Е. А. Лаптева, С. В. Бегичева
Уральский государственный экономический университет, г. Екатеринбург
УДК 004.056

АУДИТ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННОЙ СИСТЕМЕ 1С

Аннотация. В статье посвящена теме аудита безопасности в информационной системе 1С. Перечислены и описаны последовательные этапы аудита безопасности, выполнение которых позволяет организациям выявлять и устранять потенциальные угрозы безопасности информационной системе 1С, обеспечивая целостность, конфиденциальность и доступность данных.

Ключевые слова: аудит безопасности, 1С, информационная система, защита информации.

Введение. 1С — это популярная система автоматизации управления предприятием, которая широко используется в различных организациях. Однако, как и любая другая информационная система, 1С требует надежной защиты данных и контроля доступа к ним. Тему безопасности в информационных системах на предприятии рассматривали в своих работах многие авторы, например, Голубева О.Л. [1] и Вьюнов Д.А. [2].

Проблема исследования. Проблемой исследования является анализ процесса аудита в системе 1С. Аудит безопасности и контроль доступа к данным в информационной системе 1С — это процесс мониторинга и анализа действий пользователей системы с целью обеспечения целостности, конфиденциальности и доступности данных. Аудит безопасности представляет собой процесс анализа и оценки различных аспектов безопасности в информационной системе, включая контроль доступа к данным, мониторинг действий пользователей, обнаружение аномалий и проблем безопасности.

Материалы и методы. Процесс аудита безопасности включает в себя несколько важных этапов (рис. 1):

- Оценка угроз безопасности данных;
- Анализ прав доступа пользователей;
- Мониторинг действий пользователей;
- Регистрация и анализ событий;
- Внедрение дополнительных мер безопасности [3].

Рис. 1. Процесс аудита безопасности

Расскажем подробнее о каждом из перечисленных этапов.

Первым шагом в аудите безопасности информационной базы 1С является идентификация потенциальных угроз безопасности данных, таких как несанкционированный доступ к данным, утечки информации или вредоносные действия. На данном этапе определяются актуальные угрозы безопасности информации, реализация которых возможна в системах. Основными задачами оценки угроз безопасности данных являются:

- Определение негативных последствий от реализации угроз;
- Инвентаризация систем и сетей и определение возможных объектов воздействия угроз;
- Определение источников угроз и оценка возможностей нарушителей по их реализации;
- Оценка способов реализации угроз;
- Оценка возможности реализации угроз и определение их актуальности;
- Оценка сценариев реализации угроз.

По результатам оценки угроз безопасности данных выявляются актуальные угрозы, реализация которых может привести к нарушению безопасности обрабатываемой информации и прекращению функционирования системы.

Вторым шагом в аудите безопасности информационной базы 1С является анализ прав доступа пользователей. Ведь для обеспечения безопасности данных необходимо строго контролировать права доступа пользователей к информационным базам 1С. Проверка и анализ прав доступа позволяет идентифицировать проблемные моменты и принять необходимые меры для их устранения.

Следующим шагом является мониторинг действий пользователей. На данном этапе специалисты по безопасности могут проводить анализ собранных данных для отслеживания аномалий, необычных действий пользователей, несанкционированного доступа и других потенциальных угроз безопасности в базах данных. Для эффективного контроля безопасности данных в информационной базе 1С необходимо вести постоянный мониторинг действий пользователей. Это позволяет быстро реагировать на подозрительную активность и предотвращать угрозы безопасности.

Затем проводится регистрация и анализ событий, произошедших в системе, что тоже является важной частью аудита безопасности и контроля доступа к данным является регистрация всех событий, происходящих в информационной базе 1С. Анализ этих событий позволяет выявить аномалии и потенциальные угрозы безопасности. В случае обнаружения подозрительных действий или нарушений безопасности, администратор системы должен принять меры по предотвращению угрозы. Это может включать блокировку доступа пользователя, изменение прав доступа, анализ причин инцидента и принятие мер по устранению уязвимостей.

Последним шагом является внедрение дополнительных мер безопасности. На основе результатов аудита безопасности администратор системы может внедрить дополнительные меры безопасности, улучшить политику доступа к данным, модификацию прав доступа или внедрение дополнительных средств защиты, обновить программное обеспечение системы и другое для повышения общего уровня безопасности в информационной базе 1С.

Результаты. Процесс аудита является цикличным, так как безопасность информационной системы требует постоянного обновления и улучшения. После внедрения дополнительных мер безопасности необходимо регулярно проводить аудиты и мониторинг системы, чтобы выявлять новые уязвимости и проблемы. На основе полученных данных администратор может вносить изменения и улучшения в систему безопасности, чтобы обеспечить надежную защиту информационной базы 1С от внешних угроз и атак. В результате данной статьи был проведен анализ процесса аудита в информационной системе 1С.

Заключение. Таким образом, аудит безопасности в информационной системе 1С является важным процессом, обеспечивающим надежную защиту конфиденциальной информации и предотвращающим угрозы безопасности данных. Проведение аудита позволяет определить слабые места в системе и принять необходимые меры для их устранения. Ответственное отношение к защите данных и проведение регулярных аудитов помогут предотвратить утечки информации и обеспечить бесперебойную работу информационной системы.

СПИСОК ЛИТЕРАТУРЫ

1. Голубева О.Л. Методы обеспечения безопасности данных в типовых конфигурациях на платформе 1С:Предприятие 8.3 / О.Л. Голубева // Актуальные проблемы современной науки: взгляд молодых: сборник трудов VIII Всероссийской (с международным участием) научно-практической конференции студентов, аспирантов и молодых ученых, Челябинск, 23 апреля 2019 года. — Челябинск: Южно-Уральский институт управления и экономики, 2019. — С. 617-629.
2. Вьюнов Д.А. Методы повышения информационной безопасности предприятия / Д.А. Вьюнов, Д.А. Быков // Тенденции развития науки и образования. — 2022. — № 92-10. — С. 46-50.
3. Макаренко С.И. Аудит информационной безопасности: основные этапы, концептуальные основы, классификация мероприятий / С.И. Макаренко // Системы управления, связи и безопасности. — 2018. — № 1. — URL: https://cyberleninka.ru/article/n/audit-informatsionnoy-bezopasnosti-osnovnye-etapy-kontseptualnye-osnovy-klassifikatsiya-meropriyatiy (дата обращения: 18.04.2024).