

# ЭКСПЕРИМЕНТАЛЬНАЯ РАБОТА С ИНТЕРПРЕТАТОРОМ ЯЗЫКА МОДЕЛИРОВАНИЯ КАЛЬКИБЕР

Черняев М.Д.

Институт проблем управления им. В.А. Трапезникова РАН, Москва, Россия  
paladine777@gmail.com

*Аннотация. В данном докладе представлены результаты экспериментальной работы по применению аналитического инструмента – интерпретатора языка моделирования киберугроз и рисков в системах управления КАЛЬКИБЕР, который разработан в ИПУ РАН, для задачи оценки рисков от киберугроз для электронного депозитария. Приводятся описание структуры и средств защиты депозитария.*

*Ключевые слова: риск, депозитарий, безопасность, целостность, сервер.*

## Введение

В ходе работы была поставлена задача оценки рисков от киберугроз для электронного депозитария при помощи интерпретатора языка моделирования КАЛЬКИБЕР. Данные средства были выбраны благодаря прошлому опыту использования данного языка моделирования для схожих задач и для дополнительного тестирования функций и возможностей языка КАЛЬКИБЕР, разработанного в Лаборатории № 31 "Распределенных информационных, аналитических и управляющих систем им. И.В. Прангишвили" Института проблем управления им. В.А. Трапезникова РАН (ИПУ РАН). Программа написана на специализированном языке ABIS, предназначенном для разработки программного обеспечения с элементами искусственного интеллекта (ИИ), и использует стандартные форматы и функции ввода-вывода данных этого языка [1].

КАЛЬКИБЕР предназначен для автоматизации работы специалистов по защите информации на этапах жизненного цикла промышленных программно-технических комплексов (ПТК), включая проектирование и эксплуатацию, и предоставляет основу для разработки эффективной системы киберзащиты при помощи технических и программных средств. Научной основой КАЛЬКИБЕР является теория киберустойчивости, важное место в которой занимает «барьерная модель».

Использование КАЛЬКИБЕР позволяет существенно повысить уровень защищенности промышленных ПТК от киберугроз, снизить риски возникновения инцидентов и обеспечить непрерывность бизнес-процессов [2].

В рамках поставленной задачи была разработана модель электронного депозитария программ. В модель были включены различные типы киберугроз, такие как несанкционированный доступ, внедрение вредоносного кода, и т.д. Для каждой угрозы были определены соответствующие уязвимости и вероятность их использования злоумышленниками.

## 1. Работа с документами

Прежде всего были изучены документы, раскрывающие принципы работы языка моделирования КАЛЬКИБЕР [3]. Данные документы были предоставлены ИПУ РАН.

После ознакомления с документацией был проведен анализ предметной области электронных депозитариев, их структуры и основных функций, чтобы определить наиболее актуальные риски и угрозы. Были рассмотрены существующие решения, их преимущества и недостатки, а также определены ключевые требования к системе киберзащиты.

На основе полученных знаний о КАЛЬКИБЕР и специфики электронных депозитариев, началось моделирование возможных атак и уязвимостей. Был разработан прототип структуры киберзащиты депозитария, включающий в себя безопасность целостности базы знаний для хранения документов, создание резервной копии на физическом носителе и алгоритмы безопасности со списками рисков, уязвимостей и нарушителей. Процедура создания резервной копии на физическом носителе включает в себя надежное хранение носителей в защищенном месте с ограниченным доступом.

Особое внимание уделено разработке сценариев реагирования на различные типы атак. КАЛЬКИБЕР позволяет смоделировать эти сценарии и оценить их эффективность, что дает возможность заранее подготовиться к возможным инцидентам и минимизировать их последствия. Также система киберзащиты, построенная на основе КАЛЬКИБЕР, предусматривает возможность адаптации к изменяющимся условиям и новым угрозам, что обеспечивается за счет возможности оперативного внесения изменений в модель.

Также важную роль играют механизмы аутентификации и авторизации, обеспечивающие защиту от несанкционированного доступа к данным. Было учтено соответствие требованиям нормативных документов в области защиты информации.

Реализация прототипа системы киберзащиты на основе КАЛЬКИБЕР позволила оценить не только ее эффективность, но и удобство использования. Система была разработана с учетом требований эргономики и интуитивной понятности, что упростило процесс управления и мониторинга состояния кибербезопасности депозитария [4].

