

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Петербургский государственный университет путей сообщения
Императора Александра I»
(ФГБОУ ВО ПГУПС)

Факультет «Автоматизация и интеллектуальные технологии»

Кафедра «Информатика и информационная безопасность»

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

к дипломному проекту

вид выпускной квалификационной работы: бакалаврская работа, дипломный проект (работа), магистерская диссертация

Степанова Павла Александровича

Фамилия, имя, отчество обучающегося

на тему Методика оценивания защищенности ERP-системы
от угроз нарушения целостности

Обучающийся

подпись, дата

П.А. Степанов

И.О. Фамилия

И.о. заведующего
кафедрой –
главный руководитель

подпись, дата

к.т.н., В.А. Гончаренко

ученое звание, И.О. Фамилия

Руководитель ВКР

подпись, дата

к.т.н., С.В. Корниенко

ученое звание, И.О. Фамилия

Консультанты

подпись, дата

к.т.н., Р.Г. Ахтямов

ученое звание, И.О. Фамилия

к.э.н., Н.В. Сакс

ученое звание, И.О. Фамилия

Нормоконтролер

подпись, дата

М.Ф. Соломатова

ученое звание, И.О. Фамилия

Санкт-Петербург
2023

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПУТЕЙ СООБЩЕНИЯ
ИМПЕРАТОРА АЛЕКСАНДРА I»

наименование вуза

Факультет	Автоматизация и интеллектуальные технологии	Кафедра	Информатика и информационная безопасность
Специальность (направление подготовки)	10.05.03 Информационная безопасность автоматизированных систем		
Специализация (профиль)	Информационная безопасность автоматизированных систем на транспорте		

УТВЕРЖДАЮ

Зав. кафедрой

«___» _____ 20__ г.

ЗАДАНИЕ

на выпускную квалификационную работу обучающегося

Степанова Павла Александровича

фамилия, имя, отчество

1. Тема проекта (работы) Методика оценивания защищенности ERP-системы от угроз нарушения целостности

утверждена распоряжением проректора по учебной работе от «___» _____ 20__ г.
№ _____

2. Срок сдачи обучающимся законченного проекта (работы) «___» _____ 20__ г.

3. Исходные данные к проекту (работе) Федеральный закон от 27 июля 2006 г. N 149-ФЗ, Федеральный закон от 27.07.2006 г. N 152-ФЗ, Федеральный закон от 29 июля 2004 г. N 98-ФЗ

4. Содержание расчетно-пояснительной записки (перечень подлежащих разработке вопросов) _____

1. Анализ ERP-системы «1С:Управление нашей фирмой» как объекта защиты, анализ угроз нарушения целостности информации.

2. Анализ и выбор методов защиты информации от угроз нарушения целостности информации.

3. Разработка программного модуля контроля загружаемых конфигураций и расширений конфигурации.

4. Тестирование разработанного программного модуля на стенде.

5. Разработка и применение комплексной методики оценивания защищенности ERP-системы «1С:Управление нашей фирмой» от угроз нарушения целостности информации.

6. Оценивание эффективности внедрения результатов в ВКР в области охраны труда.

7. Техничко-экономическое обоснование ВКР.

5. Перечень графического материала (с точным указанием обязательных чертежей Презентация

6. Консультанты по ВКР с указанием относящихся к ним разделов проекта (работы, диссертации)

Раздел	Консультант	Подпись, дата	
		Задание выдал	Задание принял
Охрана труда	Ахтямов Расул Гумерович., к.т.н., доцент кафедры «Техносферная и экологическая безопасность»		
Техничко- экономическое обоснование	Сакс Надежда Вячеславовна. к.э.н., доцент кафедры «Экономика транспорта»		

7. Дата выдачи задания

Руководитель ВКР

(подпись)

(расшифровка подписи)

Задание принял к исполнению

(подпись)

(расшифровка подписи)

КАЛЕНДАРНЫЙ ПЛАН

№ п/п	Наименование этапов ВКР	Сроки выполнения этапов ВКР	Примечание
1	Подготовка задания на ВКР, утверждение его у зав. кафедрой, выдача задания на ВКР	03.02.2023	
2	Анализ ERP-системы «1С:Управление нашей фирмой» как объекта защиты, анализ угроз нарушения целостности информации	03.02.2023 – 10.03.2023	
3	Анализ и выбор методов защиты информации от угроз нарушения целостности информации	03.02.2023 – 10.03.2023	
4	Разработка программного модуля контроля загружаемых конфигураций и расширений конфигурации	10.03.2023 – 17.04.2023	
5	Тестирование разработанного программного модуля на стенде	10.03.2023 – 17.04.2023	
6	Разработка и применение комплексной методики оценивания защищенности ERP-системы «1С:Управление нашей фирмой» от угроз нарушения целостности информации.	17.04.2023 – 05.05.2023	
7	Оценивание эффективности внедрения результатов ВКР в области охраны труда	05.05.2023 – 15.05.2023	
8	Расчет технико-экономического обоснования ВКР	05.05.2023 – 15.05.2023	
9	Оформление пояснительной записки на ВКР	15.05.2023 – 05.06.2023	
10	Прохождение нормоконтроля	15.05.2023 – 05.06.2023	
11	Сдача ВКР (бумажная и электронная версии) на кафедру	15.05.2023 – 05.06.2023	
12	Проверка ВКР в системе «Антиплагиат ВУЗ»	05.06.2023 – 12.06.2023	
13	Получение внешней рецензии на ВКР	12.06.2023 – 20.06.2023	
14	Защита ВКР	16.06.2023 – 30.06.2023	

Обучающийся

(подпись)

(расшифровка подписи)

Руководитель ВКР

(подпись)

(расшифровка подписи)

АННОТАЦИЯ

Степанов П.А. /КИБ-812/ Методика оценивания защищенности ERP-системы от угроз нарушения целостности. Пояснительная записка к дипломному проекту (Электронный носитель, 131 200 символов, 3,61 Мб Степанов П.А. Методика оценивания защищенности ERP-системы от угроз нарушения целостности.pdf). Кафедра «Информатика и информационная безопасность», ПГУПС, СПб, 2023, 112 с., илл. 19, табл. 16, библи. 15 наименований.

Ключевые слова: МЕТОДИКА ОЦЕНИВАНИЯ ЗАЩИЩЕННОСТИ, ERP-СИСТЕМЫ, ЗАЩИТА ОТ УГРОЗ НАРУШЕНИЯ ЦЕЛОСТНОСТИ.

Данная работа посвящена разработке методики оценки защищенности ERP-системы «1С:Управление нашей фирмой» от угроз нарушения целостности. В работе анализируется ERP-система как объект защиты, функциональные и структурные особенности. Производится анализ угроз нарушения целостности и определяются слабые места системы.

В рамках методики спроектирована модель контроля целостности конфигураций и разработана система на основе модели для тестирования.

Выполняется оценка условий труда специалиста 1С, работающего с системой контроля целостности конфигураций, а также расчет потенциального экономического эффекта проекта.

Подпись: _____ Степанов П.А.

Дата: «____» _____ 2023г.

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

ЭДО	–	Электронный документооборот
УСН	–	Упрощённая система налогообложения
ОСНО	–	Общая система налогообложения
СУБД	–	Система управления базами данных
ОС	–	Операционная система
КТ	–	Коммерческая тайна
ПДн	–	Персональные данные
ИСПДн	–	Информационная система персональных данных
ИБ	–	Информационная безопасность
ПО	–	Программное обеспечение

СОДЕРЖАНИЕ

ВВЕДЕНИЕ.....	9
1. АНАЛИЗ ERP-СИСТЕМЫ «1С:УПРАВЛЕНИЕ НАШЕЙ ФИРМОЙ» КАК ОБЪЕКТА ЗАЩИТЫ.....	11
1.1. Описание и функциональные особенности ERP-системы «1С:Управление нашей фирмой»	11
1.2. Структурные особенности ERP-системы «1С:Управление нашей фирмой»	16
1.3. Определение защищаемых информационных ресурсов.....	21
1.4. Классификация уровня защищенности информационной системы, как информационной системы персональных данных	22
1.5. Определение наиболее актуальных угроз нарушения целостности информационной безопасности, оценка возможностей внешних и внутренних нарушителей	25
1.6. Анализ наиболее актуальных угроз нарушения целостности.....	27
1.7. Предложения по применению организационных и технических мер по защите информации от угроз нарушения целостности.....	31
Выводы по первой главе.....	35
2. АНАЛИЗ МЕТОДОВ И ПРОЕКТИРОВАНИЕ МОДЕЛИ КОНТРОЛЯ ЦЕЛОСТНОСТИ КОНФИГУРАЦИЙ ERP-СИСТЕМЫ	36
2.1. Анализ методов контроля целостности конфигурации	37
2.2. Разработка требований к модели контроля целостности конфигураций	42
2.3. Исследование модели контроля целостности Кларка-Вилсона.....	43
2.4. Проектирование модели контроля целостности конфигураций для ERP-системы «1С:Управление нашей фирмой»	45
Выводы по второй главе.....	47
3. РАЗРАБОТКА МЕТОДИКИ ОЦЕНИВАНИЯ ЗАЩИЩЕННОСТИ ERP-СИСТЕМЫ ОТ УГРОЗ НАРУШЕНИЯ ЦЕЛОСТНОСТИ КОНФИГУРАЦИЙ	50
3.1. Внедрение системы контроля целостности конфигураций.....	51
3.2. Эксплуатация системы контроля целостности конфигураций	52
Выводы по третьей главе	56

4. ТЕСТИРОВАНИЕ РАЗРАБОТАННОЙ МЕТОДИКИ ОЦЕНИВАНИЯ ЗАЩИЩЕННОСТИ ERP-СИСТЕМЫ.....	57
4.1. Разработка системы контроля целостности конфигураций	57
4.2. Внедрение системы контроля целостности конфигураций по разработанной методике.....	64
4.3. Эксплуатация системы контроля целостности конфигураций по разработанной методике.....	66
4.4. Анализ результатов тестирования.....	69
Выводы по четвертой главе	71
5. ОХРАНА ТРУДА	72
5.1. Анализ производственных факторов для специалиста информационной безопасности	73
5.2. Рекомендации по нормализации условий труда по каждому фактору .	78
Выводы по пятой главе.....	81
6. ТЕХНИКО-ЭКОНОМИЧЕСКОЕ ОБОСНОВАНИЕ ПРОЕКТА	82
6.1. План выполнения дипломного проекта	83
6.2. Смета затрат на научно-исследовательскую работу	85
6.3 Стоимость выполнения дипломного проекта	90
6.4. Расчет экономического эффекта	91
Выводы по шестой главе	93
ЗАКЛЮЧЕНИЕ	94
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ	97
ПРИЛОЖЕНИЯ.....	99

ВВЕДЕНИЕ

В современном мире информация является значимым ресурсом, ее сохранность и правильное использование являются одними из первоочередных задач для развития организации и производства и снижения уровня разнообразных рисков. Важнейшим актуальным вопросом для предприятия является вопрос информационной безопасности.

Каждая организация или предприятие внедряет в работу различные информационные системы для автоматизации процессов, которые происходят внутри этих организаций. Средние и крупные организации при расширении начинают испытывать трудности управления. В качестве решения в организации внедряют ERP-системы.

ERP-система представляет собой программный комплекс или информационную систему, в которой хранятся и обрабатываются данные всех процессов в единой базе данных. Преимущество использования ERP-системы заключается в централизованной и общей информационной системы, что позволяет удобно управлять организацией.

Так как в ERP-системе хранятся все данные и происходят процессы организации, то эта система является основной и приоритетной целью злоумышленников. Подход к защите системы должен быть соответствующий.

В качестве объекта защиты в данной работе рассматривается ERP-система «1С: Управление нашей фирмой».

Целью данной работы является повышение защищенности ERP-системы «1С:Управление нашей фирмой», за счёт применения разработанной методики оценивания защищенности от угроз нарушения целостности конфигураций.

Цель является выполненной, если по итогу проведенного тестирования разработанная методика покажет свою эффективность оценивания, производительность, решит проблему при возникновении нарушения целостности ERP-системы.

Для достижения поставленной цели в рамках работы решаются следующие задачи:

- Провести анализ ERP-системы «1С:Управление нашей фирмой» как объекта защиты;
- Выявить проблемные места в ERP-системе;
- Спроектировать модель контроля целостности конфигураций;
- Разработать методику оценивания защищенности ERP-системы от угроз нарушения целостности;
- Протестировать разработанную методику;
- Выполнить анализ результатов тестирования;
- Провести анализ охраны труда для специалиста 1С и рассчитать экономический эффект проекта.

1. АНАЛИЗ ERP-СИСТЕМЫ «1С:УПРАВЛЕНИЕ НАШЕЙ ФИРМОЙ» КАК ОБЪЕКТА ЗАЩИТЫ

1.1. Описание и функциональные особенности ERP-системы «1С:Управление нашей фирмой»

ERP-система «1С:Управление нашей фирмой» представляет собой готовое комплексное решение для управления, учета, контроля и планирования в малом и среднем бизнесе [2]. Данная система является отличным выбором для предпринимателей, занимающихся розничной и оптовой торговлей, интернет-торговлей и др. Она позволяет поэтапно систематизировать и автоматизировать бизнес-процессы.

Решение не перегружено излишней функциональностью и может быть настроено под любую специализацию и отрасль компании.

ERP-система «1С:Управление нашей фирмой» – единая информационная среда для управления различными аспектами деятельности организации, что обеспечивается за счет функциональных модулей, представленных на Рисунке 1.1.



Рисунок 1.1 – Функциональные модули системы

Описание функциональных модулей ERP-системы «1С:Управление нашей фирмой» [15]:

1. Управление взаимоотношениями с клиентами (CRM).

Данный модуль позволяет осуществлять управление заказами, а также счетами, анализировать процесс выполнения заказов. Помимо этого, предусмотрена возможность анализа продаж, а также планирование данного показателя. Стоит отметить возможность создания прайс-листов, планирование событий и заданий, уведомление о них. Что касается прямого взаимодействия с клиентами, модуль позволяет реализовать массовую отправку электронных писем и SMS. Еще несколько функций: оценка рисков контрагентов, генерация аналитических отчетов, сегментация контрагентов на основе различных признаков, и контроль взаиморасчетов.

2. Розничная торговля.

Модуль «Розничная торговля» позволяет надлежащим образом оформлять розничные продажи. Важно отметить возможность работы с онлайн-кассами с передачей данных в ФНС в соответствии с действующим законодательством.

3. Оптовая торговля.

Функциональный модуль «Оптовая торговля» облегчает работу с заказами и реализацией товара. Он позволяет осуществлять оперативное управление номенклатурой, а также ценами, на основе которых происходит составление прайс-листов. Функционал по планированию продаж делает модуль более гибким и эффективным.

4. Интернет-магазины.

Данный модуль открывает возможность запуска собственного сайта интернет-магазина на сторонней платформе. Реализована штатная интеграция, обеспечивающая обмен данными.

5. Работы и услуги.

Функциональный модуль отвечает за планирование и контроль выполняемых работ по заказ-нарядам, заданиям на работы. Включен учет рабочего времени, графики работы. Для наглядности предусмотрено графическое оформление стадий выполнения работ и состояния оплаты, а также степени выполнения.

6. Производство.

Модуль «Производство» позволяет отслеживать заказы, их размещение в производство. Также за счет модуля осуществляется планирование и контроль исполнения производства по заказам, формирование сдельных нарядов на основании заказов покупателей. За возможность управления ресурсами отвечают функции, позволяющие вести учет и распределять затраты, управлять производственными запасами. Учет кадровых ресурсов осуществляется за счет учета рабочего времени и составления общих отчетов.

7. Закупки и склад.

Данный модуль позволяет осуществлять управление заказами поставщикам, в том числе оформлять сводный заказ поставщику по нескольким заказам одновременно. Он отвечает за формирование счетов от поставщиков, регистрацию поступлений заказанных товаров, выводит актуальные прайс-листы поставщиков и автоматически регистрирует цены от поставщиков, удаляя неактуальные цены. Позволяет управлять номенклатурой и складскими запасами путем отслеживания: перемещения, резервирования. Построение аналитической отчетности и сверка с поставщиками – еще одни важные функции данного модуля.

8. Зарплата и кадры.

Специальный модуль, позволяющий осуществлять кадровый учет, вести документы по заработной плате сотрудников. Отвечает за оформление справочников по зарплате, табелей учета рабочего времени сотрудников, а также отчетные документы по зарплате (ведомости, расчетные листки и т. д.).

9. Финансы.

Функциональный модуль позволяет вести учет наличных и безналичных денежных средств. Осуществлять планирование финансовых потоков, а также резервировать средства для определенных целей, вести платежный календарь. Дополнительно отвечает за эквайринговые операции по картам.

10. Отчетность.

Модуль «Отчетность» позволяет осуществлять расчет налогов, формировать, а также сдавать отчетные документы через ЭДО, минуя посредников – сразу в контролирующие органы.

11. Анализ бизнеса.

Модуль включает в себя все существующие в рамках системы справочники. В него включены данные по имуществу, доступна функция планирования бюджетов и продаж, ввода начальных остатков, отчет по финансовым операциям. Предоставляет возможность электронной доставки документов (ЭДО). Есть потенциал к интеграции с другими программами.

12. Мобильная работа.

Интерфейс «1С:Управление нашей фирмой» становится доступным на мобильном устройстве благодаря данному модулю.

Система предоставляет функционал для управленческого учета, а также налогового учета для индивидуальных предпринимателей. Она поддерживает различные системы налогообложения, такие как упрощенный режим налогообложения (УСН), общая система налогообложения (ОСНО) и патентная система. В системе реализованы функции по сдаче отчетности и уплате налогов.

Для предприятий, которые состоят из нескольких юридических лиц или индивидуальных предпринимателей, система позволяет настраивать управленческий учет для всей компании или отдельно для каждой организации.

Управленческий учет основывается на данных, которые фиксируются в документах. Операции записываются один раз и автоматически отражаются в различных разделах управленческого учета, формируя управленческий баланс.

Таким образом, конфигурация «Управление нашей фирмой» обеспечивает следующие возможности:

- Руководству предприятия и управленцам, отвечающим за развитие бизнеса, предоставляются инструменты для анализа, планирования и гибкого управления ресурсами компании с целью повышения ее конкурентоспособности;

- Руководителям функциональных подразделений, менеджерам и сотрудникам, непосредственно занимающимся производственной, сбытовой, снабженческой и другой деятельностью, связанной с обеспечением процесса производства, предоставляются инструменты, которые помогают повысить эффективность их ежедневной работы в соответствии с их собственными областями ответственности.

Система предоставляет возможность регистрации и создания первичных документов, относящихся к различным аспектам хозяйственной деятельности предприятия, таким как закупки, финансы, склад и производство. Электронные версии этих документов позволяют удобно фиксировать хозяйственные операции в системе.

Для предприятий есть возможность вести управленческий учет как для всей компании в целом, так и для каждой отдельной организации внутри компании. Система предоставляет аналитические отчеты, которые позволяют пользователям получать информацию по всем разрезам учета. Пользователи могут самостоятельно настраивать уровень детализации, параметры группировки и критерии отбора данных в отчетах в соответствии с конкретными задачами, а также формировать собственные варианты для настройки отчетов.

1.2. Структурные особенности ERP-системы «1С:Управление нашей фирмой»

В системе «1С:Управление нашей фирмой» существует четкое разделение на платформу «1С:Предприятие 8» и прикладное решение. Платформа представляет собой «framework» (структура, рамки), в котором функционирует прикладное решение [1]:

- Платформа служит фундаментом для построения прикладных решений;
- Платформа является средой их исполнения;
- Платформа содержит инструментарий, необходимый для разработки, администрирования и поддержки прикладных решений.

При этом прикладное решение является самостоятельной сущностью и может выступать в качестве отдельного программного продукта. Но полностью опирается на технологии платформы. В данном случае в качестве прикладного продукта выступает «1С:Управление нашей фирмой».

Прикладные решения на платформе «1С:Предприятие 8» называются конфигурациями.

В зависимости от нужд к конфигурациям могут применяться расширения конфигурации. Расширения конфигурации позволяют значительно упростить адаптацию типового прикладного решения к потребностям организации. Для одной конфигурации может быть множество расширений конфигурации.

Расширения конфигурации могут выступать в роли решения для адаптации прикладного решения или, например, в роли исправления прикладного решения.

Обновление конфигурации или расширение конфигурации требуется, когда в процессе эксплуатации прикладного решения возникают ситуации, требующие внесения изменений в прикладное решение. Например, может выйти новая версия прикладного решения или просто потребоваться добавление новой функциональности в существующее прикладное решение.

Конфигурация и расширение конфигурации является лишь надстройкой и логикой работы системы. Для хранения данных используется база данных, в зависимости от конфигурации и расширения конфигурации выстраивается логика по работе с данными и работой с базой данных.

Для работы системы платформа поддерживает два варианта: файловый и клиент-серверный. И в том, и в другом варианте все прикладные решения работают полностью идентично.

Файловый вариант работы рассчитан на персональную работу одного пользователя или работу небольшого количества пользователей в локальной сети. В этом варианте все данные информационной базы располагаются в одном файле — в файловой СУБД. В рамках дипломного проекта данный вариант работы не рассматривается, так как подразумевается, что будет большое количество пользователей использовать ERP-систему.

Клиент-серверный вариант работы предназначен для использования в рабочих группах или в масштабе предприятия. Он реализован на основе трехуровневой архитектуры «клиент-сервер». В этом варианте информационная база хранится в одной из поддерживаемых систем управления базами данных, а взаимодействие между клиентским приложением и СУБД осуществляет кластер серверов «1С:Предприятия 8».

