, на которые стоит сосредоточиться.

Оставляем лучшее. Довольно бонально, но истинно: чтобы удержать клиентов и привлечь в свою SIEM-систему новых клиентов, сервис должен быть клиентоориентированным на все 100 %! Вот несколько рекомендаций, следуя которым можно оптимизировать пакет предложений в соответствии с запросами рынка без дополнительных финансовых вливаний [67].

- Все услуги, предлагаемые клиентам на основе устранения компьютерных инцидентов в режиме почти реального времени, должны быть востребованными минимум на 80 %. Если процент ниже, значит, услуга неэффективна, от таких ПППиУ необходимо отказаться или серьезно их доработать.
- Должны проводиться опросы потрибителей на тему удовлетворенности услугами вашей компании. Клиенты оценят ваш интерес к их мнению. Следует прислушиваться к нему и реформировать ПППиУ на основе опросов.
- Необходимо отдавать предпочтение ПППиУ, которые позволяют клиентам экономить деньги. В кризис деньги считают все, даже самые обеспеченные и не ограниченные в ресурсах люди.
- Следует вводить в предложение «дробные расчеты» – они пользуются спросом, так как в кризис люди живут днем сегодняшним и не могут заглядывать далеко в будущее. Например, можно ввести

«короткие» карты, рассчитанные на рассрочку до одного или до шести месяцев.

• Необходимо предлагать дополнительные ППП и У, связанные с возможностью покупки вашего ППП и У в рассрочку или в кредит. Особенно востребованным становится первый вариант, поскольку позволяет планировать людям свой бюджет. Если человек не готов единовременно расстаться с определенной суммой, он может разбить платежи, что намного удобнее и психологически комфортно в кризисных условиях. В дополнение к кредитным возможностям можно ввести услугу «Легкий платеж» (для карт с ежемесячной оплатой), когда один раз. введя свои данные в систему, клиент больше не думает о регулярных платежах – фиксированная сумма ежемесячно списывается автоматически.

• Помимо основного ППП и У, можно предлагать клиентам бонусные программы – лояльности, партнерских преимуществ.

• Необходимо делать в программах гибкие условия, реальные цены и комфортный для клиентов сервис.

Учет и контроль! Нужен четкий мониторинг расходов – сколько уходит денег на аренду, строительство, оснащение фитнес-центров, сервисное обслуживание и ремонт оборудования, закупку расходных материалов для сопутствующих направлений, оплату труда персонала.

Необходимо подумать и об оптимизации расходов: проводить оценку эффективности вложений на основе аудита, отказываться от балластных статей и усиливать наиболее перспективные. Многие компании в кризис сокращают персонал, экономят на заработной плате. Но отказ от услуг профессионалов чреват неприятными последствиями. Можно не сокращать штат, а просто немного пересмотреть систему бонусов и предложить сотрудникам иные формы нематериальной мотивации.

Другой пример оптимизации расходов – экономия не в ущерб качеству: если речь идет об отделке помещения, то следует отдать предпочтение не дизайнерской плитке и дорогим сортам дерева (что, безусловно, пафосно), а добротным и износостойким материалам, которые позволяют создавать уютную атмосферу.

Руководителям компании надо пересмотреть схемы работы с партнерами и поставщиками ППП и У. Они тоже испытывают влияние

кризиса и наверняка заинтересованы в стабильном пролонгированном партнерстве. Результат совместной работы повышается, если с подрядчиками выстраиваются доверительные и взаимовыгодные отношения. С арендодателями и поставщиками есть возможность договориться о серьезных скидках и отсрочках платежей.

Руководство должно своевременно получать максимально полную отчетную информацию о выполнении/невыполнении планов продаж услуг и отработке входящего трафика. Планирование дальнейшей работы базируется на изучении результатов отчетности с выявлением и учетом слабых и сильных сторон. В кризис финансовые планы хотя и остаются долгосрочными, но тактика достижения поставленных целей должна постоянно меняться с учетом вновь получаемых «вводных».

Кадры как главная ценность. Кадровый вопрос, как всегда, остается одним из самых актуальных. При работе с людьми равнодушие и формальное отношение к своим обязанностям абсолютно неприемлемы. Дефицит профессиональных, амбициозных сотрудников плохо сказывается на компании в любые времена, а в период экономической нестабильности особенно.

Кризис – отличное время, чтобы перегруппировать штат и укрепить команду. Практический опыт показывает [67], что не нужно бояться расставаться с неэффективными сотрудниками. Профессионалы своего дела не боятся перемен и готовы к новым предложениям, что позволяет привлекать к сотрудничеству ведущих специалистов отрасли.

В настоящее время большинство ИСППР ориентированы на конкретные, часто достаточно узкие сферы применения, и при возникновении новых задач часто приходится разрабатывать либо закупать новые системы, методы и технологий следствием чего будут большие временные, организационные и финансовые издержки. Поэтому возникает задача создания комплексных SIEM-систем, способных анализировать большие массивы информации различных типов и форм представления данных и метаданных, а также иметь в своем арсенале большое количество информационных технологий и методов обработки информации, быстрой перестройки на новые задачи, а также формировать альтернативные управленческие

решения для лиц, принимающих решения (ЛПР) различного уровня. Именно такими свойствами обладают ИСППР [62].

ВЫВОДЫ ПО РАЗДЕЛУ 5

В настоящем разделе рассмотрено обобщение системно-технических решений по применению онтологического подхода для построения на его основе SIEM-репозитория нового поколения с добавлением сервисного маркетингового компонента. Маркетинговый узел охватывает вопросы создания SIEM-репозитория с применением SOA-ориентированной гибридной архитектуры, его апробации и тестирования для функциональных потребностей компонентов модуля, отвечающего в SIEM-системе за моделирование, анализ безопасности и дополнительные сервисные услуги.

В разделе также рассмотрен практический опыт использования известных основных инструментов антикризисного управления в условиях сокращения доходов населения и падения спроса на платные дополнительные услуги, предоставляемые отдельными частными лицами. Предложены известные мероприятия по выходу из кризисной ситуации.

Дальнейшие исследования могут быть связаны с расширением предложенных услуг, а также с добавлением различных сервисов, которые обеспечат безопасность данных и метаданных, включая моделирование и анализ безопасности, верификацию политики безопасности и т. п.

Изучены вопросы логического вывода, ориентированного на онтологический репозиторий, а также разработаны механизмы визуализации данных и/или метаданных, количественного прогнозирования инцидентов, соответствующих ущербов и предоставления в режиме почти реального времени эффективных рекомендаций по устранению возникших компьютерных инцидентов [63].

6. МАРКЕТИНГОВАЯ ИНФОРМАЦИЯ

6.1. ХАРАКТЕРИСТИКИ СЛУЖБЫ МАРКЕТИНГА НА ПРЕДПРИЯТИИ

Среди основных задач подразделений, работающих с маркетинговой информацией, исходя из основных стратегических целей компании, на основе функционирования SIEM-системы, можно выделить следующие [68]:

- обеспечивать руководство компаний той маркетинговой информацией, которая требуется для того, чтобы разрабатывать стратегию и тактику развития и рыночного поведения организации. Подразделение обязано, если это необходимо, уточнять и дополнять указанную информацию, а также выполнять все работы, касающиеся анализа и оценки различных современных и перспективных ситуаций на рынке;
- проводить весь комплекс исследований, которые касаются рынка, товара и потребителей как при утвержденном плане исследований маркетинга, так и при специальных указаниях руководства и при заданиях других подразделений компании. Когда определяются цели и функции подразделения, работающего с маркетингом, необходимо проводить полный анализ того, как работает фирма, и выявлять существующие «узкие места» и недостатки в ее функционировании [69]. На базе полученных данных, строится гипотеза возможностей разрешения соответствующих проблем на основе формируемого подразделения маркетинга. Происходит разработка плана маркетинга. На основе стратегии маркетингового развития и целей подразделения маркетинга, можно построить гипотезу о том, какова его рациональная структура. Один из возможных примеров структуры подразделения маркетинга приведен на рис. 6.1;
- постоянно участвовать в разработках стратегий и тактик рыночного поведения компании на основе формирования товарной, ценовой, сбытовой, рекламной и сервисной стратегии маркетинга, оказывать консультационную помощь руководству фирм и других подразделений;

• организовывать рекламную деятельность, а также разрабатывать комплекс мероприятий, направленных на формирование и поддержку связей с общественностью;

• проводить непрерывный анализ и оценку эффективности маркетинга в компании;

• оказывать помощь и обеспечивать консультации по маркетингу для всех подразделений компании;

• осуществлять методическое руководство и обучать весь персонал компании основам маркетинга;

• проводить оценку психологического соответствия тех людей, которых принимают на работу в организацию на вакантную должность [70];

• проводить анализ общего психологического состояния групп, коллективов и отдельных работников компании;

• разрабатывать новые изделия на базе той маркетинговой информации, которую получают, а также дизайнерские изделия и проводить стоимостно-функциональный анализ [71].

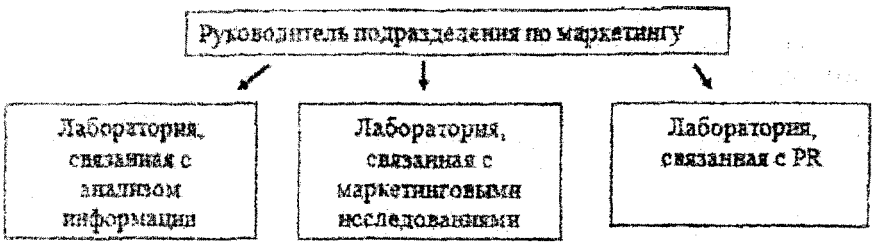

Рис. 6.1. Структура подразделения по работе с маркетингом

Одним из факторов маркетингового исследования является PR (public relations, связи с общественностью, пиар). PR - это управление потоками информации между организацией и общественностью. Цель PR – создание положительного образа организации в сознании потенциального потребителя, а также других заинтересованных сторон.)

Основные составляющие подразделения маркетинговой информации

1. Лаборатория маркетинговой информации, которая подчиняется руководителю компании. Руководителя этой лаборатории назначают и освобождают от должности приказом руководителя компании. В ее состав следующие подразделения, которые непосредственно подчиняются руководителю этой лаборатории: отделение дизайна; отделение рекламы; отделение психоанализа.

2. Лаборатория исследований маркетинга. В ее состав входит: руководитель лаборатории маркетинговой информации; экономист; помощник руководителя лаборатории маркетинговой информации; программист.

3. Лаборатори: дизайна, в которой работает дизайнер; рекламы, в которой работает создатель маркетинговых рекламно-пропагандистских программ; психоанализа, в которой работает психолог-аналитик по кадрам.