Важным аспектом разработанной модели является ее адаптивность и возможность расширения. Система киберзащиты должна быть способна адаптироваться к изменяющимся угрозам и новым технологиям. Для этого предусмотрена возможность простого и быстрого добавления в систему новых угроз, уязвимостей и мер защиты в реальном времени. Использование языка КАЛЬКИБЕР обеспечивает гибкость и понятность модели, что упрощает ее дальнейшую разработку и внедрение.

Создание базы знаний угроз и уязвимостей является ключевым элементом предложенной системы киберзащиты. Эта база данных постоянно пополняется новыми данными об актуальных угрозах, методах атак и уязвимостях, что позволяет оперативно адаптировать систему защиты к изменяющемуся ландшафту киберугроз.

Предложенная структура киберзащиты также включает в себя мониторинг и анализ событий безопасности в реальном времени. Это позволяет оперативно выявлять подозрительную активность и принимать меры по ее нейтрализации. Для анализа используются как статические правила, так и методы машинного обучения, позволяющие выявлять аномалии в поведении системы [5].

Протокол создания резервной копии на физическом носителе разработан с учетом требований безопасности и надежности. Носители хранятся в защищенном месте с ограниченным доступом.

## 2. Использование примера

Также для разработки системы оценки рисков электронного депозитария было важно ознакомиться с примером OF1, смоделированным с помощью КАЛЬКИБЕР. Это довольно подробный пример, где расписаны угрозы, источники риска, уязвимости и алгоритмы защиты и разграничения доступа. Это был крайне важный подготовительный этап, позволяющий увидеть КАЛЬКИБЕР в действии и понять основные принципы его функционирования. Эти принципы и легли в основу дальнейшей работы [6].

На основе анализа OF1 и работы с КАЛЬКИБЕР был сформирован каркас для новой системы оценки рисков. Предложенные алгоритмы защиты и разграничения доступа были адаптированы, учитывая специфику электронного депозитария и особенности хранения и обработки информации. Особое внимание было уделено выявлению потенциальных уязвимостей, присущих именно этой инфраструктуре, и разработке контрмер, направленных на их нейтрализацию.

Анализ OF1, смоделированного с помощью КАЛЬКИБЕР, сыграл важную роль в разработке системы оценки рисков электронного депозитария. Он позволил выявить ключевые угрозы и уязвимости, а также разработать эффективные меры защиты, направленные на их устранение или минимизацию потенциального ущерба. В частности, особое внимание было уделено детализации угроз и источников риска, а также способам их взаимосвязи. Это позволило создать более комплексную модель угроз, учитывающую различные аспекты безопасности [7]. В процессе разработки системы оценки рисков активно использовались методы анализа и моделирования угроз. Были изучены различные сценарии атак и определены критические компоненты инфраструктуры, требующие повышенной защиты.

В результате, созданная система оценки рисков стала надежным инструментом для выявления и управления потенциальными угрозами в электронном депозитарии. Она позволила не только оценить вероятность возникновения рисков, но и определить возможный ущерб в случае их реализации.

Среди ключевых угроз были выделены:

- Несанкционированный доступ: Попытки взлома учетных записей сотрудников и привилегированных пользователей.
- Целостность данных: Умышленное или случайное искажение, подмена или удаление записей в реестре.
- Внутренние нарушители: Злонамеренные или небрежные действия сотрудников.
- Нормативные риски: несоответствие требованиям регуляторов (Банка России, ФСФР), что влечет за собой юридическую и финансовую ответственность.

Кроме того, анализ OF1 помог определить ключевые уязвимости, которые могут быть использованы злоумышленниками для получения несанкционированного доступа к данным и источники угроз. Были

рассмотрены различные типы уязвимостей, такие как уязвимости в программном обеспечении, уязвимости в конфигурации и уязвимости, связанные с человеческим фактором. Выявление этих уязвимостей позволило найти эффективные меры защиты, направленные на их устранение или минимизацию потенциального ущерба. Разумеется, для депозитария уязвимости соответствуют его специфике, но многие из них являются универсальными, (такие как вредоносный файл, способный повредить ПО).

Постоянный мониторинг и анализ рисков также являются неотъемлемой частью жизненного цикла системы безопасности электронного депозитария. Регулярное обновление модели угроз и уязвимостей, а также адаптация мер защиты к изменяющимся условиям позволяют поддерживать высокий уровень безопасности и обеспечивать непрерывность деятельности организации.

### **3. Разработка системы оценки рисков электронного депозитария**

После анализа предметной области и изучения примера OF1 была начата непосредственная разработка системы оценки рисков электронного депозитария на языке КАЛЬКИБЕР.

