11th International Conference. September, 10 - November, 30, 2020.
UK, S Yorkshire, Sheffield

«SCIENCE AND PRACTICE: A NEW LEVEL OF INTEGRATION IN THE MODERN WORLD» • Conference Proceedings

DOI: http://doi.org/10.15350/UK_6/11

Research Article

DATA PROTECTION IN DISTRIBUTED INFORMATION SYSTEMS

X.U. Xayatov[1]
M.Sh. Muxsinova[2]

[1]Senior teacher, Department of Information Technologies, Faculty of Physics and Mathematics, Bukhara State University, Uzbekistan.
[2]Student, Faculty of Physics and Mathematics, Bukhara State University, Uzbekistan.

DOI: http://doi.org/10.15350/UK_6/11.37

Abstract

This article discusses data protection in distributed information systems and the creation of an integrated information security system.

Key words: centralized information system, distributed information system, file servers, database servers, identification code, identification, authentication, authorization.

Централизованная информационная система имеет одну точку входа, по которой производится доступ к данным. Распределенная информационная система напротив, имеет несколько таких точек входа. Например, файл-серверы, серверы баз данных (БД) или рабочие станции локальной сети. Все типы БД могут работать самостоятельно (будучи при этом компонентами распределенной информационной системы) и обладать собственной системой информационной безопасности.

Присутствие различных внутренних баз данных в распределенных информационных системах дает возможность существенно увеличить степень безопасности данных. Все БД администрируются автономно, и для каждой доступна реализация своего собственного способа защиты. Помимо этого, конфиденциальная информация в данной архитектуре легко изолируется и обслуживается. Рассмотрим методы обеспечения защиты информации на каждом уровне. Как правило, на уровне защиты рабочей станции используются программный и аппаратные методы защиты информации, где возможность пользователя иметь доступ к данным определяется следующими факторами: идентификационным кодом, благодаря которому система определяет пользователя, и паролем, который применяется для подтверждения его прав. Пользователь вводит свои реквизиты в систему только один раз – в момент регистрации. Пароли работают в течение некоторого времени и являются своего рода объектами многоразового применения.

На уровне управления информационным каналом – кадры, передаваемые по каналам связи, шифруются во время передачи и расшифровываются при приеме. Методы шифрования и дешифрования доступны только на данном уровне. На более высоких уровнях неизвестно, что происходит на этом уровне эталонной модели сети. Кроме того, кадр будет дешифроваться на всех маршрутизаторах и будет открыт для атак в каждом маршрутизаторе, если он передается через несколько маршрутизаторов.

Однако, данный метод, используется в целях увеличения уровня устойчивости к помехам, которые передаются данных посредством сетей общего пользования.

На третьем (сетевом) уровне, используются брандмауэры, которые позволяют удалять подозрительные пакеты, поступившие извне.

На транспортном уровне применяется сквозное шифрование информационного блока и всего сообщения.

DOI: http://doi.org/10.15350/UK_6/11

На верхнем уровне (уровне приложений) рассматриваются и устраняются проблемы аутентификации. Создание комплексной системы обеспечения защиты информации описывается следующей последовательностью действий:

• Оценить физическую архитектуру распределенной информационной системы. Для этого следует определить целевую аудиторию пользователей и состав технических средств, которые обеспечивают доступ к информационным ресурсам (модемы, рабочие станции, неинтеллектуальные терминалы); а также узнать, в каком месте содержатся информационные ресурсы: на мэйнфрейме, файл-серверах, серверах баз данных или рабочих станциях.

• Определить все доступные логические маршруты от пользователя к информационным ресурсам, терминала к мэйнфрейму, удаленного пользователя к коммуникационному серверу; рабочей станции к серверу базы данных и т.д. Данная схема позволяет определить физические связи на логические маршруты доступа к данным.

• Для каждого типа маршрута построить схему в терминах «маршрут доступа /средства защиты». На одном маршруте может быть использовано сразу несколько уровней защиты.

Для создания сбалансированной системы информационной безопасности необходимо изначально проанализировать рисков в области информационной безопасности. Систему информационной безопасности необходимо спроектировать таким образом, чтобы имелась возможность добиться установленного уровня риска. Результатом выполнения всех работ по созданию системной защиты информации в распределенной информационной системе являются следующие функции.

• Идентификация, аутентификация и авторизация пользователей. Всем пользователям компьютерной системы присваиваются уникальный идентификатор и пароль, по которым определяется, может ли он работать в системе, и входит ли данный пользователь в список пользователей данной системы.

• Присвоение групповых паролей. присваиваются один групповой идентификатор и один пароль для всей группы в том случае, если группа пользователей постоянно работает с общими данными.

• Аудит. Система защиты предусматривает ведение аудиторского журнала, где будут учитываться все подозрительные события за время работы системы (попытки проникновения в систему извне, подбора пароля, запуска приложений из закрытых каталогов и т.д.).

• Синхронизация паролей. У пользователей есть возможность синхронно изменять пароли на различных серверах БД благодаря системе защиты.

Проектирование системной защиты ресурсов распределенной информационной системы дает возможность оценки уровня состояния безопасности информационных ресурсов компании, снизить возможные потери путем увеличения уровня устойчивости работы информационной сети.

References:

Жук. Е. И. Концептуальные основы информационной безопасности. [электронный ресурс] – bmstu.ru. – науч. изд. им. Н. Э. Баумана. – журн. Наука и образование.

Хаятов Х. У., Жураева Л. И., Жураев З. Ш. Основные понятия теории нечетких множеств // Молодой ученый. — 2019. — № 25 (263). — С. 41-44.

Хаятов Х.У, Жалолова Н.Х. О нахождении нормы функционала погрешности интерполяционных формул типа эрмита в периодическом пространстве // Проблемы вычислительной и прикладной математики. — 2017. — № 4 (10). — С. 98-103.

Хаятов, Х. У. Оценка погрешности кубатурных формул общего вида над фактор-пространством Соболева// Молодой ученый. — 2016. — № 13 (117). — С. 58-60.

Хаятов Х.У. Об одной погрешности весовых кубатурных формул в пространстве // Научная дискуссия: вопросы математики, физики, химии, биологии — 2016. — № 4 (32). — С. 58-62.