6.2. СВОЙСТВА СИСТЕМ МАРКЕТИНГОВОГО КОНТРОЛЯ

При рассмотрении деятельности различных предприятий необходимо **анализировать** стоящие перед ними **цели.** Такие цели представляют собой исходную точку при **разработках планов и программ** в маркетинге, при процессах, исполнение которых должно обеспечивать точное продвижение к намеченным целям. Оценка степени исполнения намеченной цели и программы проводится **на основе систем маркетингового контроля** [72, 73].

Контроль маркетинга – постоянная, систематическая проверка и оценка положений и процессов в области маркетинга. Процессы контроля обычно протекают в четыре этапа:

- устанавливаются плановые величины и стандарты – цели и нормы;
- выясняются реальные значения показателей;
- проводятся сравнения;
- проводится анализ результатов сравнения.

Основные этапы процессов маркетингового контроля связаны со своевременным выявлением разных проблем и отклонений от нормального продвижения к поставленной цели, а также с

соответствующей корректировкой деятельности организаций, чтобы существующие проблемы не вылились в кризис. В качестве конкретных задач и целей могут быть следующие: определение степени достижения целей, проведение проверок того, насколько приспособляемость организаций к изменениям условий со стороны окружающие среды соответствует поставленной цели.

В системе **маркетингового контроля** проводятся отдельные его виды, которые были предназначены для того, чтобы наблюдать и оценивать эффективность деятельности компании, выявлять все недостатки и принимать соответствующие меры.

Контроль результатов проводится, чтобы определить, существуют ли совпадения или несовпадения по базовым показателям и действительно достигнутым результатам в рамках экономических (сбыту, доле рынка) и неэкономических (отношению потребителей) критериев. Проведение контроля может быть нацелено как на весь маркетинг, так и на его отдельные компоненты [74, 75].

При проведении ревизии в маркетинге осуществляется подробный анализ информационной базы планирования, проводится контроль целей и стратегий.

Проведение аудита существующих конкурентов – одна из форм маркетингового контроле. Большинством организаций не всегда проводится подробный анализ по своим конкурентам, по их преимуществам и недостаткам. Но для отдельных конкурентов необходимо пристальное внимание, так как понятно, что именно они являются претендентами на то, чтобы захватить существующую рыночную долю компании. Для того чтобы выявить весьма активных конкурентов, необходимо предварительно определить тех из них, по которым мы выигрываем, или тех конкурентов, вследствие существования которых у нас будет проигрыш. Такой анализ показывает нам тех ближайших конкурентов, которые, вероятно, применяют технологию, подобную проводимой в условной компании.

Формируя новую компанию, весьма полезно изучить опыт обычной хорошо действующей на рынке большой компании, а также опыт небольшой, но быстро растущей фирмы. Потраченное время и средства, которые вкладываются в проведение аудита конкурентов, могут дорого обойтись организации, но все это следует рассматривать с точки зрения капиталовложения. В результате исследования

конкурентов будет создано досье, а формируемые на его базе письменные отчеты, смогут из года в год пополнять руководство компании очередными подробностями.

Проведение анализа работы конкурентов необходимо начинать с общих оценок позиционирования выпускаемых ими товаров, их текущих задач, стратегий, основных достоинств и недостатков и возможных дальнейших шагов. Весьма «уязвимые места» конкурентов, которые проявляются в периоды планирования стратегий, а также различные причины, которые препятствуют росту конкурентов и снижают их способности по реагированию на изменения, которые необходимо принимать во внимание. Та информация, которая собирается, будет давать возможности для предсказания поведения существующих и будущих конкурентов и их реакции [76].

Можно рассмотреть ситуационный анализ с точки зрения его использования как инструмента для самоконтроля и самоанализа. Объектами ситуационного анализа могут быть рынки, предприятия, покупатель (физический и юридический лица), конкурент. Затем могут быть рассмотрены другие составляющие в ситуационном анализе. Покупатели могут отличаться большим числом признаков, в этой связи весьма сложно удовлетворить запросы всех без исключения потребителей. Однако на основе сегментирования рынков есть возможности для получения групп потребителей, которые будут более или менее однородными по тем характеристикам, которые интересуют организацию.

Определение анализа конкурентов и их конкретных действий дают возможность занимать более прочную позицию на рынках. Анализ работы конкурентов касается систематического накопления информации. Требуется определить конкурентов, которые смогут оказать большое влияние на то, каким образом происходит работа данной организации. Чтобы найти конкурентов, можем использовать такие критерии:

- действующие прямые конкуренты – компании, производящие товары, которые смогут удовлетворить одни и те же потребности, а также товары-заменители;
- определение потенциальных конкурентов:

а) действующие компании, которые расширяют ассортимент или используют новые технологии, совершенствуют продукцию, чтобы лучшим образом удовлетворить потребности покупателей, и, как результат, они будут прямыми конкурентами;

б) появившиеся недавно новые компании, которые вступают в конкурентную борьбу.

Работу с данными о компаниях, являющихся конкурентами, необходимо осуществлять систематическим образом. При этом на практике требуется применять такие подходы: проведение опроса по отдельным лицам, оформление «досье» на конкурентов, подготовка докладов для руководства.

ВЫВОДЫ К РАЗДЕЛУ 6

Исходя из поставленных задач, лабораторией маркетинговой информации выполняются такие виды работ.

1. Проведение сегментации рынков; изучение того, что нужно потребителям, и создание «карт потребностей»; анализ и оценка товаров и конкурентной рыночной политики; комплексное исследование рынков; разработка прогнозов развития рынков; проведение «технологических прогнозов» и исследований по отраслевым тенденциям; анализ и оценка эффективности рекламной кампании; анализ и оценка эффективности сбыта.

2. Лаборатория рекламы проводит разработки по всем рекламным и пропагандистским кампаниям предприятия и осуществляет организацию их проведения.

3. Разработки по дизайнерско-конструкторским параметрам в новых изделиях на базе полученной маркетинговой информации, которую получают.

4. Оценка психологического соответствия, принимаемых для работы в компании сотрудников на вакантную должность.

5. Рассмотрение особенностей системы маркетингового контроля, основных его стадии. Определение характеристик аудита как одной из форм маркетингового контроля. Указание подходов для поиска компаний-конкурентов.

7. СПОСОБЫ ОПИСАНИЯ ОБЪЕКТОВ
7.1. ПОСТРОЕНИЕ И ОСНОВНЫЕ КОМПОНЕНТЫ SIEM-СИСТЕМ

Учитывая характер и содержание задач защиты в сервисных и критических инфраструктурах, целесообразно положить в основу построения системы мониторинга концепцию SIEM-системы. Рассмотрим подробнее содержание этого понятия.

Основной целью построения и функционирования SIEM-систем является значительное повышение уровня информационной безопасности в информационно–телекоммуникационной инфраструктуре за счет обеспечения возможности в режиме, близком к реальному времени, манипулировать информацией о безопасности и осуществлять *проактивное управление* инцидентами и событиями безопасности.

Предполагается, что проактивное управление инцидентами и событиями безопасности основывается на автоматических механизмах, которые используют информацию об «истории» анализируемых сетевых событий и прогнозе количества будущих НС, а также на автоматической подстройке параметров мониторинга событий к текущему состоянию защищаемой системы.

Для достижения этой цели SIEM-система должна успешно решать следующий комплекс задач:

- сбор, обработка и анализ событий безопасности, поступающих в систему из множества гетерогенных источников;
- обнаружение в режиме почти реального времени атак и нарушений критериев и политики безопасности;
- оперативная оценка защищенности информационных, телекоммуникационных и других критически важных ресурсов;
- анализ и управление рисками информационной безопасности;
- проведение расследований инцидентов;
- обнаружение расхождения критически важных ресурсов и бизнес–процессов с внутренними политиками безопасности и последующее приведение их в соответствие друг с другом;
- принятие эффективных решений по защите информации;
- формирование отчетных документов.

Основными исходными данными, которые используются SIEM-системой для решения указанных задач, являются записи из различных журналов аудита, протоколирующие события в информационной инфраструктуре, называемые «событиями безопасности». Эти события отражают такие действия пользователей и программ, которые могут оказать влияние на безопасность информации. Из общего множества событий безопасности SIEM-система должна находить такие, которые свидетельствуют об атаках или иных воздействиях, причем традиционные методы поиска такой информации достаточно трудоемки.

Одним из компонентов SIEM-систем является репозиторий (хранилище данных – ХД). ХД – место, где хранятся и поддерживаются какие-либо данные. Чаще всего данные в репозитории хранятся в виде файлов, доступных для дальнейшего распространения по сети.

Многие современные операционные системы, такие как Open Solaris, Free BSD и большинство дистрибутивов Linux, имеют официальные репозитории, которые позволяют также устанавливать пакеты из других мест. Большинство репозиториев бесплатны, однако некоторые компании предоставляют доступ к собственным репозиториям за платную подписку.

Open Solaris – *операционная система с открытым исходным кодом*, созданная корпорацией Sun Microsystems на базе Solaris. Также термин Open Solaris может использоваться по отношению к открытой кодовой базе Solaris и сообществу, которое ее разрабатывает.

Free BSD – *свободная Unix-подобная операционная система*. Free BSD хорошо зарекомендовала себя как система для построения интранет-, интернет-сетей и серверов. Она предоставляет надежные сетевые службы и эффективное управление *памятью*.

Репозитории используются в системах управления версиями, в них хранятся все документы вместе с историей их изменения и другой служебной информацией. Русское сообщество *Subversion* рекомендует использовать вместо термина репозиторий термин «хранилище», поскольку он полностью соответствует как прямому переводу слова repository, так и его понятию.

Subversion (также известная как «SVN») – *свободная* централизованная *система управления версиями*, официально

выпущенная в 2004 году компанией CollabNet. Цель проекта – заменить собой распространенную на тот момент систему *Concurrent Versions System* (CVS), которая сейчас считается устаревшей. Subversion реализует все основные функции CVS и свободна от ряда недостатков последней.

Система управления версиями (от *англ.* Version Control System, VCS или Revision Control System) – *программное обеспечение* для облегчения работы с изменяющейся информацией. Система управления версиями позволяет хранить несколько версий одного и того же документа, при необходимости возвращаться к более ранним версиям, определять, кто и когда сделал то или иное изменение, и многое другое.

Понятие данных и метаданных. Данные – зарегистрированная информация, представление фактов, понятий или инструкций в форме, приемлемой для *общения, интерпретации*, или обработки человеком либо с помощью автоматических средств. Данные – поддающиеся многократной интерпретации, параметры, а также представление информации в формализованном виде, пригодном для *передачи, связи* или обработки. Данные – формы представления информации, с которыми имеют дело *информационные системы* (ИС) и их *пользователи*.

