«Утверждаю»

_____

«__» «_____» 20__ г.

ДОКУМЕНТИРОВАННАЯ ПРОЦЕДУРА ПОРЯДОК ОЦЕНКИ И ОБРАБОТКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Содержание

1 Назначение и область применения

1.1 Настоящая документированная процедура устанавливает единые требования к порядку оценки и обработки информационных рисков в ТОО «ПРИМЕР» (далее - Компания).

1.2 Требования настоящей документированной процедуры распространяются на структурные подразделения компании, информационные активы которых попадают в Область Действия СМИБ и применяются к порядку оценки и обработки информационных рисков.

2 Нормативные ссылки

2.1 В настоящей документированной процедуре использованы ссылки на следующие нормативные документы

Закон РК	«Об электронном документе и электронной цифровой подписи»;
ISO/IEC 27001:2022	Информационные технологии, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасности. Требования
ISO/IEC 27002:2022	Информационная безопасность, кибербезопасность и защита конфиденциальности. Управление информационной безопасностью
……..	……
……..	……

3 Термины 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
Информационная система	Взаимосвязанная совокупность средств, методов и персонала, используемых для хранения, обработки и выдачи информации для достижения цели управления.
Информационный актив	Информационные ресурсы или средства обработки информации организации.
Информационная безопасность	Процесс обеспечения конфиденциальности, целостности и доступности информации.
Система управления информационной безопасностью	Циклический процесс, включающий в себя сбор и анализ данных о состоянии информационной безопасности в организации, оценку информационных рисков, реализацию и внедрение соответствующих механизмов и методов контроля, а также мониторинг функционирования механизмов контроля

4 Сокращения и обозначения

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

Таблица 2. Сокращения и обозначения

№ п/п	Сокращения и обозначения	**Полное наименование** приведенных сокращений и обозначений
1	ВС	Внешняя сторона
2	ИА	Информационный актив
3	ИБ	Информационная безопасность
4	ПО	Программное обеспечение
5	ЭЦП	Электронная цифровая подпись
11	РИБ	Риски информационной безопасности
13		
14		

5 Ответственность и полномочия

5.1 Ответственность за разработку настоящей документированной процедуры несет ……..

5.2 Ответственность за управление настоящей документированной процедурой несут ……..

5.3 ……..

6 Требования

6.1 Суть процесса оценки и обработки РИБ

6.1.1 Процесс оценки и обработки РИБ состоит из трех этапов: первый этап - определение критичности уязвимостей, второй этап - оценка РИБ, третий этап - принятие решения по обработке РИБ.

6.1.2 Определение критичности уязвимостей, заключается в определении критичности уязвимостей, действующих в отношении ИА компании, входящих в ОД СУИБ, в соответствии с методом, изложенным в разделе 6.5 настоящей документированной процедуры.

6.1.3 Оценка РИБ, заключается в оценке уровня РИБ для каждого ИА компании, входящего в ОД СУИБ. Оценка РИБ каждого ИА производится по трем параметрам: конфиденциальность, целостность и доступность, в соответствии с методом, изложенным в разделе 6.6 настоящей документированной процедуры.

6.1.4 Принятие решения по обработке РИБ, заключается в определении приемлемого уровня РИБ и определении мер, применяемых для обработки данных РИБ.

6.1.5 Процесс оценки и обработки РИБ инициируется и управляется Менеджером РИБ.

6.1.6 Обязанности Менеджера РИБ выполняет Менеджер ИБ. При отсутствии в штате компании Менеджера ИБ обязанности Менеджера РИБ возлагаются на работника ДИТиС или ДРиСМ, которого назначает руководитель соответствующего департамента.

6.2 Определение критичности уязвимостей

6.2.1 Определение критичности уязвимости ИА производится Менеджером РИБ. Менеджер РИБ может привлекать к участию в процессе определения критичности уязвимостей ИА сотрудников ДИТиС, а также сотрудников структурных подразделений, являющихся владельцами ИА.

6.2.2 При определении критичности уязвимостей ИА, относящихся к типам ИА, Менеджер ИБ руководствуется Процедурой об управлении техническими уязвимостями (ПР-70-17).

6.2.3 Результаты определения критичности уязвимостей оформляются в виде перечня ИА с определенными значениями критичности уязвимостей ИА по форме, установленной в Приложении 1 («Отчет об анализе уровня рисков информационной безопасности») с заполнением граф 1-3, 5, 6, 10-17.

6.3 Оценка РИБ

6.3.1 Оценка РИБ производится Менеджером РИБ при содействии владельцев активов. Менеджеру РИБ требуется определить уровень РИБ, действующих в отношении ИА компании, по каждой угрозе и уязвимости, выявленным в отношении данных ИА.

