«Утверждаю»

_____

«__» «_____» 20__ г.

ДОКУМЕНТИРОВАННАЯ ПРОЦЕДУРА ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ РАЗРАБОТКЕ, ВНЕДРЕНИИ, СОПРОВОЖДЕНИИ И ВНЕСЕНИИ ИЗМЕНЕНИЙ В ИНФОРМАЦИОННЫЕ СИСТЕМЫ

1 Назначение и область применения

1.1 Настоящая документированная процедура устанавливает единые требования по обеспечению информационной безопасности при разработке, внедрении, сопровождении и внесении изменений в информационные системы ТОО ПРИМЕР (далее - компания).

1.2 Настоящая документированная процедура является внутренним нормативным документом компании.

1.3 Требования настоящей документированной процедуры распространяются на структурные подразделения компании и применяются к информационным системам компании, подпадающим в Область Действия или оказывающих влияние на СУИБ.

2 Нормативные ссылки

2.1 В настоящей документированной процедуре приведены ссылки на следующие нормативные документы:

- Процедура «Область действия системы управления информационной безопасностью ТОО ПРИМЕР;
- Общие требования к содержанию, изложению и оформлению внутренних регламентирующих документов компании;
- Управление документацией;
- Управление записями;
- Обеспечение информационной безопасности при взаимодействии с внешними сторонами;
- Управление доступом пользователей;
- Процедура об использовании средств криптографической защиты информации;
- Процедура о носителях информации;
- Обеспечение конфиденциальности данных информационных систем;
- Резервное копирование информации;
- Процедура об управлении непрерывностью деятельности;
- Порядок мониторинга системных событий;
- Порядок оценки и обработки рисков информационной безопасности.

3Термины и определения

3.1 В настоящей документированной процедуре компании применяются термины и соответствующие им определения в соответствии с таблицей 1.

Таблица 1. Термины и определения

Термины	Определения
Продуктивная среда	Действующая информационная система
Среда Разработки	Совокупность программно-технических средств, обеспечивающая возможность разработки программного обеспечения
Тестовая Среда	Информационная система, находящаяся в режиме тестирования и отладки

4 Сокращения и обозначения

4.1 В настоящей документированной процедуре компании применены сокращения и обозначения в соответствии с таблицей 2.

Таблица 2. Сокращения и определения

№ и /п	Сокращения и обозначения	Полное наименование приведенных сокращений и обозначений
1	ИБ	Информационная безопасность
2	ИС	Информационные системы
3	КЦД	Конфиденциальность, целостность, доступность
4	ПО	Программное обеспечение
5	СКЗИ	Средства криптографической защиты информации
6	СУИБ	Система управления информационной безопасностью
7	ТЗ	Техническое задание
8	Компания	ТОО ПРИМЕР
9		
10		
11		

5 Ответственность и полномочия

5.1 Ответственность за разработку настоящей документированной процедуры в соответствии с требованиями документированной процедуры «Общие требования к содержанию, изложению и оформлению внутренних регламентирующих документов компании» несет _____.

5.2 Ответственность за управление настоящей документированной процедурой в соответствии с требованиями документированной процедуры «Управление документацией» несет _____ и ответственное подразделение (лицо) по ИСМ.

6 Требования

Требования СУИБ учитываются и соблюдаются на всех этапах жизненного цикла ИС, а именно:

1) планирование ИС;
2) разработка/приобретение ИС;
3) внедрение ИС;
4) сопровождение ИС;
5) модернизация ИС;
6) вывод ИС из эксплуатации.

6.1 Требования ИБ при планировании ИС

6.1.1 Решение о разработке или приобретении ИС принимается Руководством компании на основании обоснованной и мотивированной заявки руководителя заинтересованного структурного подразделения компании. Заявка на разработку или приобретение ИС содержит:

1) описание процессов, подлежащих автоматизации при помощи ИС;
2) обоснование необходимости автоматизации процессов, а также преимущества и недостатки их автоматизации;
3) виды и уровни конфиденциальности информации, которые планируется обрабатывать или хранить в ИС;
4) риски, возникающие при внедрении ИС, и средства для их снижения до приемлемого уровня.

6.2 Требования ИБ при разработке или приобретении ИС

6.2.1 В случае разработки ИС внешней стороной соблюдаются требования документированной процедуры «Обеспечение информационной безопасности при взаимодействии с внешними сторонами».

6.2.2 Перед разработкой/внедрением ИС заинтересованным структурным подразделением составляется и утверждается в установленном порядке Техническое задание на данную ИС. Техническое задание согласовывается с _____.

6.2.3 В ТЗ на ИС включаются требования ИБ, установленные настоящей документированной процедурой и другие требования СУИБ, относящиеся к используемым в ИС информационным активам.

6.2.4 Разрабатываемая/приобретаемая ИС не должна:

1) создавать уязвимостей или нежелательных зависимостей для других ИС компании;
2) снижать доступность других ИС компании;
3) оказывать отрицательное влияние на процессы компании.