Передача текстовых данных как бинарных приводит к необходимости изменять кодировку в прикладном программном обеспечении (это умеют большинство прикладных ПО, отображающих текст, получаемый из разных источников), передача бинарных данных как текстовых может привести к их необратимому повреждению.

Метаданные (от *греч.* Meta и *лат.* Data) **буквально переводится как «данные о данных»**, информация о другом наборе данных. Метаданные – это структурированные, кодированные данные, которые описывают характеристики объектов – носителей информации, способствующие идентификации, обнаружению, оценке и управлению этими объектами.

Тема эта поднимается с тех пор, как существуют данные. Метаданные были необходимы для описания значения и свойств

информации с целью лучшего ее понимания, управления и использования. Классический пример – библиотеки. Книги (данные) можно классифицировать, управлять ими и находить только с помощью соответствующих метаданных (т. е. заголовка, автора и ключевых слов содержания).

Обычно под метаданными понимается любая информация, необходимая в IT для анализа, проектирования, построения, внедрения и применения компьютерной системы. В случае ИС метаданные упрощают управление, создание запросов, полноценное использование и понимание данных. Многие недавние проекты (как научные, так и практические), направлены на изучение метаданных. Генерирование, хранение и управление метаданными помогают в поддержке использования огромных объемов информации, доступных в наши дни в любой электронной форме. Так как все, с чем работает компьютер, по сути является данными и своего рода метаданные сопровождают любые данные, то это понятие имеет место в любой сфере приложений и принимает различные формы в зависимости от применения.

Популярность ХД в последние годы существенно возросла. Конкурентоспособные организации занимаются построением ХД либо расширением, перепроектированием и усовершенствованием уже имеющихся хранения данных. Метаданные считаются ключевым фактором успеха в проектах по внедрению ХД. Они содержат всю информацию, необходимую для извлечения, преобразования и загрузки данных из исходных систем, а также для последующего использования и интерпретации содержимого ХД.

Метаданные систем ХД иногда подразделяют на два типа:

- служебные метаданные, используемые для функций извлечения, преобразования и загрузки, для переноса OLTP-данных ((от *англ.* Online Transaction Processing), – обработка транзакций в реальном времени. Способ организации БД, при котором система работает с небольшими по размерам *транзакциями*, но идущими большим потоком, позволяет *клиенту* требовать от системы минимального времени отклика) в ХД;
- интерфейсные метаданные, использующиеся для описания экранов и создания отчетов.

OLTP-системы предназначены для ввода, структурированного хранения и обработки информации (операций, документов) в режиме почти *реального времени*. Приложения OLTP, как правило, автоматизируют структурированные, повторяющиеся задачи обработки данных, такие как ввод заказов и банковские транзакции. OLTP-системы проектируются, настраиваются и оптимизируются для выполнения максимального количества транзакций за короткие промежутки времени.

Различают следующие типы метаданных в ХД.

Метаданные исходной системы:

- спецификации источников данных, таких как репозитории;
- описательная информация (например, частота обновления, юридические ограничения и методы доступа);
- информация о процессах, таких как график заданий и коды извлечения.

Метаданные преобразования данных:

- информация о получении данных (например, планирование передачи данных и результатов, а также сведения об использовании файлов);
- управление таблицами измерений, например, определения измерений и присвоения суррогатных ключей;
- преобразование и агрегирование, например, расширение и отображение данных, программы (скрипты) загрузки СУБД, определение агрегатов данных;
- документирование проверок, работ и журналов, например, журналов преобразования данных и записей слежения за происхождением данных.

Метаданные СУБД

- содержание системных таблиц СУБД;
- рекомендации по обработке.

Роль метаданных в хранилище. Лучше всего объяснить суть метаданных, описывая их роль и назначение в реализации процессов ХД. Метаданные можно использовать тремя способами:

- *пассивно*, обеспечивая четкую документацию о структуре, процессе разработки и использовании системы ХД. Доступная

документация необходима всем участникам (т. е. конечным пользователям, системным администраторам, а также разработчикам приложений);

• *активно*, путем хранения конкретных семантических аспектов (например, правил преобразования) в виде метаданных, которые можно интерпретировать и использовать во время исполнения. В этом случае процессы в ХД управляются метаданными, а следовательно, код (т. е. активные метаданные) и дополнительная документация согласованно и унифицированно управляются в одном репозитории, при этом актуальность документации возрастает;

• *полуактивно*, за счет хранения статической информации (например, определений структур, спецификаций конфигураций), которую будет считывать другой программный компонент во время выполнения. Например, обработчикам запросов необходимы метаданные для проверки существования атрибутов. В отличие от активного использования здесь метаданные только читаются, но не исполняются.

Создание и управление метаданными служит двум целям

1. Минимизация работ по разработке и администрированию ХД.

• Более эффективное извлечение информации из ХД.

Первая цель в основном относится:

• *к поддержке интеграции систем*. Схемы и интеграция данных зависят от метаданных, описывающих структуру и смысл отдельных источников данных и целевых систем. Правила преобразования можно применить к исходным данным и хранить в качестве метаданных. Более того, интеграция различных инструментов возможна только тогда, когда они разделяют «данные», которые в таком случае представляют собой метаданные системы ХД;

• *поддержке анализа и проектирования новых приложений.* Метаданные повышают контролируемость и надежность процесса разработки приложений, обеспечивая информацию о смысле данных, их структуре и источниках. Более того, метаданные, касающиеся решений по проектированию приложений, можно использовать повторно;

• *повышению гибкости системы и возможности повторно использовать существующие программные модули.* Это возможно

только для активного и полуактивного использования метаданных. Быстро изменяющиеся семантические аспекты хранятся в виде метаданных вне прикладных программ. Поддержка поэтому существенно проще. Систему можно расширить и адаптировать без всяких трудностей. Этот подход также дает возможность повторно использовать «фрагменты кода»;

• *автоматизации административных процессов.* Метаданные управляют запуском различных процессов ХД (например, загрузки и обновления). Информация об их исполнении (журналы доступа, количество добавленных в хранилище записей и т. п.) также содержится в репозитории, легко доступном администратору;

• *усилению механизмов безопасности.* Метаданные должны обеспечить правила доступа и пользовательские права для всей системы ХД. Управление доступом в хранилище иногда требует применения сложных методов. Например, оперативный источник может содержать безобидную информацию об отдельных показателях работы компании, однако суммарные значения в ХД иногда оказываются важнейшим секретом. С другой стороны, персональные доходы каждого сотрудника являются тайной, но при этом итоговая сумма зарплат в ХД может вовсе не быть критической информацией.

Вторая цель относится к эффективному извлечению информации, а точнее, к *повышению качества данных.* Качество данных определяется следующими характеристиками:

• согласованностью (является ли представление данных однородным, нет ли дубликатов, данных с пересекающимися или конфликтующими определениями);
• полнотой (все ли данные присутствуют);
• точностью (совпадением хранимых и фактических значений);
• своевременностью (актуально ли хранимое значение).

7.2. ПРАВИЛА ПРОВЕРКИ КАЧЕСТВА ДАННЫХ

Правила проверки качества данных необходимо задать, сохранить в виде метаданных и проверять при каждом обновлении ХД. Кроме того, высокое качество требует поддержки контроля данных. Метаданные обеспечивают информацию о времени создания и об

авторе данных, об источнике, значении данных в момент получения (о наследовании данных) и о дальнейшем пути от источника к текущему местоположению. Таким образом, пользователи могут восстановить цепочку, по которой проходят данные за время преобразования, и проверить точность возвращенной информации:

• *улучшение взаимодействия внутри системы* ХД. Взаимодействие происходит как посредством выполнения простых запросов и отчетных приложений, так и с использованием сложных аналитических инструментов. Метаданные обеспечивают сведения о значении данных, терминологию и бизнес-концепции предприятия, а также их связь с данными. Поэтому метаданные повышают качество выполняемых запросов за счет более точной и строгой формулировки, а также сокращают расходы на пользователей, которым необходимы доступ, оценка и применение соответствующей информации;

• *улучшение анализа данных.* Методы анализа данных представлены широко – начиная от простых приложений отчетности и OLAP и заканчивая сложными приложениями Data Mining. Метаданные необходимы для понимания предметной области и ее представления в ХД, с тем чтобы адекватно применить и интерпретировать результаты. Data Mining (русск. *добыча данных, интеллектуальный анализ данных, глубинный анализ данных*) – собирательное название, используемое для обозначения совокупности методов обнаружения в данных, ранее неизвестных, нетривиальных, практически полезных и доступных интерпретации знаний, необходимых для принятия решений в различных сферах человеческой деятельности. Термин введен Григорием Пятецким-Шапиро в 1989 году.

Английское словосочетание Data Mining пока не имеет устоявшегося перевода на русский язык. При передаче на русском языке используются следующие словосочетания: *просев информации, добыча данных, извлечение данных*, а также интеллектуальный анализ данных. Более полным и точным является словосочетание «*обнаружение знаний в базах данных*» (*англ.* knowledge discovery in data bases, KDD).

Основу методов Data Mining составляют всевозможные методы классификации, моделирования и прогнозирования, основанные на

применении *деревьев решений, искусственных нейронных сетей, генетических алгоритмов, эволюционного программирования, ассоциативной памяти, нечёткой логики.* К методам Data Mining нередко относят *статистические методы* (*дескриптивный анализ, корреляционный и регрессионный анализ, факторный анализ, дисперсионный анализ, компонентный анализ, дискриминантный анализ, анализ временных рядов, анализ выживаемости, анализ связей*). Такие методы, однако, предполагают некоторые априорные представления об анализируемых данных, что несколько расходится с целями Data Mining (обнаружение ранее неизвестных нетривиальных и практически полезных знаний));

- *применению общей терминологии и языка взаимодействия внутри корпорации.* Доступность метаданных, как уникального источника документации, для пользователей имеет и другие преимущества. Она гарантирует согласованные средства взаимодействия и интерпретации информации из хранилища, а также устраняет двусмысленность и обеспечивает согласованность сведений внутри компании.

Метаданные системы ХД содержатся в репозитории – структурированной системе хранения и извлечения, реализованной на основе СУБД. Для интерпретации метаданных необходимо хранить структуру репозитория (т. е. схему метаданных) и их семантику. Существуют различные способы или методы определения и хранения метаданных в хранилище. Один из методов – использование технологии XML.

7.2.1. ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ XML

XML метаданные. XML в настоящее время охватывает практически все аспекты информационных технологий. Что касается метаданных, то переоценить использование XML здесь сложно, оно распространяется на множество приложений, в том числе и на хранилища данных.

Основная функция XML – определять другие языки разметки. XML – это метаязык, а поэтому он оказывается очень эффективным форматом представления и обмена метаданными. Язык XML имеет

множество преимуществ, которые делают его идеальным средством описания.

