УДК 004.056.5
doi:10.18720/SPBPU/2/id25-335

Корчагин Егор Олегович
Санкт-Петербургский политехнический университет Петра Великого
egkor12@gmail.com

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПРИ РАЗРАБОТКЕ БАЗЫ ДАННЫХ ДЛЯ УПРАВЛЕНИЯ НИОКР В АО «НИИАС»

Аннотация. При цифровизации процессов перед компаниями встает вызов в обеспечении защищенности ПО, особенно если речь идет о стратегически важных научных организациях, таких как АО «НИИАС». В настоящий момент в ней преобладают разрозненные системы управления проектами, что способствует не только усложнению этого процесса, но и реализации рисков потери и утечки конфиденциальной информации, что может привести к коммерческим и правовым последствиям, а также к компрометации стратегически важных данных. Цель исследования – разработка комплекса рекомендуемых принципов, архитектурных решений, инструментов и методик, который ляжет в основу создания защищенной базы данных управления НИОКР. Основные задачи представляют собой анализ текущих проблем связанных с безопасностью данных, определение возможных решений, анализ современных средств защиты данных и выбор подходящих. В результате исследования предложены принципы, архитектурные решения, методики и инструменты, обеспечивающие защищенность БД. Практическая значимость работы заключается в повышении уровня защиты информации, что способствует сохранению конкурентоспособности АО «НИИАС» и соблюдению нормативных требований.

Ключевые слова: база данных, защищенное ПО, информационная безопасность, информационные технологии, управление НИОКР.

Egor O. Korchagin
Peter the Great St. Petersburg Polytechnic University
egkor12@gmail.com

ENSURING SECURITY IN THE DEVELOPMENT AND IMPLEMENTATION OF A DATABASE FOR R & D MANAGEMENT AT JSC NIIAS

Abstract. When digitalizing processes, companies face the challenge of ensuring software security, especially when it comes to strategically important scientific organizations such as JSC NIIAS. Currently, it is dominated by disparate project management systems, which not only complicates this process, but also increases the risks of loss and leakage of confidential information, which can lead to commercial and legal consequences, as well as to the compromise of strategically important data. The purpose of the study is to develop a set of recommended principles, security architecture, tools and methods that will form the basis for creating a secure R & D management database. The main objectives are to analyze current problems related to data security, identify possible solutions, analyze

modern data protection tools and select appropriate ones. As a result of the study, principles, security architecture, methods and tools were proposed to ensure database security. The practical significance of the work lies in increasing the level of information security, which helps maintain the competitiveness of JSC NIIAS and comply with regulatory requirements.

Keywords: database, information security, information technology, R&D management, secure software

Введение

Автоматизация и цифровизация процессов управления научно-исследовательскими и опытно-конструкторскими работами (НИОКР) становится не только фактором повышения эффективности, но и источником новых угроз, связанных с безопасностью данных, которые нужно минимизировать на этапе разработки программных продуктов. Одной из таких организаций, критически зависящих от защиты информации, является АО «НИИАС» (Научно-исследовательский и проектно-конструкторский институт информатизации, автоматизации и связи на железнодорожном транспорте).

На данный момент управление НИОКР в АО «НИИАС» осуществляется при помощи разрозненных систем, что делает процесс менее прозрачным. В то же время хранение данных при такой работе сопряжено с угрозами несанкционированного доступа, утечек информации и возможных кибератак. Компрометация данных может привести к серьезным экономическим, правовым и конкурентным последствиям. Обеспечить эффективную безопасность от информационных угроз можно с помощью программно-технических средств.[1]

Один из способов решения проблемы неэффективности управлением НИОКР может стать создание централизованной системы управления в виде базы данных, в которой будет содержаться вся необходимая информация о проектах, что создает новые риски, связанные с тем, что вся информация храниться в одном месте, поэтому критически необходимо прорабатывать безопасность такой БД (базы данных), начиная с этапа планирования.

Результаты

В Таблице 1 приведены результаты анализа основных проблем и угроз в управлении НИОКР в АО «НИИАС», связанные с информационной безопасностью, их причины и возможные способы устранения в базе данных.

