Приложение 2
к Порядку проведения антикоррупционного
мониторинга и внутреннего анализа
коррупционных рисков в АО «Усть-
Каменогорские тепловые сети»

Аналитическая справка по итогам внутреннего анализа коррупционных рисков в службе информационных технологий АО «Усть-Каменогорские тепловые сети»

1. Предмет аналитической справки: внутренний анализ коррупционных рисков.
1.2. Основание для проведения коррупционных рисков: приказ № 250 от 22.04.2022г. «О проведении внутреннего анализа коррупционных рисков в службе информационных технологий АО «Усть-Каменогорские тепловые сети».
1.3. Объект проведения внутреннего анализа коррупционных рисков: служба информационных технологий (далее – СИТ).
1.4. Направление внутреннего анализа коррупционных рисков: выявление коррупционных рисков организационно-управленческой деятельности СИТ.
1.5. Период проведения внутреннего анализа коррупционных рисков: 22.04.2022 года – 13.07.2022 года.

2. Информационно-аналитическая часть.

Антикоррупционному анализу были подвергнуты следующие направления:
1) Управление персоналом, в т.ч. анализ сменяемости кадров;
2) Нарушение принятых антикоррупционных запретов;
3) Анализ системы управления рисками.

Целью внутреннего анализа деятельности СИТ является изучение и выявление возникновения причин и условий, способствующих совершению коррупционных правонарушений

Анализируемый период: 1-е полугодие 2022 года.

Анализ сменяемости кадров.
Штатная численность СИТ:
Начальник СИТ – 1 единица;
Системный администратор – 1 единица;
Инженер-электроник – 4 единицы;
Техник – 3 единицы;
Ведущий инженер-программист – 1 единица;
Инженер-программист – 4 единицы;
Веб-мастер – 1 единица;
Инженер по сопровождению программных комплексов – 1 единица;
Старший оператор ЭВМ - 1 единица;
Оператор ЭВМ -1 единица ;
Техник геоинформационной системы – 2 единицы.

ИТОГО: 20 человек.
Уволенных сотрудников по отрицательным мотивам не было.
За 1-е полугодие 2022 года работники СИТ к дисциплинарной, административной либо уголовной ответственности - не привлекались.
Устранение фактов принятия на работу лиц, ранее совершивших коррупционное нарушение, осуществляется путем истребования от кандидата справки Службой управления персоналом АО УК ТС.
Служба ИТ укомплектована согласно штатного расписания.

Нарушение принятых антикоррупционных запретов.

Рабочей группой при анализе антикоррупционных рисков фактов не выявлено:

- аффилированности при занятии должностей близкими родственниками, находящихся в непосредственной подчиненности;
- использование служебной и иной информации, не подлежащей официальному распространению;
- принятия материального вознаграждения, подарков или услуг за действия (бездействие) в пользу лиц, их предоставивших.

Также не выявлено нарушений принятых антикоррупционных ограничений и запретов.

Анализ системы управления коррупционными рисками

Система управления коррупционными рисками в сфере ИТ позволяет выявить, контролировать, минимизировать или полностью исключить воздействие коррупционных событий.

Управление коррупционными рисками - это процесс, который позволяет ИТ-структуре сбалансировать операционные и экономические затраты на защитные меры и добиться минимизации возникновения или воздействия риска.

Основные этапы системы управления коррупционными рисками с учетом особенностей ИТ-сферы:

1) Идентификация рисков:
- выявление критических точек;
- составление коррупционных схем;
- определение роли сотрудника в схеме;
- ранжирование рисков по степени значимости;
- формирование карты коррупционных рисков подразделения

2) Анализ и оценка риска:
- анализ управленческих процессов;
- определение круга вовлеченных лиц;
- анализ коррупционных факторов;
- анализ возможных коррупционных правонарушений;
- оценка вероятности реализации риска;
- оценка возможного ущерба;
- оценка значимости риска.

3) Действия по отношению к рискам:

- детальная регламентация управленческих процессов в критических точках;

- автоматизация процессов в критических точках;

- сведение к минимуму ситуаций «единоличного» принятия решений по распределению выгоды;

- исключение совмещения функций по исполнению решения и контролю за его исполнением;

- совершенствование механизма формирования комиссий, рабочих групп, принимающих управленческие решения;

- совершенствование механизмов выявления конфликта интересов;

4) Мониторинг.

