УДК 004.056.5 Вестник УрФО № 2(52) / 2024, с. 89–98

Поршнев С. В., Пономарева О. А. DOI: 10.14529/secur240209

ПРОБЛЕМЫ РАЗРАБОТКИ МОДЕЛИ УГРОЗ ДЛЯ ХРАНИЛИЩА ГЕТЕРОГЕННЫХ ДАННЫХ

В статье на примере данных ограниченного доступа металлургического производства, имеющих разнородную динамически изменяющуюся структуру, для хранения которых используется хранилище гетерогенных данных (ХГД) Автоматизированной Системы Выпуска Металлургической Продукции (АС ВМП) обсуждаются проблемы обеспечения информационной безопасности хранилищ данных данного типа и возможные подход к их решению. Для этого рассмотрена структура АС ВМП; технологии и структура системы управления ХГД МП; проведен анализ используемых в настоящее время мер защиты информации в АС ВМП; определены угрозы информационной безопасности ХГД МП, не учтенные на этапе проектирования АС ВМП.

Обоснована необходимость изменения концепции обеспечения информационной безопасности (ИБ) хранилищ данных, которая предусматривает переход от принятия мер для закрытия известных уязвимостей к созданию защищенных ХГД.

Ключевые слова: *хранилище гетерогенных данных, защищенное хранилище гетерогенных данных, концепция конфиденциальности, целостности и доступности данных, уязвимости хранилищ больших данных, металлургическое производство.*

Porshnev S. V., Ponomareva O. A.

PROBLEMS OF DEVELOPING A THREAT MODEL FOR HETEROGENEOUS DATA STORAGE CONTROL NETWORK

In the article, using the example of limited access data from a metallurgical production facility, which has a heterogeneous dynamically changing structure, for the storage of which the heterogeneous data warehouse (HDS) of the Automated System for the Production of Metallurgical Products (AS VMP) is used, the problems of ensuring information security of data storages of this type and possible approaches to their decision. For this purpose, the structure of the AS VMP is considered; technologies and structure of the control system of the HGD MP; an analysis of the information protection measures currently used in VMP automated systems was carried out; threats to the information security of the CGD MP that were not taken into account at the design stage of the VMP AS were identified.

The need to change the concept of providing information security for data warehouses is substantiated, which provides for a transition from taking measures to close known vulnerabilities to creating secure data storage systems.

Keywords: *heterogeneous data storage, secure storage of heterogeneous data, concept of confidentiality, integrity and availability of data, big data storage vulnerabilities, metallurgical production.*

Введение

Сегодня на каждом промышленном предприятии для управления бизнес-процессами и их оптимизации традиционно используют следующую иерархически выстроенную совокупность информационных систем (ИС): ERP-систему, используемую для решения задач управления предприятием; несколько различных MES-систем, обеспечивающих сбор, анализ и управление производственными процессами на соответствующих этапах жизненного цикла (ЖЦ) выпускаемой продукции, а также различные автоматизированные системы управления технологическими процессами (АСУ ТП), используемые для управления конкретными технологическими процессами и фиксации их параметров. В результате совокупная информация о единице продукции (ЕП) промышленного производства, представляет собой множество разнородных данных, описываемых различными математическими моделями, которые размещаются в различных автономных хранилищах данных (ХД) перечисленных выше ИС.

При расследовании причин выпуска бракованной продукции, закономерно, возникает нетривиальная задача поиска релевантной запросу информации, размешенной одновременно в нескольких автономных ХД. Для ее решения применительно к металлургическому производству (МП) в [7], [8] предложено создать единое ХД, названное хранилищем гетерогенных данных (ХГД), и разместить в нем все описываемые различными информационными моделями данные МП, которые характеризуют состояние единицы продукции (ЕП) МП на каждом из этапов ее жизненного цикла. Для создания ХГД была использована система управления базами данных СУБД ORACLE Stream.

С точки зрения действующих нормативно-правовых актов в области информационной безопасности данные [1]–[6], находящиеся в соответствующих ХД ERP-систем, MES-систем, АСУ, АСУ ТП, в том числе: значения параметров технологических процессов, планы производства, информация о финансовых потоках, о заказчиках и клиентах, представляют собой информацию ограниченного доступа. Значимость и ценность этой информации приводит к необходимости обеспечения защиты элементов информационной инфраструктуры предприятия и самих ХГД.