1. Он понятен людям в чтении и написании, а следовательно, доступен новичкам и не вызывает страха.

2. Это открытая технология. Стандарт XML предложен компаний W3C. Никто не имеет прав собственности на этот язык. Он – платформонезависимый.

3. XML может применяться повсеместно. Анализатор XML можно найти везде, и, используя соответствующие инструменты, несложно сразу же внедрить эту технологию.

4. Язык гибок. Пожалуй, одно из главных достоинств XML то, что нет четких рамок применения. Каждый самостоятельно решает, как использовать его в своем приложении.

5. XML недорог для внедрения как в большой, так и в малой организации.

Можно привести и иные причины использования XML, а не других средств. Во-первых, структура метаданных часто бывает сложной, в ней множество вложенных отношений, а некоторые элементы метаданных могут повторяться. Во-вторых, если для хранения метаданных используется, например, РСУБД (реляционная система управления базой данных), то таблицы в базе не отражают сложных связей между элементами метаданных (трудно сгенерировать определения таблиц для описания отношений). И наоборот, XML задает структуру документа «самоописательным» образом. Его можно использовать для задания не только содержания, но и схемы, а следовательно, несложно найти взаимосвязь между различными участками XML-документа.

XML позволяет описывать метаданные, используемые любой программой или базой данных, в виде языка общения. XML обеспечивает связь между структурированной базой и неструктурированным текстом, передаваемым в формате XML. Так как XML обладает способностью к расширению, то можно использовать все гипертекстовые возможности для хранения самих метаданных или ссылок в любом формате.

7.2.2. ЗАДАЧА ПОСТРОЕНИЯ РЕПОЗИТОРИЯ

Центральным компонентом SIEM-системы является репозиторий, или информационное хранилище, в котором хранятся данные о событиях, правилах и инцидентах безопасности. Поэтому построение репозитория является ключевой задачей. Особую значимость эта задача приобретает в критической информационной инфраструктуре, где учитываются не только традиционные события безопасности компьютерной инфраструктуры, но также и параметры безопасности физического уровня.

Для разработки архитектуры репозитория SIEM-системы был проведен анализ стандартов в области управления событиями, таких как Security Content Automation Protocol (SCAP – Протокол автоматизации управления данными безопасности). SCAP – набор открытых стандартов, определяющих технические спецификации для представления и обмена данными по безопасности. Эти данные могут быть использованы для нескольких целей, включая автоматизацию процесса поиска уязвимостей, оценки соответствия технических механизмов контроля уровню защищенности. На основе описанных выше стандартов, как правило, разрабатываются реляционные модели данных при разработке программного обеспечения в области управления информацией и событиями безопасности, а в качестве хранилища используются реляционные СУБД. Однако при этом возникают различные трудности по выражению всех необходимых отношений между сущностями предметной области. Модель получается перегруженной и выборка данных занимает значительное время. Это обусловлено недостаточной гибкостью и низкой выразительностью языка запросов SQL, используемого в реляционных СУБД. Вторая проблема заключается в необходимости обновления схемы данных в соответствии с требованиями активно меняющейся предметной области. Для реляционных СУБД эта задача влечет за собой серьезные затраты временных ресурсов на больших объемах данных.

В качестве альтернативного решения по представлению данных предлагается использовать *онтологический подход*.

Актуальность использования онтологий в SIEM-системах, где необходимо хранить разнородную и быстро изменяющуюся

информацию, обусловлена также тем, что в этом случае изменение модели данных требует значительно меньших усилий, чем в реляционных моделях. При проектировании SIEM-системы необходимо обеспечить наиболее общую и в то же время неперегруженную модель данных, которая будет адаптирована и конкретизирована для каждой области применения в процессе внедрения.

Веб-сервисы – обработка и корреляция событий, поддержка решений, обнаружение угроз, визуализация, моделирование. Всемирная паутина является готовой платформой для создания и использования распределенных машинно-ориентированных систем на основе веб-сервисов. Веб-сервер выступает в качестве сервера приложений, к которым обращаются не конечные пользователи, а сторонние приложения. Это позволяет многократно использовать функциональные элементы, устранить дублирование кода, упростить решение задач интеграции приложений.

Веб-служба (веб-сервис, *англ.* web-service) – это сетевая технология, обеспечивающая межпрограммное взаимодействие на основе веб-стандартов. Консорциум W3C определяет веб-сервис как «программную систему, разработанную для поддержки межкомпьютерного (machine-to-machine) взаимодействия через сеть».

Концепции и протоколы веб-службы: Веб-сервис идентифицируется строкой URI (URI (/ˌjuː ɑːr ˈaɪ/ *англ. Uniform Resource Identifier*) – унифицированный (единообразный) идентификатор ресурса. URI – последовательность символов, идентифицирующая абстрактный или физический ресурс). Веб-сервис имеет программный интерфейс, представленный в машинно-обрабатываемом формате **WSDL** (Web Services Description Language – язык описания внешних интерфейсов веб-службы). Другие системы взаимодействуют с этим веб-сервисом путем обмена сообщениями протокола **SOAP** (Simple Object Access Protocol – протокол обмена сообщениями между потребителем и поставщиком веб-сервиса). В качестве транспорта для сообщений используется протокол HTTP (*англ.* Hyper Text Transfer Protocol) на прикладном уровне протокол передачи данных. Основой HTTP является технология «клиент–сервер», т. е. предполагается существование потребителей (клиентов),

которые инициируют соединение и посылают запрос, и поставщиков (серверов), которые ожидают соединения для получения запроса, выполняют необходимые действия и возвращают обратно сообщение с результатом.

Все спецификации, используемые в технологии, основаны на XML и соответственно наследуют его преимущества (структурированность, гибкость и т. д.) и недостатки (громоздкость, медлительность).

SOAP (Simple Object Access Protocol) – простой протокол доступа к объектам (компонентам распределенной вычислительной системы), основанный на обмене структурированными сообщениями. Как любой текстовый протокол, SOAP может использоваться с любым протоколом прикладного уровня: SMTP, FTP, HTTPS, но чаще всего SOAP используется поверх HTTP.

7.3. БАЗОВЫЕ ЭЛЕМЕНТЫ

В настоящее время мир информационной безопасности подвержен постоянному изменению. С целью поддержания своей актуальности развиваются и адаптируются системы защиты. Количество источников информации, из которых поступают данные по текущему состоянию защищенности, растет с каждым днем. Но в то же время с ростом инфраструктуры бывает сложно проследить за общей картиной происходящего в ней. Если своевременно не реагировать на возникающие угрозы и не предотвращать их, то не справится с угрозами даже сотня систем обнаружения вторжений. В этом случае на помощь приходят SIEM-системы.

Как правило, SIEM-система включает в себя следующие компоненты:

- средства, осуществляющие сбор данных;
- средства хранения;
- средства, осуществляющие обработку и анализ;
- средства управления, мониторинга и формирования уведомлений и отчетов.

Современные SIEM работают по двум направлениям сбора информации:

- первое – сбор информации о произошедших в ИС событиях,

сохраненных в журналах событий (логах) этих систем (в качестве источников событий выступает активное сетевое оборудование, операционные системы, средства защиты информации, облачные среды и т. д.)

- второе – сбор информации о сетевом трафике со SPAN-портов (Зеркалирование *англ.* port mirroring, SPAN – от Switched Port Analyzer) – дублирование пакетов одного порта *сетевого коммутатора* (или VPN) на другом. Большое количество управляемых сетевых коммутаторов позволяет дублировать трафик от одного до нескольких портов и/или ВЛВС (VLAN). В основном это применяется для мониторинга всего трафика в целях безопасности либо оценки производительности / загрузки сетевого оборудования с применением аппаратных средств или TAP-устройств (TAP — виртуальные сетевые драйверы ядра системы). Анализ сетевого трафика ведется вплоть до уровня приложений модели OSI (сетевая модель OSI (*англ.* oper. systems interconnection basic re-ference model – Базовая Эталонная Модель Взаимодействия Открытых Систем (ЭМВОС)) – сетевая модель стека (магазина) сетевых протоколов OSI/ISO (ГОСТ Р ИСО/МЭК 7498-1-99). Посредством данной модели различные сетевые устройства могут взаимодействовать друг с другом. Модель определяет различные уровни взаимодействия систем. Каждый уровень выполняет определенные функции при таком взаимодействии.

Рынок SIEM-решений представлен более чем 80 продуктами. Все продукты в той или иной степени обеспечивают выполнение следующих функций:

- сбор событий и захват сетевого трафика;
- нормализация собранной информации;
- централизованное хранение данных;
- фильтрация полученных данных;
- классификация информации;
- корреляция;
- визуализация и информирование.

SIEM-система сочетает функции двух других классов систем, относящихся к системам мониторинга и управления безопасностью информации: SIM (Security Information Management) и SEM (Security

Event Management). Иными словами, SIEM-система реализует функции, одновременно свойственные SIM- и SEM-системам. К функциям SIM-системы относятся сбор, хранение и анализ записей журналов, а также формирование необходимой отчетности. К функциям SEM-системы относится мониторинг событий безопасности в реальном времени, а также выявление инцидентов безопасности и реагирование на них.

Раскроем содержание основных механизмов функционирования SIEM-системы.

Нормализация означает приведение форматов записей журналов, собранных из различных источников, к единому внутреннему формату, который затем будет использоваться для их хранения и последующей обработки.

Фильтрация событий безопасности заключается в удалении избыточных событий из поступающих в систему потоков.

Классификация позволяет для атрибутов событий безопасности определить их принадлежность определенным классам.

Агрегация объединяет события, сходные по определенным признакам.

Корреляция выявляет взаимосвязи между разнородными событиями, что позволяет обнаруживать атаки на инфраструктуры, а также нарушения критериев и политики безопасности. Поиск общих атрибутов, связывание событий в значимые кластеры. Технология обеспечивает применение различных технических приемов для интеграции данных из различных источников для превращения исходных данных в значимую информацию. Корреляция является типичной функцией подмножества Security Event Management.

Анализ событий, инцидентов и их последствий включает процедуры моделирования событий, атак и их последствий, анализа уязвимостей и защищенности системы, определения параметров нарушителей, оценки риска, прогнозирования событий и инцидентов.

Генерация отчетов и предупреждений означает формирование, передачу, отображение и (или) печать результатов функционирования.

Принятие решений определяет выработку мер по реконфигурированию средств защиты с целью предотвращения атак или восстановления безопасности инфраструктуры.

Визуализация информаций предполагает представление в графическом виде данных, характеризующих результаты анализа событий безопасности и состояние защищаемой инфраструктуры и ее элементов.