Таблица 1

Проблемы и риски в информационной безопасности и способы их решения

Причина	Проблемы и риски [2]	Решение в БД
Отсутствие единой системы разграничения прав доступа	Несанкционированный доступ, утечки конфиденциальной информации	Реализация ролевой модели доступа (RBAC) [9] и принципа минимально необходимого доступа [5]
Отсутствие автоматизированного мониторинга	Сложность выявления угроз, невозможность оперативного реагирования	Внедрение SIEM, IDS/IPS, логирование событий безопасности с анализом аномалий [3]
Высокая степень зависимости от человека	Ошибки администраторов, отсутствие контроля за изменениями	Многофакторная аутентификация (MFA) [13], автоматизированные системы аудита и контроля
Отсутствующие или слабые механизмы резервного копирования	Потеря данных при сбоях, кибератаках, аппаратных отказах	Политика резервного копирования Disaster Recovery Plan [12]

Для решения этих проблем должна быть разработана защищенная база данных, включающая принципы, архитектуру, инструменты и методы, отраженные в Таблице 2.

Таблица 2

Принципы, архитектурные решения, инструменты и методы обеспечения защищенности БД

Категория	Описание	Причина использования и решаемая проблема
Принципы безопасности	*Основные правила и подходы к обеспечению защиты данных и управления доступом*	*Позволяют минимизировать риски утечек, контроль над доступом, соблюдение нормативов*
Принцип Least Privilege	Каждый пользователь получает только те права, которые необходимы для его задач	Предотвращает несанкционированный доступ, снижает риск инсайдерских атак [4]
Принцип Separation of Duties	Функции распределяются между разными пользователями, никто не получает полный контроль	Уменьшает риск злоупотребления полномочиями и ошибок из-за человеческого фактора [5]
Принцип Deny by Default	Пользователям запрещен доступ без специального разрешения [6]	Предотвращает случайный доступ к критически важным данным

Категория	**Описание**	**Причина использования и решаемая проблема**
Принцип Data Integrity	Поддержание целостности данных. Действия по изменению данных фиксируются и являются обратимыми [7]	Гарантирует, что данные не были подделаны или повреждены
Архитектура безопасности	*Способы построения структуры БД с учетом защиты информации*	*Позволяет создать устойчивую к атакам систему*
Многоуровневая архитектура	Разделение системы на уровни: приложение, логика, база данных. Каждый имеет свою защиту [8]	Ограничивает влияние потенциальных атак на всю систему
Ролевая модель доступа (RBAC)	Определяет права пользователей в зависимости от их ролей [9]	Пользователи могут работать только с разрешенными данными
Модульная архитектура безопасности	Функции безопасности разделяются на независимые модули [10]	Повышает устойчивость системы, взлом одного модуля не приводит к компрометации всей системы
Инструменты безопасности	*Программные и аппаратные решения для защиты базы данных*	*Для мониторинга, обнаружения и предотвращения угроз*
Шифрование данных (AES-256, TLS)	Кодирование информации для предотвращения несанкционированного доступа	Защищает конфиденциальные данные при передаче и хранении
Мониторинг активности (SIEM, IDS/IPS) [11]	Отслеживание действий пользователей и анализ потенциальных угроз	Позволяет вовремя обнаруживать атаки и подозрительное поведение
Резервное копирование	Регулярное создание копий с возможностью восстановления [12]	Предотвращает потерю данных в случае сбоев или атак
Методы защиты	*Практические подходы к обеспечению безопасности*	*Помогают эффективно реализовать защиту данных*
Аутентификация, многофакторная защита (MFA)	Подтверждение личности пользователей с использованием нескольких факторов	Минимизирует риски, связанные с человеческим фактором, неправильными паролями и потерянными устройствами [13]
Журналирование и аудит	Фиксация всех действий в системе и их анализ	Выявляет подозрительную активность и проводитанализ инцидентов

Категория	Описание	Причина использования и решаемая проблема
Периодическое тестирование на уязвимости	Проверка на уязвимости с помощью моделирования атак	Помогает превентивно выявить слабые места системы

Внедрение вышеприведенных решений поможет обеспечить достаточный уровень защищенности для управления НИОКР.

Заключение

Было проведено исследование по поиску решений по обеспечению защищенности базы данных для управления НИОКР в АО «НИИАС», в результате которого был создан рекомендуемый комплекс принципов безопасности, архитектурные подходы, а также инструменты и методики защиты данных. Внедрение централизованной базы данных с рекомендуемыми в работе решениями позволит АО «НИИАС» не только повысить эффективность управления НИОКР, но и улучшить защиту конфиденциальных данных и сохранить конкурентные преимущества в условиях цифровой трансформации.