6.3.2 Результаты оценки РИБ оформляются в виде перечня И А с определенными значениями уровня РИБ по форме, установленной в Приложении 1 («Оценка рисков информационной безопасности») с заполнением граф 4, 7-9, 18.

6.4 Принятие решения по обработке РИБ

6.4.1 Приемлемым уровнем РИБ признается такой уровень РИБ, при котором размер вероятного ущерба не оказывает существенного влияния на нормальное функционирование бизнес-процессов компании.

6.4.2 Предложение о приемлемом уровне РИБ формируется и вносится на рассмотрение руководства компании Менеджером РИБ, утверждается руководством компании.

6.4.3 После оценки и определения приемлемого уровня РИБ Менеджеру РИБ требуется проанализировать значения РИБ и определить меры обработки, которые необходимо принять по отношению к данным РИБ.

6.4.4 Менеджер РИБ может привлекать к участию в процессе определения мер обработки РИБ сотрудников структурных подразделений, являющихся владельцами ИА.

6.4.5 Способами обработки риска являются:

- принятие риска;
- снижение риска;
- уклонение от риска;

- передача риска.

6.4.6 Принятие риска осуществляется в том случае, если уровень риска признается приемлемым.

6.4.7 Снижение риска - это выбор и внедрение мер по снижению вероятности нанесения ущерба.

6.4.8 Уклонение от риска - это полное устранение источника риска.

6.4.9 Передача риска - перенесение ответственности за риск на третьи лица (например, поставщику оборудования или страховой компании) без устранения источника риска.

6.4.10 Приемлемый уровень РИБ и перечень мер обработки РИБ оформляются в виде перечня мер по форме, установленной в Приложении 2 («План обработки рисков информационной безопасности»).

6.5 Метод определения критичности уязвимостей ИА

6.5.1 Настоящий метод определяет принципы, правила и методику определения критичности уязвимостей ИА.

6.5.2 Критичность уязвимости информационного актива определяется на основании следующих коэффициентов:

1) **Доступность уязвимости (VS)** - коэффициент, определяющий сложность реализации угрозы с использованием данной уязвимости;

2) **Эффективность защитных мер (СЕ)** - оценочный коэффициент, отражающий степень защищенности ИА от конкретной угрозы, при применении данных защитных мер.

6.5.3 Доступность уязвимости (VS) определяется методом экспертной оценки по 3-х уровневой шкале показателей влияния. При оценке доступности уязвимости для всех типов ИА, кроме ИА типа «Человеческие ресурсы», применяется таблица категорирования 3.

Таблица 3. ^ оступность уязвимости (VS)

Доступность уязвимости (VS)	Описание доступности уязвимости
1	Данный коэффициент присваивается, если применимы все нижеперечисленные условия: • Круг потенциальных злоумышленников ограничен только работниками Общества; • Уязвимость не может быть использована удаленно : • Использование административного уровня доступа; • Недоступность методов использования уязвимости в открытых источниках; • Отсутствие автоматизированных инструментов для использования уязвимости.
2	Данный коэффициент присваивается, если применимо, хотя бы одно из нижеперечисленных условий: • Круг потенциальных злоумышленников ограничен экспертами либо специалистами в данной области; • Уязвимость не может быть использована удаленно); • Для использования уязвимости необходим, как минимум, пользовательский уровень доступа; • Использование административного уровня доступа; • Недоступность методов использования уязвимости в открытых источниках; • Отсутствие автоматизированных инструментов для использования уязвимости.
3	Данный коэффициент присваивается, если применимо, хотя бы одно из нижеперечисленных условий: • Круг злоумышленников неограничен; • Уязвимость может быть использована удаленно; • Для использования уязвимости не требуется специального уровня доступа; • Использование методов использования уязвимости в открытых источниках; • Наличие автоматизированных инструментов для использования уязвимости.

6.5.1 Эффективность защитных мер определяется методом экспертной оценки. При оценке эффективности защитных мер применяются значения пяти типовых критериев, определяемые ответами на соответствующие вопросы. Для оценки эффективности защитных мер для всех типов И А, кроме И А типа «Человеческие ресурсы», применяется таблица категорирования 4.