7.4. СТРУКТУРА МОДЕЛИ ДАННЫХ, ОПИСЫВАЕМЫХ В ФОРМЕ ТРИПЛЕТОВ

Триплет является минимальной единицей хранения информации. Под триплетом понимается элементарное логическое утверждение, т. е., утверждение, высказываемое о ресурсе, имеет вид «субъект-предикат-объект».

Триплеты являются основой построения предложенной консорциумом W3C (World Wide Web Consortium) модели представления данных Resource Description Framework (RDF), предназначенной для записи утверждений о ресурсах различной природы в виде, пригодном для машинной обработки. Ресурсом в RDF может быть любая сущность – как информационная (например, веб-сайт или изображение), так и неинформационная (например, человек, город или некое абстрактное понятие). Для обработки RDF-данных используются различные языки запросов. Языком запросов, рекомендуемым W3C, является SPARQL Protocol and RDF Query Language (SPARQL). Множество RDF-утверждений создают ориентированный граф, в котором вершины – это субъекты и объекты, а ребра помечены предикатами. Однако RDF-граф, взятый в отдельности, не раскрывает семантики описываемой предметной области. Для этой цели необходимы дополнительные средства.

Исходя из сказанного видим, что RDF и триплетная модель хранения связанных данных предоставляют гибкие и унифицированные средства для хранения распределенных иерархически организованных данных. Для хранения триплетов связанных данных применяются специализированные хранилища. Таким образом, моделирование данных с помощью триплетов и реализация возможности их хранения и обработки в SIEM-системе являются достаточно привлекательными.

Системы хранения, ориентированные на работу с триплетами, получили название хранилищ триплетов (triple stores). Хранилища

триплетов – это новое и интенсивно развивающееся направление в области баз данных.

Хранилища триплетов можно разделить на две основные группы:

1) реализованные, как независимые решения (автономные);

2) являющиеся компонентом комплексной семантической системы хранения.

Примеры автономных решений: Allegro Graph, Big OWLIM и Pellet Db. Примеры второй группы хранилищ: системы Virtuoso, Open Anzo и Semantics.Server.

Система Virtuoso Open Source наиболее удобна и обеспечивает гибридный подход к построению репозитория в перспективных SIEM–системах. Virtuoso с полным основанием может считаться комплексной системой хранения, так как кроме RDF-данных она обеспечивает хранение и интеграцию данных в других наиболее популярных форматах. В этом плане для перспективных SIEM-систем она выглядит предпочтительней, чем другие SIEM-системы. Оценки показали, что производительность Virtuoso при выполнении запросов на выборке RDF-данных была выше, чем у остальных, в 1,5...2,5 раза (7352 запроса/час).

Virtuoso состоит из модулей однородных хранилищ и модулей виртуальных баз данных. Модули однородных хранилищ обеспечивают хранение данных в RDF-формате (для хранения триплетов). RDF-граф строится на основе элементарных высказываний (триплетов). Форма высказывания – бинарное отношение (S-P-O). Для обработки RDF-данных предлагается реализовать языки запросов: SPARQL. Virtuoso поддерживает язык запроса SPARQL встроенный в SQL.

7.5. СРЕДСТВА, ПОЗВОЛЯЮЩИЕ ОСУЩЕСТВЛЯТЬ ВСЕ ВИДЫ ЗАПРОСОВ

Реляционная модель, десятилетиями служившая основой технологии работы с данными, теперь не является главенствующей, – появляются новые задачи, требующие учета и выявления существенно большего количества взаимосвязей. Среди новых методов – модель RDF.

Наиболее распространенной моделью хранения данных с конца 1971-х годов была реляционная, она и до сих пор является стандартом де-факто на хранение структурированных данных, а язык SQL – стандартом на их обработку. Однако доля структурированных данных становится все меньше, и реляционная модель испытывает все больше проблем при работе со значительными объемами данных давно.

Основа RDF – это хорошо известное специалистам по искусственному интеллекту представление данных в виде утверждений «субъект–предикат–объект», описывающих направленную связь от субъекта к объекту. Для идентификации субъектов, объектов и предикатов используется идентификатор Uniform Resource Identifier (URI), являющийся обобщением понятия URL (**Единый указатель ресурса** (*англ. Uniform Resource Locator*) – единообразный локатор (определитель местонахождения) ресурса. Ранее назывался Universal Resource Locator – **универсальный указатель ресурса**. URL служит стандартизированным способом записи адреса ресурса в сети Интернет.). То есть, RDF –это информационная подсистема, предназначенная для хранения RDF-триплетов и выполнения запросов к ним.

Модель RDF служит для описания данных, но не описывает методы их обработки. Существует целый ряд языков запросов к RDF-данным: DQL, N3QL, R-DEVICE, RDFQ, RDQ, RDQL, но самым популярным стал SPARQL, принятый в качестве стандарта W3C. Язык SPARQL в отличие от SQL обладает более стройной структурой и мощью. Основная часть запроса на SPARQL – шаблон, описывающий подграф, который требуется найти в общем графе.

SPARQL (от *англ.* SPARQL Protocol and RDF Query Language) – *язык запросов к данным*, представленным по модели RDF, а также *протокол* для передачи этих запросов и ответов на них. SPARQL является рекомендацией *консорциума W3C* и одной из *технологий семантической паутины*.

Общая схема SPARQL-запроса выглядит так:

```
PREFIX foaf: <http://example.com/resources/>
# префиксные объявления
FROM...
# источники запроса
```

```
SELECT...
# состав результата
WHERE {...}
# шаблон запроса
ORDER BY...
# модификаторы запроса
```

Префиксные объявления служат для указания сокращений универсальных идентификаторов ресурса (URI).

7.6. АЛГОРИТМ ОСУЩЕСТВЛЕНИЯ ЗАПРОСОВ

Постановка задачи. Найти даты выхода серий всех сезонов сериала «Клан Сопрано». Требуется вывести на экран серию, дату, номер эпизода и номер сезона сериала «Клан Сопрано». Отсортировать все данные по убыванию даты выхода сериала.

Решения задачи

Алгоритм

Шаг 1. Открываем среду Open Link iSPARQL: http://dbpedia.org/isparql/

(нажмите Ctrl и щелкните ссылку).

Шаг 2. В рабочую область SPARQL Query пишем код (рис. 7.1):

```
PREFIX dbpo: <http://dbpedia.org/ontology/> SELECT *
    WHERE
    {
    ?e dbpo:series <http://dbpedia.org/resource/The_Sopranos>.
    ?e dbpo:releaseDate ?date.
    ?e dbpo:episodeNumber ?number.
    ?e dbpo:seasonNumber ?season.
    }
ORDER BY DESC(?date)
```

В этом запросе префикс «dbpo» обозначает «http://dbpedia. org/ ontology/»

Мы ссылаемся на этот адрес и вытаскиваем все нужные нам данные из этой базы.

[Здесь, SELECT – выбрать, WHERE – где, а дальше в {} идут запросы]
Subject Predicate Object
?e dbpo:series (имя серий) dbpedia:The_Sopranos
?e dbpo:releaseDate (дата серий) ?date (результат)
?e dbpo:episodeNumber (номер эписода) ?number (результат)
?e dbpo:seasonNumber (номер сезона) ?season (результат)

ORDER BY DESC (? date) – сортировка по убыванию даты выхода серии.

Шаг 3. В верхней панели нажимаем ВЫПОЛНИТЬ ЗАПРОС – Run Query  и получаем результат.

Шаг 4. Результат выявил 655 триплетов для этого запроса.

Для идентификации субъектов, объектов и предикатов используем идентификатор URI (Uniform Resource Identifier). В табличном виде мы можем увидеть отдельные столбцы «S–P–O» с URI адресами, в которых были выявлены триплеты.

Subject
http://dbpedia.org/sparql?default-graph-uri=http://dbpedia.org&maxrows=50&query= PREFIX dbpo: SELECT * WHERE {?e dbpo:series .?e dbpo:releaseDate?date.?e dbpo:episodeNumber?number.?e dbpo:seasonNumber?season. } ORDER BY DESC(?date) &format=application/rdf+xml#r0c0
Predicete http://www.w3.org/2005/sparql-results#value
Object http://dbpedia.org/resource/Made_in_America_(The_Sopranos)

Шаг 5. Чтобы было понятно покажем результат в виде графических триплетов. Для этого в верхней панели нажимаем на кнопку – Visualize и получаем результат (рис. 7.1).

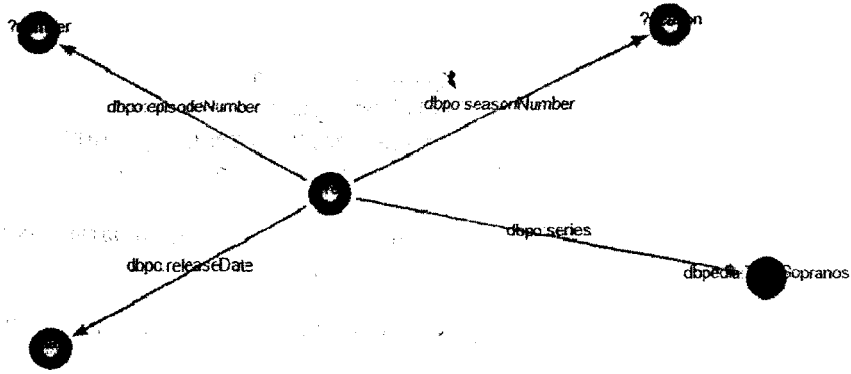

Рис. 7.1. Результат в виде графических триплетов

Здесь утверждения RDF создают ориентированный граф, в котором вершины – это субъекты и объекты, а ребра помечены предикатами;

вершина:?e – **субъект;**

вершины: dbpedia:The_Sopranos,?date,?number,?season - **объекты**

ребра: dbpo:series, dbpo:releaseDate, dbpo:episodeNumber, dbpo: seasonNumber – **предикаты**

Шаг 6. Проверим выполнение запросов данной задачи. Для этого покажем результат в виде ROW TRIPLES (в виде содержание столбца «объекта») (рис. 7.2) и в табличном виде без ссылок на адрес (рис. 7.3).