Разрабатываемая/приобретаемая ИС должна:

1) обеспечивать возможность управления доступом к информации и сервисам, включая управление правами, обязанностями и ресурсами, в соответствии с требованиями документированной процедуры «Управление доступом пользователей»;
2) включать средства регистрации событий ИБ в журнале и оповещения администраторов ИБ о значительных событиях в ИС для целей повседневного контроля или специальных расследований;
3) обеспечивать механизмы проверки и обеспечения целостности данных на всех стадиях их обработки;
4) обеспечивать защиту конфиденциальных данных от несанкционированного раскрытия,

в том числе возможность использования СКЗИ, в соответствии с требованиями Процедуры об использовании средств криптографической защиты информации;

5) обеспечивать контроль вывода информации и ее маркирования в соответствии с требованиями документированной процедуры «Обеспечение конфиденциальности данных информационных систем»;

6) обеспечивать возможность резервного копирования данных и состояния ИС в соответствии с требованиями документированной процедуры «Резервное копирование информации»;

7) обеспечивать механизмы восстановления ИС после отказов в соответствии с требованиями Процедуры об управлении непрерывностью деятельности.

6.2.5 В ТЗ на ИС включаются методика и критерии тестирования ИС перед ее вводом в эксплуатацию. Методика тестирования составляется в виде алгоритма действий по проверке, где указаны предмет проверки, состав проверки и допустимые пределы результатов проверки.

6.2.6 Разработка ИС производится в среде разработки, изолированной от Тестовой среды и Продуктивной среды Требования ИБ при приемке и внедрении ИС.

6.2.7 Приемка ИС от Разработчика/Поставщика осуществляется на основании приемо-сдаточных испытаний (тестирования) ИС на предмет:

1) соответствия требованиям ТЗ;

2) производительности и устойчивости к несанкционированным доступам и пиковым нагрузкам;

3) типов разграничения доступа и их реализации;

4) законодательных требований в области лицензирования ПО;

5) взаимодействия с другими ИС включая требования к коммуникационным каналам;

6) используемых СКЗИ;

7) возможности резервирования;

8) методов восстановления при сбоях и наличие плана аварийного восстановления;

9) используемых встроенных и внешних средств обеспечения и управления ИБ.

Не допускается ввод в эксплуатацию ИС, не прошедших тестирование.

6.2.8 Перед началом тестирования ИС проверяется комплектность и содержание требуемых эксплуатационных документов и процедур.

6.2.9 Тестирование ИС выполняется назначенными представителями заинтересованных структурных подразделений компании, координируемых Ответственным Заказчиком или Менеджером ИС, совместно с официальными представителями Разработчика/Поставщика ИС.

6.2.10 Тестирование ИС выполняется в Тестовой среде, логически изолированной от Продуктивной среды. При тестировании используются только тестовые учетные записи и другие данные, не совпадающие с реальными данными, используемыми в Продуктивной среде.

6.2.11 При тестировании ИС необходимо использование реальных данных или информации из продуктивной среды. Для Тестовой среды необходимо обеспечить уровень защищенности, как для Продуктивной среды. После окончания тестирования реальные данные из продуктивной среды удаляются из Тестовой среды.

6.2.12 В Тестовой среде не допускается использование данных, содержащих конфиденциальную информацию.

6.2.13 Процесс и результаты тестирования документируются и подписываются всеми сторонами, принимавшими участие в тестировании.

6.2.14 До введения ИС в эксплуатацию проводится обучение Пользователей и Администраторов ИС по вопросам использования и администрирования ИС.

6.2.15 Решение о вводе ИС в эксплуатацию принимается Руководством компании на основании положительных результатов приемо-сдаточных испытаний (тестирования) ИС.

6.3 Требования ИБ при сопровождении ИС и внесении изменений в ИС

6.3.1 Переведенные в Продуктивную среду ИС не должны содержать исходные коды разработки, тестовые утилиты и другие средства разработки.

6.3.2 Доступ пользователей к ресурсам введенной в эксплуатацию ИС осуществляется с соблюдением требований документированной процедуры «Управление доступом пользователей».

6.3.3 Менеджер ИС проводит регулярный мониторинг и анализ событий ИС в соответствии с требованиями документированной процедуры «Порядок мониторинга системных событий».

6.3.4 Для целей унификации управления изменениями в компании принимается следующая классификация изменений для ИС:

1) *текущие обновления* - обновления, поставляемые разработчиками стандартных компонентов ИС (операционные системы, СУБД, стандартные клиентские приложения);

2) *существенные изменения* - изменения, затрагивающие архитектуру ИС, структуру данных ИС, алгоритмы обработки информации, средства обеспечения ИБ, протоколы и методы связи компонентов ИС; изменения, требующие замены компонентов ИС и иные изменения, которые могут существенно повлиять на КЦД ИС;

3) *срочные изменения* - изменения/обновления, которые устраняют критичные уязвимости или ошибки в ИС, наличие которых создает высокие риски ИБ для данной ИС.

6.3.5 Текущие обновления эксплуатационного программного обеспечения, приложений и программных библиотек выполняют только администраторы, обладающие необходимыми знаниями и квалификацией, с соответствующей санкции Менеджера ИС.