При клиент-серверном варианте сервер «1С:Предприятия 8» является сервером приложений.

Клиентское приложение — это программа, работающая на компьютере пользователя и обеспечивающая интерактивное взаимодействие системы «1С:Предприятие 8» с пользователем, в отличие от других компонент системы (программ и рабочих процессов), предназначенных исключительно для программного взаимодействия с другими частями системы или с другими программными объектами.

В системе «1С:Предприятие 8» существует 5 клиентских приложений:

- толстый клиент;

- тонкий клиент;
- веб-клиент;
- мобильный клиент;
- конфигуратор.

Возможности этих клиентских приложений можно представить в сводном виде. В качестве иллюстрации сводных данных по возможностям клиентских приложений выступает таблица 1.1.

Таблица 1.1 – Виды клиентских приложений «1С:Предприятие 8»

	Толстый клиент	Тонкий клиент	Веб-клиент	Мобильный клиент	Конфигуратор
Разработка прикладных решений	Нет	Нет	Нет	Нет	Да
Работа в локальной сети	Да	Да	Да	Нет	Да
Работа через Интернет	Нет	Да	Да	Да	Нет
Необходимость предварительной установки	Да	Да	Нет	Да	Да
Работа на мобильных устройствах	Нет	Нет	Да	Да	Нет

Помимо этого, программа «1С:Управление нашей фирмой» поддерживает возможность подключения удаленных пользователей через Интернет с помощью тонкого клиента и веб-клиента. Для этого используется специально настроенный веб-сервер, который обеспечивает взаимодействие между этими пользователями и базой данных или кластером. Такое решение позволяет удаленным пользователям безопасно работать с системой, получая доступ к необходимым функциям и данным через Интернет.

Обобщённая архитектура системы «1С:Управление нашей фирмой» представлена на рисунке 1.2.

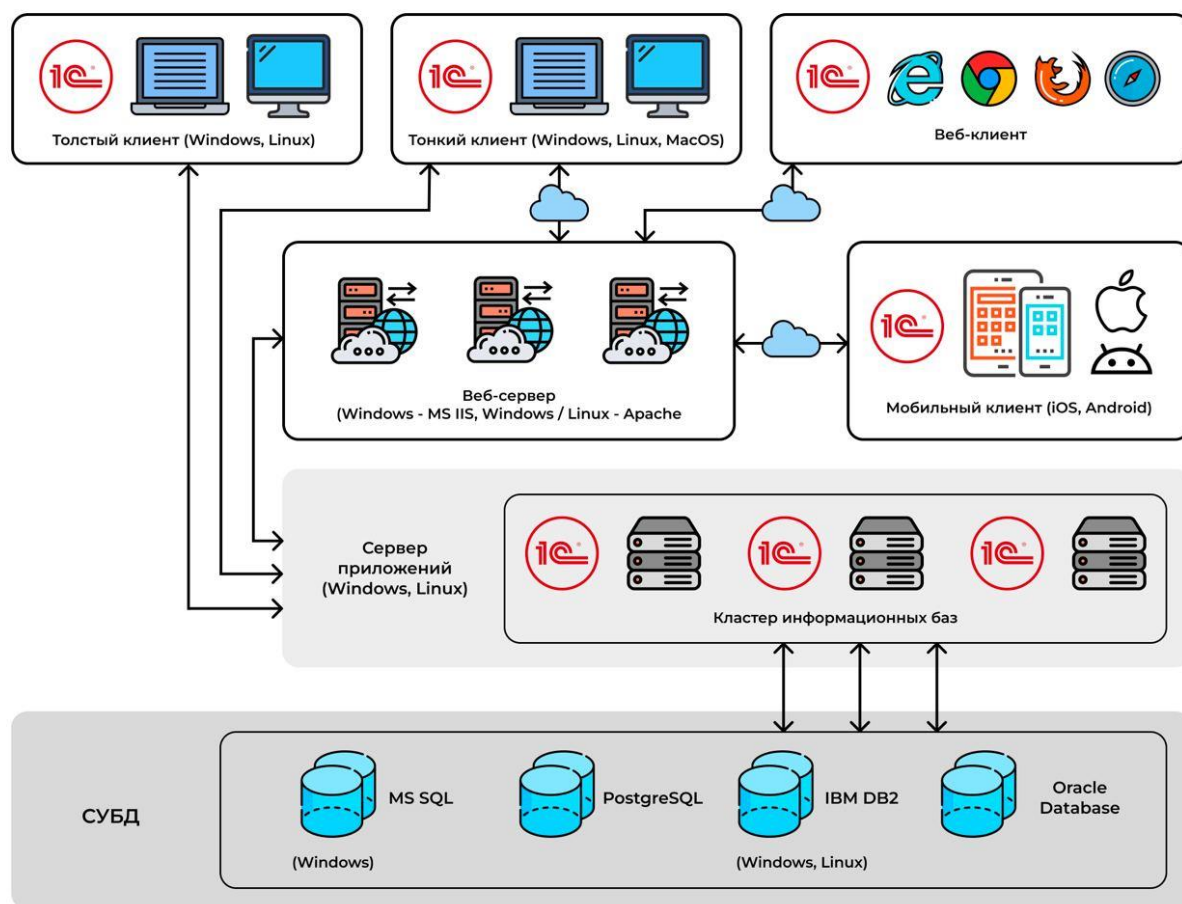


Рисунок 1.2 – Архитектура системы «1С:Управление нашей фирмой»

Для работы клиентских приложений необходимы обозначены системные требования, описанные в таблице 1.2.

Таблица 1.2 – Системные требования для клиентских приложений

	ОС	Браузер
Тонкий клиент	Windows XP SP3 и выше; Astra Linux Special Edition 1.6 и выше; Linux: РЕД ОС 7.3 МУРОМ; CentOS 7; Debian 10 и выше;	
Толстый клиент		
Конфигуратор		
	Mint 19 и выше; Red Hat Enterprise 7 и выше; Oracle Linux 7 и выше; Ubuntu 18.04 LTS и выше; macOS 10.12 и выше; Эльбрус 7.0; Эльбрус 7.1.	

Продолжение таблицы 1.2

Веб-клиент		Google Chrome версии 49 и выше; Mozilla Firefox версии 52 и выше;
		Microsoft Edge; Safari версии 4.0.5 и выше; Google Chrome для Android, Safari для iPhone/iPad; Браузеры на базе Chromium: chromium-gost; Яндекс.Браузер версии 22 и выше.
Мобильный клиент	iOS 8.0 — 14.X; Android 4.1 — 11.X; Windows 10.	

Для работы сервера приложений «1С:Предприятие 8» необходимы следующие требования к ОС:

- Windows XP SP3 и выше;
- Windows Server 2003 и выше;
- Astra Linux Special Edition 1.6 и выше;
- Linux: РЕД ОС 7.3 МУРОМ;
- CentOS 7;
- Debian 10 и выше;
- Mint 19 и выше;
- Red Hat Enterprise 7 и выше;
- Oracle Linux 7 и выше;
- Ubuntu 18.04 LTS и выше;
- macOS 10.12 и выше;
- Эльбрус 7.0;
- Эльбрус 7.1.

На сервере баз данных необходима одна из представленных СУБД:

- Microsoft SQL Server 2005 SP3 и выше;
- PostgreSQL 8.1.5 и выше;

- IBM DB2 9.7 FixPack 6 и выше;
- Oracle Database 11gR2 и выше.

Платформа «1С:Предприятие 8» поддерживает два приложения веб-сервера Apache и IIS. Для веб-сервера Apache версия 2.0 и выше, она представлена на ОС Windows и Linux. Для веб-сервера IIS поддерживается с версии 5.1 и выше.

1.3. Определение защищаемых информационных ресурсов

К конфиденциальной информации, обрабатываемой в системе «1С:Управление нашей фирмой» можно отнести все данные, так как они относятся бизнес-процессам ERP-системы. Разглашение, потеря или искажение данных может сказаться на отдельном процессе или в целом на системе, что несёт за собой убытки.

Можно выделить из обрабатываемой информации следующие группы данных:

1.3.1. Коммерческая тайна (КТ)

Коммерческая тайна определяется в соответствии с Федеральным законом «О коммерческой тайне» от 29.07.2004 N 98-ФЗ.

В общих случаях определяются:

1. Финансы, денежные обороты по закупкам, продажам и прочим;
2. Список контрагентов, как клиенты, так и поставщики и прочие;
3. Отчетность, как бухгалтерская, управленческая, так и налоговая;
4. Взаиморасчеты с различными контрагентами, дебиторские и кредиторские задолженности;

1.3.2. Персональные данные (ПДн)

К персональным данным относится любая информация, прямо или косвенно относящаяся к физическому лицу, и позволяющая его определить [14], в соответствии с Федеральным законом «О персональных данных» от 27.07.2006 N 152-ФЗ. В частности, в системе ведется кадровый учёт.

Кадровый учет подразумевает изначально обработку ПДн сотрудников организации. Так как система обрабатывает персональные данные её можно классифицировать как информационную систему персональных данных (ИСПДн).

1.4. Классификация уровня защищенности информационной системы, как информационной системы персональных данных

Классификация уровня защищенности ИСПДн производится в соответствии с Постановлением Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». Данное постановление устанавливает требование по защите ПДн в ИСПДн, меры по обеспечению защиты описаны в Приказе ФСТЭК России от 18.02.2013 N 21 (ред. от 14.05.2020) «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Для начала определяется тип ИСПДн, который зависит от ПДн обрабатываемых в системе. В системе обрабатываются персональные данные сотрудников организации, предоставленные самим сотрудником, что соответствует общедоступным персональным данным. Далее определяется тип актуальных угроз. Существует три типа актуальных угроз ИСПДн:

1. К угрозам первого типа относятся наличие не декларированных, т.е. не задокументированных возможностей в системном ПО (ОС, сервисные программы, антивирусы).

2. К угрозам второго типа относятся не декларированные возможности в прикладном ПО. Прикладное ПО может быть общего назначения, такие как СУБД и специального назначения, например, бухгалтерские программы.

3. К третьему типу относятся угрозы в системном и программном ПО, не связанные с вышеперечисленными угрозами.

Для ИСПДн «1С:Управление нашей фирмой» характерны актуальные угрозы третьего типа, так как прикладное решение содержит конфигурацию типовую или нетиповую и расширение конфигурации, которое поставляется разработчиками с соответствующей документацией.

На основании типа обрабатываемых ПДн и типа актуальных угроз можно ИСПДн установить 4 уровень защищенности, в соответствии с Постановлением Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Классифицировать ИСПДн можно сравнительным анализом требований по Приказу ФСТЭК России от 18.02.2013 N 21 (ред. от 14.05.2020) «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

В таблице 1.3 представлены требования для ИСПДн 4 уровня защищенности и соответствие существующим возможностям реализации мер обеспечения защищенности.

Часть мер по обеспечению безопасности ПДн необязательна для работы с самой системой, но существует возможность для расширения и обеспечения данных мер. Для полноценного обеспечения безопасности используемая система в организации должна быть настроена и внедрены основные организационные меры обеспечения безопасности.

Таблица 1.3 – Сравнение требований защищенности и возможности реализации мер обеспечения защищенности

Содержание мер по обеспечению безопасности ПДн	Соответствие требований и возможности реализации мер обеспечения защищенности
Идентификация и аутентификация пользователей, являющихся работниками оператора	+

Продолжение таблицы 1.3

Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	+
Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств	+
Аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	+
Защита обратной связи при вводе аутентификационной информации	+
Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	+
Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	+
Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	+
Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами	+
Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	+
Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	+
Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	+
Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	+
Регламентация и контроль использования в информационной системе технологий беспроводного доступа	+
Регламентация и контроль использования в информационной системе мобильных технических средств	+

Продолжение таблицы 1.3

Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)	+
Определение событий безопасности, подлежащих регистрации, и сроков их хранения	+
Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	+
Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	+
Защита информации о событиях безопасности	+
Реализация антивирусной защиты	+
Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	+
Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	+
Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации	+

На основании сравнительного анализа требуемых мер защиты информации и возможности реализации мер обеспечения защищенности информации ИСПДн можно присвоить 4 класс защищенности.

1.5. Определение наиболее актуальных угроз нарушения целостности информационной безопасности, оценка возможностей внешних и внутренних нарушителей

Важную роль в ERP-системах выполняет, хранящая в ней конфиденциальная информация. Как было определено в п.1.3 данной работы, к конфиденциальной информации относится все данные хранящиеся и обрабатываемые внутри системы, так как они влияют на отдельные бизнес-процессы в организации и на всю систему в целом. Потеря, несанкционированное изменение и прочие операции дискредитирующие или уничтожающие информацию влекут за собой убытки, вплоть до остановки

всех процессов организации с последующими простоями. Следовательно, стоит выделить основным аспектом защиты информации именно целостность. Угрозы нарушения целостности являются более уязвимы в ERP-системах.

Список угроз формируется на основании банка данных угроз безопасности информации [3]. Актуальность и выделение наиболее актуальных угроз определяется методом экспертной оценки. Для снижения субъективных факторов при оценке была создана экспертная группа. Формирование группы и проведение экспертной оценки проводилось по методическому документу «Методика оценки угроз безопасности информации» (утв. Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г.).

Экспертная группа состоит из:

- Соболевский Артём Александрович – Специалист ИБ, сертифицированный специалист по платформе «1С:Предприятия 8»;
- Самарцев Александр Олегович – Специалист ИБ, сертифицированный специалист по платформе «1С:Предприятия 8».

Перечень наиболее актуальных угроз нарушения целостности представлены в таблице 1.4.

Таблица 1.4 – Перечень наиболее актуальных угроз нарушения целостности

№	Код угрозы	Наименование угрозы
1	УБИ.006	Угроза внедрения кода или данных
2	УБИ.007	Угроза воздействия на программы с высокими привилегиями
3	УБИ.122	Угроза повышения привилегий
4	УБИ.090	Угроза несанкционированного создания учётной записи пользователя
5	УБИ.109	Угроза перебора всех настроек и параметров приложения
6	УБИ.188	Угроза подмены программного обеспечения
7	УБИ.191	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения

Продолжение таблицы 1.4

8	УБИ.210	Угроза нарушения работы информационной системы, вызванного обновлением используемого в ней программного обеспечения
---	---------	---

На основании перечня наиболее актуальных угроз нарушения целостности описываются необходимые требования к информационной безопасности к ERP-системе «1С:Управление нашей фирмой».

Также можно составить модель нарушителей информационной безопасности с потенциалом нарушения информационной безопасности. Нарушители делятся на два типа внутренние и внешние:

Внутренние нарушители:

1. Операторы ERP-системы – низкий потенциал;
2. Разработчики – высокий потенциал;
3. Системный администратор – высокий потенциал;
4. Административный персонал – средний потенциал.

Внешние нарушители:

1. Внештатные разработчики, поставщики прикладного решения – высокий потенциал;
2. Неустановленные внештатные субъекты – низкий потенциал;
3. Конкуренты – средний потенциал.

По составленным моделям нарушителей можно сделать вывод, что наибольший потенциал нарушения информационной безопасности представляют внутренние и внешние нарушители имеющие высокий уровень доступа к информационной системе или имеющие возможность удалять, добавлять и изменять конфигурации системы.

1.6. Анализ наиболее актуальных угроз нарушения целостности

На основании определенных наиболее актуальных угроз нарушения целостности для ERP-системы «1С:Управление нашей фирмой» можно провести анализ, в каких ситуациях и как угроза может быть реализована нарушителем, для дальнейшего определения мер защиты информации от наиболее актуальных угроз.

1) Угроза внедрения кода или данных

Данная угроза может быть реализована в нескольких случаях:

1. Повышенные привилегии – свободный доступ к конфигурационным данным или прикладным решениям системы;
2. Доступ к открытию внешних файлов – система поддерживает открытие внешних конфигурационных файлов. Файл может внедрить код или изменить данные.

Для снижения рисков угрозы требуется более тонкая настройка прав доступа на открытие внешних файлов и доступа к конфигурационным файлам.

2) Угроза воздействия на программы с высокими привилегиями

В конфигурациях системы могут возникать ошибки или конфликты между конфигурациями, которые могут дать возможность пользователю воздействовать на систему выше своих привилегий.

Угроза характерна в случаях, когда в системе используются нестабильные конфигурации, в которых возникают ошибки.

Возможные меры для обеспечения защиты – это использование проверенных и протестированных конфигураций и версий конфигураций в системе.

3) Угроза повышения привилегий

В системе используется ролевая модель управления доступом. Роли состоят из различных прав доступа к объектам системы. Выданные роли пользователям могут содержать права доступа более высокого уровня.

В таких случаях требуется тестировать все роли пользователей и ограничивать в правах доступа к данным конкретно к каждому пользователю.

Система поддерживает возможность ограничения доступа к данным по различным условиям, что позволяет снизить риск угрозы.

4) Угроза несанкционированного создания учётной записи пользователя

Пользователи с повышенными привилегиями имеют возможность создавать пользователей для работы в системе с разными целями, это может быть тестирование ролей доступа или новое рабочее место.

Вход в систему должен быть под контролем и соответствовать требованиям аутентификации. И для ролей определены возможности создания пользователей, кому это требуется.

5) Угроза перебора всех настроек и параметров приложения

Любые роли в системе могут содержать изъяны, намеренно или нет пользователь может получить доступ к защищаемой информации или нарушить целостность данных конфигураций.

Требуется углубленное тестирование на уровне ролей пользователей и ограничение на уровне прав доступа к настройкам и параметрам.

6) Угроза подмены программного обеспечения

Угроза подмены программного обеспечения в системе может иметь серьезные последствия для безопасности и стабильности работы. Подмена ПО означает замену официального программного кода в конфигурациях на измененный или вредоносный вариант, который может содержать вредоносные функции или уязвимости, предназначенные для получения несанкционированного доступа или нанесения вреда системе.

Конфигурации системы делятся на 3 типа: основная конфигурация, расширения конфигурации и дополнительные обработки и отчеты. Конфигурации обновляются и дорабатываются, пользователи с повышенными привилегиями имеют доступ к конфигурациям. Санкционировано или не санкционировано конфигурации могут быть подменены и содержать вредоносный код или в следствии дискредитировать хранимую в системе информацию.

Ведение контроля над конфигурациями системы способствует снижению риска угрозы.

7) Угроза внедрения вредоносного кода в дистрибутив программного обеспечения

Как и в угрозе подмены программного обеспечения вредоносный код может быть поставлен в дистрибутив программного обеспечения, затем установлен в саму систему. Контроль над конфигурациями системы так же является хорошей мерой для защиты.

8) Угроза нарушения работы информационной системы, вызванного обновлением используемого в ней программного обеспечения

Может возникнуть при внесении изменений в существующий программный код конфигураций или при неправильном обновлении системы. Это может привести к нарушению функциональности, стабильности и безопасности системы.

Возможные проблемы при обновлении системы:

- Несовместимость обновлений. При обновлении могут возникнуть проблемы совместимости между новой версией и текущей конфигурацией информационной системы. Это может привести к конфликтам, ошибкам и нарушению работы системы;
- Ошибки при обновлении. Неправильное выполнение процедуры обновления может привести к ошибкам, которые могут повредить файлы, базу данных или другие компоненты информационной системы. Это может привести к потере данных, сбою работы системы или невозможности доступа к системе;
- Непредвиденное поведение. Обновление может привести к изменениям в работе системы, которые не были ожидаемыми или задуманными. Это может привести к неожиданному поведению, ошибкам и нарушению функциональности системы.

Как меру защиты можно использовать резервное копирование для восстановления после неудачного обновления, так же контролировать изменения и ошибки после обновлений в конфигурациях.

По анализу наиболее актуальных угроз можно сделать вывод что угрозы возможны в следствии неправильного или неполного тестирования и разработки ролевой политики и прав доступа в системе, а также изменения в конфигурациях систем могут содержать вредоносный код, вызывать ошибки, в следствии дискредитировать данные хранимые в системе.

Для возможности сохранения данных хранимых в системе и возврата в стабильное состояние требуется производить резервное копирование системы.

1.7. Предложения по применению организационных и технических мер по защите информации от угроз нарушения целостности

Проанализированы наиболее актуальные угрозы для ERP-системы «1С:Управление нашей фирмой», были выявлены проблемные места. Можно выделить два проблемных места системы:

- Ролевая политика безопасности;
- Контроль целостности конфигураций.

1.7.1. Ролевая политика безопасности

При использовании ролевой системы прав доступа в информационных системах необходимо применять организационные и технические меры для защиты информации от угроз нарушения целостности. Целостность информации в данном контексте означает, что данные должны оставаться неповрежденными, неизменными и достоверными.

Организационные меры:

- Разделение обязанностей. Необходимо придерживаться принципа разделения обязанностей, чтобы пользователи имели доступ только к тем информационным ресурсам и функционалу системы, которые необходимы для выполнения их рабочих обязанностей. Правильная настройка ролей ограничит возможность несанкционированного изменения данных;
- Управление доступом. Реализация строгой политики управления доступом, включая процедуры назначения, изменения и удаления прав доступа. Доступ к информационным ресурсам и функционалу системы

осуществляется только по необходимости и на основе принципа «принцип наименьших привилегий»;

- Обучение персонала. Проведение регулярного обучения сотрудников относительно политик безопасности, включая принципы ролевой системы прав доступа и значимость поддержания целостности информации. Это поможет повысить осведомленность и ответственность персонала.

Технические меры:

- Аутентификация и авторизация. Использование надежных методов аутентификации. ERP-система «1С:Управление нашей фирмой» поддерживает различные возможности аутентификации, такие как пароль, аутентификация операционной системы или аутентификация с помощью OpenID или OpenID Connect, для подтверждения легитимности пользователей. Кроме того, система должна правильно авторизировать пользователей и предоставлять доступ только к соответствующим информационным ресурсам и функционалу системы на основе их роли.