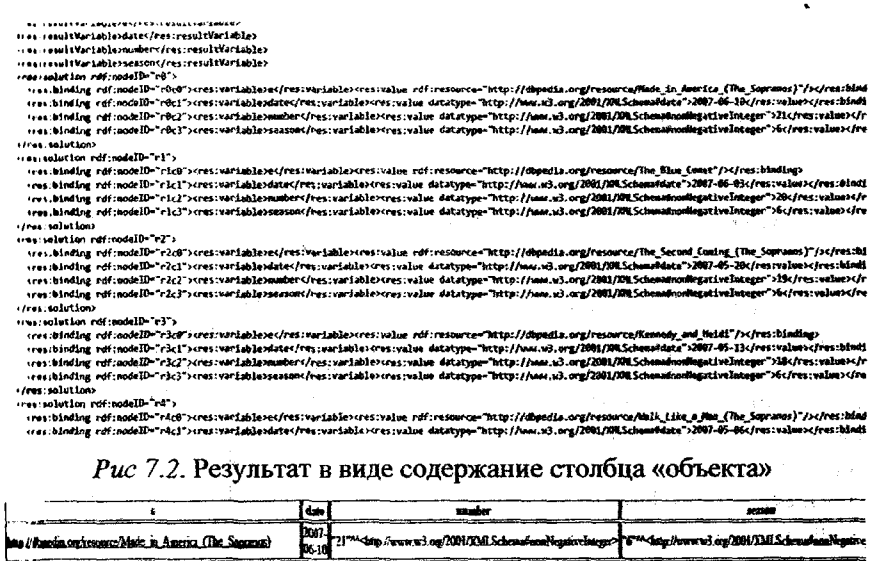

Рис 7.2. Результат в виде содержание столбца «объекта»

e	date	number	season
http://dbpedia.org/resource/Made_in_America_(The_Sopranos)	2007-06-10	"21"^^<http://www.w3.org/2001/XMLSchema#nonNegativeInteger>	"6"^^<http://www.w3.org/2001/XMLSchema#nonNegative
http://dbpedia.org/resource/The_Blue_Comet	2007-05-07	"20"^^<http://www.w3.org/2001/XMLSchema#nonNegativeInteger>	"6"^^<http://www.w3.org/2001/XMLSchema#nonNegative
http://dbpedia.org/resource/Kennedy_and_Heidi	2007-05-13	"18"^^<http://www.w3.org/2001/XMLSchema#nonNegativeInteger>	"6"^^<http://www.w3.org/2001/XMLSchema#nonNegative
http://dbpedia.org/resource/Soprano_Home_Movies	2007-04-08	"13"^^<http://www.w3.org/2001/XMLSchema#nonNegativeInteger>	"6"^^<http://www.w3.org/2001/XMLSchema#nonNegative
http://dbpedia.org/resource/Luxury_Lounge	2006-04-23	"7"^^<http://www.w3.org/2001/XMLSchema#nonNegativeInteger>	"6"^^<http://www.w3.org/2001/XMLSchema#nonNegative
http://dbpedia.org/resource/Mr._&_Mrs._John_Sacrimoni_Request	2006-04-09	"5"^^<http://www.w3.org/2001/XMLSchema#nonNegativeInteger>	"6"^^<http://www.w3.org/2001/XMLSchema#nonNegative
http://dbpedia.org/resource/The_Fleshy_Part_of_the_Thigh	2006-04-02	"4"^^<http://www.w3.org/2001/XMLSchema#nonNegativeInteger>	"6"^^<http://www.w3.org/2001/XMLSchema#nonNegative
http://dbpedia.org/resource/Pass_the_Club	2006-03-19	"2"^^<http://www.w3.org/2001/XMLSchema#nonNegativeInteger>	"6"^^<http://www.w3.org/2001/XMLSchema#nonNegative
http://dbpedia.org/resource/All_Due_Respect_(The_Sopranos)	2004-06-06	"13"^^<http://www.w3.org/2001/XMLSchema#nonNegativeInteger>	"5"^^<http://www.w3.org/2001/XMLSchema#nonNegative
http://dbpedia.org/resource/Long_Term_Parking	2004-05-23	"12"^^<http://www.w3.org/2001/XMLSchema#nonNegativeInteger>	"5"^^<http://www.w3.org/2001/XMLSchema#nonNegative
http://dbpedia.org/resource/Marco_Polo_(The_Sopranos)	2004-04-25	"9"^^<http://www.w3.org/2001/XMLSchema#nonNegativeInteger>	"5"^^<http://www.w3.org/2001/XMLSchema#nonNegative
http://dbpedia.org/resource/In_Camelot	2004-04-18	"7"^^<http://www.w3.org/2001/XMLSchema#nonNegativeInteger>	"5"^^<http://www.w3.org/2001/XMLSchema#nonNegative
...	2004-...	...	...

Рис. 7.3. Результат в табличном виде без ссылок на адрес

Из полученного результата видно, что условие задачи было выполнено. Все запросы сделаны. Выведенный на экран Имя серий (e), дату выхода (date), номер серий (number) и сезон серий (season). И все эти триплеты отсортировали по убыванию даты выхода серий.

Мы заметили, что на столбце date серия вышла 10 июня 2007 года, а следующая – 3 июня 2007 года, дальше – 13 мая 2007 года и так дале идет по обратной сортировке.

7.7. АЛГОРИТМ ДЛЯ ОПРЕДЕЛЕНИЯ УРОВНЯ ПОЛИТИКИ БЕЗОПАСНОСТИ RDF-ДАННЫХ

В настоящее время семантическая технологии быстро развиваются и играют важную роль на предприятии. Известно, что в информационной среде существуют угрозы, такие как Троянский конь, вирусы, черви осуществляющие разрушающие действия в работе с базами данных в Интернете. Так как сеть Интернет направленно развивается в сторону семантической сети, то угроза безопасности информации будет возрастать. Проблему безопасности данных необходимо рассматривать с самого начала процесса разработки семантической сети. Для обеспечения её безопасности необходимо обеспечить безопасность всех её компонентов.

В современных работах по безопасности семантических данных приводится много решений по вопросу безопасности XML-данных, но мало практических работ по безопасности RDF-данных и их взаимодействию [77]. В данном разделе показаны начальные этапы по обеспечению безопасности RDF-данных, предлагаются алгоритмы для контроля доступа пользователей к элементам триплета или самому RDF-триплету.

Рассмотрим метку безопасности для триплета RDF-данных. Каждый RDF-документ состоит из графов (триплетов), являющихся набором троек: субъект (s), предикат (p), объект (o). В целях безопасности RDF-данных каждые элементы триплета находятся на своих уровнях безопасности согласно своим меткам обеспечения (sl_1, sl_2,..., sl_n), созданными пользователями. Например, sl_1 соответствует отсутствию уровня безопасности, sl_2 соответствует конфиденциальности, ..., sl_n соответствует сверхсекретности.

В триплете субъект, предикат, объект могут иметь одинаковую метку sl или разные метки безопасности sl_s, sl_p, sl_o (где sl_s - метка для

субъекта, sl_p - метка для предиката, sl_o - метка для объекта). В случае, когда три элемента имеют одну метку sl, то sl является меткой безопасности для триплета. Если три метки являются разными (sl_s, sl_p, sl_o), то надо реализовывать минимальную границу метки sl_{min} этих меток, тогда sl_{min} является меткой безопасности триплета. К этому методу чувствительна метка данных, связанная с RDF-данными и ограничивает несанкционированный доступ к триплетам, ресурсам и к наследованным триплетам, образованным в результате операции наследования.

Один и тот же ресурс может являться субъектом или объектом (иногда является предикатом) в разных ситуациях, следовательно, он может иметь разные чувствительные метки (sl_1, sl_2,..., sl_n) в зависимости от своего положения. Триплет, имеющий ресурс в конкретном положении, должен иметь конкретную метку sl_t, охватывающую соответствующую метку ресурса в данной позиции, и обозначается $sl_t \leq \min(sl_1, sl_2, \ldots, sl_n)$. В этом случае триплет может быть доступен только пользователям с метками st_{user}, охватывающими метки триплета и ресурса, и обозначается $st_{user} \leq sl_t$.

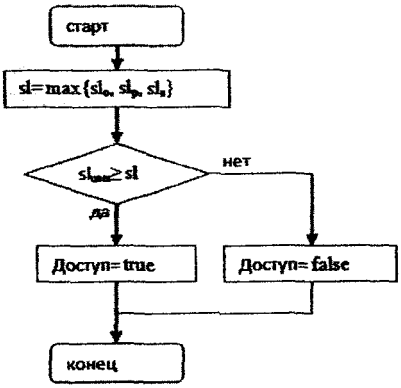

Рис. 7.4. Алгоритм для определения метки безопасности триплета RDF-данных

Для определения минимальной чувствительности метки безопасности триплета и возможности доступа пользователя к триплету в [78] предложен алгоритм 1, приведённый на рисунке 7.4.

Например, если sl_s = неклассифицированной, sl_p = неклассифицированной, sl_o = секретной. Тогда метка безопасности для триплета является секретной. Если секретная метка охватывает уровень доступа пользователя, то у пользователя нет доступа над триплетом. В другом случае, если его уровень доступа является секретностью, или сверхсекретностью, то он может выполнять разные операции на этом триплете.

Безопасность для компонентов триплета RDF-данных. Как правило, ресурсы, входящие в положении объекта триплета, могут быть описаны с помощью использования дополнительных утверждений RDF. Ресурс RDF, находящийся в позиции объекта этого триплета, может указываться в позиции субъекта другого триплета. Тогда если ресурс в позиции объекта не имеет чувствительной метки, то метка, связанная с таким ресурсом в позиции субъекта, является меткой по умолчанию для объекта [79].

Ресурс появляется в роли субъекта триплета, когда утверждение сделано о ресурсе. В этом случае, чувствительная метка sl_s, связанная с ресурсом, должна обладать следующими характеристиками:

1. sl_t представляет минимальную чувствительную метку для любого триплета, использующего ресурс в качестве субъекта. Иными словами, чувствительная метка sl_t для триплета должна охватывает метку для субъекта sl_s, где $st_t \geq sl_s$;
2. метка sl_{tnew} для нового добавленного триплета является инициализированной пользователем, только если она доминирует метку, связанную с субъектом триплета, значит $sl_{tnew} \geq sl_s$;
3. только пользователь, имеющий доступную метку st_{user}, доминирующую метку субъекта и триплета, может читать триплет, значит $st_{user} \geq sl_t$ и $st_{user} \geq sl_s$.

По умолчанию sl_s возникает в среде использования пользователя, когда ресурс RDF принимается в роли субъекта триплета при начальном времени. Чувствительная метка по умолчанию в этом

случае устанавливается в начальной чувствительной метке триплета пользователя. Чувствительная метка по умолчанию является меткой, вставленной пользователем для всех триплетов.

Для проверки правильности меток безопасности триплетов SL $=\{sl_1, sl_2, , sl_n\}$ и добавления нового триплета T_{new}, в которых субъект S имеет метку безопасность, используется алгоритм 2 (рис. 7.5).

Для определения минимальной чувствительности метки безопасности триплета и возможности доступа пользователя к триплету в [78] предложен алгоритм 1, приведённый на рисунке 7.4.

Например, если sl_s = неклассифицированной, sl_p = неклассифицированной, sl_o = секретной. Тогда метка безопасности для триплета является секретной. Если секретная метка охватывает уровень доступа пользователя, то у пользователя нет доступа над триплетом. В другом случае, если его уровень доступа является секретностью, или сверхсекретностью, то он может выполнять разные операции на этом триплете.