Таблица 4. Таблица категорирования

Критерий	Вопросы по оценке эффективности защитных мер	Применимость (Да-1, Нет-0)
Ответственность	Установлена ли ответственность за нарушения информационной безопасности данного актива?	0/1
Осведомленность	Внедрены ли механизмы повышения осведомленности работников	0/1
Документированность	Документированы ли процессы, в которых используется актив, и исполняются ли эти документированные процедуры?	0/1
Технологичность	Способны ли применяемые технологии снизить уровень угрозы?	0/1
Уровень аудита	Достаточно ли эффективны применяемые методы аудита, чтобы	0/1
	Эффективность защитных мер (CE):	Сумма

Критичность уязвимости (VL) - совокупность свойств уязвимости в терминах ее доступности, сложности использования и модели злоумышленника, а также степени эффективности применяемых контрмер. Критичность уязвимости вычисляется по формуле:

$$VL = VS + (5 - CE)$$

6.6 Метод оценки РИБ

6.6.1 Базовый уровень РИБ определяется на основании следующих коэффициентов:

1) **Ценность актива (AVc, AVi, AVa)** - ценность информационного актива по отношению к конфиденциальности, целостности и доступности данного актива, определенная на стадии категорирования ИА;

2) **Степень влияния (I)** - степень воздействия реализованной угрозы на информационный актив;

3) **Вероятность (P)** - вероятность реализации угрозы.

Степень влияния определяется методом экспертной оценки по 3-х уровневой шкале показателей влияния. При оценке степени влияния для всех типов ИА, кроме ИА типа «Человеческие ресурсы», применяется таблица категорирования 5.

Таблица 5. Категорирование

Степень влияния (I)	Описание влияния
1	Реализация угрозы: • не оказывает существенного влияния на актив; • не вызывает разглашения конфиденциальной информации; • не вызывает существенных нарушений доступности информационного ресурса; • не может повлечь внесение невосстановимых, либо сложно восстановимых несанкционированных изменений в информационном ресурсе.
2	Реализация угрозы: • оказывает существенное влияние на актив; • может вызвать разглашение информации, предназначенной только для внутреннего использования; • может вызвать существенные перебои в доступности информационного актива; • может повлечь внесение сложно восстановимых несанкционированных изменений.
3	Реализация угрозы: • оказывает критичное влияние на актив; • может вызвать разглашение секретной и конфиденциальной информации; • может вызвать полную недоступность информационного актива; • может вызвать полную утрату актива; • может повлечь внесение невосстановимых несанкционированных изменений.

6.6.2 При оценке степени влияния для ИА типа «Человеческие ресурсы», применяется таблица категорирования 6.

Таблица 6. Категорирование

Степень влияния (1)	Описание влияния
1	Реализация угрозы может повлечь недоступность работника не более 1 рабочего дня.
2	Реализация угрозы может повлечь недоступность работника не более 3 рабочих дней.
3	Реализация угрозы может повлечь недоступность работника более 3 рабочих дней.

6.6.1 Вероятность рассчитывается на основании статистической информации по инцидентам, связанным с данной уязвимостью, за предыдущий аналитический период. При оценке применяется относительная 3-х уровневая шкала вероятности. При оценке вероятности для всех типов ИА, кроме ИА типа «Человеческие ресурсы», применяется таблица категорирования 7.

Таблица 7. Категорирование

Вероятность (P)	Описание вероятности
1	В течение предыдущего аналитического периода не было зафиксировано инцидентов информационной безопасности, связанных с данной уязвимостью.
2	В течение предыдущего аналитического периода был зафиксирован однократный инцидент информационной безопасности, связанный с данной уязвимостью, в рамках Общества, либо подобные инциденты неоднократно были зафиксированы в аналогичных предприятиях отрасли.
3	В течение предыдущего аналитического периода были неоднократно зафиксированы инциденты информационной безопасности, связанные с данной уязвимостью.

Вероятность для ИА типа «Человеческие ресурсы» рассчитывается на основании соотношения времени отсутствия сотрудника на рабочем месте к общему рабочему времени за аналитический период. При оценке вероятности применяется относительная 3-х уровневая шкала уровней вероятности в соответствии с таблицей категорирования 8.

Таблица 8. Таблица категорирования

Вероятность (P)	Описание вероятности
1	Работник отсутствовал от 0 % до 15 % от общего рабочего времени
2	Работник отсутствовал от 16 % до 30 % от общего рабочего времени
3	Работник отсутствовал свыше 30 % от общего рабочего времени

6.6.1 **Базовый уровень РИБ (BR)** - это уровень РИБ, обусловленный свойствами актива, его ценностью для бизнеса, объективными свойствами угроз и уязвимостей, статистикой инцидентов. Базовый уровень РИБ не имеет прямой зависти от применяемых мер по обработке РИБ.

