«УТВЕРЖДАЮ»
Председатель правления компании
_____ А.Ж. Раматов

«14» февраля 2012 г.

ПОЛОЖЕНИЕ
об управлении обеспечения информационной безопасности и информационного развития компании

1. Общие положения

1.1. Управление обеспечения информационной безопасности и информационного развития (далее Управление) является самостоятельным структурным подразделением компании.

1.2. Управление создано на основании приказа № 52-Н от 30 января 2012 года.

1.3. Управление находится в непосредственном подчинении заместителя председателя правления компании.

1.4. Управление возглавляет начальник, назначаемый на должность приказом председателя Правления компании.

1.5. Управление в своей деятельности руководствуется действующим законодательством Республики Узбекистан, инструкциями, нормативными документами и распоряжениями компании, а также Уставом ГАЖК «Узбекистон темир йуллари» и настоящим Положением.

1.6. Положение, структура и штатное расписание Управления утверждается председателем правления ГАЖК «Узбекистон темир йуллари». Управление в своем составе имеет 2 отдела:

– отдел обеспечения информационной безопасности;

– отдел развития информационно-коммуникационных технологий.

1.7. На период отсутствия начальника Управления руководство Управлением осуществляется заместителем начальника Управления – начальником отдела обеспечения информационной безопасности.

1.6. Условный шифр Управления – НИБ.

2. Задачи Управления

2.1. Разработка и реализация концепций и программ развития информационных технологий в отраслях компании.

2.2. Реализация Концепции создания системы обеспечения информационной безопасности (СОИБ) компании;

2.3. Определение целей и постановка задач по созданию информационных технологий, отвечающих требованиям комплексной защиты информации;

2.4. Разработка нормативно-распорядительных документов по обеспечению функционирования СОИБ;

2.5. Организация подготовки специалистов по внедрению информационных технологий и информационной безопасности в предприятиях компании.

2.6. Контроль и оценка эффективности принятых мер и применяемых средств защиты информации.

2.7. Координация работ по разработке и внедрению современных информационно-коммуникационных технологий, а также внедрению средств вычислительной техники.

2.8. Координация деятельности структурных подразделений компании по вопросам информационной безопасности и информационно-коммуникационных технологий.

3. Функции Управления

3.1. Разработка и реализация мероприятий по внедрению информационно-коммуникационных технологий в предприятиях компании.

3.2. Разработка технических заданий на проектирования, построение и модернизацию сетей передачи данных.

3.3. Модернизация автоматизированных программно-технологических информационно-коммуникационных систем компании.

3.4. Организация и мониторинг реализации инвестиционных проектов по внедрению ИКТ.

3.5. Обеспечение сертификации и лицензирования внедряемого программно-технологического обеспечения систем АСУ.

3.6. Разработка организационных и технических мероприятий по комплексной защите информации.

3.7. Организация и координация выполнения проектов по защите информации, внедрения технических средств контроля.

3.8. Разработка технических заданий на выполняемые исследования и разработки по защите информации.

3.9. Контроль соблюдения, нормативных требований по обеспечению информационной безопасности.

3.10. Согласование проектной и другой технической документации в части выполнения требований по защите информации.

3.11. Контроль выполнения предусмотренных мероприятий, анализ материалов контроля, выявление нарушений.

3.12. Разработка и реализация мер по устранению выявленных недостатков по защите информации.

3.13. Организация проведения аттестации объектов, помещений, технических средств, программ на предмет соответствия требованиям защиты информации.

3.14. Разработка регламента санкционированного допуска сотрудников к отдельным каналам информации, плана защиты информации, положений об определении степени защищенности ресурсов информационных систем.

3.15. Координация работ по вопросам реализации и внедрения научно-исследовательских и опытно-конструкторских разработок (НИОКР) в области информационно-коммуникационных технологий.

3.16. Участие в разработке и согласовании технических заданий на разработку НИОКР в области информационно-коммуникационных технологий.

3.17. Подготовка материалов для работников компании, участвующих в заседаниях Совета по железнодорожному транспорту, а также комиссий и рабочих групп в рамках ЦСЖТ по курируемым вопросам.

3.18. Совместно с причастными подразделениями компании обеспечение подготовки материалов к заседаниям Комиссии специалистов по информатизации железнодорожного транспорта.

3.19. Организация, проведение и участие совместно с причастными управлениями, центрами и предприятиями компании конференций, совещаний, семинаров, школ передового опыта и выставок по курируемым вопросам.