Отметим, что традиционно каждый производитель СУБД ограничивается развитием концепции конфиденциальности, целостности и доступности данных. В этой связи, предлагаемые производителями СУБД решения в области обеспечения безопасности СУБД предназначены, в основном, на преодоление существующих и уже известных уязвимостей. При этом очевидно, что данный подход обеспечивает решение конкретных задач, но не способствует выработки универсальной концепции безопасности СУБДи ХГД.

В статье на примере АС ВМП проведен анализ современных проблем, особенностей защиты, требований к обеспечению безопасности ХГД МП.

Структура автоматизированной системы выпуска металлургической продукции (АС ВМП)

Автоматизированная Система Выпуска Металлургической Продукции (АС ВМП), обеспечивающая сбор данных, хранение, формирование запросов по слежению, контролю, моделированию, анализу и выдаче рекомендаций по оптимизации как на отдельных этапах производства, так и полного цикла выпуска металлургической продукции была разработана в рамках выполнения договора № 02.G25.31.0055 с Минобрнауки России от 12 февраля 2013 г., срок выполнения с 10.01.2013 по 30.11.2015 г. (проект 2012-218-03-167), заключенного в рамках выполнения Постановления № 218 Правительства Российской Федерации и технические решения изложены в [1, 2].

Из рисунка 1 видно, что АС ВМП состоит из двух взаимосвязанных подсистем: автоматизированной информационной системы сбора и анализа данных (АИС САД) производства и автоматизированной информационной системы моделирования организационной деятельности (АИС МОД) предприятия.

В состав подсистемы АИС САД входят следующие модули: модуль «Хранилище гетерогенных данных металлургического производства» (ХГД МП); модуль «Конструктор запросов» (КЗ);модуль обмена данными с автоматизированными системами предприятия (ОДАСП).

Перечисленные модули выполняют следующие функции: 1) обмен данными между ХГД МП АИС САД и автоматизированными системами МП всех уровней ОДАСП; 2) надежное хранение и быстрый доступ к ХГД МП, поддержка их хронологии, целостности и непротиворечивости, что обеспечивает воз-

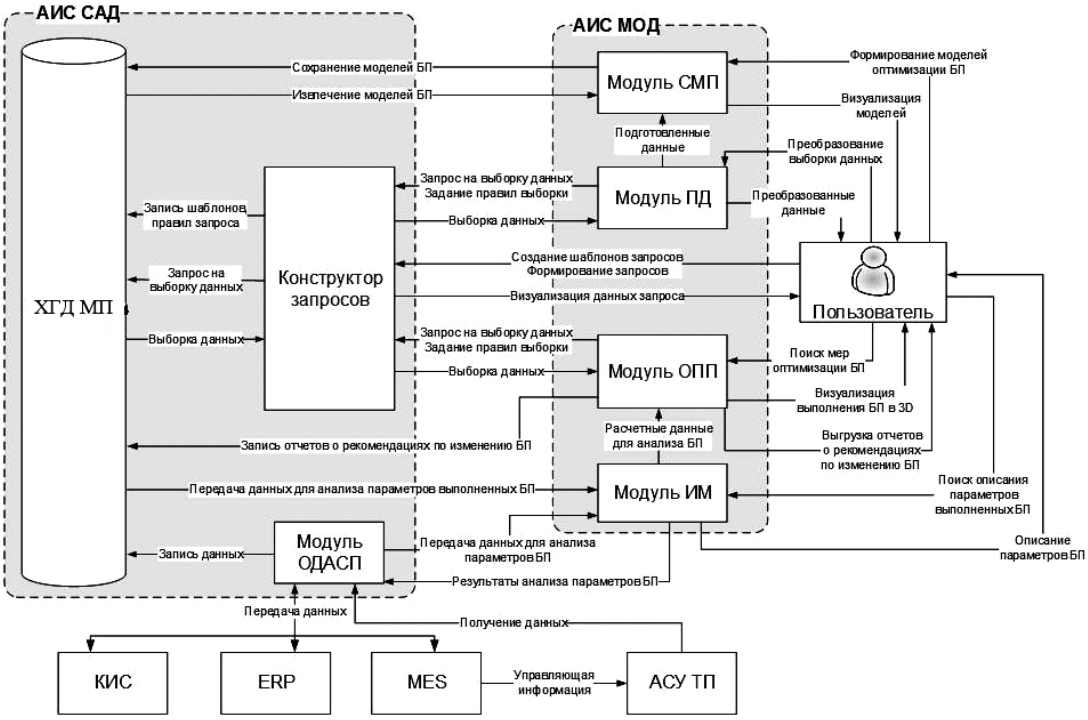

Рис. 1. Структурная схема АС ВМП

можность создания единого информационного пространства данных МП, построение единого интерфейса пользователя, разработка общих алгоритмов обработки данных и осуществление высокопроизводительной аналитической обработки данных; 3) предоставление пользователю удобного интерфейса для создания требуемых выборок информационных параметров и формирование нерегламентированных отчетов (КЗ).