- Контроль доступа и аудит. Применение механизмов контроля доступа может включать установку ограничений на запись или модификацию конкретных полей или объектов для ограничения возможности несанкционированного изменения данных. В платформе «1С:Предприятие 8» реализован механизм RLS (ограничение прав на уровне записей), который позволяет включать установку ограничений и модификацию конкретных полей. Кроме того, должно быть ведение аудита доступа, чтобы регистрировать действия пользователей и обнаруживать любые попытки несанкционированного доступа или изменения данных.

- Резервное копирование и восстановление. Регулярное создание резервных копий данных и информационной системы производится, чтобы в случае нарушения целостности можно было восстановить данные до предшествующего стабильного состояния.

Важно применять как организационные, так и технические меры для обеспечения защиты информации от угроз нарушения целостности в системах с ролевой системой прав доступа. Это позволит минимизировать риски и обеспечить надежность и безопасность данных.

1.7.2. Контроль целостности конфигураций

Платформа «1С:Предприятие 8» не имеет должного функционала для контроля целостности конфигураций в системе, соответственно и в самой ERP-системе.

В подобных системах постоянно происходят регулярные обновления, в следствии изменяется конфигурация. Конфигурации могут полностью отличаться от предыдущего своего состояния и повлиять на целостность данных ERP-системы. В такой основной конфигурации относится так же «1С:Управление нашей фирмой».

В ERP-системе есть возможность добавлять, изменять, обновлять и удалять такие конфигурации как «расширения конфигурации» и «дополнительные отчёты и обработки», которые так же могут напрямую влиять на целостность данных.

Все перечисленные конфигурации зачастую в организациях требуется дорабатывать под определенные бизнес-процессы. Доработкой могут заниматься различные организации, так же и внутренними средствами. В этом процессе конфигурации изменяются, в следствии и данные. Плохое тестирование, халатность разработчиков, аналитиков и прочих, может повлечь за собой нарушение целостности данных ERP-системы. По статистике только сама фирма «1С» выпускает 18 обновлений в день основной конфигурации, и исправлений своих ошибок, в виде расширений конфигурации [10].

Для уменьшения риска угроз и повышения безопасности ERP-системы «1С:Управление нашей фирмой» предлагается реализовать методику оценивания защищенности ERP-системы от угроз нарушения целостности. Она должна включать в себя модель контроль целостности, спроектированная

под специфику данной ERP-системы. Методика необходима для стандартизации процессов при возникновении нарушения целостности, методов обнаружения, фиксации изменений и способов устранения этого нарушения, а также восстановления целостности ERP-системы.

Выводы по первой главе

Проведен анализ ERP-системы «1С:Управление нашей фирмой», как объекта защиты информационной безопасности:

- Проанализированы функциональные и структурные возможности ERP-системы «1С:Управление нашей фирмой», выделены информационные ресурсы для защиты;
- Определен и присвоен уровень защищенности по Постановлению Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», в соответствии реализованными и требуемыми мерами защиты информации;
- Путем экспертной оценки определены наиболее актуальные угрозы нарушения целостности ERP-системы «1С:Управление нашей фирмой». Определена модель внутреннего и внешнего нарушителя информационной безопасности;
- Проанализированы наиболее актуальные угрозы нарушения целостности, выделены основные риски угроз и возможные меры защиты;
- На основании анализа наиболее актуальных угроз составлены предложения по устранению слабых мест ERP-системы «1С:Управление нашей фирмой».

По результатам проведенного анализа ERP-системы «1С:Управление нашей фирмой» сделан вывод, что система имеет слабое место в контроле целостности конфигураций. В следствии чего предлагается к разработке методика оценивания защищенности от угроз нарушения целостности конфигураций. Для данной методики потребуется разработка и реализация необходимого модуля ERP-системы для контроля целостности конфигураций.

2. АНАЛИЗ МЕТОДОВ И ПРОЕКТИРОВАНИЕ МОДЕЛИ КОНТРОЛЯ ЦЕЛОСТНОСТИ КОНФИГУРАЦИЙ ERP-СИСТЕМЫ

В данной главе дипломного проекта рассматривается анализ методов и проектирование модели контроля целостности конфигураций для ERP-системы «1С:Управление нашей фирмой». Контроль целостности является важным аспектом в области информационных систем, особенно для организаций, использующих ERP-системы.

Модель контроля целостности конфигураций представляет собой описание или абстракцию, которая определяет правила, стандарты и механизмы для обеспечения целостности конфигураций в ERP-системе. В свою очередь метод контроля целостности конфигураций определяет конкретную реализацию или алгоритм, который применяется для проверки целостности конфигураций в рамках модели.

В начале главы проводится анализ и выбор метода контроля целостности для дальнейшего использования в модели контроля целостности конфигураций.

Затем разрабатываются требования к модели контроля целостности конфигураций, учитывая особенности ERP-системы «1С:Управление нашей фирмой». Анализируются специфические требования, которые должны быть учтены при выборе модели контроля целостности конфигураций.

За основу проектирования модели предлагается взять модель контроля целостности Кларка-Вилсона. После делается проектирование модели контроля целостности конфигураций, адаптируя модель Кларка-Вилсона. Производится анализ полученных данных и делаются соответствующие выводы.

Цель данной главы состоит в проектировании оптимальной модели контроля целостности конфигураций, учитывая установленные требования и специфику ERP-системы «1С:Управление нашей фирмой». Это обеспечивает значимую роль в реализации методики оценки защищенности от угроз нарушения целостности системы.

2.1. Анализ методов контроля целостности конфигурации

В системах на платформе «1С:Предприятие 8» конфигурация относится к набору настроек, параметров и данных, определяющих функциональность и поведение конкретного программного продукта. Конфигурация определяет структуру базы данных, логику и связи, отчеты, формы, правила доступа и другие аспекты системы. Конфигурацию можно представить, как файл или структуру файлов. Следовательно, для конфигураций можно определить методы контроля целостности для файлов и данных.

Данные методы позволяют проверять что содержимое конфигураций было изменено или повреждено в результате ошибок или злонамеренных действий.

1) Полная копия

Суть данного метода заключается в том, что создаются полные копии конфигураций, затем сверяют копию конфигурации и хранимую копию конфигурации в системе – схематично она изображена на Рисунке 2.1.

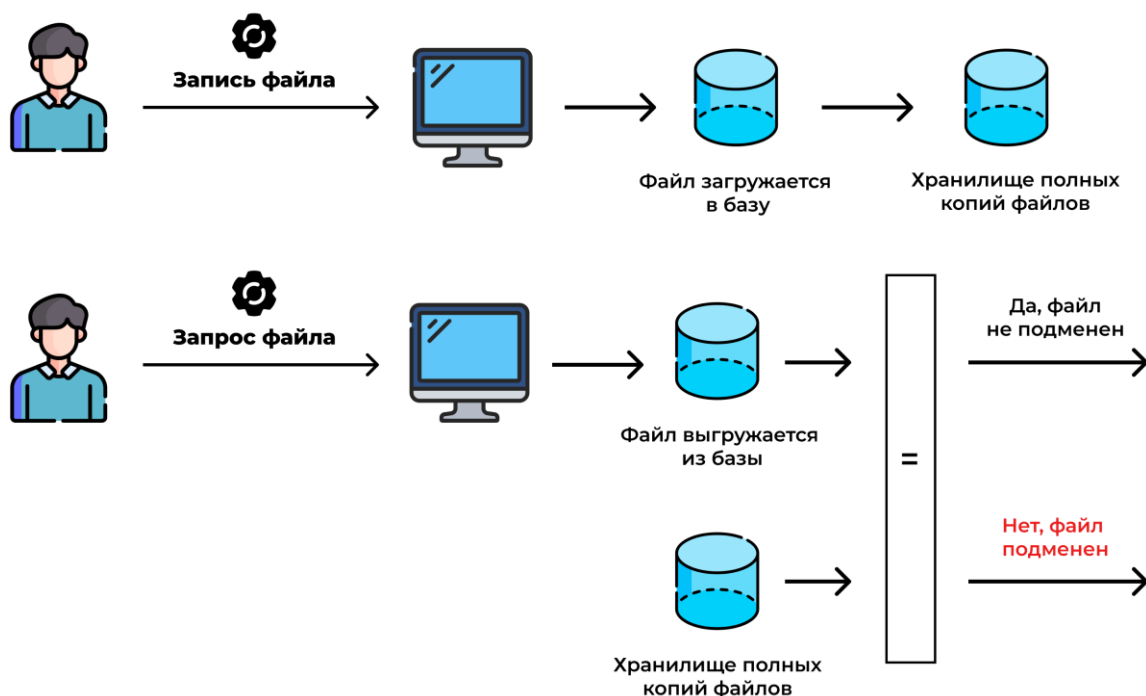


Рисунок 2.1 – Метод контроля целостности с помощью полного копирования.

Можно выделить некоторые преимущества данного метода, например, простота реализации метода и полный контроль данных, вплоть до бита. Но также есть существенные недостатки, такие как большой объем конфигураций, копии конфигураций можно подменить [9]. Если копия является объектом защиты, то копия является уязвимой.

2) Контрольная сумма

Контрольная сумма – это значение, рассчитанное по входным данным с помощью определенного алгоритма. Схематично этот метод описан на рисунке 2.2.

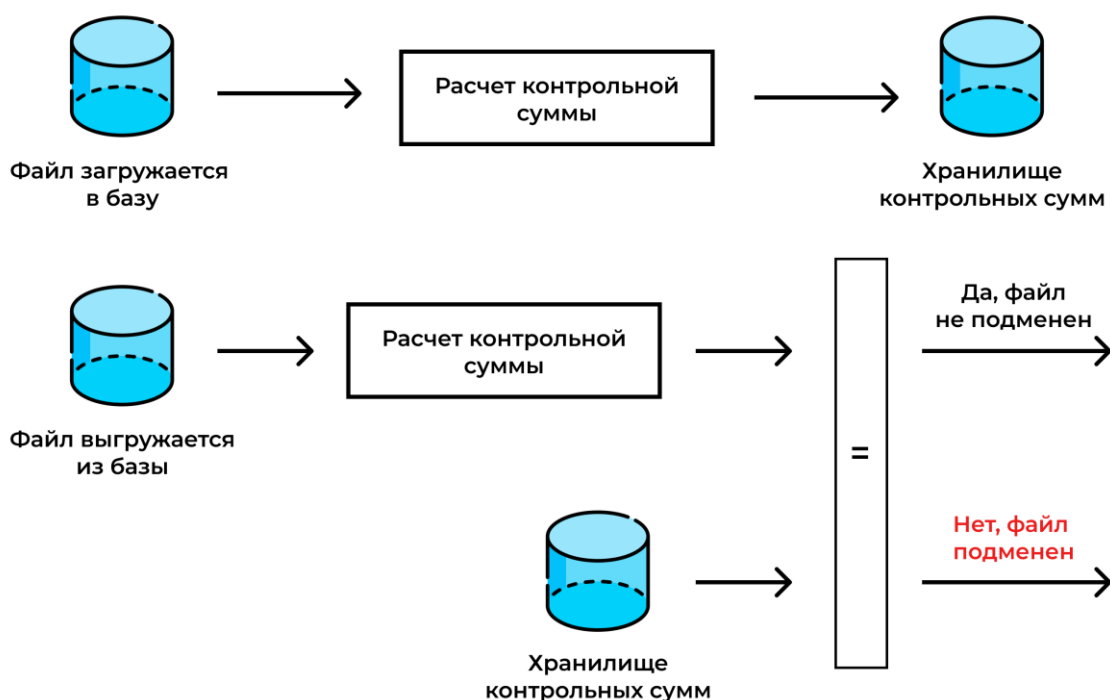


Рисунок 2.2 – Метод контроля целостности с помощью контрольной суммы

Например, алгоритм «Циклический избыточный код» или CRC предназначен для нахождения контрольной суммы определенных данных.

Преимущество данного метода заключается в его малых объемах хранения, быстротой вычислений и стандартизированного размера.

В свою очередь недостатками этого метода являются возможность подмены путём подбора контрольной суммы. В случае с переставленными

байтами в данных контрольная сумма останется прежней, хотя данные могут содержать совершенно конфигурацию.

3) Хеш-функция

Хеш-функции представляют собой криптографические алгоритмы, с помощью которых вычисляют уникальную контрольную сумму или же хеш-сумму конфигурации [9].

Основным отличием от предыдущего метода заключается в том, что хеш-сумма вычисляется исходя из содержимого данных, исходя из этого его основным преимуществом является сложность подбора исходных данных к значению хеш-суммы за приемлемое время – это отражено на рисунке 2.3. Так же остальные преимущества предыдущего метода сохраняются, но и из-за более сложных вычислений скорость снижается.

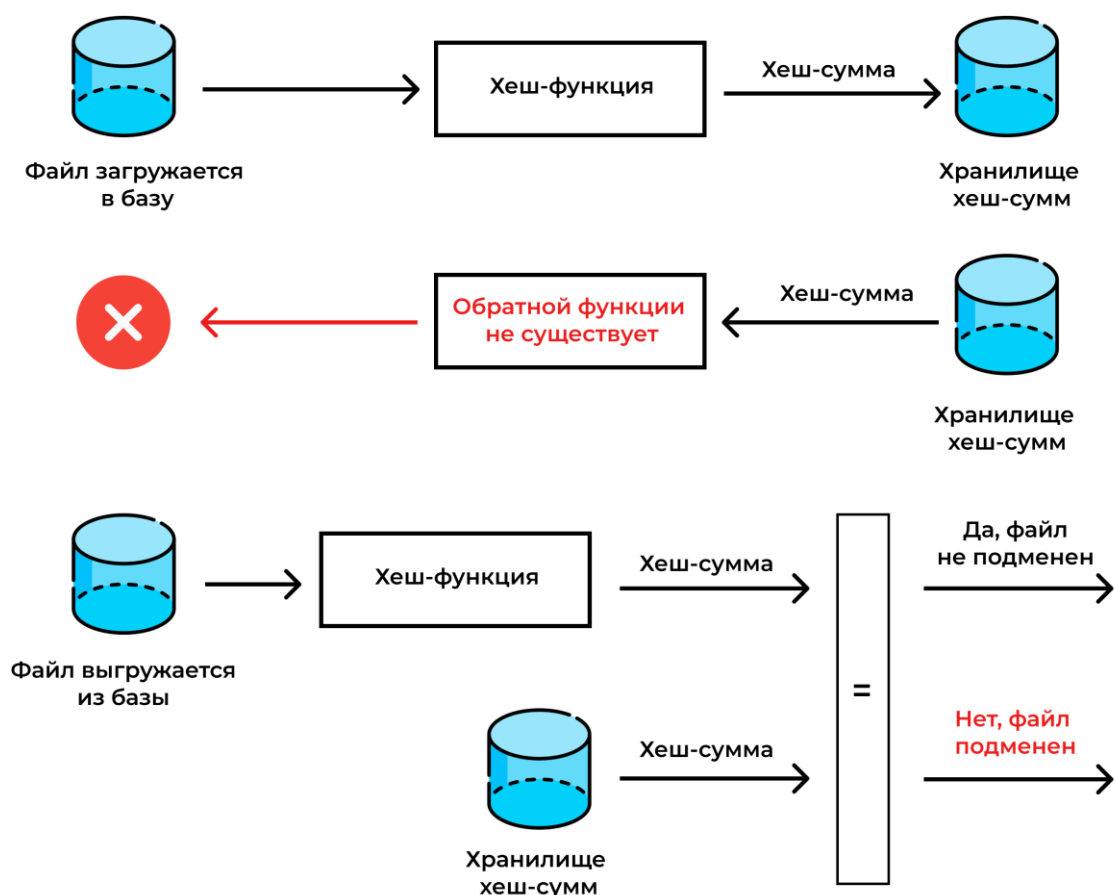


Рисунок 2.3 – Метод контроля целостности с помощью хеш-функций

Например, хеш-функции MD5, SHA1, SHA256, SHA512 имеют различный размер хеш-суммы, в следствии чего скорость вычисления тоже разная.

4) Электронная цифровая подпись

Электронная цифровая подпись представляет собой криптографический механизм, который позволяет проверить подлинность и целостность конфигурации.

Принцип работы метода состоит из следующих шагов:

- Система использует свой закрытый ключ для создания цифровой подписи, которая является уникальным математическим представлением содержимого конфигурации. Цифровая подпись гарантирует, что содержимое не было изменено после создания подписи.

- Пользователь использует публичный ключ отправителя для проверки цифровой подписи и проверки целостности конфигурации. При этом проверяется, соответствует ли цифровая подпись исходным данным. Если цифровая подпись действительна, это указывает на целостность и подлинность конфигурации.

Данные этапы проиллюстрированы на рисунке 2.4.

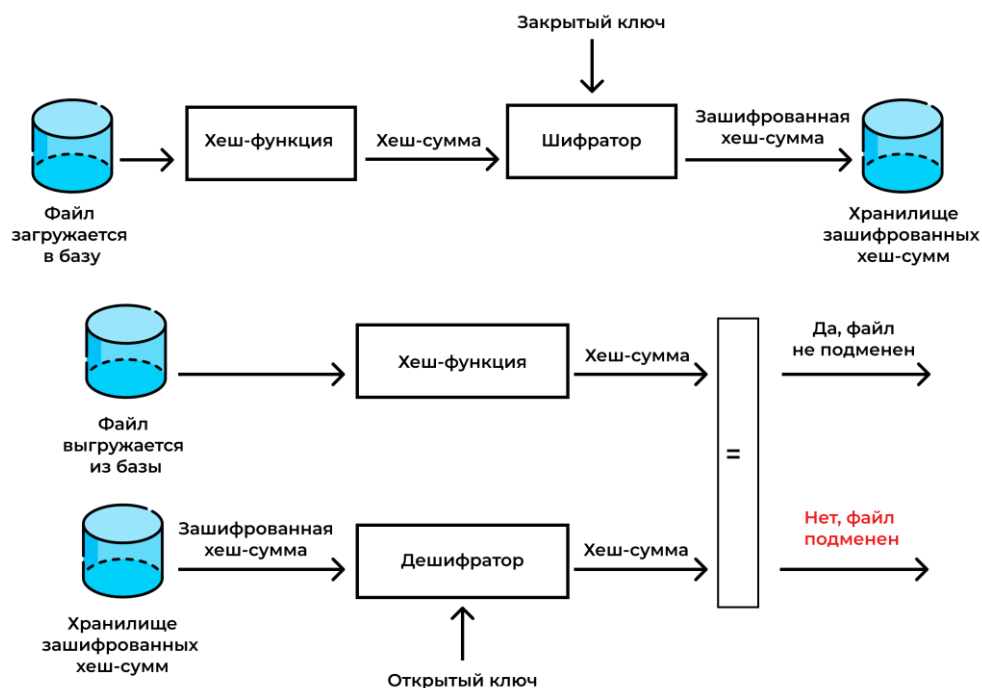


Рисунок 2.4 – Метод контроля целостности с помощью ЭЦП

Любое изменение данных, даже незначительное, приводит к изменению цифровой подписи. Таким образом, метод контроля целостности с помощью ЭЦП представляет собой усовершенствованный вариант метода контроля целостности с помощью хеш-функции.

К недостаткам этого метода относится ещё более низкая скорость вычисления и необходимость дополнительных модулей для работы с электронной цифровой подписью в ERP-системе.

После проведения анализа основных методов контроля целостности можно сделать вывод, что для контроля целостности конфигураций ERP-системы «1С:Управление нашей фирмой» наиболее подходит метод Хеш-функций. Размер конфигураций представляет довольно значимый объём памяти и метод полных копий не оптимален. Метод, использующий ЭЦП требует дополнительной реализации или использования модулей ERP-системы работы с электронными подписями, что несёт за собой дополнительные угрозы и возможные уязвимости. В свою очередь метод

контрольных сумм не раскрывает основного преимущества хеш-функций вычисления на уровне содержания конфигураций.

2.2. Разработка требований к модели контроля целостности конфигураций

Первым и основным требованием к модели контроля целостности конфигураций является возможность определения эталонной конфигурации с которой будет сравниваться измененная конфигурация. Должно учитываться, что конфигураций может быть неопределенное множество и трёх типов, поддерживаемых ERP-системой «1С:Управление нашей фирмой».

К специфике изменения этих конфигураций можно отнести регулярное обновление и изменение конфигураций, как со стороны поставщика ERP-системы «1С:Управление нашей фирмой», так и от сторонних поставщиков прикладных решений для этой системы. Конфигурации могут быть добавлены или удалены. Внутри организаций, где используется эта ERP-система могут быть и внутренние разработчики, которые так же влияют на состояния конфигураций. Должна быть возможность считывания текущего состояния конфигураций и присвоения статуса эталонной.

Состояние эталонных конфигураций имеет возможность изменения, добавления или удаления. В таком случае требуется ведение журнала изменений конфигураций, в какой момент времени был присвоен новое эталонное состояние конфигурации. Так же сравнение состояний конфигураций в разные периоды времени.

Изменение состояний конфигураций может происходить без участия пользователей, в момент изменения должно быть записано новое состояние конфигурации и присвоен новый статус эталонного [7]. Записанное состояние конфигураций в системе должно быть неизменяемым.

Для работы с журналом изменений конфигурации и сравнением состояний конфигураций должно быть разделение пользователей и их прав доступа.

Также система изначально поддерживает аутентификацию пользователей, соответственно пользователь, взаимодействующий с данным журналом и контролем целостности конфигураций, должен проходить аутентификацию, как минимум с паролем обычной сложности.

