УДК 004.056 https://doi.org/10.33619/2414-2948/87/27

ОСНОВНЫЕ ПРИНЦИПЫ РАБОТЫ ЗАЩИЩЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

*©**Лиманова Н. И.**, ORCID: 0000-0003-2924-5602, SPIN-код: 9799-8380, д-р техн. наук, Поволжский государственный университет телекоммуникаций и информатики, г. Самара, Россия, nataliya.i.limanova@gmail.com*
*©**Анашкин А. С.**, ORCID: 0000-0003-4803-3058, Поволжский государственный университет телекоммуникаций и информатики, г. Самара, Россия, a_anashkinn@icloud.com*

BASIC PRINCIPLES OF SECURE INFORMATION SYSTEMS

*©**Limanova N.**, ORCID: 0000-0003-2924-5602, SPIN-code: 9799-8380, Dr. habil., Povolzhsky State University of Telecommunications and Informatics, Samara, Russia, nataliya.i.limanova@gmail.com*
*©**Anashkin A.**, ORCID: 0000-0003-4803-3058, Povolzhsky State University of Telecommunications and Informatics, Samara, Russia, a_anashkinn@icloud.com*

Аннотация. Актуальность работы заключается в том, что темпы развития сферы информационной безопасности не соответствуют прогрессу в сфере разработки способов обработки данных, вследствие чего образуется серьезный недостаток практических знаний предметной области, который препятствует созданию условий для безопасной записи, обработки и хранения данных. Изучены современные способы и принципы обеспечения информационной безопасности, включающие в себя мандатный подход, а также дана краткая характеристика программных продуктов, поддерживающих этот подход. Мандатный метод защиты информации подразумевает выдачу прав доступа к определенным действиям в соответствии со статусом пользователя. Такими действиями могут быть, например, запись, чтение и изменение данных. Примерами же статусов пользователей являются «администратор» и «читатель», где администратору, как правило, предоставляется весь перечень доступных действий, а читателю — лишь минимальный, достаточный для ознакомительной деятельности. В своей архитектуре мандатный подход нередко содержит инструменты проведения кластерного анализа. Кластерный анализ можно применять как для проведения работ по анализу и оценке рисков, так и для определения степени защиты объекта. В любом случае, при построении кластера нужно учитывать, что некоторые уровни защиты могут быть представлены большим количеством объектов, чем остальные. На рынке средств защиты информации существуют программные продукты, которые позволяют использовать мандатный метод обеспечения информационной безопасности. Одним из ярких примеров является система управления БД PostgreSQL, которая имеет аппарат меток, присваиваемых в соответствии с уровнем прав пользователя: чем выше уровень прав — тем выше уровень доступа.

Abstract. The relevance of the work lies in the fact that the pace of development of the field of information security does not correspond to progress in the development of data processing methods, resulting in a serious lack of practical knowledge of the subject area, which prevents the creation of conditions for secure recording, processing and storage of data. In the process of writing the article, modern methods and principles of ensuring information security, including a mandatory approach, were studied, and a brief description of software products supporting this approach was given. The mandatory method of information protection implies granting access rights to certain actions in

Т. 9. №2. 2023
https://doi.org/10.33619/2414-2948/87

accordance with the user's status. Such actions can be, for example, writing, reading and changing data. Examples of user statuses are 'administrator' and 'reader', where the administrator, as a rule, is provided with the entire list of available actions, and the reader is provided with only a minimum, sufficient for familiarization activities. In its architecture, the mandatory approach often contains tools for conducting cluster analysis. Cluster analysis can be used both to carry out work on risk analysis and assessment, and to determine the degree of protection of an object. In any case, when building a cluster, it should be taken into account that some levels of protection may be represented by more objects than others. There are software products on the information security market that allow the use of a mandatory method of ensuring information security. One of the striking examples is the PostgreSQL database management system, which has an apparatus of labels assigned according to the user's level of rights: the higher the level of rights, the higher the access level.

Ключевые слова: СУБД, информационная безопасность, права доступа, информационные системы, мандатное управление.

Keywords: DBMS, information security, access rights, information systems, mandate management.

Предприятия по всему миру вкладывают большое количество ресурсов и средств в разработку информационных систем, необходимых для оптимизации производства и сокращения издержек. В этой связи зачастую разработчики информационных систем делают акцент скорее на оптимизационной составляющей программы, уделяя вопросу безопасности недостаточное внимание.

Актуальность работы обусловлена тем, что расхождение в уровнях развития методов обработки информации и способов защиты этой информации привели к недостаточному количеству научной базы знаний, которая могла бы позволить оценивать целесообразность тех или иных подходов при разработке средств защиты системы. Безопасность информационной системы не является величиной абсолютной, поскольку виды и способы хакерских атак постоянно совершенствуются, и, в случае, например, атаки на стратегически важный объект, например, атомную электростанцию, последствия таких действий могут оказаться фатальными для общества. Именно поэтому параметр безопасности системы относится к той сфере, в которой применяется информационный продукт.