АИС САД обеспечивает сбор, хранение и предоставление информации пользователям, которая может быть использована, в том числе, для создания имитационных моделей технологических, логистических и организационных (бизнес) процессов.

Подсистема АИС МОД состоит из следующих модулей: 1) создания моделей предприятия (СПМ); 2) подготовки данных (ПД); 3) организационных процессов предприятия (ОПП); 4) имитационного моделирования (ИМ).

Модуль ПД предназначен для решения следующих задач: 1) получение выборки данных, сформированной по запросу из модуля КЗ; 2) задание набора правил на обработку выборки данных с помощью графического инструмента создания правил обработки данных; 3) совместное функционирование множества модулей ПД при интеграции в единый программный интерфейс модулей ПД(модулей-источников данных, модулей обработки данных, модулей анализа и модулей верификации); 4) персистентное (долговременное) хранение пользовательских настроек процесса подготовки данных для размещения в ХГД МП; 5) анализ, верификация и преобразование выборки данных в соответствии с заданным набором правил; 6) восстановление пропущенных данных на основе анализа накопленной статистики; 7) анализ данных параметров технологических, логистических и организационных (бизнес) процессов (ТЛОБП) на основе методов машинного обучения (анализ распределённых лагов, фильтры временных рядов, полосовой анализ, методы автоматической классификации данных, нейронные сети) для решения задач прогнозирования и интерпретации подготавливаемых данных.

Модуль СМП реализует следующие функции: 1) создание, модифицирование и запись в ХГД МП моделей ТЛОБП с помощью визуального конструктора моделей мультиагентных имитационных процессов, деревьев анализа параметров процесса, вновь разработанных функциональных элементов для представления графических элементов создания моделей на основе web-интерфейса; 2) оценивание соответствия результатов контрольного

прогона разработанного процесса заданным значениям (отличия не должны превышать 80.%); 3) независимое от пользователя исполнение модели процесса в виде отдельного вычислительного процесса; 4) запуск и одновременное исполнение нескольких экземпляров моделей процессов, создаваемых с помощью модуля СМП; 5) согласование входных и выходных параметров модели процессов, создаваемой с помощью модуля СМП, с параметрами реальных технологических процессов для выполнения модели в модуле ИМ; 6) создание протоколов совещаний, проводимых в рамках реализации типового постоянно действующего бизнес-процесса предприятия по изменению производственных процессов; 7) создание средств обработки обращений пользователей для выполнения обработки инцидентов, связанных с эксплуатацией автоматизированной системы выпуска металлургической продукции (АС ВМП).

Модуль ИМ предназначен для решения следующих задач: 1) получение данных из модуля ОДАСП; получение данных из модуля КЗ; 3) получение данных из модуля ПД; 4) получение описания выполненных на производстве ТЛОБП из модуля ХГД МП; 5) анализ параметров выполненных ТЛОБП (продолжительность анализа – не более 30 мин); 6) выдача результатов анализа в модуль ОДАСП; 7) отображение результатов анализа процессов в зависимости от ролей пользователей; 8) функционирование в режиме разделения процессов выполнения модели и отображения результатов для обеспечения нескольких представлений каждой из выполняющихся моделей; 9) одновременный запуск нескольких модулей ИМ, в каждом из которых выполнение моделей производится независимо друг от друга без средств отображения функционирования модуля ИМ, без ожидания и временных остановок выполняющихся потоков вычислений (в асинхронном неблокирующем режиме выполнения); 10) загрузка имитационной модели в модуль ИМ, созданной в СМП; 11) управление выполняющимися моделями в модуле ИМ с помощью команд на старт, останов и отслеживание состояния.