По итогам разработки требований, можно выделить следующий список требований к модели контроля целостности конфигураций:

- Возможность определения эталона конфигурации;
- Поддержка нескольких типов конфигураций, из-за специфики ERP-системы «1С:Управление нашей фирмой»;
- Считывание текущих конфигураций;
- Возможность сравнения текущих конфигураций с их эталонными состояниями;
- Неизменяемость состояний конфигураций после записи в систему;
- Журнал изменений состояний конфигурации с моментом времени изменений;
- Отдельная роль в системе для работы с системой контроля целостности конфигураций;
- Аутентификация пользователя с паролем обычной сложности;
- Универсальность модели для ERP-систем «1С:Управление нашей фирмой», вне зависимости от использования других конфигураций.

2.3. Исследование модели контроля целостности Кларка-Вилсона

Для проектирования модели контроля целостности конфигураций ERP-системы «1С:Управление нашей фирмой» предлагается использовать за основу модель контроля целостности Кларка-Вилсона. Затем адаптировать данную модель под требования, определенные выше для данной системы.

Модель Кларка-Вилсона, разработанная Ричардом Кларком и Дэвидом Уилсоном в 1987 году, является одной из основных моделей обеспечения целостности данных в области информационной безопасности. Она представляет собой систематический подход к обеспечению целостности

данных в коммерческой среде. Основная концепция модели заключается в контроле доступа к данным и применении определенных преобразований данных, которые обеспечивают их соответствие заранее установленным правилам.

Для лучшего понимания модели Кларка-Вилсона, можно ввести следующие обозначения:

D – конечное множество данных;

CDI – ограниченные элементы данных;

UDI – неограниченные элементы данных.

Причем: $D = CDI \cup UDI$, $CDI \cap UDI = \emptyset$ [4, с. 88].

Субъекты в модели представляют собой компоненты, которые инициируют процедуры преобразования (ПП). Процедуры преобразования состоят из последовательности элементарных действий, где каждое элементарное действие представляет собой переход состояния, вызывающий изменения определенных элементов данных. ПП может быть представлено в виде функции, которая связывает субъект, элемент данных и новый элемент данных следующим образом: ПП: $xD \rightarrow D$.

ПП – это действия, которые субъекты выполняют над данными и которые могут изменять определенные данные.

«У данной модели существует список правил, определяющих модель Кларка-Вилсона:

- В системе должны иметься процедуры утверждения целостности (IVP) – утверждают, что данный CDI имеет надлежащий уровень целостности, утверждающие любой CDI . Например, в качестве процедуры утверждения целостности может выступать сравнение контрольной суммы данных.
- Применение любого ПП к любому CDI должно сохранять целостность CDI .
- Только ПП может внести изменения в CDI .

- Субъекты могут инициировать только определенные ПП над определенными CDI.

- Соответствующая политика в отношении разделения обязанностей субъектов. То есть система определяет такую политику, чтобы не позволить субъектам изменять CDI без соответствующего вовлечения других субъектов.

- Некоторые ПП могут преобразовать UDI в CDI.

- Каждое применение CDI должно регистрироваться в специальном CDI, в который может производиться только добавление информации, достаточной для восстановления картины о процессе работы этого CDI. То есть применение специального регистрационного журнала.

- Система должна распознавать субъекты, пытающаяся инициализировать ПП. Это правило определяет механизмы предотвращения атак, при которых один субъект пытается выдать себя за другого.

- Система должна разрешать производить изменения в списках авторизации только специальным субъектам.

Данные правила определяют, как может быть проверена целостность, как и кем могут изменяться CDI, и как UDI могут быть превращены в CDI. Здесь происходит отслеживание всех изменений и тех, кто пытается внести эти изменения» [4, с. 88].

Преимущество для исследования данной модели заключается в том, что модель разрабатывалась на основе опыта коммерческих организаций, данная модель формируют существующие практики по контролю целостности, и её следует применить за основу в проектировании модели контроля целостности конфигураций ERP-системы «1С:Управление нашей фирмой».

2.4. Проектирование модели контроля целостности конфигураций для ERP-системы «1С:Управление нашей фирмой»

В исследовании модели контроля целостности Кларка-Вилсона были определены основные правила, в ходе проектирования предлагается адаптировать эту модель под специфику ERP-системы «1С:Управление нашей фирмой», добавив некоторые правила, исходя из требований, определенных под модель контроля целостности конфигураций.

Требуется определить использованные обозначения из модели Кларка-Вилсона:

1. D – конечно множество данных хранимое в ERP-системе;
2. CDI – множество данных, включающие основную конфигурацию расширения конфигурации и дополнительные обработки и отчеты, хранимые в базе данных ERP-системы, являющиеся эталонными;
3. UDI – множество данных, включающие основную конфигурацию, расширения конфигурации и дополнительные обработки и отчеты, которые путём определенных процедур преобразования перейти в состояние CDI.

Процедуры преобразования (ПП) – процедуры, изменяющие состояние и данные основной конфигурации, расширений конфигурации или дополнительных обработок и отчётов из состояния UDI в состояние CDI. В последствии ПП состояние и данные хранимые в ERP-системе будут изменены. В системах на платформе «1С:Предприятие 8» ПП является добавлением, изменением или удалением CDI, например, изменением, преобразуя UDI в CDI. ПП могут выполнять субъекты, имеющие должные привилегии и права доступа.

Необходимо определить правила для модели контроля целостности конфигураций, исходя из модели Кларка-Вилсона, требований и специфики ERP-системы «1С:Управление нашей фирмой»:

– В системе должны быть процедуры утверждения целостности конфигураций, утверждающая, что конфигурации, хранимые в базе данных ERP-системы, соответствует целостности эталона. В качестве метода вычисления целостности требуется использовать хеш-функцию.

- Применение любого ПП к любому CDI должно сохранять целостность CDI.
- Только ПП может изменить состояние CDI.
- Субъекты могут инициировать только определенные ПП над определенными CDI.
- В системе должна быть определена политика определения субъектов, которые имеют возможность использования ПП. Для систем на платформе «1С:Предприятие 8» субъектам должны быть присвоены соответствующие роли в ролевой политике безопасности.
- Некоторые ПП могут преобразовать UDI в CDI.
- Состояние CDI должно регистрироваться в определенном регистре. Любому субъекту системы ограничен доступ к изменению и удалению записей в регистре состояний CDI.
- Система должна распознавать субъекты, пытающаяся инициализировать ПП. В системе на платформе «1С:Предприятие 8» регистрировать запись в Журнал регистрации любую инициализацию ПП.
- Использование модели должно быть универсальной при работе на платформе «1С:Предприятие 8».
- Инициализация записей в регистр состояний CDI может производиться автоматизировано системой, используя механизм регламентных процедур.
- Любой субъект, имеющий право доступа на чтение регистра состояний CDI должен проходить аутентификацию.
- Регистр состояний CDI должен хранить информацию о дате состояния CDI и типе CDI.

Выводы по второй главе

Во второй главе дипломного проекта были рассмотрены различные методы контроля целостности и выполнен анализ этих методов. Выбран наиболее оптимальный для метода контроля целостности конфигураций метод хеш-функций.

В рамках анализа методов контроля целостности были рассмотрены следующие методы:

- Полная копия;
- Контрольная сумма;
- Хеш-функция;
- Электронная цифровая подпись (ЭЦП).

Было проведено исследование модели целостности Кларка-Вилсона для использования за основу в проектировании модели контроля целостности конфигураций ERP-системы «1С:Управление нашей фирмой».

Для проектируемой модели контроля целостности конфигураций определены основные требования, учитывая специфику ERP-системы.

При проектировании модели контроля целостности конфигураций были определены основные правила формирования модели, определены необходимые определения. Модель включает в себя сбор и хранение состояний конфигураций, определен метод контроля целостности, процедуры записи и сбора состояний конфигурации, требования к субъектам системы и интерфейс в виде регистра или журнала состояний конфигураций для взаимодействия с моделью.

Основным преимуществом разработанной модели является использование за основу общепринятой модели контроля целостности Кларка-Вилсона и адаптировано под систему на платформе «1С:Предприятие 8», чем обеспечивает использование данной модели высокую эффективность и надежность.

Использование данной модели может быть в рамках других решений на платформе «1С:Предприятие 8» помимо решения «1С:Управление нашей

фирмой», так как включает в себя общие правила, практики и определяет метод контроля целостности.

Результаты данной главы могут быть использованы для дальнейшей разработки методики оценивания защищенности от угроз нарушения целостности конфигураций, что включает в себя использование за техническую основу данный метод контроля целостности конфигураций.

3. РАЗРАБОТКА МЕТОДИКИ ОЦЕНИВАНИЯ ЗАЩИЩЕННОСТИ ERP-СИСТЕМЫ ОТ УГРОЗ НАРУШЕНИЯ ЦЕЛОСТНОСТИ КОНФИГУРАЦИЙ

Решаемыми задачами, разрабатываемой методики оценивания защищенности ERP-системы «1С:Управление нашей фирмой» от угроз нарушения целостности конфигураций является:

- Стандартизация контроля целостности конфигураций систем на базе платформы «1С:Предприятие 8»;
- Контроль целостности всех типов прикладных решений, возможных для реализации на платформе;
- Своевременное реагирование на несогласованные изменения в прикладных решениях;
- Ведение журнала изменений прикладных решений по датам;
- Регламентация действий оператора системы контроля целостности конфигураций;
- Унифицированное рабочее место оператора системы контроля целостности конфигураций.

Процесс оценивания защищенности заключается в контроле целостности конфигураций с помощью соответствующей системы, основанной на модели спроектированной во второй главе данного дипломного проекта.

Разработку методики предлагается разделить на два этапа, эти этапы будут так же соответствовать этапам использования этой методики:

- Внедрение системы контроля целостности конфигураций, на основе спроектированной модели;
- Эксплуатация системы и процедуры реагирования на нарушение целостности.

Так же во втором этапе будут описаны возможные действия реагирования на нарушение целостности.

3.1. Внедрение системы контроля целостности конфигураций

Процесс внедрения системы должен начинаться со сбора входных данных для последующей настройки системы.

Так как система основана на модели спроектированной во второй главе, то входными данными является:

- Определение типов конфигураций, используемых в системе. Это может быть только основная конфигурация (используется всегда), так же дополнительно расширения конфигурации и(или) дополнительные обработки и отчёты;
- Частота мониторинга состояний конфигурации или же частота обновления эталона конфигураций. Данный показатель влияет на производительность системы, чем чаще происходит сбор данных о состоянии конфигураций, тем больше потребуется вычислительных ресурсов системы;
- В модели используется метод контроля целостности хеш-функций, требуется определить оптимальный алгоритм, в зависимости от производительности;
- Определение пользователей, назначенных на роль оператора контроля целостности конфигураций.

Как определено было выше, система должна соответствовать модели спроектированной во второй главе, в случае если данная система отсутствует, её требуется разработать.

Система, интегрированная в ERP-систему на платформе «1С:Предприятие 8» является впоследствии является модулем ERP-системы. Так как модуль ERP-системы является прикладным решением или же конфигурацией, он может быть реализован как в основной конфигурации, так и в качестве расширения конфигурации, или дополнительной обработкой, или отчётом, должен так же фиксироваться, согласно модели, в определенном регистре состояний конфигурации.

На основе входных данных производится настройка модуля контроля целостности конфигураций. В данной настройке учитывается включение регламентных процедур сбора состояний конфигураций по определенному расписанию или частоте. Так же определенным пользователям выданы необходимые права доступа ролевой политики безопасности системы. В случае отсутствия усилены методы аутентификации этих пользователей.

Один из основных этапов внедрения является настройка резервного копирования системы, так как является основным решением при нарушении целостности системы.

Пользователи, назначенные как операторы модуля контроля целостности, должны обладать необходимыми навыками и квалификации в работе с системами на платформе «1С:Предприятие 8» и принципами информационной безопасности.

3.2. Эксплуатация системы контроля целостности конфигураций

На этом этапе методики разбирается процесс эксплуатации системы контроля целостности конфигураций, под эти подразумевается описание технической реализации системы вывод информации требуемой для оператора системы, а также процесс его действий. Процессы, используемые в данном, соответствуют циклу Деминга, это означает что процесс происходит зациклено.

С точки зрения технической реализации системы существует журнал изменений состояний конфигурации, с которым взаимодействует оператор. Реестр состояний конфигураций хранит в себе все состояния конфигураций, в случае, если состояние не соответствует предыдущему, тогда это означает, что конфигурация была изменена, а запись попадает в журнал изменений с описанием даты изменения и описанием самой конфигурации, которая была изменена. Состояния конфигурации записываются в реестр по регламентным процедурам, определенным на этапе внедрения. Так же у оператора должна быть возможность вручную получить сбор данных о состояниях

конфигураций. Следовательно, данный процесс системы можно представить в виде фрагмента алгоритма системы, представленного на рисунке 3.1.

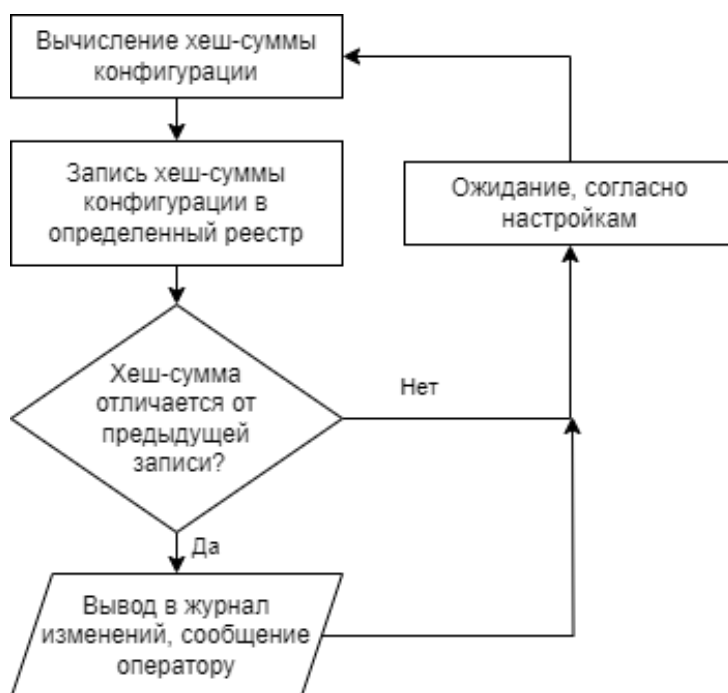


Рисунок 3.1 – Процесс системы контроля целостности

Далее можно определить процесс работы оператора системы контроля целостности. В момент мониторинга или получения сообщения в журнале изменений о том, что, какая-то конфигурация была изменена, оператор следует алгоритму действий для оценки угрозы безопасности нарушения целостности и предпринимает необходимые действия. На этом моменте происходит оценка, является ли данное изменение легитимным и согласованным.

В случае, если изменение было произведено не согласовано следует сообщить об этом ответственному лицу принимающему решение о предстоящих мерах.

Меры по устранению нарушения целостности могут начаться с обследования, для уточнения является ли действительно данное изменение не согласованным.

Если изменение было не согласованным необходимо провести мероприятия по устранению утечки и определить уязвимость системы. Только

после полного устранения утечки возможно предпринять меры для восстановления системы.

Восстановление системы можно представлять, как исследование что было изменено и исправление, или же самым эффективным способом является восстановление из резервной копии системы. В таком случае целостность данных, в том числе конфигураций системы сохранится и вернется в защищенное состояние до изменений.

Алгоритм действий оператора можно так же представить в виде фрагмента алгоритма на рисунке 3.2.



Рисунок 3.2 – Алгоритм работы оператора системы
контроля целостности

Как определено, наиболее эффективным восстановлением системы является загрузка из резервной копии, на этапе внедрения настраивается изначальная частота формирования резервных копий. Так же во время работы с системой контроля целостности можно выявить необходимую частоту резервного копирования. И частота считывания сбора данных о состоянии конфигураций может быть тоже изменена.

Процесс работы с методикой описанный в этом этапе происходит непрерывно, до момента пока не произойдёт вывод из эксплуатации системы контроля целостности конфигураций. Методика не завязана с другими данными системы, поэтому остановка не несёт за собой нужды в особых процессах вывода из эксплуатации.

Выводы по третьей главе

В данной главе была разработана методика оценивания защищенности ERP-системы «1С:Управление нашей фирмой» от угроз нарушения целостности конфигураций. Методика состоит из двух этапов.

В первом этапе методики описывается подход и процесс внедрения системы контроля целостности конфигураций в ERP-систему. Для работы по данной методике в ERP-системе должна быть интегрирована система контроля целостности конфигураций, соответствующая модели описанная во второй главе. В процессе внедрения происходит так же первоначальная настройка необходимая для дальнейшей работы.

Второй этап методики представляет собой описание алгоритма работы системы контроля целостности, каким образом в журнал изменений конфигураций попадает запись об изменении, и описание работы оператора системы контроля целостности, кто оценивает защищенность. Описан алгоритм действий в случае, когда была нарушена целостность ERP-системы, какие следует предпринять шаги и действия.

Для определения степени выполнения задач, поставленных в дипломном проекте, требуется провести тестирование данной методики. На основе анализа результатов тестирования можно сделать вывод о том, что задачи по данному дипломному проекту выполнены.

4. ТЕСТИРОВАНИЕ РАЗРАБОТАННОЙ МЕТОДИКИ ОЦЕНИВАНИЯ ЗАЩИЩЕННОСТИ ERP-СИСТЕМЫ

В данной главе дипломного проекта будет протестирована разработанная методика оценивания защищенности. В качестве стенда для данной методики будет использована копия ERP-системы «1С:Управление нашей фирмой» демонстративная база, предоставляемой фирмой «1С».

Версия платформы, используемая на стенде соответствует версии 8.3.21.1709. Версия конфигурации 3.0.3.169 «1С:Управление нашей фирмой».

Данная ERP-система зачастую в организациях находится в постоянной доработке, как со стороны, так и внутри организации, так же происходят своевременные обновления конфигураций. Это означает, что в данной системе может использоваться все типы конфигураций и имеются постоянные изменения в системе.

Следуя разработанной методике, в систему требуется интегрировать систему контроля целостности конфигураций, соответствующая модели разработанной во второй главе. Так как подходящих прикладных решений для систем на платформе «1С:Предприятие 8» в начале главы будет реализована данная система и включена как модуль в ERP-систему.

После интеграции системы контроля целостности конфигураций можно произвести поэтапное тестирование самой методики.

Конечными выводами будут результаты анализа тестирования методики.

4.1. Разработка системы контроля целостности конфигураций

Наиболее оптимальным вариантом разработки системы контроля целостности конфигураций является разработка на языке программирования BSL на платформе «1С:Предприятие 8», который является тем же языком, используемым для написания самой ERP-системы «1С:Управление нашей фирмой».

Система контроля целостности может быть разработана как конфигурация типа расширение конфигурации. Данное прикладное решение тогда может быть использовано и в других подобных системах на платформе «1С:Предприятие 8».

В ходе разработки конфигурация типа расширение конфигурации представляет собой структуру различных объектов метаданных, изображенных на рисунке 4.1.

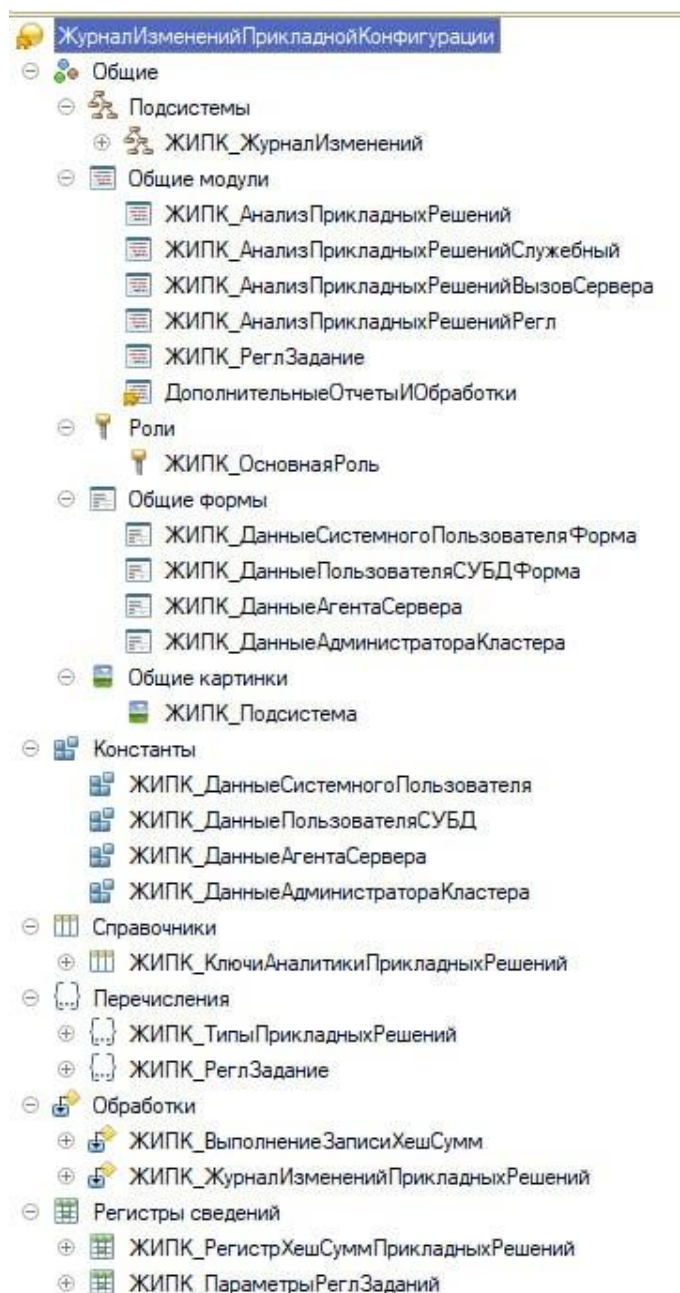


Рисунок 4.1 – Структура объектов конфигурации системы контроля целостности

1) Общие модули

Данные объекты содержат процедуры и функции реализующие логику и поведение при работе системы. В рамках проекта реализованы следующие модули:

- ЖИПК_АнализПрикладныхРешений – содержит процедуры для определения конфигураций, находящихся в базе данных системы, всех возможных типов;
- ЖИПК_АнализПрикладныхРешенийСлужебный – содержит процедуры, которые создают или изменяют статус конфигураций, для дальнейшего сбора данных о состояниях;
- ЖИПК_АнализПрикладныхРешенийВызовСервера – содержит процедуры активируемые в начале работы системы, в том числе запускает процедуры из общего модуля ЖИПК_АнализПрикладныхРешений;
- ЖИПК_АнализПрикладныхРешенийРегл – содержит процедуры выгрузки из базы данных конфигураций всех 3 возможных типов. Производится расчет хеш-сумм по этим конфигурациям алгоритмом SHA256, затем происходит запись этих данных хеш-сумм в отдельный регистр. Для отслеживания ошибок реализован функционал делающий записи в журнал регистрации;
- ЖИПК_РеглЗадание – содержит процедуру, где в зависимости от входа происходит вызов определённой п;
- ДополнительныеОтчетыИОбработки – используется как дополнительный функционал для создания регламентных процедур, которые могут быть настроены на запуск с определенной частотой или по определенному расписанию.