6.3.6 Текущие обновления, вносимые посредством автоматизированных систем обновления, выполняются в автоматическом режиме, в соответствии с политикой автоматического обновления ИС, согласованной и утвержденной Менеджером ИС. Все обновления, вносимые в автоматическом режиме, регистрируются в электронных журналах системы автоматического обновления. При разработке политики автоматического обновления ИС учитываются риски, связанные с таким видом обновления.

6.3.7 Существенные изменения вносятся в ИС только после оценки рисков ИБ, создаваемых этими изменениями, согласно документированной процедуре «Порядок оценки и обработки рисков информационной безопасности», и с санкции Менеджера ИС, согласованной с владельцами ИА, обрабатываемых данной ИС.

6.3.8 Перед внесением в ИС существенных изменений разрабатываются и утверждаются следующие документы:

1) отчет об оценке рисков ИБ в отношении данных изменений;
2) план работ по внесению существенных изменений;
3) план резервного копирования и восстановления ИС в случае сбоев при внесении изменений;
4) если процесс внесения изменений приведет к недоступности ИС, оповещение о недоступности ИС с указанием даты, времени и периода недоступности ИС доводится до сведения заинтересованных лиц не позднее, чем за один рабочий день до начала работ.

6.3.9 Внесение существенных изменений в Продуктивную среду допускается только после проведения тестирования этих изменений в Тестовой среде.

6.3.10 Перед внесением существенных изменений в ИС проводится полное резервное копирование ИС, согласно требованиям документированной процедуры «Резервное копирование информации».

6.3.11 Процесс внесения изменений документируется Менеджером ИС в Журнале изменений ИС по форме, установленной в Приложении 1 к настоящей документированной процедуре, с указанием:

1) даты и времени внесения изменения;
2) Ф.И.О. администратора (-ов) выполняющего (-их) внесение изменения;
3) краткого описания изменения;
4) результатов внесения изменений;
5) для существенных изменений указываются ссылки на наименование и место хранения плана работ и результатов анализа рисков ИБ.

6.4 Требования ИБ ири выводе ИС из эксплуатации

6.4.1 Решение о выводе ИС из эксплуатации принимается Руководством компании на основании обоснованной и мотивированной заявки Менеджера ИС, согласованной с владельцами ИА, обрабатываемых данной ИС.

6.4.2 Перед выводом ИС из эксплуатации проводится полное резервное копирование ИС, согласно требованиям документированной процедуры «Резервное копирование информации».

6.4.3 Все носители информации, входившие в состав выводимой из эксплуатации ИС, подвергаются процедуре уничтожения, содержащейся на них информации, в соответствии с требованиями Процедуры о носителях информации.

6.4.4 При выводе ИС из эксплуатации, все исходные коды ПО, инсталляционные пакеты,

проектная и эксплуатационная документация, резервные копии ИС и другие относящиеся к ИС информационные активы передаются в архив для хранения, с соблюдением требований документированной процедуры «Обеспечение конфиденциальности данных информационных систем».

7 Записи

7.1 В настоящей документированной процедуре формируются следующие записи (таблица 3), которые должны управляться в соответствии с требованиями документированной процедуры «Управление записями».

Таблица 3. Перечень записей

№ п/п	Наименование	Форма записей	Ответственность за ведение записей	Место хранения	Периодичность составления записи
1	Технические задания на разработку ПО	В зависимости от ПО	Ответственные за ПО лица	_____	по мере необходимости
2	Записи о результатах тестирования	В зависимости от ПО	Ответственные за ПО лица		по мере необходимости
3	Записи о выводе ИС из эксплуатации	В зависимости от ПО	Ответственные за ПО лица		по мере необходимости
4	Журнал регистрации изменений ИС	Приложение 1	Ответственные за ПО лица		по мере необходимости

8 Пересмотр, внесение изменений, хранение и рассылка

8.1 Пересмотр (актуализация), внесение изменений, хранение и рассылка настоящей документированной процедуры осуществляется в соответствии с требованиями документированной процедуры «Управление документацией».

8.2 Учтенные бумажные копии настоящей документированной процедуры при необходимости, в заинтересованные структурные подразделения центрального аппарата компании.

8.3 Учтенные бумажные копии с «Контрольного экземпляра» документированной процедуры подразделениями (лицами) по ИСМ филиалов, при необходимости, рассылаются в заинтересованные структурные подразделения компании.

Приложение 1

Форма «Журнал регистрации изменений ИС»

Журнал регистрации изменений ИС

Наименование ИС_____

Ответственное лицо:_____ _____
Ф. И. О. *Должность*

Журнал открыт «____ »_____20 _г.

№№	Дата и время внесения изменения	Администратор, вносивший изменения	Краткое описание изменения	Результат внесения изменения	Сопроводительная документация

Журнал закрыт «____ »_____20 _г.

Сдан в архив «____ »_____20 _г., архивное дело №

Лист регистрации изменений

Номер изменения	Номера страниц	Всего листов в документе	Номера разделов, к которым относятся изменения	Описание изменений	Отметка о внесении изменений		
					Ф.И.О.	Подпись	Дата