Модуле ОПП предназначен для решения следующих задач: 1) получение расчётных данных из модуля ИМ; 2) получение выборки данных из модуля КЗ; 3) получение результатов выполнения настроек подготовки данных, созданных в модуле ПД; 4) получение значений параметров выполненных ТЛОБП при взаимодействии с модулем ОДАСП; 5) оптимизация ТЛОБП на основе методов имитационного моделирования (мультиагентного, экспертного, ситуационного моделирования), метода анализа и устранения узких мест ТЛОБП; 6) выдача рекомендаций по изменению технологических, логистических и организационных (бизнес) процессов предприятия; 7) создание отчетов о выполненных процессах предприятия и их запись в ХГД МП, содержащие информацию о времени начала и окончания выполнения процессов предприятия); 8) создание отчетов с рекомендациями по недопущению выявленных инцидентов и вывод отчетов в форматах .doc, .xlsx, .csv, .xml; 9) визуализация выполнения процессов предприятия в формате 3D-анимации; 10) визуальное отображение входных и выходных переменных.

Модуль ХГД МП обеспечивает: 1) централизованное хранение данных АС ВМП; 2) выполнение аналитических запросов КЗ; 3) индексирование данных; 4) кэширование данных; 5) резервное копирование данных АС ВМП.

Для этого в ХГД МП реализованы следующие функции: 1) функция записи параметров ЕП, поступивших от АС ТП, КИС, MES, ERP-систем; 2) функции получения статистических данных; 3) функция создания резервной копии; 4) функция восстановления ХГД МП из резервной копии; 5) вспомогательные функции. В соответствие с ТЗ проекта создания АС ВМП длительность записи данных от: 1)АС ТП должна составлять не более 10 мин; 2)КИС, MES, ERP-систем – не более 30 мин.

Таким образом, модуль ХГД МП осуществляет сбор, хранение и предоставление данных по запросам из других подсистем и/или модулей АС ВМП, в которой предусмотрены следующие сценарии взаимодействия с ХГД МП с другими ее подсистемами и модулями: 1) получение данных из модуля ОДАСП; 2) выборка данных из ХГД МП по запросам модуля КЗ (конструктор запросов) и хранение шаблонов правил запросов; 3) передача данных из ХГД МП в АИС МОД и хранение моделей БП МП.

Для управления ХГД была использована система управления базами данных (СУБД) Oracle Streams [9] и объем хранимых данных составляет около 7 терабайт, выбор которой был определен техническим заданием договора № 02.G25.31.0055.

Технологии и структура системы управления ХГД МП

МП представляет собой сложный многоэтапный процесс: этапа подготовки производства, этап доменного производства, этап сталеплавильного производства, этап прокатного производства. При этом на каждом из этапов происходят как изменение физического состояния единицы продукции (ЕП) МП (шихта – чугун – сталь – прокат), так и, соответственно, информационная модель ЕП МП и ее контент. Описать изменяющуюся структуру информационной модели удается за счет использования кортежей вида «Событие, ЕП, Источник информации». Здесь сущность «событие» обеспечивает создание и хранение контрольных точек производственного процесса, в которых создается фиксируемая информация о ЕП МП (например, начало производства партии продукции, завершение производства партии продукции, отклонение параметром производственного процесса и другие факты), сущность «ЕП» –интегрирует в себе множество разнородных данных, которые собираются в автономных базах данных АСУ ПТ, MES- и ERP-систем, сущность «Источник информации» –множество имен серверов автономных баз данных, которые импортируют данные в АС ВМП.

Схема сущностей, используемых для описания процесса хранения информации о событиях, происходящих в течение жизненного цикла ЕП МП, представлена на рисунке 2 и схема взаимодействия информационных потоков, взаимосвязанных с процессом выпуска ГП МП – на рисунке 3.

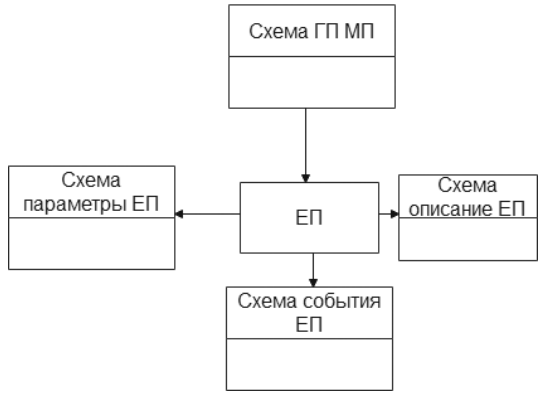

Рис. 2. Схема связей сущностей, используемых для описания схем атрибутов ЕП

Таким образом, основная особенность единого ХГД МП состоит в том, что структура записи данных в единое ХГД МП формируется в момент получения данных от соответствующих источников информации. В этой связи, в едином ХГД МП одновременно с данными необходимо размещать информацию об их структуре, на основе которой далее будет выполняться поиск информации, релевантной запросу пользователя к единому ХГД МП. Применяется технология Oracle Streams, предназначенная для интеграции данных, обмена данными и сообщениями с помощью механизма Advanced Queuing [10] в однородной среде и гетерогенных средах.