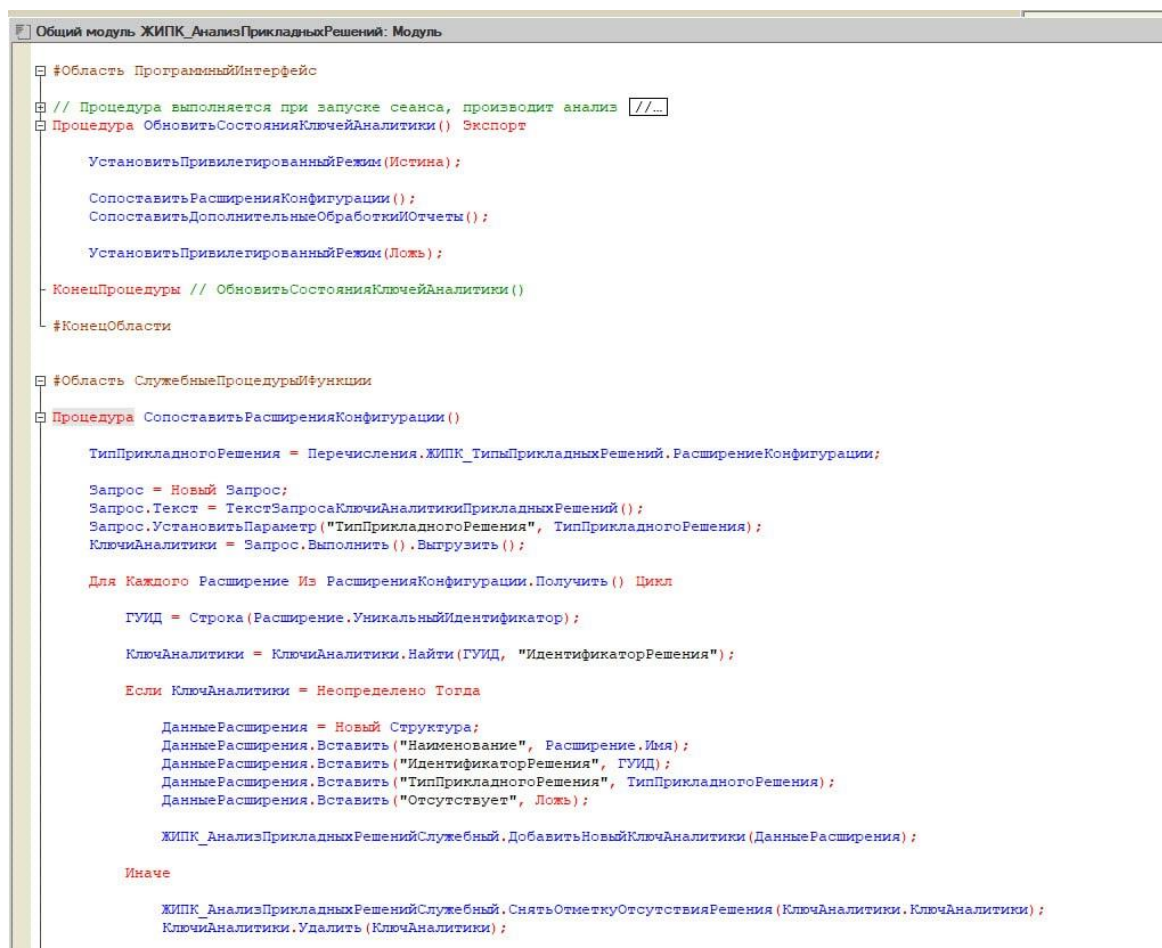


Рисунок 4.2 – Фрагмент кода общего модуля
ЖИПК_АнализПрикладныхРешений

2) Роли

Роли – это объект конфигурации, который определяет конкретные права данных на объекты системы.

В разрабатываемой системе потребуется лишь одна роль на чтение данных и использования общего журнала для отслеживания изменений, а так же служебной нормативно-справочной информации.

3) Общие формы

Содержит в себе графическое представление Констант для ввода данных, таких как доступы системного пользователя в информационную базу, адрес, порт и доступы к агенту сервера, доступы к кластеру этой информационной базы и доступы к СУБД необходимой при работе в клиент-серверном режиме.

4) Константы

Константы представляют из себя хранилище каких-либо статичных данных, стандартных типов, например, «Строка» и прочих. Является необходимым для заполнения в данной системе из-за специфики платформы «1С:Предприятие 8».

Ввод этих данных происходит через объект общих форм, где реализованы необходимые для заполнения поля для всех констант.

На рисунке 4.3 представлена общая форма для константы «ЖИПК_ДанныеАгентаСервера» с полями для заполнения.

Рисунок 4.3 – Фрагмент свойств константы

5) Справочники

В системе потребуется лишь один объект. Он хранит данные о всех конфигурациях, используемых в системе, так же с описанием к какому типу

относится. Изначально определена основная конфигурация, так как используется всегда.

Элементы данного справочника могут как добавляться, так и отмечаться как недействительные, например, в случае удаления какой-либо конфигурации.

Так же каждая конфигурация имеет свой определенный уникальный идентификатор, помимо основной конфигурации, этот объект метаданных как раз и хранит всю информацию о конфигурациях, используемых в системе.

6) Перечисления

Этот объект метаданных используется для определения различных типов, и использования их в других объектах. Например, в рамках проекта используется объект «ЖИПК_ТипыПрикладныхРешений», который описывает все 3 типа возможных конфигураций и объект «ЖИПК_РеглЗадание» с возможными операциями регламентных заданий – рисунок 4.4.

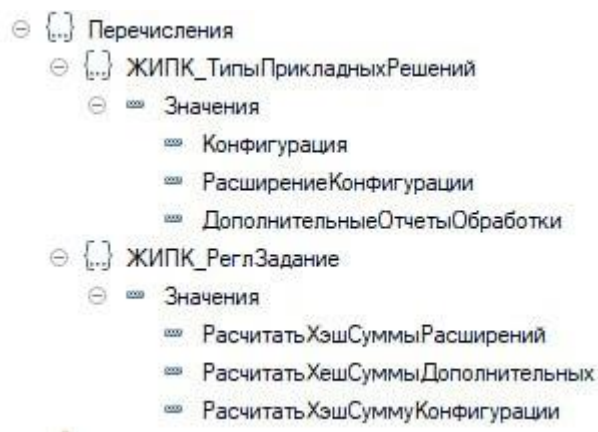


Рисунок 4.4 – Значения объекта конфигурации перечисления

7) Обработки

Данный объект предназначен для какого-либо графического представления или исполняемых процедур и функций. В системе контроля целостности используются 2 таких объекта:

1. «ЖИПК_ВыполнениеЗаписиХешСумм» предназначен для ручного сбора данных о состояниях конфигураций – рисунок 4.5;

2. «ЖИПК_ЖурналИзмененийПрикладныхРешений» — для отображения журнала изменений конфигураций.

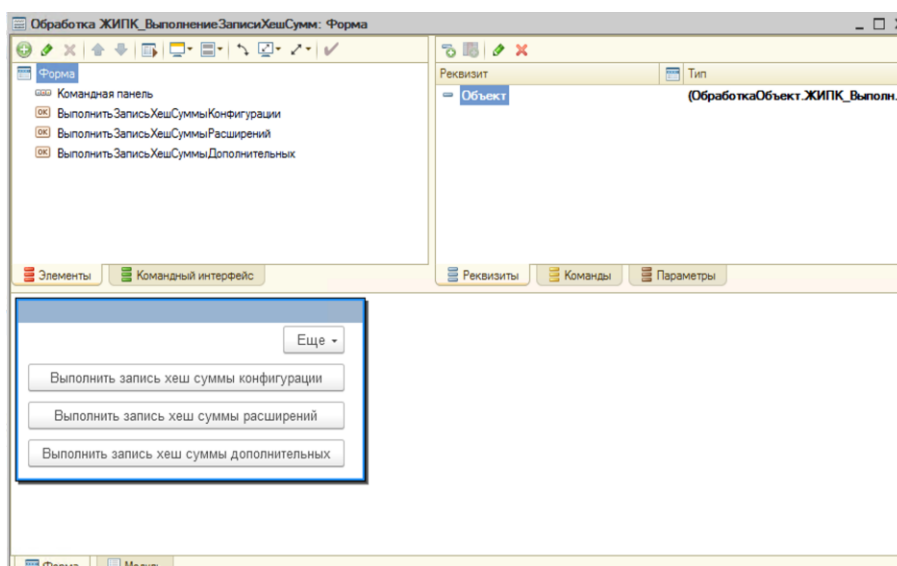


Рисунок 4.5 – Графическое представление команд ручного сбора состояний конфигурации

8) Регистры сведений

Согласно модели контроля целостности конфигураций, необходим определенный реестр, в котором хранятся данные о состояниях конфигураций. Соответственно в данном объекте конфигурации реализован этот реестр под наименованием «ЖИПК_РегистрХешСуммПрикладныхРешений», этот регистр хранит информацию о дате изменения, хеш-сумме и ссылкой на справочник «ЖИПК_КлючиАналитикиПрикладныхРешений», который является описанием конфигураций. Записи данного регистра могут добавляться, но изменение и удаление невозможно.

Так же существует регистр «ЖИПК_ПараметрыРеглЗаданий», он предназначен для настройки регламентных процедур, необходимых для сбора данных о состояниях конфигураций. В этом регистре хранится расписание или частота этих процедур.

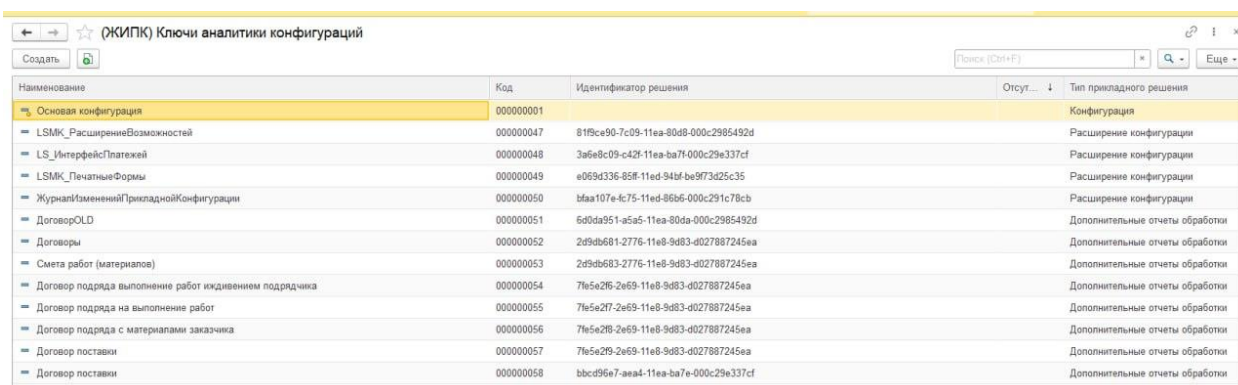
Процедуры и функции, реализованные в рамках дипломной работы описаны, в полном объеме в приложении А.

4.2. Внедрение системы контроля целостности конфигураций по разработанной методике

На этапе внедрения, согласно методике, требуется в начале определить некоторые параметры ERP-системы.

Как было описано выше, система находится в статусе постоянных обновлений и изменений. На текущий момент, включая интегрированную систему контроля целостности подключены основная конфигурация, 4 расширений конфигурации и 8 дополнительных отчетов и обработок, следовательно, требуется сбор данных о состояниях всех этих конфигураций, соответственно, 3 типа конфигураций.

После интеграции система контроля целостности конфигураций произвела идентификацию всех конфигураций, было присвоено наименование самого прикладного решения, его внутренний идентификатор в базе и тип. На рисунке 4.6 изображен список конфигураций в системе.



Наименование	Код	Идентификатор решения	Отсут...	Тип прикладного решения
Основная конфигурация	000000001			Конфигурация
LSMK_РасширениеВозможностей	000000047	81f9ce90-7c09-11ea-80d8-000c2985492d		Расширение конфигурации
LS_ИнтерфейсПлатежей	000000048	3a6e8c09-c42f-11ea-ba7f-000c29e337cf		Расширение конфигурации
LSMK_ПечатныеФормы	000000049	e069d336-95f8-11ed-94bf-ba9f73425c35		Расширение конфигурации
ЖурналИзмененийПрикладнойКонфигурации	000000050	bfaa107e-4c75-11ed-85b6-000c291c78cb		Расширение конфигурации
ДоговорOLD	000000051	6d0da951-a5a5-11ea-80da-000c2985492d		Дополнительные отчеты обработки
Договоры	000000052	2d9db681-2776-11e8-9d83-d027887245ea		Дополнительные отчеты обработки
Смета работ (материалов)	000000053	2d9db683-2776-11e8-9d83-d027887245ea		Дополнительные отчеты обработки
Договор подряда выполнение работ икдвением подрячка	000000054	7f65a2f6-2e69-11e8-9d83-d027887245ea		Дополнительные отчеты обработки
Договор подряда на выполнение работ	000000055	7f65a2f7-2e69-11e8-9d83-d027887245ea		Дополнительные отчеты обработки
Договор подряда с материалами заказчика	000000056	7f65a2f8-2e69-11e8-9d83-d027887245ea		Дополнительные отчеты обработки
Договор поставки	000000057	7f65a2f9-2e69-11e8-9d83-d027887245ea		Дополнительные отчеты обработки
Договор поставки	000000058	bbcd9567-aea4-11ea-ba7e-000c29e337cf		Дополнительные отчеты обработки

Рисунок 4.6 – Список конфигураций в ERP-системе

Из-за ограничений платформы «1С:Предприятие 8» для сбора данных о состояниях происходит с помощью регламентных процедур, это означает, что система будет производить периодически по расписанию запуск процедур сбора. Частота процедур может быть произвольной, в зависимости от производительности системы и размера самой конфигурации. Для конфигураций типа расширения конфигураций и дополнительных отчетов и обработок можно выставить запуск каждые 15 минут, т. к. они имеют относительно основной конфигурации небольшой размер. В свою очередь

основную конфигурацию резонно выставить запуск каждый час. В настройках системы будет отображаться следующим образом, для каждого типа задаётся своё расписание запуска. Список регламентных процедур и расписание для примера для расширений конфигурации изображено на рисунке 4.7.

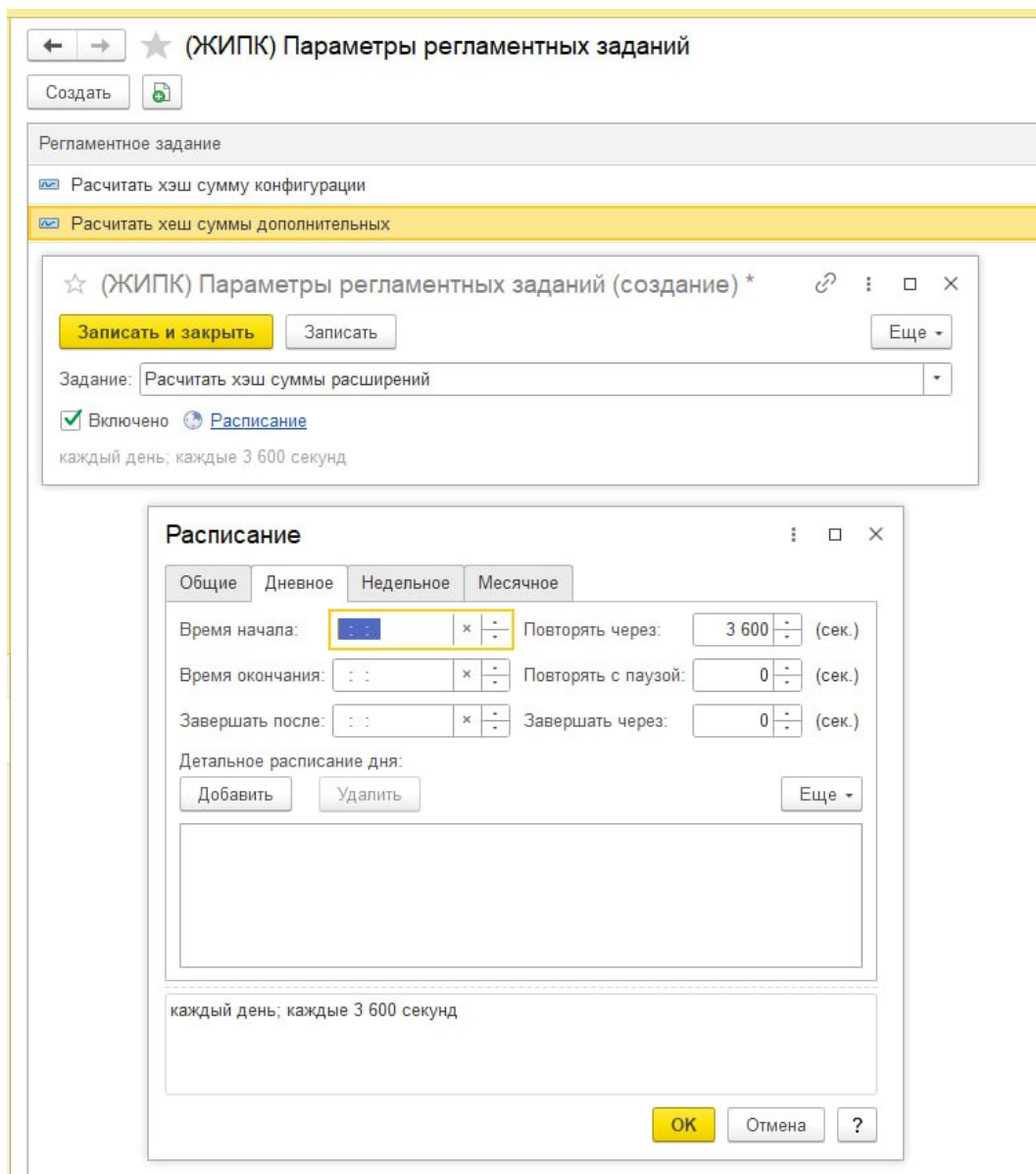


Рисунок 4.7 – Список регламентных процедур

При реализации системы контроля целостности для определения состояний конфигураций был выбран алгоритм хеш-функции SHA256, так как система изначально поддерживает вычисления по данному алгоритму и является наиболее распространенным в любых подобных системах.

Для методики так же необходимо определить пользователя, который будет работать с этой системой, но в рамках тестирования будет определен пользователь с высокими привилегиями, которому назначена роль оператора системы контроля целостности.

На этом этапе будет выполнено резервное копирование ERP-системы для дальнейшего тестирования в рамках эксплуатации.

После необходимых настроек системы этап внедрения является завершенным.

4.3. Эксплуатация системы контроля целостности конфигураций по разработанной методике

Далее можно перейти к этапу эксплуатации системы. После завершеного внедрения система работает автономно по заданным настройкам. Можно перейти в определенный реестр, где хранятся данные о состояниях конфигураций, где будет отображено проверяемое прикладное решение из идентифицированных ранее, дату сбора данных и хеш-сумму конфигурации. Хеш-сумма отображает текущее состояние конфигурации.