3.20. Участие и подготовка материалов для проведения заседаний Научно-технического совета компании по курируемым вопросам.

3.21. Своевременное рассмотрение и принятие решений по письмам, жалобам, заявлениям и предложениям граждан.

3.22. Подготовка материалов для рассмотрения на правлениях компании по вопросам, относящимся к компетенции управления.

3.23. Обеспечение режима секретности и своевременное осуществление мероприятий по защите секретных и служебных сведений от разглашения.

3.24. Составление и представление в установленном порядке отчетности.

3.25. Ведение делопроизводства в соответствии с установленным порядком.

3.26. Обеспечение соблюдения техники безопасности, правил и норм охраны труда.

4. Права Управления

Начальник Управления, начальники отделов и сотрудники Управления имеют право:

4.1. Осуществлять контроль за деятельностью структурных подразделений предприятия по выполнению ими требований информационной безопасности.

4.2. Давать структурным подразделениям компании и отдельным специалистам обязательные для исполнения указания по вопросам, входящим в компетенцию Управления.

4.3. Запрашивать и получать от структурных подразделений сведения, справочные и другие материалы, необходимые для осуществления деятельности Управления.

4.4. Представлять в установленном порядке компанию в органах государственной власти, иных учреждениях и организациях, по вопросам, входящим в компетенцию Управления.

4.5. Принимать меры при обнаружении несанкционированного доступа к информации как внутри предприятий компании, так и извне и докладывать о принятых мерах с представлением информации о субъектах, нарушивших режим доступа.

4.6. По согласованию с руководством компании привлекать экспертов и специалистов в сфере защиты информации для консультаций, подготовки заключений, рекомендаций и предложений.

5. Взаимодействие Управления с подразделениями компании

Для выполнения функций предусмотренных настоящим Положением, Управление взаимодействует:

5.1. С Управлением стратегического развития по вопросам:

– разработки программ и мероприятий по созданию системы СОИБ;

– проведения Научно-технических советов по вопросам внедрения СОИБ;

– организации научно-исследовательских работ по защите информации;

– предоставления отчетов и материалов в вышестоящие органы государственного управления республики.

5.2. Со Специальной службой по вопросам:

– принятия руководителями компании решений о допуске работника к сведениям, составляющим государственную или коммерческую тайну;

– разработки памяток работникам предприятия компании о сохранении коммерческой тайны предприятия для согласования и выдачи работникам предприятий.

5.3. С Юридическим Управлением по вопросам:

– проверки соответствия закону ограничений, принимаемых отделом по защите информации;

– разработки порядка привлечения к ответственности работников и сторонних лиц, виновных в разглашении сведений, являющихся коммерческой и служебной тайной, утечке информации, повреждении информационных баз компании;

5.4. С остальными структурными подразделениями и предприятиями компании по вопросам:

– получения сведений об особенностях используемых и разрабатываемых информационных технологий, подлежащих защите;

– составления списков сотрудников, выполняющих работы, связанные с использованием информации, являющейся коммерческой или государственной тайной;

– составления отчетов о порядке и состоянии организации защиты информации;

– предоставления данных о защищенности информационных баз от несанкционированного доступа;

– оценки ответственных сотрудников подразделений знаний в области информационной безопасности и ИКТ.

6. Ответственность начальника Управления и начальников отделов

Начальник Управления несет персональную ответственность за:

6.1. Несвоевременное, а также некачественное выполнение планов работ, исполнение документов и распоряжений руководства компании.

6.2. Допущения использования информации сотрудниками Управления в неслужебных целях.

6.3. Ненадлежащего контроля режима доступа к информации, повлекшего утечку информации.

6.4. Несоблюдения трудового распорядка и требований по охране труда сотрудниками Управления.

7. Ответственность сотрудников Управления

В соответствие с должностными инструкциями сотрудники Управления несут ответственность за:

7.1. Необеспечение сохранности принимаемой и передаваемой информации.

7.2. Необеспечение сохранности программных и технических средств защиты информации.

7.3. Некачественное выполнение работ и распоряжений руководства компании.

7.4. Нарушение трудовой дисциплины, требований противопожарной безопасности.

5. Действие положения

Настоящее Положение вступает в силу с момента его утверждения председателем правления компании и действует на весь срок функционирования Управления.

Начальник Управления обеспечения информационной безопасности и информационного развития компании **Р.Р. Рахманбердыев**

Согласовано:

НЗК Садыков Ш.М.