Безопасность для компонентов триплета RDF-данных. Как правило, ресурсы, входящие в положении объекта триплета, могут быть описаны с помощью использования дополнительных утверждений RDF. Ресурс RDF, находящийся в позиции объекта этого триплета, может указываться в позиции субъекта другого триплета. Тогда если ресурс в позиции объекта не имеет чувствительной метки, то метка, связанная с таким ресурсом в позиции субъекта, является меткой по умолчанию для объекта [79].

Ресурс появляется в роли субъекта триплета, когда утверждение сделано о ресурсе. В этом случае, чувствительная метка sl_s, связанная с ресурсом, должна обладать следующими характеристиками:

4. sl_t представляет минимальную чувствительную метку для любого триплета, использующего ресурс в качестве субъекта. Иными словами, чувствительная метка sl_t для триплета должна охватывает метку для субъекта sl_s, где $st \geq sl_s$;

5. метка sl_{tnew} для нового добавленного триплета является инициализированной пользователем, только если она доминирует метку, связанную с субъектом триплета, значит $sl_{tnew} \geq sl_s$;

6. только пользователь, имеющий доступную метку st_{user}, доминирующую метку субъекта и триплета, может читать триплет, значит $st_{user} \geq sl_t$ и $st_{user} \geq sl_s$.

По умолчанию sl_s возникает в среде использования пользователя, когда ресурс RDF принимается в роли субъекта триплета при начальном времени. Чувствительная метка по умолчанию в этом случае устанавливается в начальной чувствительной метке триплета пользователя. Чувствительная метка по умолчанию является меткой, вставленной пользователем для всех триплетов.

Для проверки правильности меток безопасности триплетов SL $=\{sl_1, sl_2, , sl_n\}$ и добавления нового триплета T_{new}, в которых субъект S имеет метку безопасность, используется алгоритм 2 (рис. 7.5).

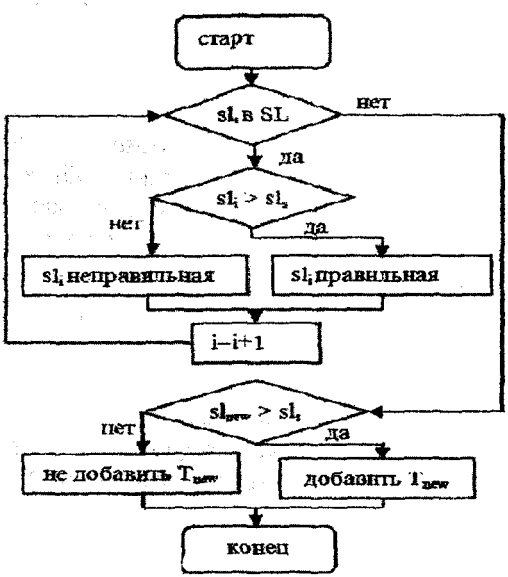

Рис. 7.5. Алгоритм для добавления нового триплета

RDF-данные являются основными элементами семантических данных. Для безопасности семантической базы данных необходимо обеспечить безопасность RDF-данных. В данном разделе были рассмотрены основные элементы RDF-данных. Описаны алгоритмы для определения меток безопасности триплета, а также для проверки права доступа пользователей к триплетам.

В RDF-данных ресурс может иметь разные роли (субъект, предикат, объект) в различных триплетах. Из-за этого метки безопасности триплетов, составленные для конкретного вида ресурса, зависят от его меток безопасности. Для проверки правильности меток безопасностей триплетов используется алгоритм 2.

ВЫВОДЫ ПО РАЗДЕЛУ 7

В этом разделе раскрываются содержание основных механизмов функционирования SIEM-системы: нормализация; фильтрация событий безопасности; классификация для атрибутов событий безопасности; агрегация, объединяющая события, сходные по определенным признакам; корреляция взаимосвязи между разнородными событиями; оценки риска; прогнозирование событий и инцидентов; генерация отчетов и предупреждений, означающая формирование, передачу, отображение и (или) печать результатов функционирования.

Кроме того, дается описание структуры модели данных в форме триплетов, а также алгоритмов, осуществляющих запрос компонентов базы данных и описание процедуры обработки RDF-данных.

ЗАКЛЮЧЕНИЕ

Для успешной реализации мероприятий защиты информационных инфраструктур необходимо решить ряд задач, основная из которых связана с созданием системы мониторинга угроз безопасности. Системы мониторинга реализуют *апостериорный* подход к защите информации, главной целью создания которой является снижение воздействия на инфраструктурные объекты до минимального уровня риска и минимизация возникающего ущерба.

Одним из наиболее перспективных и эффективных направлений в создании систем мониторинга угроз безопасности в настоящее время считается применение SIEM-системы, обеспечивающей управление информацией и событиями безопасности. Исследования вопросов построения SIEM-систем для сервисных информационных инфраструктур проводятся в настоящее время в проекте MASSIF Седьмой рамочной программы Европейского Союза. Целью подготовки настоящего учебного пособия было изложение основных взглядов на построение SIEM-систем и результатов рассмотренного выше полученных специалистами в рамках проекта MASSIF. Значительное повышение уровня информационной безопасности в информационной инфраструктуре за счет обеспечения возможности манипулировать в режиме времени, близком к реальному, информацией о безопасности и осуществлять проактивное управление инцидентами и событиями безопасности. «Проактивный» означает «действующий до того, как ситуация станет критической». Предполагается, что проактивное управление инцидентами и событиями безопасности основывается на автоматических механизмах, которые используют информацию об «истории» анализируемых сетевых событий и прогнозе будущих событий, а также на автоматической подстройке параметров мониторинга событий к текущему состоянию защищаемой системы.

В качестве системообразующей технологии, реализующей указанные функциональные возможности, представляется целесообразным применять технологию SIEM. Однако системы мониторинга безопасности для сервисных инфраструктур, созданные на ее основе, следует относить к SIEM-системам нового поколения,

разработке которых посвящен проект MASSIF. Сценарии применения SIEM-системы, определенные в MASSIF, в полной мере задают функциональные и реализационные требования к данной системе.

Задачи, описанные количественными и качественными признаками с преобладанием последних, относятся к слабоструктурированным проблемам. Современный подход их к решению базируется на методах искусственного интеллекта (ИИ). Считается, что ИИ – это самообучающийся инструмент, усиливающий деятельность человека по генерации и принятию решений. Кроме того, по последней трактовке, ИИ – это экспериментальная научная дисциплина, в которой роль эксперимента заключается в проверке и уточнении ИИ, представляющих собой аппаратно-программные комплексы.

Разработка методов и моделей в области представления, сбора, хранения и обработки информации о событиях безопасности, позволяющих реализовать требования, предъявляемые к SIEM-системе нового поколения, является актуальной научной задачей, имеющей большое государственное и народнохозяйственное значение и определяющей новые направления научных исследований в области информационной безопасности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Котенко И.В. Проактивные механизмы защиты от сетевых червей: подход, реализация и результаты экспериментов / И.В. Котенко, В.В. Воронцов, А.А. Чечулин, А.В. Уланов // Информационные технологии. –2009. –№ 1. – С. 37–42.

2. *Котенко И.В.* Интеллектуальные механизмы управления кибербезопасностью // Управление рисками и безопасностью: труды института системного анализа Российской академии наук (ИСА РАН). – Т. 41. – М., URSS, 2009. – С. 57–103.

3. Miller D.R., Harris Sh., Harper A.A., VanDyke S., Black Ch. Security Information and Event Management (SIEM) Implementation. McGraw–Hill Companies. 2011. – 430 p.

4. Nicolett M., Kavanagh K.M. Magic Quadrant for Security Information and Event Management. Gartner, 12 May 2011. – 20 p.

5. ArcSight Express. http://www.arcsight.com/products/products–esm/arcsight–express.

6. ArcSight Logger. http://www.arcsight.com/products/products–logger/

7. Common Event Format. http://www.arcsight.com/solutions/solutions–cef.

8. RSA enVision. http://www.rsa.com/node.aspx?id=3170

9. QRadar SIEM. http://q1labs.com/Products/QRadar–SIEM.aspx

10. Tivoli Security Information and EventManager. http://www–14.ibm.com/software/products/ru/ru/securityinforma-tionandeventmana ger/

11. Symantec Security Information Manager. http://www.symantec.com/business/security–information manager

12. Loglogic. http://loglogic.com

13. Novell Sentinel Log Manager 1.0.0.5. Installation Guide. March 31, 2010.

14. Проект MASSIF «Управление информацией и событиями безопасности в инфраструктурах услуг». Проект Седьмой рамочной программы Европейского Союза.http://www.massif–project.eu/

15. OSSIM. http://www.alienvault.com/community

16. Prelude as a Hybrid IDS Framework. SANS Institute InfoSec Reading Room, 2009. 43 p.

17. The Intrusion Detection Message Exchange Format (IDMEF). RFC 4765. 2007.

18. *Саенко И.Б.* Разработка информационного хранилища системы управления информацией и событиями безопасности для гетерогенной инфраструктуры / И.Б. Саенко, О.В. Полубелова, И.В. Котенко // Методы и технические средства обеспечения безопасности информации: матер. XX Общеросс. науч.-техн. конф. 27 июня – 1 июля 2011 года. – Санкт-Петербург: Изд-во Политехн. ун-та. 2011. – С. 41–42.

19. SCAP [Электронный ресурс]- http://scsp.nist.gov/.

20. Ogle D., Kreger H., Salahshour A., Compropst J., Labadie E., Chessell M., Horn B.,Gerken J., Schoech J., Wamboldt M. Canonical Situation Data Format: The Common Base Event V1.0.1. International Business Machines Corporation, 2004, 73 p.

21. Common Information Model (CIM) Standards, DMTF. http://dmtf.org/ standards/cim

22. Kotenko I., Stepashkin M. Attack Graph based Evaluation of Network Security // Lecture Notes in Computer Science. V 4237 / 2006. P 216-227.

23. Alien Vault User's Manual. 2011.

24. Reasons for Migrating from Cisco MARS to Accel Ops. http://www.accclops.net/product/marsbeyond.php

25. Prelude as a Hybrid IDS Framework. SANS Institute Info Soc Reading Room, 2009.

26. ShenkJ. Arc Sight Logger Review. A SANS Whltepaper. January 2009.
http://www.arcsight.com/collateral/whitepapers/ArcSight_Combat_Cyber_Crime_ with_Logger.pdf.

27. Buecker A., Amado J., Druker D., LorenzC., Muehlenbrock F, Tan R. IT Security Compliance Management Design Quidewith IBM Tivoli Security Information and Event Manager. IBM Redbooks. 2010.