Результаты исследования в последствии могут быть использованы для развития других безопасных информационных систем в сфере НИОКР.

Библиографический список

1. Седов О. Информационная безопасность результатов НИОКР // Директор информационной службы. – 2011. – № 5.

2. Грошева Е. К., Невмержицкий П. И. Информационная безопасность: современные реалии // Бизнес-образование в экономике знаний. – 2017. – № 3. – С. 35–38.

3. Токарев М. Н. SIEM-система как инструмент обеспечения информационной безопасности в организации // Актуальные исследования. – 2024. – № 2 (184).

4. Мирошниченко М. А. Архитектура нулевого доверия как инновационный инструмент в системе обеспечения защиты корпоративной информации // Актуальные проблемы обеспечения информационной безопасности систем электронного документооборота в рамках цифровой трансформации. – 2020. – С. 45–50.

5. Основы безопасности информационных систем [Электронный ресурс] // Habr. – URL: https://habr.com/ru/companies/ruvds/articles/547324/ (дата обращения: 01.03.2025).

6. Принцип «отказать по умолчанию» [Электронный ресурс] // ISMS Online. – URL: https://www.isms.online/glossary/deny-by-default-principle/ (дата обращения: 01.03.2025).

7. Целостность данных (Data Integrity) [Электронный ресурс] // LPI. – URL: https://lpi.by/blog-ru/data-integrity/ (дата обращения: 01.03.2025).

8. Многоуровневая архитектура [Электронный ресурс] // AppMaster. – URL: https://appmaster.io/ru/glossary/mnogourovnevaia-arkhitektura (дата обращения: 05.03.2025).

9. Управление доступом на основе ролей (RBAC) [Электронный ресурс] // Keeper Security. – URL: https://www.keepersecurity.com/ru_RU/resources/glossary/what-is-role-based-access-control/ (дата обращения: 05.03.2025).

10. Зачем использовать модульную архитектуру в разработке ПО? [Электронный ресурс] // AppMaster. – URL: https://appmaster.io/ru/blog/zachem-ispol-zovat-modul-nuiu-arkhitekturu-v-razrabotke-programmnogo-obespecheniia (дата обращения: 05.03.2025).

11. Основы резервного копирования данных [Электронный ресурс] // Habr. – URL: https://habr.com/ru/sandbox/42949/ (дата обращения: 05.03.2025).

12. Резервное копирование данных [Электронный ресурс] // AWS. – URL: https://aws.amazon.com/ru/what-is/data-backup/ (дата обращения: 07.03.2025).

13.Андреев А. А., Королев А. В. Информационная безопасность в системе государственного управления в условиях цифровой трансформации // Вестник университета. – 2015. – №6. – С. 123–128.

УДК 004.891.00
doi:10.18720/SPBPU/2/id25-336

Классен Софья Андреевна*, Вдович Светлана Анатольевна
Оренбургский государственный университет
**klassen.sofia@mail.ru*

ОПТИМИЗАЦИЯ ПРОЦЕССОВ ОЦЕНКИ И СТИМУЛИРОВАНИЯ СОТРУДНИКОВ НА ПЛАТФОРМЕ «1С:ПРЕДПРИЯТИЕ 8.3»

Аннотация. На фоне стремительного развития технологий и увеличения конкуренции, организации сталкиваются с необходимостью оптимизации внутренней структуры и внедрения систем, направленных на вовлечение работников в деятельность компании и повышения качества предоставляемых услуг. От того, насколько сотрудники компании профессиональны, насколько рабочие обязанности человека соответствуют его возможностям и наклонностям, зависит то, как динамично будет развиваться и функционировать компания. Оценка персонала позволяет не только увидеть сильные и слабые стороны сотрудников, но также дает возможность наметить план профессионального развития конкретного человека и выявить его потенциал и наклонности. Цель работы – создание инструмента, позволяющего анализировать деятельность сотрудников и внедрять мотивационные механизмы в виде стимулирующих выплат. Задачи, поставленные в рамках данного исследования, включают в себя предварительный анализ предметной области, определение структуры прикладного решения и разработку конфигурации системы. Ключевым элементом данного процесса является определение ключевых показателей эффективности, которые будут использоваться для оценки работы сотрудников.

Ключевые слова: оценка сотрудников, стимулирующие выплаты, показатели эффективности, мотивационные механизмы.