Для создания системы были описаны и внедрены модели угроз, рисков, нарушителей, программного и машинного обеспечения депозитария, а также мер защиты [8]. Для систематизации и использования этого в рамках практической системы оценки рисков и были использованы средства КАЛЬКИБЕР.

Испытания проводились на виртуальной машине с системой LICS, установленной на одной из рабочих станций Лаборатории 31 ИПУ РАН. Были выделены и описаны соответствующие проекту уязвимости, риски, источники угроз и методы защиты, после чего проект был приведен в исполнение, используя наработки примера OF1 как основу. Были проведены испытания, а также устранены несоответствия и выявившиеся в ходе испытаний ошибки. В ходе разработки системы оценки рисков электронного депозитария особое внимание уделялось обеспечению безопасности хранимых данных и предотвращению несанкционированного доступа к ним.

Использование наработок примера OF1 в качестве основы позволило значительно сократить сроки выполнения задачи и снизить риски, связанные с созданием системы оценки рисков с нуля. На этапе проектирования КАЛЬКИБЕР позволил разработать эффективную систему киберзащиты при помощи технических и программных средств.

Важным аспектом разработки являлось соответствие системы нормативным требованиям и стандартам в области информационной безопасности [9]. Были учтены требования законодательства о защите персональных данных. Это гарантирует легитимность функционирования депозитария и минимизирует риски, связанные с нарушением требований регуляторов.

Были приняты во внимание риски, связанные со спецификой электронного депозитария. Например, для обеспечения отказоустойчивости и высокой доступности данных была реализована система их резервного копирования и восстановления. Регулярно будут создаваться резервные копии данных, которые хранятся на отдельных носителях в защищенном месте (банковской ячейке, доступ к которой имеют отдельные привилегированные пользователи). В случае возникновения сбоев или аварийных ситуаций можно будет быстро восстановить данные из резервных копий, минимизируя простои и потери информации.

В рамках разработанной системы оценки рисков предусмотрена процедура регулярного мониторинга и анализа угроз [10]. Это позволяет оперативно реагировать на возникающие угрозы и принимать меры по их нейтрализации. Результаты мониторинга используются для корректировки модели рисков и совершенствования мер защиты.

Перспективы дальнейших исследований связаны с расширением модели электронного депозитария, включением в нее дополнительных элементов и угроз, а также с разработкой более сложных сценариев атак. Можно провести сравнительный анализ эффективности различных мер защиты, а также полностью раскрыть потенциал применения методов машинного обучения для автоматизации процесса оценки рисков.

Разработанная система оценки рисков электронного депозитария представляет собой комплексное решение, которое обеспечивает высокий уровень безопасности хранимых данных и предотвращает несанкционированный доступ к ним. Система соответствует нормативным требованиям и стандартам в области информационной безопасности и обеспечивает эффективное управление рисками.

Полученные результаты испытаний показали высокую эффективность разработанной системы в обнаружении и предотвращении угроз безопасности электронного депозитария. Система позволяет существенно снизить риски, связанные с потерей, повреждением или несанкционированным доступом к данным. Разработанная система оценки рисков электронного депозитария является гибкой и масштабируемой. Это позволяет адаптировать ее к изменяющимся требованиям и условиям

эксплуатации. Система может быть легко расширена и настроена для поддержки новых типов данных и операций. Ее дальнейшее развитие и совершенствование позволит повысить уровень защиты и обеспечить сохранность ценной информации [11].

#### 4. Заключение

В результате работы была проведена оценка рисков электронного депозитария, способного хранить и управлять цифровыми объектами, обеспечивая их целостность и доступность. Были разобраны рабочая документация и пример использования КАЛЬКИБЕР, после чего с их помощью и была создана система оценки рисков, разобраны уязвимости, злоумышленники, а также средства защиты от каждой угрозы. Кроме того, были предложены процедуры резервного копирования и восстановления данных, что позволит сделать управление документацией еще эффективнее.

Созданная система оценки риска демонстрирует потенциал языка КАЛЬКИБЕР для автоматизации работы специалистов по защите информации на этапах жизненного цикла промышленных ПТК, а также в целом для обеспечения безопасности путем моделирования угроз и проведения оценки рисков.