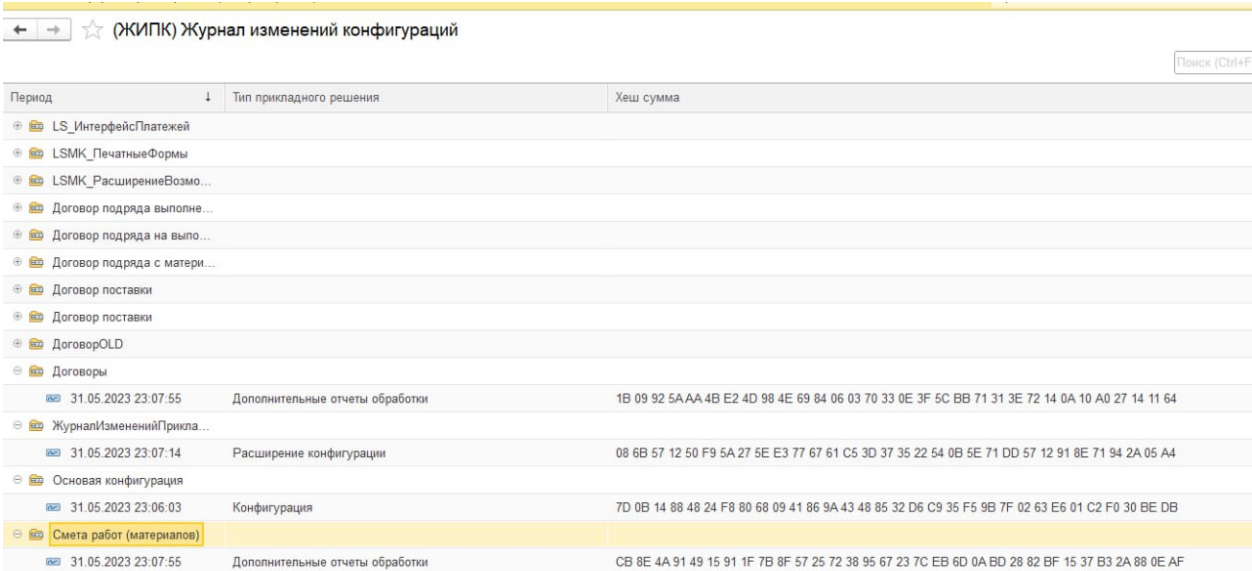
На рисунке 4.8 отображена выборка подобных записей за некоторый период времени. По этой выборке можно сделать вывод что все прикладные решения, идентифицированные ранее попадают в реестр. Так же разница считывания данных соответствуют настройкам регламентных процедур определенные на этапе внедрения и равняется минуте. Размер хеш-сумм в записях равняется 256 бит, что соответствует алгоритму SHA256. Хеш-сумма отображена в системе в виде шестнадцатеричного кода.

Период	Прикладное решение	Хеш сумма
31.05.2023 23:06:03	Основная конфигурация	7D 0B 14 88 48 24 F8 80 68 09 41 86 9A 43 48 85 32 D6 C9 35 F5 9B 7F 02 63 E6 01 C2 F0 30 BE DB
31.05.2023 23:06:22	LSMK_РасширениеВозможностей	A3 7C 4C 86 75 E9 74 64 AA B0 DB 52 13 76 1B 52 67 82 3C AC 2E D1 0A D6 DF 11 DF 10 EE 4A 0F A5
31.05.2023 23:06:39	LS_ИнтерфейсПлатежей	7C 6B 7B 5E C5 F4 48 38 1F B6 0F FF 2B 87 C0 05 B9 15 DF 9B FE C5 70 A6 98 F0 10 05 10 FC 5F 9F
31.05.2023 23:06:57	LSMK_ПечатныеФормы	D5 49 D9 86 B2 33 A4 51 8F B8 3E 6B E6 25 E3 30 07 A1 11 14 63 97 2C 4C 7E 4F 2B 8D A1 46 A5 E0
31.05.2023 23:07:14	ЖурналИзмененийПрикладнойКонфигурации	08 6B 57 12 50 F9 5A 27 5E E3 77 67 61 C5 3D 37 35 22 54 0B 5E 71 DD 57 12 91 8E 71 94 2A 05 A4
31.05.2023 23:07:54	Договор подряда выполнение работ иждивением подрядчика	C6 B6 30 58 B0 44 31 2A 30 6B 6F 1A C4 8C F9 32 27 20 0B 43 AE 86 70 5F C8 42 C8 98 05 62 7D A5
31.05.2023 23:07:54	Договор подряда на выполнение работ	0B CF 3B 64 84 69 8F 91 EE A1 7D 6E B0 61 C7 D0 40 4D 0A 11 DF 0E 9E 76 EB 65 CA 4B 63 14 20 8A
31.05.2023 23:07:54	Договор подряда с материалами заказчика	0E 12 94 4B FD 18 7E 7A C5 69 1A 75 E5 7D D0 E1 0B 59 CC 52 C2 7D 6C 1B 81 A0 D6 92 B6 D8 80 A7
31.05.2023 23:07:55	ДоговорOLD	66 3F D8 DA 6F 35 2B 5F BAA7 22 90 9D 30 5B 30 B2 30 28 DA 85 0C 7E 15 E1 5F 9E D6 2E DE 35
31.05.2023 23:07:55	Договоры	1B 09 92 5AAA 4B E2 4D 98 4E 69 84 06 03 70 33 0E 3F 5C BB 71 31 3E 72 14 0A 10 A0 27 14 11 64
31.05.2023 23:07:55	Смета работ (материалов)	CB 8E 4A 91 49 15 91 1F 7B 8F 57 25 72 38 95 67 23 7C EB 6D 0A BD 28 82 BF 15 37 B3 2A 88 0E AF
31.05.2023 23:07:55	Договор поставки	09 D8 01 18 2E 65 45 0F AE A1 6E CA 75 B3 D2 50 75 BC 52 34 39 72 99 62 B1 51 40 A3 6A 4A C0 44
31.05.2023 23:07:55	Договор поставки	C2 7B 2A A5 C2 49 1C 13 71 5E 44 A5 37 8F CC 65 77 CC 70 8C C0 FD AE 1D DF 46 84 EA 5B 0D 8A 90

Рисунок 4.8 – Выборка реестра состояний конфигураций

Реестр соответствует модели контроля целостности конфигураций, разработанной во второй главе данной работы.

Основным рабочим местом оператора является журнал изменений. На рисунке 4.9 изображен данный журнал.



Период	Тип прикладного решения	Хеш сумма
LS_ИнтерфейсПлатежей		
LSMK_ПечатныеФормы		
LSMK_РасширениеВозмо...		
Договор подряда выполне...		
Договор подряда на выпо...		
Договор подряда с матери...		
Договор поставки		
Договор поставки		
ДоговорOLD		
Договоры		
31.05.2023 23:07:55	Дополнительные отчеты обработки	1B 09 92 5A AA 4B E2 4D 98 4E 69 84 06 03 70 33 0E 3F 5C BB 71 31 3E 72 14 0A 10 A0 27 14 11 64
ЖурналИзмененийПрикла...		
31.05.2023 23:07:14	Расширение конфигурации	08 6B 57 12 50 F9 5A 27 5E E3 77 67 61 C5 3D 37 35 22 54 0B 5E 71 DD 57 12 91 8E 71 94 2A 05 A4
Основная конфигурация		
31.05.2023 23:06:03	Конфигурация	7D 0B 14 88 48 24 F8 80 68 09 41 86 9A 43 48 85 32 D6 C9 35 F5 9B 7F 02 63 E6 01 C2 F0 30 BE DB
Смета работ (материалов)		
31.05.2023 23:07:55	Дополнительные отчеты обработки	CB 8E 4A 91 49 15 91 1F 7B 8F 57 25 72 38 95 67 23 7C EB 6D 0A BD 28 82 BF 15 37 B3 2A 88 0E AF

Рисунок 4.9 – Журнал изменений конфигураций

Журнал содержит в себе все прикладные решения, используемые ERP-системой, а также записью с изменениями. Первой записью, отображаемой в журнале, является первоначальное состояние. Т. к. эти конфигурации уже присутствовали изначально, то состояние указывает на момент внедрения и интеграции системы контроля целостности.

Если добавить и загрузить тестовую конфигурацию в виде расширения в базу данных ERP-системы, тогда она отобразится в журнале с записью на момент добавления и хеш-суммой. В случае удаления конфигурации, записи в журнале остаются, и хеш-сумма соответствует на момент удаления.

На примере прикладного решения системы контроля целостности конфигураций можно внести периодические изменения в содержание. Будет совершено два изменения, где первое является согласованным, а второе нет. Для обоих изменений в код будут содержать какой-то фрагмент кода, дискредитирующий некоторые персональные данные физических лиц,

которые являются сотрудниками. Этот фрагмент кода изображен на рисунке 4.10.

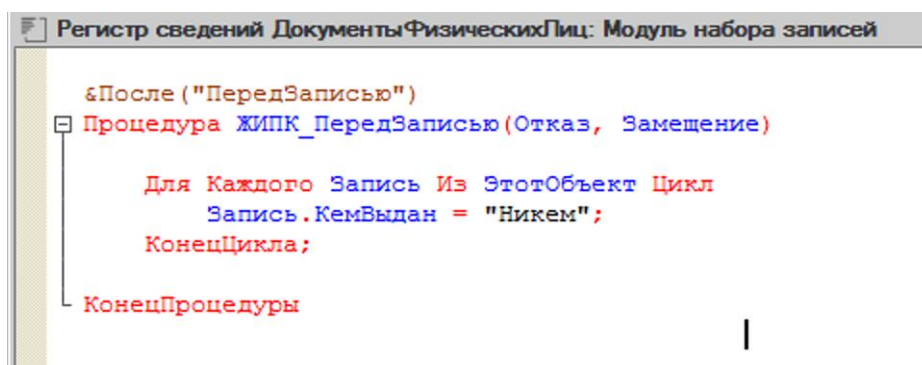


Рисунок 4.10 – Фрагмент кода изменения конфигурации

Данный код изменяет персональные данные, находящиеся в базе, а конкретно паспортные данные физических лиц.

После изменений конфигурации в журнале добавятся две различные записи, где последняя запись соответствует текущему состоянию конфигурации. Эти записи изображены на рисунке 4.11.

← → ☆ (ЖИПК) Журнал изменений конфигураций

Поиск (Ctrl+F) 🔍 - Ещё ▾

Период	Тип прикладного решения	Хеш сумма
LS_ИнтерфейсПлатежей		
LSMK_ПечатныеФормы		
LSMK_РасширениеВозмо...		
Договор подряда выполне...		
Договор подряда на выпо...		
Договор подряда с матери...		
Договор поставки		
Договор поставки		
ДоговорOLD		
Договоры		
ЖурналИзмененийПрикла...		
31.05.2023 23:07:14	Расширение конфигурации	08 6B 57 12 50 F9 5A 27 5E E3 77 67 61 C5 3D 37 35 22 54 0B 5E 71 D0 57 12 91 8E 71 94 2A 05 A4
31.05.2023 23:10:58	Расширение конфигурации	73 84 E0 DA 0B 90 97 57 2E 96 64 3E F2 3D 86 63 56 29 3D 01 DC 7A 55 99 00 72 D7 DC 1F 48 67 DE
31.05.2023 23:26:21	Расширение конфигурации	09 D4 7C 73 E7 2F FF CD 18 4A E9 F8 F5 F0 80 81 C3 14 0A 48 68 DC B3 12 1E 07 3B 66 83 FF 0C 82
Основная конфигурация		
Смета работ (материалов)		

Рисунок 4.11 – Журнал изменений после изменений конфигурации

На рисунке отчетливо видно, что в записях хеш-суммы отличаются, это указывает о том, что в конфигурации произошли изменения, также в разные моменты времени.

Следуя методике, необходимо определить являются ли эти изменения согласованными или нет. В случае согласованного изменения, оператор может быть предупреждён заранее о планируемых изменениях. Могут быть случаи, когда оператор не предупрежден об изменениях, но изменения являются

согласованными, тогда можно провести опрос пользователей, имеющих права доступа на изменения конфигураций. В обратном случае изменение является несогласованным и была нарушена целостность конфигураций, в следствие чего могут быть нарушена целостность хранимых данных в ERP-системе. Этот процесс и позволяет оценить защищенность системы от угроз нарушения целостности.

После определения нарушение целостности конфигураций делается вывод, что данные ERP-системы могут быть повреждены или дискредитированы. Необходимо предпринять меры по устранению утечки и восстановить систему в защищенное состояние, например, путем восстановления из резервной копии. В таком случае все данные вернутся в исходное состояние, измененная конфигурация примет защищенное состояние.

4.4. Анализ результатов тестирования

По итогам тестирования предлагается провести анализ полученных результатов и выявить преимущества и возможные перспективы развития разработанной методики оценивания защищенности ERP-системы от угроз нарушения целостности.

Так же стоит выделить разработанную систему контроля целостности конфигураций, на основе модели спроектированной во второй главе, данная система показала высокую эффективность и производительность сбора данных, вычислений и простоту использования. Использованная модель полностью выполняет поставленные задачи и позволяет отслеживать любые изменения в прикладных решениях ERP-системы «1С:Управление нашей фирмой» и сохранять неизменность этих показателей.

Первый этап методики необходим для определения входных данных для настройки системы контроля целостности. После настройки система контроля целостности работает автономно и не требуется ручного сбора данных по

конфигурациям, что позволяет автоматизировать процесс контроля целостности.

На втором этапе происходит сам процесс работы с системой, где требуется работа оператора. Для оператора рабочим интерфейсом является журнал изменений. При каждом изменении любой из конфигураций происходит оценка защищенности системы.

Но из данных для оценки в системе представлены только хеш-суммы конфигураций, без подробного описания самих изменений. В таком случае единственным эффективным способом восстановления целостности ERP-системы является полное восстановление из резервной копии, в таком случае есть перспектива внедрения и доработки модели контроля целостности, добавив подсистему контроля версий, например, такое ПО как «Git» позволит отслеживать изменения на уровне кода, тогда давать оценку защищенности станет проще и удобней, так же можно будет выявить как изменение может повлиять на ERP-систему в целом.

Журнал изменений хранит так же момент времени, в которое произошло изменение. Это может является ещё одним преимуществом системы, если была нарушена целостность данных изменением конфигураций действиями, совершенные согласованно. Отслеживание изменений позволит выявить момент времени, когда ERP-система имела состояние стабильной.

Выводы по четвертой главе

На основе проведенного тестирования разработанной методики оценивания защищенности ERP-системы от угроз нарушения целостности можно сделать итоговые выводы.

В рамках главы была разработана система контроля целостности конфигураций на основе модели, спроектированной во второй главе данной работы, из чего можно так же сделать вывод и по модели. Система показала высокую эффективность и производительность сбора данных и вычислений, простоту и удобство использования. Приведена структура, описаны основные процедуры и функции, используемые в самой системе, и взаимосвязь различных частей. По итогу система выполняет свою основную задачу – фиксирование любых изменений конфигураций в ERP-системе.

Тестирование второго этапа методики показала возможность оценки защищенности от угроз нарушения целостности, а также процесс устранения нарушений, необходимые действия при возникновении несогласованных изменений. Если ERP-система подвергнется нарушению целостности, то в методике описаны эффективные методы предотвращения нарушений и восстановления системы.

5. ОХРАНА ТРУДА

Целью данной работы является повышение защищенности ERP-системы «1С:Управление нашей фирмой», что достигается путем применения разработанной методики оценивания защищенности от угроз нарушения целостности и внедрения дополнительного программного модуля контроля целостности конфигураций.

Процесс выполнения данной работы включал в себя несколько шагов:

1. Анализ ERP-системы «1С:Управление нашей фирмой» как объекта защиты;
2. Анализ методов и выбор модели контроля целостности конфигураций ERP-системы;
3. Разработка методики оценивания защищенности «1С:Управление нашей фирмой» от угроз нарушения целостности конфигураций. В процессе реализации методики был разработан программный модуль контроля целостности конфигураций для вышеописанной ERP-системы.

Согласно Трудовому Кодексу Российской Федерации под условиями труда понимается «совокупность факторов производственной среды и трудового процесса, оказывающих влияние на работоспособность и здоровье работника» [11]. Процесс трудовой деятельности всегда сопряжен с риском возникновения опасных и вредных факторов. Контроль данной стороны рабочего процесса завязан на нескольких процессах: идентификации опасностей, оценке рисков и, если появляется необходимость, – их ликвидации.

Методика оценивания защищенности, разработанная в рамках данной дипломной работы, подразумевает, что для осуществления работы с ней в профессиональном плане необходим человек, обладающий исчерпывающими знаниями в области функционирования ERP-системы «1С:Управление нашей фирмой», специфики ее защиты. Таким образом, в данном разделе будут рассмотрены условия охраны труда для сертифицированного 1С-специалиста,

деятельность которого направлена на обеспечение информационной безопасности данной системы. Рабочий процесс специалиста данного профиля сопряжен с длительным нахождением в помещениях с электронным оборудованием, а также активным взаимодействием с ним. Подобная ситуация негативно сказывается на здоровье рабочего, поэтому необходимо с особой внимательностью отнестись к соблюдению норм в сфере охраны труда, чтобы предотвратить возможные последствия.

5.1. Анализ производственных факторов для специалиста информационной безопасности

Основную часть рабочего времени сотрудник тратит на выполнение трудовых обязанностей, что невозможно без использования персонального компьютера. Комфорт и безопасность являются ключевыми факторами, которые благотворно влияют на производительность людей, занимающихся работой с электронным оборудованием.

В процессе работы возникает множество факторов, которые ухудшают состояние сотрудника и, в результате, снижают его продуктивность, производительность. В некоторых случаях даже возникает риск нанесения вреда здоровью.

Когда работник взаимодействует с электронным оборудованием, включая персональный компьютер, он подвергается воздействию различных опасных и вредных производственных факторов, которые могут оказывать негативное воздействие на его состояние здоровья (далее – ОВПФ).

В качестве основных видов ОВПФ, с которыми может столкнуться специалист информационной безопасности на рабочем месте, можно выделить следующие:

1. Физические факторы. Воздействие ОВПФ данного вида может спровоцировать появление у работника профессиональных заболеваний, а также появление травм, которые будут препятствовать выполнению рабочих задач. Основополагающие из них:

- Световая среда;
- Виброакустические факторы.

2. Химические факторы. Во время рабочего процесса специалист информационной безопасности сталкивается со следующими химическими факторами: повышенное содержание в воздухе рабочей зоны двуокиси углерода, озона, аммиака, фенола и т. д.

3. Психофизиологические факторы. К возможным рискам, причинами которых являются психофизиологические факторы, как правило, относят следующие виды перегрузок: статистического и динамического характера, а также нервно-психологические. Специалист часто сталкивается с перенапряжением зрения, монотонным рабочим процессом, а также напряжением внимания. Результатом нерациональной организации условий труда может стать умственное перенапряжение. Подобные последствия могут встретиться у специалистов информационной безопасности в связи со следующими психофизиологическими факторами:

- Длительное сосредоточенное наблюдение;
- Активное наблюдение за ходом производственного процесса.

В процессе работы специалиста информационной безопасности могут возникнуть различные неблагоприятные факторы. Они могут быть вызваны не только разными компонентами персонального компьютера, такими как монитор, системный блок или сетевой фильтр, но и внешними факторами, которые зависят от условий работы и организации. Поскольку сотрудник большую часть рабочего времени взаимодействует с электронным оборудованием, одним из основных воздействующих факторов является уровень электромагнитного излучения.

На основе исследования информационных источников формируется исходная база потенциальных опасностей. Затем она корректируется для конкретной организации и рабочего места, составляется перечень

идентифицированных опасностей. Этот перечень регулярно и своевременно обновляется.

Оценка риска на рабочем месте – важный этап организации работы на любом предприятии. В общем случае для решения данной задачи используют N-уровневую шкалу ущерба – каждому уровню присваивается определенный весовой коэффициент, основанный на экспертной оценке. Методика оценки раскрыта в ГОСТ 12.0.010-2009 и включает следующие этапы:

1. Выявление опасностей, характеризующих их проявлений и возможных последствий;

2. Каждой опасности присваивается показатель ущерба и соответствующий ему весовой коэффициент (таблица 5.1) [5].

Таблица 5.1 – Трехуровневая шкала ущерба.

Тяжесть ущерба	Весовой коэффициент	Вербальное описание ущерба
Малый	5	Работнику, пострадавшему на рабочем месте, не требуется оказание медицинской помощи; худший исход ситуации – 3-х дневное отсутствие на рабочем месте
Средний	10	Пострадавший работник нуждается в оказании специальной медицинской помощи – его доставляют в организацию здравоохранения или требуется ее посещение; работник отсутствует на рабочем месте до 30 дней; развитие хронического заболевания
Большой	15	Несчастный случай на рабочем месте становится причиной серьезного (неизлечимого) заболевания; необходимо лечение в стационаре; отсутствие на рабочем месте более 30 дней; стойкая утрата трудоспособности или смертельный исход

Для определения вероятности наступления ущерба, вызванного проявлением j-й опасности, необходимо произвести деление i-го весового коэффициента, который представлен в таблице 5.2, на сумму весовых

коэффициентов, присвоенных идентифицированным опасностям и исходу, не связанному с наступлением ущерба. Данные значения указанных вероятностей рассчитываются по формуле: $P_j = \frac{A_j}{\sum_{j=1}^{k+1} A_j}$.

Таблица 5.2 – Шкала вероятностей

Вероятность	Весовой коэффициент	Вербальное описание вероятностей проявления опасностей и наступления ущерба
Низкая	1	Опасность или ее проявления, которые могут вызвать определенный ущерб, не должны возникнуть за все время профессиональной деятельности работника.
Средняя	3	Опасность и ее проявления, которые могут вызвать определенный ущерб, возникают лишь в определенные периоды профессиональной деятельности работника.
Высокая	7	Опасность или ее проявления, которые могут вызвать определенный ущерб, возникают постоянно в течении всей профессиональной деятельности работника.

Для всех идентифицированных опасностей есть возможность определения рисков, что выполняется посредством перемножения значений вероятностей наступления весовые коэффициенты соответствующих ущербов. Для оценки значимости рисков используется соответствующая система – шкала оценки значимости рисков. Распространенный вариант – трехуровневая шкала оценки значимости рисков – представлен в таблице 5.3.

Таблица 5.3 – Трехуровневая шкала вероятностей

Интервал значений	$0 < R \leq 5$	$5 < R \leq 10$	$10 < R \leq 15$
Значимость риска	Низкий	Умеренный	Высокий

Путем проведения вышеописанных подсчетов можно оценить оформить сводную таблицу, т. е. разработать карту рисков, которая представлена в таблице 5.4.