В концепции антикоррупционной политики Республики Казахстан на 2022-2026 годы в системе противодействия коррупции основополагающим звеном определено выявление и минимизация коррупционных рисков, условий и причин сопутствующих их возникновению. В этой связи, в целях исключения причин и условий коррупции в государственном и частном секторе Законом РК «О противодействии коррупции» предусмотрен такой инструмент превенции как анализ коррупционных рисков.

Выявление коррупционных рисков в деятельности СИТ: СИТ является структурным подразделением Акционерного общества «Усть-Каменогорские тепловые сети» и подчиняется непосредственно финансовому директору. СИТ в своей деятельности руководствуется Постановлением Правительства Республики Казахстан «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности», Стандартами Республики Казахстан «Информационные технологии. Интернет-ресурс, интернет-портал, интернет-портал. Общие описания», Законом Республики Казахстан «Об информатизации», иными нормативными правовыми актами Республики Казахстан, Уставом Общества, приказами, письменными и устными распоряжениями финансового директора.

Основной целью СИТ является создание, сопровождение и развитие электронных информационных ресурсов, программного обеспечения, Интернет-ресурсов и информационно-коммуникационной инфраструктуры, а также обеспечения информационной безопасности на Предприятии.

Основные задачи СИТ:

1) Разработка и реализация концепции развития инфраструктуры информационных систем и прочих программных продуктов, поддержание высокого информационного потенциала Предприятия.

2) Обеспечение бесперебойного функционирования существующих информационных систем, программно-аппаратных комплексов, вычислительной техники, периферийного оборудования, копировально-множительной техники в структурных подразделениях предприятия.

3) Обеспечение требуемого уровня информационной безопасности.

4) Обеспечение квалифицированной обработки информации, технической помощи и организационно – методического руководства в применении программных комплексов, вычислительной техники, сетевого оборудования,

программного обеспечения, периферийного оборудования, копировально-множительной техники.

5) Разработка предложений о приоритетных направлениях развития в сфере информатизации.

6) Проведение работ по оптимизации использования информационно-технических ресурсов с целью максимальной эффективности их эксплуатации.

7) Участие в подготовке проектов договоров на оказание комплекса услуг разработки, администрирования и технического сопровождения инфраструктуры информационных систем предприятия.

8) Обеспечение процессов управления инфраструктурой информационных систем с целью своевременного и качественного предоставления ИТ услуг.

9) Разработка и внедрение новых информационных систем и технологий согласно плану развития, оптимизация и модернизация существующих программных продуктов и ИТ услуг.

10) Поддержание в рабочем состоянии собственными силами, либо силами подрядчиков, и разработка планов по усовершенствованию систем служебной и технологической связи.

Основные функции СИТ:

1) Анализ и обработка потоков данных на всех стадиях производственных процессов и подготовка предложений по автоматизации обработки информации.

2) Разработка и сопровождение прикладного программного обеспечения в соответствии с утвержденными планами, построение архитектуры программных систем, определение технических и программных требований к ПО.

3) Подготовка спецификаций для закупки программного и аппаратного обеспечения.

4) Установка, настройка, техническое сопровождение и обслуживание средств вычислительной техники и сетей.

5) Анализ поступающей информации о сбоях в работе ПО, связанных с ошибками в ПО, и принятие мер к их оперативному устранению.

6) Диагностика и устранение неисправностей вычислительной, офисной техники и средств служебной связи.

7) Обеспечение рационального использования материальных, финансовых и трудовых ресурсов.

8) Координация работ с поставщиками и производителями вычислительной и офисной техники по вопросам гарантийного обслуживания и ремонта.

9) Координация работ с подрядчиками и субподрядчиками – производителями программного обеспечения по вопросам приобретения, обновления и модификации.

10) Прогнозирование перспективных направлений деятельности в сфере IT-технологий и определение текущей потребности в ресурсах по ее осуществлению, источниках их формирования.

11) Анализ потребностей подразделений Предприятия в дополнительных средствах вычислительной техники и обработки информации.