Анализ использованных мер защиты информации в АС ВМП

Основными видами воздействий на информационные ресурсы и компоненты информационной системы АС ВМП, которые мо-

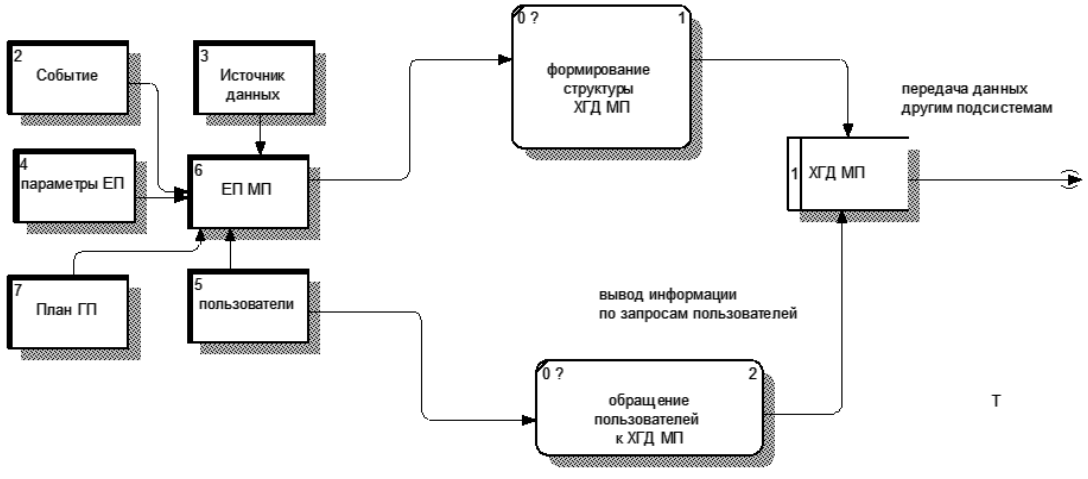

Рисунок 3. Диаграмма потоков данных, размещаемых в едином ХГД МП

гут привести к негативным последствиям, являются: а) утечка (перехват) конфиденциальной информации или отдельных данных (нарушение конфиденциальности); б) несанкционированный доступ к компонентам, защищаемой информации, системным, конфигурационным, иным служебным данным; в) отказ в обслуживании компонентов (нарушение доступности); г) несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационных, иных служебных данных (нарушение целостности); д) несанкционированное использование вычислительных ресурсов в интересах решения несвойственных им задач; е) нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передачи и хранения информации.

В этой связи в техническом задании были предусмотрены следующие меры защиты информации в ХГД МП [1], [11]: 1) выполнение резервного копирования данных; 2) защита от несанкционированного доступа к данным (НСД); 3) обеспечение контроля целостности данных; 4) журналирование (логирования) событий, возникающих в процессе использования ХГД МП.

Выполнение резервного копирования данных

Для реализации функции резервного хранения данных, размещенных в ХГД МП, на языке PL\SQL были реализованы следующие функции: формирование последовательности команд резервного копирования сигнальных данных; резервное копирование оперативных данных; резервное копирование структуры данных; резервное копирование дат, к которым привязаны оперативные данные.

Восстановление данных ХГД МП проходит в следующем строго определенном порядке: актуализация схем данных, восстановление справочных данных, восстановление оперативных данных, восстановление сигнальных данных, актуализация схем.

В процессе актуализации данных ХГД МП: создается начальное состояние схемы базы данных; восстанавливается история изменений структуры данных ХГД МП в виде сохраненных скриптов; восстанавливается схема соответствующей дате (входным параметром для данной процедуры является дата); восстанавливаются только справочные данные, входные параметры dict_data, восстанавливаются сигнальные данные.

Защита от несанкционированного доступа (НСД)

В связи с тем, что ХГД МП реализовано на базе СУБД Oracle, очевидным оказывается решение о применении внутренних механизмов обеспечения защиты от НСД встроенными средствами СУБД, т.к. любая надстройка над СУБД будет работать на более высоком уровне и не обеспечит необходимую степень защиты.