Таблица 5.4 – Карта риска до рекомендаций по улучшению условий труда

Идентифицированные опасности	Возможный ущерб	Весовой коэффициент ущерба	Качественное значение вероятности наступления ущерба	Весовой коэффициент вероятности наступления ущерба	Численное значение вероятности наступления ущерба	Риски по идентифицированным опасностям	Оценка значимости риска по отдельной опасности	Риск на рабочем месте	Оценка значимости риска на рабочем месте
Световая среда	Средний	10	Высокая	7	7/24 0,29	2,9	Низкий	9,4	Умеренный
Виброакустические факторы	Средний	10	Низкая	1	1/24 0,04	0,4	Низкий		
Химические факторы	Большой	15	Средняя	3	3/24 0,13	1,9	Низкий		
Длительность сосредоточенного наблюдения	Средней	10	Высокая	7	7/24 0,29	2,9	Низкий		
Активное наблюдение	Средний	10	Средняя	3	3/24 0,13	1,3	Низкий		
Исход, не связанный с наступлением ущерба	0	0	Средняя	3	3/24 0,13	0			

5.2. Рекомендации по нормализации условий труда по каждому фактору

Разработанная карта рисков, представленная в Таблице 5.4, наглядно демонстрирует возможные опасные ситуации. Важный этап в работе над их предупреждением – разработка перечня мер по предотвращению идентифицированных рисков, которые позволят улучшить условия труда, что, в свою очередь, снизит вред здоровью работникам организации.

Разработаем рекомендации по нормализации условий труда:

- Снабжение рабочих мест источниками освещения, которые соответствуют нормам [13];
- Планировка помещения в рабочей зоне должна быть составлена с учетом шума, который исходит от техники; в случае необходимости организации рабочего процесса в помещении с сильным шумом необходимо установить на источники шума специальные кожухи для поглощения;
- Регулярная очистка и увлажнение воздуха в области рабочего места при помощи кондиционеров в соответствии с нормами СанПиН [12];
- Организация уборки помещений в соответствии с заранее разработанным графиком; создание комфортных помещений для отдыха сотрудников;
- Установление графика режима работы для сотрудников с обязательными перерывами при работе в состоянии повышенной концентрации;
- Монтаж электронного оборудования с учетом действия фоновое электромагнитного поля.

Внедрение данных рекомендаций позволит улучшить условия труда и, соответственно, снизить риски возникновения идентифицированных ОВПФ, что отражено в таблице 5.5.

Таблица 5.5 – Карта риска после рекомендаций по нормализации условий труда

Идентифицированные опасности	Возможный ущерб	Весовой коэффициент ущерба	Качественное значение вероятности наступления ущерба	Весовой коэффициент вероятности наступления ущерба	Численное значение вероятности наступления ущерба	Риски по идентифицированным опасностям	Оценка значимости риска по отдельной опасности	Риск на рабочем месте	Оценка значимости риска на рабочем месте
Световая среда	Низкий	5	Средняя	3	3/12 0,25	1,25	Низкий	4,12	Умеренный
Виброакустические факторы	Низкий	5	Низкая	1	1/12 0,08	0,41	Низкий		
Химические факторы	Средний	10	Низкая	1	1/12 0,08	0,8	Низкий		
Длительность сосредоточенного наблюдения	Низкий	5	Средняя	3	3/12 0,25	1,25	Низкий		
Активное наблюдение	Низкий	5	Низкая	1	1/12 0,08	0,41	Низкий		
Исход, не связанный с наступлением ущерба	0	0	Средняя	3	3/12 0,25	0			

Выводы по пятой главе

В рамках данной главы были выявлены основные опасные и вредные производственные факторы, которые сопряжены с работой 1С-специалиста. На основе идентифицированных опасностей была разработана карта рисков, приведенная в сводную таблицу, которая позволяет определить ущерб здоровью работника. Данная карта рисков стала отправной точкой для разработки перечня рекомендаций, способствующих улучшению условий труда, согласно нормативным документам.

6. ТЕХНИКО-ЭКОНОМИЧЕСКОЕ ОБОСНОВАНИЕ ПРОЕКТА

Себестоимость продукции определяют следующим образом: «стоимостная оценка текущих затрат предприятия на производство и реализацию продукции (товаров, работ, услуг). Полная (коммерческая) себестоимость складывается из производственной себестоимости, затрат, связанных с реализацией продукции, и др. внепроизводственных расходов» [6].

Оценка уровня затрат предприятия играет ключевую роль, поскольку она способствует контролю использования ресурсов, позволяет составлять прогнозы возникновения новых, получать наибольшую отдачу от их использования. Она также способствует оптимальному управлению издержками с целью их сокращения, выявлению основных источников снижения затрат и разработке конкретных мероприятий для их реализации на предприятии. Все эти меры помогают снизить себестоимость продукции и повысить общую эффективность деятельности предприятия [8].

Стоимость продукции является не только важнейшей экономической категорией, но и качественным показателем, так как она характеризует уровень использования всех ресурсов (переменного и постоянного капитала), находящихся в распоряжении предприятия.

Управление себестоимостью продукции предприятия представляет собой процесс, нацеленный на формирование затрат на производство всей продукции, а также себестоимость отдельных производимых изделий. Также данный процесс включает в себя контроль поставленных задач, направленных на снижение себестоимости продукции, производимой на предприятии. Элементы, без которых не может существовать система управления себестоимостью продукции, это: прогнозирование, планирование, анализ и контроль за себестоимостью.

Цель дипломного проекта: повышение защищенности ERP-системы «1С:Управление нашей фирмой», что достигается путем применения разработанной методики оценивания защищенности от угроз нарушения

целостности и внедрения дополнительного программного модуля контроля целостности конфигураций.

6.1. План выполнения дипломного проекта

В соответствие с формулированной темой дипломного проекта определяются этапы НИР, а также их содержание. Этапы научно-исследовательской работы отражены в Таблице 6.1.

Таблица 6.1 – Этапы НИР

№	Этап и содержание работы	Длительность цикла, час	Участники НИР		
			Д	Р	К
1	Постановка задачи и подготовка исходных данных к разработке ВКР	20	15	5	–
2	Глава 1. Анализ ERP-системы «1С:Управление нашей фирмой», как объекта защиты	25	22	3	–
3	Глава 2. Анализ методов и проектирование модели контроля целостности конфигураций ERP-системы	25	22	3	–
4	Глава 3. Разработка методики контроля целостности конфигураций ERP-системы	60	50	10	–
5	Глава 4. Тестирование разработанной методики контроля целостности конфигураций ERP-системы	25	20	5	–
6	Подбор данных и написание части в области охраны труда	15	13	–	2
7	Расчёт экономической части проекта и обоснование экономической эффективности	20	18	–	2

Продолжение таблицы 6.1

8	Оформление пояснительной записки на ВКР	10	10	–	–
9	Прохождение нормоконтроля	2	2	–	–
10	Сдача ВКР (бумажная и электронная версии) на кафедру	2	2	–	–
11	Проверка ВКР в системе «Антиплагиат ВУЗ»	2	2	–	–
12	Получение внешней рецензии на ВКР	2	2	–	–
13	Защита ВКР	1	1	–	–
	Итого:	209	179	26	4

Исполнитель: Д – дипломник; К – консультант; Р – руководитель.

Таким образом, работа над ВКР заняла 209 часов. Из общего количества потраченных часов большая часть составляет работа дипломника – 179 часов, работа дипломного руководителя – 26 часов, работа консультантов по охране труда и экономике составила 4 часа.

Для иллюстрации графика работ над ВКР был разработан ленточный график, представленный в Таблице 7.2.

Таблица 6.2 – Ленточный график выполнения работ

№	Этап и содержание работы	Начало работ	Окончание работ	Дни
1	Постановка задачи и подготовка исходных данных к разработке ВКР	13.02.2023	02.03.2023	17
2	Глава 1. Анализ ERP-системы «1С:Управление нашей фирмой», как объекта защиты	03.02.2023	20.02.2023	17
3	Глава 2. Анализ методов и проектирование модели контроля целостности конфигураций ERP-системы	21.02.2023	09.03.2023	16

Продолжение таблицы 6.2

4	Глава 3. Разработка методики контроля целостности конфигураций ERP-системы	10.03.2023	16.04.2023	37
5	Глава 4. Тестирование разработанной методики контроля целостности конфигураций ERP-системы	17.04.2023	04.05.2023	17
6	Подбор данных и написание части в области охраны труда	05.05.2023	14.05.2023	9
7	Расчёт экономической части проекта и обоснование экономической эффективности	05.05.2023	14.05.2023	9
8	Оформление пояснительной записки на ВКР	15.05.2023	24.05.2023	9
9	Прохождение нормоконтроля	25.05.2023	03.06.2023	9
10	Сдача ВКР (бумажная и электронная версии) на кафедру	04.06.2023	04.06.2023	1
11	Проверка ВКР в системе «Антиплагиат ВУЗ»	05.06.2023	11.06.2023	6
12	Получение внешней рецензии на ВКР	12.06.2023	20.06.2023	8
13	Защита ВКР	27.06.2023	27.06.2023	1
	Итого:			147

Так, согласно разработанному ленточному графику, работа над ВКР заняла 147 дней.

6.2. Смета затрат на научно-исследовательскую работу

Смета затрат на НИР может быть представлена по следующим статьям калькуляции:

- Материалы, покупные изделия и полуфабрикаты;
- Спецоборудование для научных исследований;

- Расходы на электроэнергию;
- Заработная плата;
- Взносы на социальное страхование и обеспечение;
- Косвенные (накладные) расходы отдела (кафедры);
- Производственные командировки;
- Общеуниверситетские косвенные расходы;
- Расходы на научно-техническую информацию;
- Расходы на зарубежные лицензии и патенты;
- Затраты на эксплуатацию оборудования (амортизацию).

6.2.1. Материалы, покупные изделия и полуфабрикаты

Для выполнения дипломного проекта необходимо рассчитать стоимость покупных изделий. Расчет стоимости покупных изделий в Таблице 6.3.

Список покупных изделий:

- бумага формата А4;
- краска для принтера (тонер);
- папка;
- канцелярские принадлежности (ручка, блокнот).

Стоимость материалов и покупных изделий рассчитана по формуле (1.2).

$$C = K \times Ц \quad (1.2)$$

где:

С – стоимость изделия за штуку;

К – количество изделий;

Ц – цена изделия.

Таблица 6.3 – Стоимость материалов и покупных изделий

Изделие	Количество	Цена за единицу, руб.	Стоимость, руб.
Бумага А4	1 пачка	310	310

Продолжение таблицы 6.3

Тонер	1 шт.	335	335
Папка	1 шт.	201	201
Блокнот	1 шт.	99	99
Ручка	2 шт.	35	70
ИТОГО:			1015

Таким образом, общая стоимость материалов и покупных изделий, необходимых для выполнения дипломной работы, по актуальной оценке, составила 1015 руб.

6.2.2. Спецоборудование для научных исследований

Специального оборудования для выполнения дипломного проекта не использовалось.

6.2.3. Расходы на электроэнергию

Затраты на электроэнергию определяются по следующей формуле (1.3).

$$Z_{эi} = \sum_1^n Q_{эi} \times C_{э} \quad (1.3)$$

где:

$Z_{эi}$ – затраты на электроэнергию i-оборудованием;

$Q_{эi}$ – количество энергии потребляемой i-оборудованием в час;

$C_{э}$ – стоимость одного кВт/ч.

Количество энергии, потребляемой i-оборудованием, рассчитывается по формуле (1.4).

$$Q_{эi} = N_i \times T_i \times n_i \times k_{экв} \quad (1.4)$$

где:

где N_i - мощность используемого i-оборудования, кВт;

T_i - длительность расчетного периода, ч;

n_i - количество оборудования, шт. (единиц).

Мощность, используемых источников питания:

- Компьютер – мощность 750 Вт или 0,75 кВт;
- Монитор – мощность 100 Вт или 0,1 кВт;
- Лампа – мощность 40 Вт или 0,04 кВт.

Длительность использования источников питания можно определить как 184 часов в месяц, что соответствует стандартному режиму работы 5/2.

Соответственно, можно рассчитать количество потребляемой электроэнергии:

$$Q_{\text{экомп}} = 0,75 \cdot 184 \cdot 1 = 138 \text{ (кВт/ч)}$$

$$Q_{\text{эмон}} = 0,1 \cdot 184 \cdot 1 = 18,4 \text{ (кВт/ч)}$$

$$Q_{\text{элам}} = 0,04 \cdot 184 \cdot 1 = 7,36 \text{ (кВт/ч)}$$

Цена за электроэнергию соответствует общему тарифу по г. Санкт-Петербург, 4,98 руб/кВт-ч.

В таблице 6.4 представлены результаты расхода электроэнергии.

Таблица 6.4 – Расходы на электроэнергию

Оборудование	Расход электроэнергии, кВт-ч	Цена за единицу, руб/кВт-ч	Длительность работы оборудования, ч	Сумма, руб.
Компьютер	688	688	688	688
Монитор	92	92	92	92
Лампа	110	110	110	110
ИТОГО:				890

Таким образом, расходы на электроэнергию составили 890 руб.

6.2.4. Затраты на оплату труда

Затраты на оплату труда состоят:

- Стипендия студента;
- Зарплата дипломного руководителя;
- Зарплата консультанта «экономика транспорта»;

– Зарплата консультанта кафедры «безопасность жизнедеятельности».

Общие расходы на выплату заработной платы состоят из заработной платы студента и заработной платы консультантов.

Затраты на оплату труда рассчитывается по следующей формуле (1.6).

$$C_{тр} = \frac{ЗП}{160} \times t_p \quad (1.6)$$

где:

$C_{тр}$ – затраты на оплату труда;

ЗП – заработная плата работника;

t_p – затраченное время на работу.

В таблице 6.5 представлен расчет затрат на оплату труда.

Таблица 6.5 – Затраты на оплату труда

Исполнитель	Заработная плата, руб.	Затраченное время, ч.	Затраты на оплату труда, руб.
Дипломник	2 500 (стипендия)	179	2 797
Дипломный руководитель	40 000	26	6 500
Консультант по экономике	36 000	4	900
Консультант по охране труда	36 000	4	900
ИТОГО:			11 097

Таким образом, затраты на оплату труда составили 11 097 руб.

6.2.5. Взносы на социальное страхование и обеспечение

Отчисления на социальное страхование и обеспечение составляют 30,2 % от суммы всех заработных плат и определяются по формуле (1.7).

$$ВСС = 0,302 \times (11\,097 - 2\,500) = 2\,915 \quad (1.7)$$

6.2.6. Производственные командировки

Во время выполнения дипломного проекта производственные командировки не проводились.

6.2.7. Расходы на научно-техническую информацию

Расходы на научно-техническую информацию не производились.

6.2.8. Расходы на зарубежные лицензии и патенты

Расходы на зарубежные лицензии и патенты не производились.

6.2.9. Затраты на эксплуатацию оборудования (амортизацию)

К амортизации основных фондов относятся все амортизационные отчисления по основным средствам за отчетный период. Амортизации подвергается оборудование и офисные принадлежности при разработке дипломного проекта. Амортизации подвергаются изделия общей стоимостью не менее 40000 руб.

Расчет основных средств, представлен в таблице 6.6.

Таблица 6.6 – Расчет на амортизацию

№ п/п	Наименование	Количество, шт.	Цена, руб.	Затраты, руб.
1	Системный блок	1 шт.	20 000	20 000
2	Монитор	1 шт.	5 000	5 000
3	Клавиатура	1 шт.	1 200	1 200
4	Мышь	1 шт.	700	700
5	Принтер	1 шт.	5 000	5 000
6	Стол	1 шт.	3 000	3 000
7	Стул	1 шт.	1 500	1 500
8	Лампа	1 шт.	600	600
ИТОГО:				37 000

Так как общая стоимость основных средств составляет 37 000 руб., то вся сумма уходит в стоимость дипломного проекта.

6.3 Стоимость выполнения дипломного проекта

Итоговая стоимость работы представляет собой сумму всех вышеперечисленных расходов.

Т. е. необходимо суммировать все расходы, составив на основе полученных данных сводную таблицу. В таблице 6.7 представлена калькуляция по статьям расходов и общая стоимость дипломного проекта.

Таблица 6.7 – Калькуляция по статьям расходов и общая стоимость дипломного проекта

п/п	Статья расходов	Сумма, руб.
1	Материалы, покупные изделия и полуфабрикаты	1 015
2	Расходы на электроэнергию	890
3	Заработная плата	11 097
4	Взносы на социальное страхование и обеспечение	2 596
5	Амортизация оборудования	37 000
ИТОГО:		52 598

Таким образом, была высчитана стоимость разработки методики оценивания защищенности от угроз нарушения целостности и внедрения дополнительного программного модуля контроля целостности конфигураций. В процессе вычисления были учтены материальные расходы и расходы на приобретение оборудования. Также были определены расходы на оплату труда исполнителя проекта, дипломного руководителя и консультантов, были вычислены размеры социальных отчислений. Помимо этого, рассчитаны косвенные расходы кафедры и общеуниверситетские косвенные расходы. Так как вся научно-техническая информация находится в свободном доступе, то на нее расходы не производились. Общая стоимость дипломного проекта составила 52 598 руб.

6.4. Расчет экономического эффекта

Необходимо рассчитать экономический эффект от внедрения разработанной методики. Формула для расчета экономического эффекта:

$$\mathcal{E} = \Pi - \mathcal{Z} \quad (8.10)$$

где \mathcal{E} – экономический эффект;

Π – результат деятельности;

\mathcal{Z} – сумма, потраченная на разработку.

Сумма, потраченная на разработку, была подсчитана в предыдущем пункте. Необходимо рассчитать прибыль, которая может быть получена в результате внедрения разработанной методики.

Данная методика должно оказать положительный эффект на защищенность ERP-системы организаций, которые будут её внедрять в свои процессы. Эффект заключается в том, что снижается риск дискредитации и потери конфиденциальной информации, а также снижение риска простоя и лишних издержек. Таким образом можно рассчитать экономический эффект исходя из возможной реализации системы контроля целостности конфигураций ERP-системы «1С:Управление нашей фирмой». На примере организации с режимом налогообложения индивидуального предпринимателя. Есть клиентская база организаций использующих данную ERP-систему. С учетом конверсии заинтересованы 12 клиентов из имеющихся во внедрении и дальнейшем обслуживании данной системы. По оценке организации франчайзи 1С стоимость данного внедрения оценивается в 7 500 рублей, а также дальнейшее обслуживание 2 500 рублей в месяц. Учитывая, что заинтересованных клиентов 12 организаций, тогда прибыль за год составит:

$$\Pi = 12 * 7500 + (12 * 2500) * 12 = 450000 \text{ (руб.)}$$

Следовательно, экономический эффект составит:

$$\mathcal{E} = 450000 - 55598 = 394402 \text{ (руб.)}$$

Выводы по шестой главе

В технико-экономическом обосновании разработки произведены расчеты материальных расходов, расходов на электроэнергию, фонда заработной платы и взносов на социальное страхование и обеспечение, а также косвенных расходов кафедры и общеузовских расходов. Общие затраты на дипломное проектирование составляют 55 598 рублей. Был подсчитан экономический эффект, который равен 394 402 рублей, достигаемый внедрением и дальнейшем обслуживании разработанной системы контроля целостности конфигураций ERP-системы «1С:Управление нашей фирмой». За счёт внедрения и обслуживания системы можно достигнуть показатель результата деятельности в 450 000 рублей, учитывая, что 12 потенциальных клиентов уже заинтересованы во внедрении данной системы.

ЗАКЛЮЧЕНИЕ

На текущий момент на рынке ERP-систем в России фирма «1С» занимает лидирующую позицию, и учитывая мировые тенденции спрос на эти ERP-системы только возрастёт. Представителем ERP-систем от фирмы «1С» является прикладное решение «1С:Управление нашей фирмой», реализованное на платформе «1С:Предприятие 8». В рамках работы данная ERP-система выступает как объект защиты.

В начале был выполнен анализ этой ERP-системы, выявлены наиболее актуальные угрозы нарушения целостности путём метода экспертной оценки. После анализа сделаны выводы, что существуют 2 слабых места, которые необходимо контролировать, таким образом повысить защищенность. Одним из таких слабых мест являются прикладные решения или конфигурации, реализованные на платформе «1С:Предприятие 8», в том числе для основного прикладного решения «1С:Управление нашей фирмой». В результате не обнаружилось необходимых методов и возможностей контроля за конфигурациями, в следствии этого система требуется в доработке для повышения защищенности, в частности методике оценки защищенности от угроз нарушения целостности конфигураций.

Для реализации методики была спроектирована модель контроля целостности конфигураций, в последствии является основой для систем контроля. Модель основана на общепринятой модели контроля целостности Кларка-Вилсона, что повышает эффективность и защищенность системы. Спроектированная модель была адаптирована и доработана для работы с решениями на платформе «1С:Предприятие 8».

Методика представляет собой инструкцию и описание процессов необходимых для оценивания защищенности, поэтому было описано 2 этапа этой методики. Первый этап описывает необходимые для контроля целостности систему, основанную на спроектированной модели, входные данные и настройку ERP-системы. Второй этап в свою очередь описывает процессы, которые происходят при работе с системой контроля целостности и

каким образом происходит оценка защищенности. Сама система контроля целостности является автономной и замкнутой, то есть сбор данных о целостности конфигураций может без обязательного участия оператора системы. Процесс работы оператора системы описывается как набор действий, которые нацелены на оценку защищенности ERP-системы, а также действия при нарушении целостности.