Базовый уровень РИБ для каждой угрозы каждого информационного актива рассчитывается по формуле:

$$BR = A\ V(c,i,a)\ *1*P$$

Базовый уровень РИБ подлежит переоценке не реже 1 раза в год. Переоценка базового уровня РИБ производится периодически, в порядке, установленном настоящей процедурой.

Текущий уровень РИБ (R) − это уровень РИБ, обусловленный базовым уровнем РИБ, текущим уровнем развития информационных технологий и эффективностью мер, применяемых компании для снижения РИБ. Внедряемые компанией меры по снижению РИБ оказывают прямое воздействие на текущий уровень РИБ.

Текущий уровень РИБ для каждой уязвимости каждого информационного актива рассчитывается по формуле:

$$R = (BR*VL)/216*100$$

Значение текущего уровня РИБ (R) округляется в большую сторону до ближайшего целого числа.

Примечание: в настоящем методе оценки РИБ уровни рисков считаются по 216-уровневой шкале, однако, для удобства анализа рисков итоговые значения рисков приводятся к более удобной и наглядной 100-бальной шкале.

7 Записи

В таблице 9 приведены записи, которые формируются в настоящей документированной процедуре и должны управляться в соответствии с требованиями документированной процедуры компании «Управление записями».

Таблица 9. Перечень записей

№ п/п	Наименование	Форма записей	Ответственность за ведение записей	Место хранения	Периодичность составления записи
1	Оценка рисков информационной безопасности	Приложение 1	Ответственные за ПО лица		По мере необходимости
2	Отчет "План обработки рисков информационной безопасности"	Приложение 2	Ответственные за ПО лица		По мере необходимости

8 Пересмотр, внесение изменений, хранение и рассылка

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

8.2 «Оригинал» в бумажном виде настоящей документированной процедуры оформляется и хранится …… компании. «Контрольные экземпляры» настоящей документированной процедуры в бумажном виде оформляются и хранятся ответственными подразделениями (лицами).

8.3 Сканированная версия настоящей документированной процедуры размещается на Интранет-портале компании (……).

8.4 Учтенные бумажные копии настоящей документированной процедуры при необходимости, рассылаются во все структурные подразделения центрального аппарата компании.

8.5 Учтенные бумажные копии с «Контрольного экземпляра» настоящей документированной процедуры ответственными подразделениями (лицами), при необходимости, рассылаются во все структурные подразделения компании.

Приложение 1
Форма "Оценка рисков информационной безопасности"

Опенка рисков информационном безопасности

Дата составления отчета:	Качественная шкала рисков		
Ответственное лицо: /	Пределы базового риска	Пределы текущего риска	Уровень
	0- 8	0- 15	Низкий
	9- 17	16-40	Средний
подпись фамилия, инициалы Исполнитель: /	18- 27	41 - 100	Нысокии

№ п/п	Наименование информационного актива	Уровень ценности		Идентифицированные угрозы	Существующие уязвимости	Степень влияния	Степень вероятности	Базовый уровень риска	Эффективность защитных мер						Доступность уязвимости	Критичность уязвимости	Текущий уровень риска
									Ответственность	Осведомленность	Документированность	Технологичность	Уровень аудита	Эффективность защитных мер			
	Тип актива	КЦД	$ЦА_{КЦД}$			I	P	BR						CE	VS	VL	R
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1		К															
		Ц															
		Д															
2		К															
		Ц															
		Д															

Приложение 2
Форма отчета "План обработки рисков информационной безопасности"

ОТЧЕТ
"План обработки рисков информационной безопасности"

Дата составления отчета: _____

Ответственное лицо: _____
подпись фамилия, инициалы

Исполнитель: _____
подпись фамилия, инициалы

Качественная шкала рисков		
Пределы базового риска	Пределы текущего,	Уровень
0-	0-	Низкий
1 -	1 -	Средний
1 - 27	1 - 100	

№ п/п	Наименование информационного актива	Идентифицированные угрозы	Существующие уязвимости	До прим мер			Меры по снижению риска	После применения мер.									
				<Базовый уровень риска	Критичность уязвимости	Текущий уровень риска		Эффективность защитных мер						Доступность уязвимости	Критичность уязвимрсти	Остаточный уровень риска	Действие по остаточному риску
	Тип актива			**BR**	**VL**	**R**		Ответственность	Осведомленность	Документированность	Технологичность	Уровень аудита	Эффективность принятых мер				
													CE1	VS1	VL1	R1	
I	2	3	*4*	5	6	7	8	9	10	11	12	13	14	1S	16	17	18
1																	
2																	

Лист регистрации изменений

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

Лист ознакомления

№ п	Ф. И. О.	Должность	Дата	Подпись
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				
24				
25				
26				
27				
28				
29				
30				