Защита от НСД ХГД МП была реализована с использованием Oracle Database Vault, которая обеспечивает выполнение следующих функций: привилегированный пользовательский доступ к данным приложений; управление доступом к ХГД с помощью многофакторных политик, основанных на заданных условиях; обнаружение и составление отчетов о привилегиях и ролях (матрица доступа), используемых в базе данных; ограничение нерегламентированного доступа к данным приложений за счет предотвращения обхода приложений.

Средства проверки целостности данных

Для проверки целостности данных, находящихся в ХГД МП, использованы соответствующие механизмы проверки и контроля целостности данных, реализованные в СУБД Oracle:средства проверки физической целостности журнала транзакций LGWR (Log Writer) и значения контрольных сумм файлов; средства проверки логической целостности данных (Data Integrity), представленные классическими элементами СУБД Oracle: первичными и внешними ключами (ссылочная целостность), ограничениями (непротиворечивость данных), каскадные удаления.

Журналирование (логирование) событий, возникающих в процессе использования ХГД МП

Журналирование и логирование действий пользователя ХГД МП в системном журнале ХГД МП, а также решение задач мониторинга критический событий ХГД МП (например, проверку объема свободного места на диске, нахождение устаревших индексов), ведение пользовательских логов, осуществляется с помощью функций СУБД Oracle и функций, созданных разработчиком ХГД МП.

Таким образом, при разработке АС ВМП были выполнены требования по обеспечению информационной безопасности в соответствие с техническим заданием (ТЗ), составленного в соответствие с требованиями нормативно-правовой базы в области ИБ на мо-

Таблица 1.

Анализ угроз для ХГД, перечисленных в базе данных угроз ФТЭК России

НомерБДУ	Описание угрозы
УБИ.050: Угроза неверного определения формата входных данных, поступающих в хранилище больших данных	Угроза заключается в возможности искажения информации, сохраняемой в хранилище больших данных, или отказа в проведении сохранения при передаче в него данных в некоторых форматах. Данная угроза обусловлена слабостями технологий определения формата входных данных на основе дополнительной служебной информации (заголовки файлов и сетевых пакетов, расширения файлов и т.п.), а также технологий адаптивного выбора и применения методов обработки мультиформатной (гетерогенной) информации в хранилищах больших данных. Реализация данной угрозы возможна при условии, что дополнительная служебная информация о данных по какой-либо причине не соответствует их фактическому содержимому, или в хранилище больших данных не реализованы методы обработки данных получаемого формата
УБИ.097: Угроза несогласованности правил доступа к большим данным	Угроза заключается в возможности предоставления ошибочного неправомерного доступа к защищаемой информации или, наоборот, возможности отказа в доступе к защищаемой информации легальным пользователям в силу ошибок, допущенных при делегировании им привилегий другими легальными пользователями хранилища больших данных. Данная угроза обусловлена недостаточностью мер по разграничению и согласованию доступа к информации различных пользователей в хранилище больших данных. Реализация данной угрозы возможна при условии использования различных политик безопасности, несогласованных между собой (например, одно средство защиты может отказать в доступе, а другое – предоставить доступ)
УБИ.105: Угроза отказа в загрузке входных данных неизвестного формата хранилищем больших данных	Угроза заключается в возможности отказа хранилищем больших данных в приёме входных данных неизвестного формата от легального пользователя. Данная угроза обусловлена отсутствием в хранилище больших данных механизма самостоятельной (автоматической) адаптации к новым форматам данных. Реализация данной угрозы возможна при условии поступления запроса на загрузку в хранилище входных данных неизвестного формата

мент составления ТЗ (2015 г.) Однако всовременных условиях перечисленных мер по обеспечение ИБ ХГД МПнедостаточно, в связи с возникновением новых угроз [6]. Втаблице 1приведены угрозы информационной безопасности (УБИ), которых не было на момент составления техническогозадания и которые появились в БД ФСТЭК России в настоящее время, актуальные для ХГД МП.

В этой связи, требуется разработка новой концепции обеспечения ИБ ХГД МП, которую можно будет использовать для защиты любых БД, ХД и ХГД.