Риски при создании, сопровождении и развитии электронных информационных ресурсов, программного обеспечения, Интернет-ресурсов и информационно-коммуникационной инфраструктуры, а также обеспечения информационной безопасности:

1) Попытка несанкционированного доступа к информационным ресурсам.

2) Использование в личных или групповых интересах информации, полученной при выполнении должностных обязанностей, если такая информация не подлежит официальному распространению.

3) Умышленное нарушение порядка резервного копирования информации.

4) Порча или изменение состава хранимых резервных копий.

5) Умышленное изменение требований к ИС и ПО, с целью нарушения алгоритма действия процессов и процедур.

6) Значительный рост затрат на ИТ, как капитальных, так и операционных.

7) Установка оборудование привилегированном сотрудникам.

8) Использование ЭЦП при подписании документов.

9) Получение доступа к интернет-порталам под чужими регистрационными данными.

10) Закуп по нерыночным ценам.

11) Завышение объема работ, услуг, условий по сравнению с предложенными ценами.

Предотвращение рисков при организации работы в области информационных технологий:

1) Для неправомерного доступа к информационным ресурсам с целью ее использования или порчи предусмотрены следующие мероприятия:

– распределение прав доступа к ИС и авторизация в соответствии с должностными обязанностями

– аутентификация пользователей средствами операционной системы

– контроль допуска к информации для пользователей разных уровней;

– обнаружение и регистрация попыток НСД, принятие мер для блокировки источника;

– контроль работоспособности используемых систем защиты информации;

– обеспечение безопасности во время профилактических или ремонтных работ.

2) Для предотвращения умышленного нарушения порядка резервного копирования предусмотрены следующие мероприятия:

– соблюдение и контроль процедур регламента резервного копирования;

– автоматизация процесса резервного копирования средствами программно-аппаратного комплекса;

– контроль восстановления резервных копий и условий их хранения.

3) Для избежание умышленного изменения требований к информационным системам предусмотрены следующие мероприятия:

– Контроль и выполнение всех планов и процедур, связанных с получением достоверной информации о текущем состоянии проекта

– Контроль реализации требований на всех этапах выполнения проекта

– Проработка и согласование с участниками проекта всех этапов разработки проекта, контрольных точек, требуемых ресурсов

– Проведение приемочных испытаний на соответствие техническому заданию в соответствии с программой и методикой приёмочных испытаний

– Распределение прав, обязанностей и ответственности между участниками процесса разработки

4) Во избежание значительных затрат на ИТ предусмотрены следующие мероприятия:

– Контроль расходных статей бюджета на ИТ

– Объективная оценка сметы ИТ-проекта

– Критическая оценка состояния ИТ-инфраструктуры руководством и внешними экспертами

– Создание условий полной нетерпимости к злоупотреблениям в сфере ИТ

5) Для исключения случаев установки оборудование привилегированном сотрудникам предусмотрены следующие мероприятия:

– Утвержденный план-график установки, перемещения, замены офисной техники, контроль исполнения

– Контроль списания офисной техники и комплектующих

6) Для предотвращения несанкционированного использования ЭЦП предусмотрены следующие мероприятия:

– Организация порядка получения ключевой информации, контроль выполнения процедуры

– Организация условий хранения и доступа к ключевой информации

– Разграничение ответственности за получение, хранение и использование ключевой информации.

3. Заключительная часть.

За анализируемый период не выявлены факты наличия конфликта интересов, не выявлено нарушений принятых антикоррупционных ограничений и запретов. По результатам проведенного анализа не установлено положений, способствующих принятию решений должностными лицами СИТ по своему усмотрению, способствующих созданию барьеров при реализации физическими и юридическими лицами своих прав и законных интересов, правовых пробелов, создающих возможность произвольного толкования нормативных правовых актов. Наличие дискреционных полномочий и норм не установлено.

Рекомендации по устранению выявленных коррупционных рисков: продолжать работу по превенции коррупции. Отслеживать соблюдение работниками СИТ Политики противодействия коррупции в АО УК ТС, устранять факты конфликта интересов.

Начальник СИТ **А.Грохотов**

ВИЗЫ:

Секретарь Усть-Каменогорского городского маслихата А.А. Светаш

Системный администратор В.В. Виттих