Произведено тестирование разработанной методики. В рамках тестирования была разработана система контроля целостности конфигураций, основываясь на модели. Система контроля целостности конфигураций показала высокие результаты производительности, эффективности и неизменности, из чего делается вывод в успешном выполнении проектирования модели контроля целостности конфигураций. Тестирование методики так же было разбито поэтапно. Этап внедрения показал простоту настройки и подготовки ERP-системы. В свою очередь этап эксплуатации так же прошёл успешно, нарушение целостности было определено и оценена защищенность ERP-системы. Следуя методики целостность ERP-системы была восстановлена и защищаемая информация нетронута. Выявлено преимущество данной методики, оно заключается в том, что использовать её можно на всех системах, разработанных на платформе «1С:Предприятие 8». Выявлены остальные преимущества методики и дальнейшие перспективы развития.

Оператором системы контроля целостности конфигураций является специалист 1С и имеющий необходимую квалификацию. Специалист 1С подвержен различным факторам, которые негативно сказываются на его здоровье, были так же предложены меры, способствующие улучшению условий труда.

В последней главе да так же был определены различные экономические показатели в рамках данной работы. Была определена стоимость разработки методики, включая систему контроля целостности. Опрошены потенциальные клиенты, готовые использовать данную методику. По итогу главы за год

можно получить показатель выручки в 450 000 рублей, что является отличным показателем, относительно затрат на разработку.

На основе выполненных заданий, можно сделать вывод что основная цель была выполнена, защищенность ERP-системы «1С:Управление нашей фирмой» была повышена, риски угроз нарушения целостности снижены.

Стоит отметить, что результаты дипломной работы могут служить основой для дальнейших исследований и разработок в области информационной безопасности ERP-систем и систем, реализованных на платформе «1С:Предприятие 8».

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Архитектура платформы 1С:Предприятие: Базовые механизмы [Электронный ресурс] // ООО «1С» - URL: <https://v8.1c.ru/platforma/bazovye-mehanizmy/> (Дата обращения: 16.03.2023).
2. Бандуля И.В. Реальная автоматизация малого бизнеса “1С:Управление нашей / И. В. Бандуля, Ю. В. Павлов. - Москва: ООО «1С-Публишинг», 2020. - 432 с.
3. Банк данных угроз безопасности информации [Электронный ресурс] / ФСТЭК России; ФАУ «ГНИИИ ПТЗИ ФСТЭК России». - Дата обновления: 16.03.2023. - URL: <https://bdu.fstec.ru/threat/> (Дата обращения: 16.03.2023).
4. Голиков А. М. Основы информационной безопасности: учебное пособие / А. М. Голиков. – Томск: Томск. гос. ун-т систем упр. и радиотехники, 2007. – 288 с.
5. ГОСТ Р 12.0.010-2009. Системы управления охраной труда. Определение опасностей и оценка рисков : дата введения 2011-01-01. – Москва : Стандартформ, 2011. – 21 с.
6. Кузнецов О. Е. Себестоимость // Большая российская энциклопедия. – Том 29. – Москва, 2015. – С. 588-589.
7. Мозолина Н. В. Предложения по архитектуре средства контроля конфигурации произвольных информационных систем // Вопросы защиты информации. – 2018. – № 2 (121). – С. 14-17.
8. Морозова Н. С. Анализ себестоимости продукции / Н. С. Морозова, Е. Ю. Меркулова // Социально-экономические явления и процессы. – 2016. – Т. 11. – №3. – С. 15-20.
9. Основы криптографии. Контроль целостности данных. Хеш-функции. Имитовставка. ЭЦП : лекция [Электронный ресурс] // Виртуальная среда обучения КНИТУ (КХТИ); Кафедра «Информационная безопасность». – URL: <https://moodle.kstu.ru/mod/page/view.php?id=9359> (Дата обращения: 21.04.2023).

10. Работа фирмы «1С» со стороны. Или статистика выпуска релизов [Электронный ресурс] // INFOSTART.RU. – 2019. – 24 июня. – URL: <https://infostart.ru/1c/articles/1056840/> (Дата обращения: 21.04.2023).
11. Российская Федерация. Законы. Трудовой кодекс Российской Федерации : собрание законодательства Российской Федерации, 2002, № 1, ст. 3. - 16-е изд. - Москва : Ось-89, 2012. - 271, [1] с.
12. СанПиН. Гигиенические требования к микроклимату производственных помещений : дата введения 01-10-1996. – Москва : Стнадартформ, 2013. – 12 с.
13. СНиП. Естественное и искусственное освещение : дата введения 2017-05-08. – Москва : Стнадартформ, 2017. – 89 с.
14. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (ред. от 21.07.2014) // КонсультантПлюс.
15. 1С:Управление нашей фирмой: [Документация для пользователей] // ООО «1С-Софт». - Доступ: ограниченный. - URL: <https://its.1c.ru/db/unfdoc> (Дата обращения: 16.03.2023).

ПРИЛОЖЕНИЯ

ПРИЛОЖЕНИЕ А

Исходный код системы контроля целостности конфигураций

Общий модуль «ЖИПК_АнализПрикладныхРешений»

#Область ПрограммныйИнтерфейс

// Процедура выполняется при запуске сеанса, производит анализ

// и изменяет состояния ключей аналитики прикладных решений

//

//

Процедура ОбновитьСостоянияКлючейАналитики() Экспорт

УстановитьПривилегированныйРежим(Истина);

СопоставитьРасширенияКонфигурации();

СопоставитьДополнительныеОбработкиИОтчеты();

УстановитьПривилегированныйРежим(Ложь);

КонецПроцедуры // ОбновитьСостоянияКлючейАналитики()

#КонецОбласти

#Область СлужебныеПроцедурыИФункции

Процедура СопоставитьРасширенияКонфигурации()

ТипПрикладногоРешения =
Перечисления.ЖИПК_ТипыПрикладныхРешений.РасширениеКонфигурации;

```
Запрос = Новый Запрос;  
Запрос.Текст = ТекстЗапросаКлючиАналитикиПрикладныхРешений();  
Запрос.УстановитьПараметр("ТипПрикладногоРешения",  
ТипПрикладногоРешения);  
КлючиАналитики = Запрос.Выполнить().Выгрузить();
```

Для Каждого Расширение Из РасширенияКонфигурации.Получить() Цикл

```
ГУИД = Строка(Расширение.УникальныйИдентификатор);
```

```
КлючАналитики = КлючиАналитики.Найти(ГУИД,  
"ИдентификаторРешения");
```

Если КлючАналитики = Неопределено Тогда

```
ДанныеРасширения = Новый Структура;  
ДанныеРасширения.Вставить("Наименование", Расширение.Имя);  
ДанныеРасширения.Вставить("ИдентификаторРешения", ГУИД);  
ДанныеРасширения.Вставить("ТипПрикладногоРешения",  
ТипПрикладногоРешения);  
ДанныеРасширения.Вставить("Отсутствует", Ложь);
```

```
ЖИПК_АнализПрикладныхРешенийСлужебный.ДобавитьНовыйКлючАналитики(  
ДанныеРасширения);
```

Иначе

```
ЖИПК_АнализПрикладныхРешенийСлужебный.СнятьОтметкуОтсутствияРешения  
(КлючАналитики.КлючАналитики);  
КлючиАналитики.Удалить(КлючАналитики);
```

КонецЕсли;

КонецЦикла;

Для Каждого КлючАналитики Из КлючиАналитики Цикл

ЖИПК_АнализПрикладныхРешенийСлужебный.ПометитьОтсутствиеРешения(КлючАналитики.КлючАналитики);

КонецЦикла;

КонецПроцедуры

Процедура СопоставитьДополнительныеОбработкиИОтчеты()

Если Не
ДополнительныеОтчетыИОбработки.ИспользуютсяДополнительныеОтчетыИОбработки()
Тогда

Возврат;

КонецЕсли;

ТипПрикладногоРешения =
Перечисления.ЖИПК_ТипыПрикладныхРешений.ДополнительныеОтчетыОбработки;

Запрос = Новый Запрос;

Запрос.Текст = ТекстЗапросаДополнительныеОтчетыИОбработки();

Дополнительные = Запрос.Выполнить().Выгрузить();

Запрос = Новый Запрос;

Запрос.Текст = ТекстЗапросаКлючиАналитикиПрикладныхРешений();

Запрос.УстановитьПараметр("ТипПрикладногоРешения",
ТипПрикладногоРешения);

КлючиАналитики = Запрос.Выполнить().Выгрузить();

Для Каждого Обработка Из Дополнительные Цикл

ГУИД = Строка(Обработка.Ссылка.УникальныйИдентификатор());

КлючАналитики = КлючиАналитики.Найти(ГУИД,
"ИдентификаторРешения");

Если КлючАналитики = Неопределено Тогда

ДанныеДобавления = Новый Структура;

ДанныеДобавления.Вставить("Наименование",
Обработка.Наименование);

ДанныеДобавления.Вставить("ИдентификаторРешения", ГУИД);

ДанныеДобавления.Вставить("ТипПрикладногоРешения",
ТипПрикладногоРешения);

ДанныеДобавления.Вставить("Отсутствует", Ложь);

ЖИПК_АнализПрикладныхРешенийСлужебный.ДобавитьНовыйКлючАналитики(
ДанныеДобавления);

Иначе

ЖИПК_АнализПрикладныхРешенийСлужебный.СнятьОтметкуОтсутствияРешения
(КлючАналитики.КлючАналитики);

КлючиАналитики.Удалить(КлючАналитики);

КонецЕсли;

КонецЦикла;

Для Каждого КлючАналитики Из КлючиАналитики Цикл

ЖИПК_АнализПрикладныхРешенийСлужебный.ПометитьОтсутствиеРешения(КлючАналитики.КлючАналитики);

КонецЦикла;

КонецПроцедуры

#Область ТекстыЗапросов

функция ТекстЗапросаКлючиАналитикиПрикладныхРешений()

ТекстЗапроса = "ВЫБРАТЬ
 | ЖИПК_КлючиАналитикиПрикладныхРешений.Ссылка КАК
КлючАналитики,
 | ЖИПК_КлючиАналитикиПрикладныхРешений.Наименование КАК
Наименование,
 |
 ЖИПК_КлючиАналитикиПрикладныхРешений.ИдентификаторРешения КАК
ИдентификаторРешения
 |ИЗ
 | Справочник.ЖИПК_КлючиАналитикиПрикладныхРешений КАК
ЖИПК_КлючиАналитикиПрикладныхРешений
 |ГДЕ
 |
 ЖИПК_КлючиАналитикиПрикладныхРешений.ТипПрикладногоРешения =
&ТипПрикладногоРешения";
Возврат ТекстЗапроса;

КонецФункции

Функция ТекстЗапросаДополнительныеОтчетыИОбработки() Экспорт

```
ТекстЗапроса = "ВЫБРАТЬ
                |    ДополнительныеОтчетыИОбработки.Ссылка КАК Ссылка,
                |    ДополнительныеОтчетыИОбработки.ХранилищеОбработки КАК
ХранилищеОбработки,
                |    ДополнительныеОтчетыИОбработки.Наименование КАК
Наименование
                |ИЗ
                |    Справочник.ДополнительныеОтчетыИОбработки КАК
ДополнительныеОтчетыИОбработки";
Возврат ТекстЗапроса;
```

КонецФункции

#КонецОбласти

#КонецОбласти

Общий модуль «ЖИПК_АнализПрикладныхРешенийСлужебный»

#Область СлужебныйПрограммныйИнтерфейс

Процедура ДобавитьНовыйКлючАналитики(СтруктураДобавления) Экспорт

```
ДобКлюч =
Справочники.ЖИПК_КлючиАналитикиПрикладныхРешений.СоздатьЭлемент();
ДобКлюч.Наименование = СтруктураДобавления.Наименование;
ДобКлюч.ИдентификаторРешения =
СтруктураДобавления.ИдентификаторРешения;
```

ДобКлюч.Отсутствует = СтруктураДобавления.Отсутствует;
ДобКлюч.ТипПрикладногоРешения =
СтруктураДобавления.ТипПрикладногоРешения;

Попытка

ДобКлюч.Записать();

Исключение

КонецПопытки;

КонецПроцедуры

Процедура ПометитьОтсутствиеРешения(КлючАналитики) Экспорт

Если ТипЗнч(КлючАналитики) <>
Тип("СправочникСсылка.ЖИПК_КлючиАналитикиПрикладныхРешений") Тогда

Возврат;

КонецЕсли;

ЭлементОбъект = КлючАналитики.ПолучитьОбъект();

ЭлементОбъект.Отсутствует = Истина;

Попытка

ЭлементОбъект.Записать();

Исключение

КонецПопытки;

КонецПроцедуры

Процедура СнятьОтметкуОтсутствияРешения(КлючАналитики) Экспорт

Если ТипЗнч(КлючАналитики) <>
Тип("СправочникСсылка.ЖИПК_КлючиАналитикиПрикладныхРешений") Тогда

Возврат;

КонецЕсли;

Если Не КлючАналитики.Отсутствует Тогда

Возврат;

КонецЕсли;

ЭлементОбъект = КлючАналитики.ПолучитьОбъект();

ЭлементОбъект.Отсутствует = Ложь;

Попытка

ЭлементОбъект.Записать();

Исключение

КонецПопытки;

КонецПроцедуры

#КонецОбласти

Общий модуль «ЖИПК_АнализПрикладныхРешенийВызовСервера»

#Область ПрограммныйИнтерфейс

Процедура ПриЗапускеМодуля() Экспорт

ЖИПК_АнализПрикладныхРешений.ОбновитьСостоянияКлючейАналитики();

КонецПроцедуры

#КонецОбласти

Общий модуль «ЖИПК_АнализПрикладныхРешенийРегл»

#Область ПрограммныйИнтерфейс

Процедура ВыполнитьЗаписьХешСуммыКонфигурации() Экспорт

УстановитьПривилегированныйРежим(Истина);

ЛогинПароль = Константы.ЖИПК_ДанныеСистемногоПользователя.Получить();

ЛогинПароль = СтрРазделить(ЛогинПароль, ";");

Если ЛогинПароль.Количество() <> 2 Тогда

 Возврат;

КонецЕсли;

Логин = ЛогинПароль[0];

Пароль = ЛогинПароль[1];

УстановитьПривилегированныйРежим(Ложь);

ВремПуть = КаталогВременныхФайлов() + "1cv8.cf";

Программа = КаталогПрограммы() + "1cv8";

ФайлПрограммы = Новый Файл(Программа);

Если Не ФайлПрограммы.Существует() Тогда

 Программа = Программа + ".exe";

 Программа = "" + Программа + "";

 ВремПуть = "" + ВремПуть + "";

КонецЕсли;

СтрокаЗапуска = Программа + " DESIGNER";

СтрокаЗапуска = СтрокаЗапуска + " /IBConnectionString "" +
СтрокаСоединенияИнформационнойБазы() + """;

СтрокаЗапуска = СтрокаЗапуска + " /N " + Логин;

СтрокаЗапуска = СтрокаЗапуска + " /P " + Пароль;

СтрокаЗапуска = СтрокаЗапуска + " /DumpDBCfg " + ВремПуть;

Линукс = ОбщегоНазначения.ЭтоLinuxСервер();

Если Линукс Тогда

ТекстЗапуска = "#!/bin/bash" + Символы.ПС;

ПутьСкрипта = КаталогВременныхФайлов() + "Dumpcfg.sh";

ТекстовыйДокумент = Новый ТекстовыйДокумент;

ТекстовыйДокумент.УстановитьТекст(СтрокаЗапуска);

ТекстовыйДокумент.Записать(ПутьСкрипта);

СтрокаЗапуска = "bash " + ПутьСкрипта;

КонецЕсли;

КодОтвета = Неопределено;

ЗапуститьПриложение(СтрокаЗапуска,, Истина, КодОтвета);

ДвоичныеДанные = Новый ДвоичныеДанные(КаталогВременныхФайлов() +
"1cv8.cf");

ХешСумма = Новый ХешированиеДанных(ХешФункция.SHA256);

ХешСумма.Добавить(ДвоичныеДанные);

ХешСумма = ХешСумма.ХешСумма;

КлючАналитики =
Справочники.ЖИПК_КлючиАналитикиПрикладныхРешений.ОсноваяКонфигурация;

Запись =
РегистрыСведений.ЖИПК_РегистрХешСуммПрикладныхРешений.СоздатьМенеджерЗапи
си();

Запись.Период = ТекущаяДатаСеанса();

Запись.ПрикладноеРешение = КлючАналитики;

Запись.ХешСумма = Строка(ХешСумма);

Запись.Записать(Ложь);

КонецПроцедуры

Процедура ВыполнитьЗаписьХешСуммыРасширений() Экспорт

Для Каждого Расширение Из РасширенияКонфигурации.Получить() Цикл

ГУИД = Строка(Расширение.УникальныйИдентификатор);

ХешСумма = Новый ХешированиеДанных(ХешФункция.SHA256);

ХешСумма.Добавить(Расширение.ПолучитьДанные());

ХешСумма = ХешСумма.ХешСумма;

КлючАналитики =

Справочники.ЖИПК_КлючиАналитикиПрикладныхРешений.НайтиПоРеквизиту("ИдентификаторРешения", ГУИД);

Если КлючАналитики =

Справочники.ЖИПК_КлючиАналитикиПрикладныхРешений.ПустаяСсылка() Тогда

ТипПрикладногоРешения =

Перечисления.ЖИПК_ТипыПрикладныхРешений.РасширениеКонфигурации;

СтруктураНового = Новый Структура;

СтруктураНового.Вставить("Наименование", Расширение.Имя);

СтруктураНового.Вставить("ИдентификаторРешения", ГУИД);

СтруктураНового.Вставить("ТипПрикладногоРешения",
ТипПрикладногоРешения);

СтруктураНового.Вставить("Отсутствует", Ложь);

ЖИПК_АнализПрикладныхРешенийСлужебный.ДобавитьНовыйКлючАналитики(
СтруктураНового);

КлючАналитики =
Справочники.ЖИПК_КлючиАналитикиПрикладныхРешений.НайтиПоРеквизиту("ИдентификаторРешения", ГУИД);

КонецЕсли;

Запись =
РегистрыСведений.ЖИПК_РегистрХешСуммПрикладныхРешений.СоздатьМенеджерЗаписи();

Запись.Период = ТекущаяДатаСеанса();

Запись.ПрикладноеРешение = КлючАналитики;

Запись.ХешСумма = Строка(ХешСумма);

Запись.Записать(Ложь);

КонецЦикла;

КонецПроцедуры

Процедура ВыполнитьЗаписьХешСуммыДополнительных() Экспорт

Запрос = Новый Запрос;

Запрос.Текст =
ЖИПК_АнализПрикладныхРешений.ТекстЗапросаДополнительныеОтчетыИОбработки();

Дополнительные = Запрос.Выполнить().Выгрузить();

Для Каждого Стр Из Дополнительные Цикл

ГУИД = Строка(Стр.Ссылка.УникальныйИдентификатор());

КлючАналитики =
Справочники.ЖИПК_КлючиАналитикиПрикладныхРешений.НайтиПоРеквизиту("ИдентификаторРешения", ГУИД);

Если КлючАналитики =
Справочники.ЖИПК_КлючиАналитикиПрикладныхРешений.ПустаяСсылка() Тогда

```

        ТипПрикладногоРешения =
Перечисления.ЖИПК_ТипыПрикладныхРешений.ДополнительныеОтчетыОбработки;

        СтруктураНового = Новый Структура;

        СтруктураНового.Вставить("Наименование", Стр.Наименование);

        СтруктураНового.Вставить("ИдентификаторРешения", ГУИД);

        СтруктураНового.Вставить("ТипПрикладногоРешения",
ТипПрикладногоРешения);

        СтруктураНового.Вставить("Отсутствует", Ложь);

```

```

        ЖИПК_АнализПрикладныхРешенийСлужебный.ДобавитьНовыйКлючАналитики(
СтруктураНового);

```

```

        КлючАналитики =
Справочники.ЖИПК_КлючиАналитикиПрикладныхРешений.НайтиПоРеквизиту("Иденти
фикаторРешения", ГУИД);

```

```

        КонецЕсли;

```

```

        ДвоичныеДанные = Стр.ХранилищеОбработки.Получить();

```

```

        Если ТипЗнч(ДвоичныеДанные) <> Тип("ДвоичныеДанные") Тогда

```

```

            Возврат;

```

```

        КонецЕсли;

```

```

        ХешСумма = Новый ХешированиеДанных(ХешФункция.SHA256);

```

```

        ХешСумма.Добавить(ДвоичныеДанные);

```

```

        ХешСумма = ХешСумма.ХешСумма;

```

```

        Запись =

```

```

РегистрыСведений.ЖИПК_РегистрХешСуммПрикладныхРешений.СоздатьМенеджерЗапи
си();

```

```

        Запись.Период = ТекущаяДатаСеанса();

```

```

        Запись.ПрикладноеРешение = КлючАналитики;

```

```

        Запись.ХешСумма = Строка(ХешСумма);

```

```

        Запись.Записать(Ложь);

```

КонецЦикла;

КонецПроцедуры

#КонецОбласти

Общий модуль «ЖИПК_АнализПрикладныхРешенийРегл»

&После("ВыполнитьОбработкуПоРегламентномуЗаданию")

Процедура ЖИПК_ВыполнитьОбработкуПоРегламентномуЗаданию(ВнешняяОбработка,
ИдентификаторКоманды)

Если ТипЗнч(ИдентификаторКоманды) =
Тип("ПеречислениеСсылка.ЖИПК_РеглЗадание") Тогда

ЖИПК_РеглЗадание.ОбработатьРегламентноеЗадание(ИдентификаторКоманды);

Иначе

ПродолжитьВызов(ВнешняяОбработка, ИдентификаторКоманды);

КонецЕсли;

КонецПроцедуры