Обоснование концепции обеспечения ИБ защищенных ХГД

Современные ХД и/или ХГД имеют в своем составе два неотъемлемых друг от друга компонента: данные (собственно ХД и/или ХГД) и программы управления данными. В этой связи, очевидно, что обеспечение безопасности хранимой информации невозможно без обеспечения безопасного управления данными. Исходя из этого, все уязвимости и вопросы безопасности ХД и/или ХГД можно разделить на зависящие от данных и не зависящие от данных. Уязвимости, независящие от данных, являются типичными для любого типа программного обеспечения (ПО). Их причиной, например, может стать несвоевременное обновление ПО, наличие неиспользуемых функций или недостаточная квалификация администраторов ПО. Уязвимости, зависящие от данных, обусловлены, например, тем, что большинство ХД, ХГД поддерживают запросы к данным с помощью того или иного языка запросов, содержащего наборы доступных пользователю функций (которые, в свою очередь, тоже можно считать операторами запросного языка) или произвольные функции на языке программирования. При этом архитектура используемых языков запросов оказывается напрямую связанной с моделью данных, размещаемых в ХД, ХГД.

Следовательно, наличие в ХД, ХГД тех или иных уязвимостей определяется моделью данных. При этом такие уязвимости как, например, инъекции, в зависимости от используемого синтаксиса языка запросов будут реализовываться по-разному (sql-инъекция, java-инъекция).

В связи с выше изложенным, понятно, что, аналогично, можно выделить зависящие и независящие от данных меры обеспечения безопасности хранилищ информации. К независящим от данных можно отнести следующие требования к безопасной системе БД:

1. Функционирование в доверенной среде. (Здесь доверенная средой мы понимаем инфраструктуру предприятия и ее защитные механизмы, предусмотренные к использованию действующими политиками безопасности, то есть в соответствие с правилами безопасности, применяемыми и к каждой из ИС предприятия).

2. Организация физической безопасности файлов данных, которые, в целом, не отличаются от требований, применяемых к любым другим файлам пользователей и приложений.

3. Организация безопасной и актуальной настройки системы управления данными ХД, ХГД, предусматривающая, в том числе, решение общих задач обеспечения безопасности, например, таких как своевременная установка обновлений, отключение неиспользуемых функций или применение эффективной политики паролей.

Следующие требования можно отнести к требованиям, зависящим от данных:

1. Безопасность пользовательского ПО, используемого для управления ХД, ХГД, и доступа к данным, в том числе, построение безопасных интерфейсов и механизмов доступа к данным.

2. Безопасная организация и работа с данными, находящимися в ХД и ХГД, в том числе, обеспечивающая контроль их целостности и доступности (особую актуальность данная задача имеет для ХГД с динамических изменяющейся структурой данных).

Заключение

Для решения обозначенных проблем обеспечения ИБ ХД, ХГД, с нашей точки зрения, целесообразно, перейти от широко используемой сегодня концепции закрытия уязвимостей к концепции комплексного обеспечения их безопасности.

Для практической реализации предложенной концепции необходимо разработать соответствующие методики обеспечения безопасности ХД, ХГД промышленных предприятий, которые позволят избежать ошибок при разработке и реализации организационных и организационно-технических мероприятий в области обеспечения ИБ систем управления ХД и ХГД, а также защититься от наиболее распространенных на сегодняшний день уязвимостей.

Дальнейшие результаты исследований, проводимые авторами в данном направлении (в том числе, разработанные модели угроз и полученные оценки рисков ИБ для ХД, ХГД), являются предметом последующих публикаций.

Литература

1. ГОСТ Р 51275-2006 Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

2. ГОСТ Р 56546-2015 Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем.

3. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 15.02.2013 № 17.

4. Состав и содержание организационных и технических мер по обеспечению безопасности информации при их обработке в информационных системах информации с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите информации для каждого из уровней защищенности. Утверждены приказом ФСБ России от 10.07.2014 № 378.

5. Методический документ. Методика оценки угроз безопасности информации. Утвержден ФСТЭК России 5 февраля 2021 г.

6. Банк данных угроз безопасности информации ФСТЭК России, URL: https://bdu.fstec.ru/.

7. Porshnev S. The Development of a Heterogeneous MP Data Model Based on the Ontological Approach / S. Porshnev, A. Borodin, O. Ponomareva, S. Mirvoda and O. Chernova // Symmetry. – 2021. – Vol. 13(5). – No. 813.

8. Поршнев С.В., Пономарева О.А. Методология структурного синтеза хранилищ гетерогенных данных промышленного предприятия/ Монография Научно-техническое издательство «Горячая линия – Телеком», Москва, 2022 г.

9. Документация по Oracle Streams URL: https://docs.oracle.com/en/database/oracle/oracle-database/18/strms/index.html.