Информационная система, оснащенная достаточной для данной отрасли степенью защиты, призвана обеспечить целостность и конфиденциальность обрабатываемых ею данных. В этой связи важно отметить, что в данном случае речь не идет о наличии у системы определенного стандартного модуля защиты данных, поскольку, как говорилось выше, степень и способ защиты зависят от области применения этой системы. Как правило, для систем защиты информации, предназначенных для работы в государственных органах, используются следующие способы защиты:

- использование специальных программно-аппаратных средств для защиты информации от несанкционированного доступа;
- применение средств криптографической защиты информации (СКЗИ);
- использование средств электронной цифровой подписи (ЭЦП) с использованием средств криптографической защиты информации;
- управление доступом.

Безопасность системы должна отражать основное назначение ее разработки: это такое ее состояние, при котором она способна отражать внешние злоумышленные действия,

подрывающие ее работоспособность, а также способна стабильно существовать, не создавая угроз для внутренних компонентов самой системы. Еще одним основополагающим свойством подобной системы является способность автоматизации обработки конфиденциальной информации [2, с. 48].

На объектах стратегического назначения информационные системы оснащаются мандатным управлением, которое подразумевает предоставление системой прав доступа к конфиденциальной информации согласно уровню доверенности пользователя. Такой метод подразумевает, что пользователь с наименьшим уровнем доверенности может получить доступ только к информации с наименьшей степенью конфиденциальности. Мандатное управление также предполагает наличие механизмов дифференциации, под которыми понимаются операции, обеспечивающие правила доступа (просмотр, запись, чтение), и операции управления правами доступа (владение, создание, удаление). Это классический подход к организации безопасности, который обеспечивает засекреченность данных для тех лиц, для которых обладание той или иной информацией не было предусмотрено внутренней политикой предприятия [3, с. 6].

Для организации мандатного управления часто используется кластерный анализ. Его суть заключается в последовательном выполнении классификации объектов защиты, их выделении и определении степени защиты, необходимой для данной системы [1, с. 94].

Среди программных продуктов, активно использующих принцип мандатного управления — ОС Astra Linux Special Edition, которая предоставляет хранилище информации о правах пользователей, связанное с хранилищем пользователей операционной системы, а также располагает средствами, предоставляющими инструменты контроля доступа к объектам, защищаемым мандатным управлением.

Еще одним продуктом, который в своей работе поддерживает мандатное управление, является система управления базами данных PostgreSQL, которая связана с хранилищем учетных записей и меток прав доступа ОС. Система также позволяет присваивать мандатные метки к объектам кластеров, таблиц баз данных, столбцов и записей.

В целом, поддержка мандатного управления актуальна и рекомендована для информационных систем, которые разрабатываются с целью их внедрения на крупные предприятия, например, на объектах стратегического и оборонного назначений и не только. Иерархическое устройство доступа к данным способно обеспечить их надежную сохранность, однако, в случае утечки данных нельзя забывать о человеческом факторе.

Список литературы:

1. Соколова С. П., Горковенко Е. В. Интеллектуальная система классификации с иерархической структурой множества объектов защиты в системах с мандатным разграничением доступа к информации // Актуальные проблемы экономики и управления. 2015. №1 (5). С. 93-106

2. Соколинская Н. Э., Куприянова Л. М. Риски развития информационных технологий в банковском секторе // Мир новой экономики. 2020. №3. С. 44-53

3. Аль-Хаммуд Ибрахим. Модели и алгоритмы повышения уровня информационной безопасности корпоративных информационно-телекоммуникационных сетей: автореф. … канд. техн. наук. Владимир, 2007. 16 с.

References:

1. Sokolova S. P., Gorkovenko E. V. Intellektual'naya sistema klassifikatsii s ierarkhicheskoi strukturoi mnozhestva ob"ektov zashchity v sistemakh s mandatnym razgranicheniem dostupa k informatsii // Aktual'nye problemy ekonomiki i upravleniya. 2015. №1 (5). S. 93-106

2. Sokolinskaya N. E., Kupriyanova L. M. Riski razvitiya informatsionnykh tekhnologii v bankovskom sektore // Mir novoi ekonomiki. 2020. №3. С. 44-53

3. Al'-Khammud Ibrakhim. Modeli i algoritmy povysheniya urovnya informatsionnoi bezopasnosti korporativnykh informatsionno-telekommunikatsionnykh setei: avtoref. … kand. tekhn. nauk. Vladimir, 2007. 16 s.

Работа поступила
в редакцию 07.01.2023 г.

Принята к публикации
14.01.2023 г.

Ссылка для цитирования:

Лиманова Н. И., Анашкин А. С. Основные принципы работы защищенных информационных систем // Бюллетень науки и практики. 2023. Т. 9. №2. С. 235-238. https://doi.org/10.33619/2414-2948/87/27

Cite as (APA):

Limanova, N., & Anashkin, A. (2023). Basic Principles of Secure Information Systems. *Bulletin of Science and Practice, 9*(2), 235-238. (in Russian). https://doi.org/10.33619/2414-2948/87/27