28. Novell Sentinel Log Manager 1.0.0.5. Installation Guide. March 31, 2010.

29. SCAP. http://scap.nist.gov.

30. Ogle D., Kreger H, Salahshour A., Compropst J., Labadie E., Chessell M., Horn B., GerkenJ., SchoechJ., Wamboldt M. Canonical

Situation Data Format: The Common Base Event V1.0.1 // International Business Machines Corporation. 2004.

31. Common Information Model (CIM) Standards, DMTF. http://dmtf.org/ standards/cim

32. Parmelee M.C. Toward an Ontology Architecture for Cyber-Security Standards it Proceedings of the 2010 Semantic technology for intelligence, defense, and security conference. 2010.

33. Lopez de Vergara J.E., Viltagrd V.A., Berrocal J. Applying the Web Ontology Language to management information definitions // IEEE Communications Magazine. 2004. P. 68–74.

34. MASSIF FP7 Project. MAnagement of Security information and events in Service Infrastructures Электронный ресурс]. – Режим доступа: http://www. massif-project.eu

35. Verissimo P., Neves N., Correia M. The middleware architecture of MAFTIA: A blueprint // Proceedings of the IEEE Third Survivability Workshop, October 2000. – P. 157–161.

36. *Котенко И.В.* Построение системы интеллектуальных сервисов для защиты информации в условиях кибернетического противоборства / И.В. Котенко, И.Б. Саенко // Труды СПИИРАН. Вып. 3(22). – СПб.: Наука, 2012. – С. 84–100.

37. *Полубелова О.В.* Применение онтологий и логического вывода для управления информацией и событиями безопасности / О.В. Полубелова, И.В. Котенко, И.Б. Саенко, А.А. Чечулин // Системы высокой доступности. – 2012. – № 2. – Т. 8. – С. 100–108.

38. Kotenko I., Polubelova O., Saenko I. Data Repository for Security Information and Event Management in Service Infrastructures H SECRYPT2012. International Conference on Security and Cryptography. Proceedings. Rome, Italy. 24–27 July 2012. – P. 308–313.

39. VirtuosoUniversalServer [Электронный ресурс]. – Режим доступа: http://virtuoso.openlinksw.com/.

40. Schutte J., RiekeR., WinkelvosT. Model-based security event management // Lecture Notesin Computer Science, vol. 7531, Springer, 2012, p. 181-190.

41. Kotenko I., Chechulin *A*. Common Framework for Attack Modeling and Security Evaluation in SIEM Systems // 2012 IEEE International Conference on Green Computing and Communications, Conference on Internet of Things, and Conference on Cyber, Physical and Social

Computing. Bевапзоп, France, November 20–23, 2012. Los Alamitos, California. IEEE Computer Society. 2012. P. 94–101.

42. Strauss C., Stummer C. Multiobjective decision support in IT-risk management // International Journal of Information Technology & Decision Making, vol. 1, no. 2, 2002. – P. 251–268.

43. Sun M., Steuer R.E. InterQuad: An interactive quad tree based procedure for solving the discrete alternative multiple criteria problem // European Journal of Operational Research, vol. 89, no. 3, 1996. – P. 462–472.

44. Jobson J.D. Applied Multivariate Data Analysis: Volume II: Categorical and multivariate methods, Berlin / Heidelberg: Springer, 1992. – 731 p.

45. Stummer C., Kiesling E., Gutjahr W.J. A multicriteria decision support system for competence- driven project portfolio selection И International Journal of Information Technology & Decision Making, vol 8, no. 2, 2009. – P. 379–401.

46. OrBAC. Organization based Access Control Telecom Bretagne [Электронный ресурс]. – Режим доступа:http://orbac.org/.

47. *Новикова Е.С.* Механизмы визуализации в SIEM-системах // Системы высокой доступности / Е.С. Новикова, И.В. Котенко. – № 2. – 2012. – С. 91–99.

48. Miller D.R., Harris Sh., Harper A.A. Van-Dyke S., Black Ch. Security Information and Event Management (SIEM) Implementation. McGrawHill Companies. 2011. – 430 p.

49. Risk management: Implementation principles and inventories for risk management/risk assessment methods and tools. ENISA (European Network and Information Security Agency). 2006.

50. Chi-Chun Lo, Wan-Jia Chen. A hybrid information security risk assessment procedure considering interdependences between controls // Expert Systems with Applications. 2011. – V. 39. – P. 248–257.

51. *Абденов А.Ж.*. Оценивание риска в информационных системах на основе объективных и экспертных оценок / А.Ж. Абденов, Р.Н. Заркумова-Райхель // Вопросы защиты информации. – 2015. – № 1. – С. 64–70.

52. *Kumamoto H., Henley E.* Probabilistic risk assessment and management for engineers and scientists. 2-nd edition. Institute of Electrical and Electronics Engineers. Inc. – New York, 1996. – 620 p.

53. *Заркумова-Райхель Р.Н., Абденов А.Ж.* Прогнозирование количества инцидентов в системе информационной безопасности предприятия при помощи динамической модели / Р.Н. Заркумова-Райхель, А.Ж. Абденов // Фундаментальные исследования. – 2012. – № 6 (2). – С. 429–434.

54. *Синицын И.Н.* Фильтры Калмана и Пугачева: учебное пособие. – М.: Университетская книга, Логос, 2006. – 640 с.

55. *Мещеряков Р.В* Теоретические основы компьютерной безопасности. Раздел 2 / Р.В. Мещеряков, Г.А. Праскурин. – Томск: Томский государственный университет систем управления и радиоэлектроники, 2004. – С. 97–148.

56. *Абденов А.Ж.* Методика расчета рисков на основе объективных и субъективных оценок в соответствующих узлах SIEM-системы / А.Ж. Абденов, В.А. Трушин, Г.А. Абденова, Ю.А. Иноземцева // Искусственный интеллект и принятие решений. – 2016. – № 3. – С. 87–99.

57. NIST SP 800-30:2012. Guide for conducting Risk Assessments [электронный ресурс] // National Institute of Standards and Technology. – URL:

58. *Климова Е.Г.* Разработка системы усвоения об окружающей среде на основе ансамблевого фильтра Калмана / Е.Г. Климов, Г.А. Платов, Р.В. Киланова // Вычислительные технологии. – 2014. – Т. 19. – № 3. – С. 27–37.

59. *Абденов А.Ж.* Методика оценки риска для информационных систем на основе экспертных оценок: учебное пособие / А.Ж. Абденов, С.А. Белкин, Р.Н. Заркумова-Райхель. – Новосибирск: Изд-во НГТУ, 2014. – 71 с.

60. *Котенко И.В.* Применение онтологий и логического вывода для управления информацией и событиями безопасности / И.В. Котенко, И.Б. Саенко О.В. Полубелова, А.А. Чечулин // Системы высокой доступности. – № 2. –Т. 8. – 2012. – С. 100–108.

61. *Котенко И.В.* Применение онтологий и логического вывода для управления информацией и событиями безопасности / И.В. Котенко, И.Б. Саенко, О.В. Полубелова, А.А. Чечулин // Системы высокой доступности. – № 2. – Т. 8, 2012. – С. 100–108.

62. *Луганский В.Э.* К вопросу о функционировании интеллектуальных систем поддержки принятия решений / В.Э.

Луганский, А.А. Марков, С.А. Селиванов // Информатизация и связь. – 2013. – № 3. – С. 55–59.

63. Abdenov A.Zh., Trushin V.A., Abdenova G.A. Complex method to calculate objective assessments of information systems protection to improve expert assessments reliability // IOP Conf. Series: Journal of Physics: Conf. 2018, Series 944. – P. 1-15.

64. *Фицурина М.С.* Антикризисное использование инструментов маркетинга в фитнес индустрии / М.С. Фицурина, А.А. Кузьменко // Sciences Europe. – № 8(8). – 2016. – Экономические науки. – С. 115–118.

65. *Синяева И.М.* Маркетинг: учебное пособие. – М.: Вузовский учебник: НИЦ ИНФРА – М, 2014. – 384 с.

66. *Зуб А.Т.* Антикризисное управление организацией: учебное пособие / А.Т. Зуб, Е.М. Панина. – М.: ИД ФОРУМ: НИЦ ИНФРА–М, 2014. –256 с.

67. Анализ отрасли фитнес – услуг в России // URL: http://www.yurii.ru/ ref/ref-15994php (дата обращения 4.10.16).

68. *Петрашук Г.И.* Применение менеджмента в телекоммуникационных услугах // Вестник Воронежского института высоких технологий. – 2010. – № 7. – С. 228–230.

69. *Завьялов Д.В.* О применении информационных технологий // Современные наукоемкие технологии. – 2013. – № 8. – С. 71–72.

70. *Ряжских А.М.* Построение стохастических моделей оптимизации бизнес-процессов / А.М. Ряжских, Ю.В. Преображенский // Известия Воронежского института высоких технологий. – 2008. – № 3. – С. 79–81.

71. *Королков Р.В.* Контроллинг в торговой организации // Вестник Воронежского института высоких технологий. – 2013. – № 10. – С. 287–290.

72. *Черников С.Ю.* Использование системного анализа при управлении организациями / С.Ю. Черников, Р.В. Корольков // Моделирование, оптимизация и информационные технологии. – 2014. – № 2 (5). – С. 16.

73. *Исакова М.В.* Моделирование работы подразделений в компании / М.В. Исакова, А. В. Данилова // Моделирование, оптимизация и информационные технологии. – 2015. – № 2. – С. 15.

74. *Землянухина Н.С.* О применении информационных технологий в менеджменте // Успехи современного естествознания. – 2012. – № 6. – С. 106–107.

75. *Гуськова Л.Б.* О построении автоматизированного рабочего места менеджера / Л.Б. Гуськова // Успехи современного естествознания. – 2012. – № 6. – С. 106.

76. *Филипова В.Н.* Применение интернет технологий в маркетинге / В.Н. Филипова, Е.В. Киселева // Моделирование, оптимизация и информационные технологии. – 2015. – № 2. – С. 19.

77. R. Sandhu, E. J. Coyne, H. Feinstein. Role- based access control models // IEEE Computer. – 1996. - Vol 29, -№ 2. – P. 38–47.

78. Хоанг Ван Кует, Тузовский А.Ф. Алгоритм для определения уровня политики безопасности RDF-данных // X Международная научно-практическая конференция студентов, аспирантов и молодых ученых «Молодежь и современные информационные технологии», г. Томск, Россия, Томский политехнический университет. – С. 17-18.

79. P. Stachour and B. Thuraisingham. Design of LDV: A multilevel secure relational database management system // IEEE Trans. Knowledge and Data Eng. – 1990. – Vol 2, - № 2. – P. 190–209.

ОГЛАВЛЕНИЕ