10. Документация по Advanced Queuing URL: https://docs.oracle.com/en/database/oracle/oracle-database/21/jjdbc/advanced-queuing.html

11. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения от 30 марта 1992 года URL: https://normativ.kontur.ru/document?moduleId=1&documentId=198553.

References

12. GOST R 51275-2006 Ob"yekt informatizatsii. Faktory, ozdeystvuyushchiye na informatsiyu. Obshchiye polozheniya. [In Rus]

13. GOST R 56546-2015 Zashchita informatsii. Uyazvimosti informatsionnykh sistem. Klassifikatsiya uyazvimostey informatsionnykh sistem. [In Rus]

14. Trebovaniya o zashchite informatsii, ne sostavlyayushchey gosudarstvennuyu taynu, soderzhashcheysya v gosudarstvennykh informatsionnykh sistemakh. Utverzhdeny prikazom FSTEK Rossii ot 15.02.2013 № 17. [In Rus]

15. Sostav i soderzhaniye organizatsionnykh i tekhnicheskikh mer po obespecheniyu bezopasnosti informatsii pri ikh obrabotke v informatsionnykh sistemakh informatsii s ispol'zovaniyem sredstv kriptograficheskoy zashchity informatsii, neobkhodimykh dlya vypolneniya ustanovlennykh Pravitel'stvom Rossiyskoy Federatsii trebovaniy k zashchite informatsii dlya kazhdogo iz urovney zashchishchennosti. Utverzhdeny prikazom FSB Rossii ot 10.07.2014 № 378. [In Rus]

16. Metodicheskiy dokument. Metodika otsenki ugroz bezopasnosti informatsii. Utverzhden FSTEK Rossii 5 fevralya 2021 g. [In Rus]

17. Bank dannykh ugroz bezopasnosti informatsii FSTEK Rossii, URL: https://bdu.fstec.ru/. [In Rus]

18. Porshnev S. The Development of a Heterogeneous MP Data Model Based on the Ontological Approach / S. Porshnev, A. Borodin, O. Ponomareva, S. Mirvoda and O. Chernova // Symmetry. – 2021. – Vol. 13(5). – No. 813.

19. Porshnev S.V., Ponomareva O.A. "Metodologiya strukturnogo sinteza khranilishch geterogennykh dannykh promyshlennogo predpriyatiya". Monografiya. Nauchno-tekhnicheskoye izdatel'stvo «Goryachaya liniya – Telekom», Moskva, 2022 g. [In Rus]

20. Dokumentatsiya po Oracle Streams URL: https://docs.oracle.com/en/database/oracle/oracle-database/18/strms/index.html. [In Rus]

21. Dokumentatsiya po Advanced Queuing URL: https://docs.oracle.com/en/database/oracle/oracle-database/21/jjdbc/advanced-queuing.html [In Rus]

22. Rukovodyashchiy dokument. Zashchita ot nesanktsionirovannogo dostupa k informatsii. Terminy i opredeleniya ot 30 marta 1992 goda URL: https://normativ.kontur.ru/document?moduleId=1&documentId=198553 [In Rus]

ПОРШНЕВ Сергей Владимирович, доктор технических наук, профессор, директор Учебно-научного центра «Информационная безопасность» федерального государственного автономного образовательного учреждения высшего образования «Уральский федеральный университет им. первого Президента России Б.Н. Ельцина». 620002, г. Екатеринбург, ул. Мира, 32. E-mail: s.v.porshnev@urfu.ru

ПОНОМАРЕВА Ольга Алексеевна, кандидат технических наук, доцент Учебно-научного центра «Информационная безопасность» федерального государственного автономного образовательного учреждения высшего образования «Уральский федеральный университет им. первого Президента России Б.Н. Ельцина». 620002, г. Екатеринбург, ул. Мира, 32. E-mail: o.a.ponomareva@urfu.ru

PORSHNEV Sergey Vladimirovich, Doctor of Technical Sciences, Professor, Director of the Educational and Scientific Center «Information Security» of the Federal State Autonomous Educational Institution of Higher Education «Ural Federal University named after the first President of Russia B.N. Yeltsin». 620002, Yekaterinburg, st. Mira, 32. E-mail: s.v.porshnev@urfu.ru

PONOMAREVA Olga Alekseevna, Candidate of Technical Sciences, assistant professor of the Federal State Autonomous Educational Institution of Higher Education “Ural Federal University named after the first President of Russia B.N. Yeltsin". 620002, Yekaterinburg, st. Mira, 32. E-mail: o.a.ponomareva@urfu.ru