Разработанная модель позволила количественно оценить риски, связанные с различными киберугрозами, а также определить наиболее критичные элементы системы, требующие усиленной защиты. Интерпретатор языка КАЛЬКИБЕР предоставил возможность проводить сценарное моделирование атак, оценивая эффективность различных мер защиты и разрабатывая стратегии реагирования на инциденты. Проведенная работа по моделированию с использованием интерпретатора КАЛЬКИБЕР позволила не просто перечислить потенциальные угрозы, а оценить риски информационной безопасности для электронного депозитария программ и обосновать выбор конкретных мер защиты на основе анализа их эффективности. Одним из ключевых преимуществ разработанной системы является ее гибкость и возможность адаптации к изменяющимся условиям. Благодаря использованию языка КАЛЬКИБЕР, система может быть легко модифицирована и расширена для поддержки новых типов угроз и уязвимостей [12]. Это особенно важно в условиях быстрого развития информационных технологий и постоянного появления новых видов кибератак.

Итак, разработанная система оценки рисков электронного депозитария была успешно протестирована и использована для лучшего понимания организации защиты данных. КАЛЬКИБЕР может стать важным инструментом для обеспечения целостности и доступности ценных научных данных, а также для защиты интеллектуальной собственности Лаборатории 31 ИПУ РАН. Полученный опыт и наработки могут быть использованы для создания аналогичных систем в других организациях, занимающихся научными исследованиями и разработками, кроме того, данная система будет в дальнейшем улучшаться и оптимизироваться. Дальнейшие исследования могут быть направлены на разработку более сложных моделей угроз и уязвимостей, учитывающих специфику используемых технологий. Важным направлением является исследование возможностей применения методов машинного обучения для автоматизации процесса оценки рисков и выявления потенциальных угроз. Это позволит значительно повысить эффективность системы и снизить зависимость от экспертных оценок. Не менее важным направлением является расширение функциональности системы за счет добавления новых модулей и инструментов.

#### Литература

1. *Промыслов В.Г., Акимов Н.Н., Абдулова Е.А., Голубев П.А., Жарко Е.Ф., Жмайлов В.В., Лепехин И.Ю., Лобанок О.И., Исхаков А.Ю., Мецзяков Р.В., Полетыкин А.Г., Мусихин А.М., Пронин В.В., Семенов К.В., Цыренов Д.В.* Оценка риска и обеспечение кибербезопасности атомных электростанций. М.: ИПУ РАН, 2022. – 193 с. <https://www.ipu.ru/sites/default/files/publications/71754/67499-71754.pdf>.
2. *Полетыкин А.Г.* Формализованный метод оценки и управления рисками для обеспечения кибербезопасности больших систем управления // Материалы 8-ой Международной конференции «Управление развитием крупномасштабных систем» (MLSD'2015, Москва). Москва: ИПУ РАН, 2015. – Т. I. – С. 123–129.
3. *Полетыкин А.Г.* Интерпретатор языка моделирования киберугроз и рисков в системах управления КАЛЬКИБЕР: Свидетельство о государственной регистрации программы для ЭВМ № 2025618703 РФ; Заяв. 07.04.2025.
4. *Полетыкин А.Г.* Cyber Security Risk Assessment Method for SCADA of Industrial Control Systems // Proceedings of 2018 International Russian Automation Conference (RusAutoCon). Сочи: IEEE Catalog Number CFP18RUS-ART, 2018. – С. 1–5. <https://ieeexplore.ieee.org/document/8501811> (дата обращения 25.08.2025).
5. Аналитический инструмент - Интерпретатор языка моделирования киберугроз и рисков в системах управления КАЛЬКИБЕР. <https://www.ipu.ru/science/applied-research/software/kalkiber> (дата обращения 25.08.2025).

6. Компилятор-интерпретатор языка ABIS ИПУ РАН <https://www.ipu.ru/science/applied-research/software/abis/abis.ova> (дата обращения 25.08.2025).
7. ISO. BS ISO/IEC 27005:2011, Information technology. Security techniques. Information security risk management, 2011.
8. ISO. BS ISO 31000:2009, Risk management. Principles and guidelines, 2009.
9. ISO/IEC 27002:2013, Code of practice for information security controls - essentially a detailed catalog of information security controls that might be managed through the ISMS, 2013.
10. *Byvaikov M.E., Zharko E.F., Mengazetdinov N.E. and Poletykin A.G.* Experience from design and application of the top-level system of the process control system of nuclear power-plant // Automation and Remote Control. – 2006. – Vol. 67, № 5. – P. 735–747.
11. *Cherdantseva Yu., Burnap P., Blyth A., Eden P. and Jones K.* A review of cyber security risk assessment methods for SCADA systems // Computers & Security. – 2016. – Vol. 56. – P. 1–27.
12. *Babaev D.I., Poletykin A.G., Promyslov V.G. and Timofeev M.Yu.* Managing cyber security safety of APCS of nuclear power plants // Problems of Management. – 2018. – № 3. – P. 47–55.