УТВЕРЖДАЮ
Председатель правления
АО "Алмалыкский ГМК"
Хурсанов А.Х.
«11» марта 2021 г.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АО «АЛМАЛЫКСКИЙ ГОРНО-МЕТАЛЛУРГИЧЕСКИЙ КОМБИНАТ»

Алмалык – 2021 г.

Содержание

1. ВВЕДЕНИЕ

Акционерное общество «АЛМАЛЫКСКИЙ ГОРНО-МЕТАЛЛУРГИЧЕСКИЙ КОМБИНАТ» (далее - Комбинат) является одним из крупнейших промышленных предприятий и флагманом цветной металлургии Республики Узбекистан. Введен в строй в 1949 году.

Сегодня АО «Алмалыкский ГМК» представляет собой сложный промышленный комплекс по добыче и переработке руд благородных и цветных металлов, состоящий из 46 структурных подразделений, включая шесть рудников, пять обогатительных комплексов, три металлургических завода, Ангренский трубный завод, Джизакский и Шерабадский цементные заводы, собственную транспортную инфраструктуру, а также вспомогательное производство и предприятия соцкультбыта.

Комплекс мер по информационной безопасности (ИБ) защищает информацию (данные) от широкого спектра угроз с целью обеспечения непрерывности и надёжности работы информационных систем и ресурсов, прогнозирования и предотвращения воздействия угроз, поддержания деловой репутации и соблюдения требований законодательства.

ИБ рассматривает информацию с позиций конфиденциальности, целостности и доступности, достигается путём внедрения приемлемого набора мер и механизмов, который может включать политики, практики, процедуры и организационные структуры. Все эти меры необходимы для достижения конкретных задач в области обеспечения ИБ.

Политика информационной безопасности Комбината по защите информационных систем и ресурсов, служит основой для принятия соответствующих документов по управлению безопасностью и предполагает построение системы управления информационной безопасности.

Настоящая Политика согласована с Министерством по развитию информационных технологий и коммуникаций Республики Узбекистан (письмо № 27-8/3766 от «03» июля 2020 года) и Службой государственной безопасности Республики Узбекистан (письмо № 13/1069 от «28» октября 2020 года).

2. НОРМАТИВНЫЕ ССЫЛКИ

Политика ИБ Комбината разработана в соответствии с нижеследующими нормативными документами по обеспечению информационной безопасности Республики Узбекистан:

Закон Республики Узбекистан от 11 декабря 2003 года № 560-II «Об информатизации»;

Закон Республики Узбекистан от 11 декабря 2003 года № 562–II «Об электронной цифровой подписи»;

Закон Республики Узбекистан от 29 апреля 2004 года № 611-II «Об электронном документообороте»;

Закон Республики Узбекистан от 11 сентября 2014 года № 374 «О коммерческой тайне»;

Закон Республики Узбекистан от 9 декабря 2015 года № 395 «Об электронном правительстве»;

Закон Республики Узбекистан № ЗРУ-547 от 2 июля 2019 года «О персональных данных»;

Постановление Кабинета Министров Республики Узбекистан от 26 марта 1999 года № 137 «Об утверждении Положения о порядке подготовки и распространения информационных ресурсов Республики Узбекистан на сети передачи данных, включая Интернет»;

Постановление Кабинета Министров Республики Узбекистан от 22 ноября 2005 года № 256 «О совершенствовании нормативно-правовой базы в сфере информатизации»;

Постановление Президента Республики Узбекистан от 3 апреля 2007 года № ПП-614 «О мерах по организации криптографической защиты информации в Республике Узбекистан»;

Постановление Кабинета Министров Республики Узбекистан от 21 ноября 2007 года № 242 «Об утверждении Положения о лицензировании деятельности по проектированию, разработке, производству, реализации, ремонту и использованию средств криптографической защиты информации»;

Постановление Кабинета Министров Республики Узбекистан от 4 мая 2011 года № 126 «О мерах по внедрению и использованию единой защищённой электронной почты и системы электронного документооборота в исполнительном аппарате Кабинета Министров, органах государственного и хозяйственного управления, государственной власти на местах»;

Постановление Президента Республики Узбекистан от 8 июля 2011 года № ПП-1572 «О дополнительных мерах по защите национальных информационных ресурсов»;

Постановление Кабинета Министров Республики Узбекистан от 14 июня 2013 года № 170 «О дополнительных мерах по дальнейшему совершенствованию системы аттестации объектов информатизации»;

Поручение Премьер-министра Республики Узбекистан № 08/1-438 от 19.07.2013 года (ДСП 101/1);

Постановление Кабинета Министров Республики Узбекистан от 16 октября 2015 года №295 «Об утверждении Положения о порядке организации и обеспечения безопасности конфиденциальной информации на объектах информатизации Республики Узбекистан»;

Постановление Президента Республики Узбекистан от 21 ноября 2018 года № ПП-4024 «О мерах по совершенствованию системы контроля за внедрением информационных технологий и коммуникаций, организации их защиты»;

Постановление Президента Республики Узбекистан от 14 сентября 2019 года № ПП-4452 «О дополнительных мерах по совершенствованию системы контроля за внедрением информационных технологий и коммуникаций, организации их защиты»;

O'z DSt 1204:2009 «Информационная технология. Криптографическая защита информации. Требования безопасности к криптографическим модулям»;

O'z DSt ISO/IEC 27005:2013 «Информационная технология. Методы обеспечения безопасности. Управление рисками информационной безопасности»;

O'z DSt ISO/IEC 27000:2014 «Информационная технология. Методы обеспечения безопасности. Системы управления информационной безопасностью. Обзор и словарь»;

O'z DSt ISO/IEC 27011:2014 «Информационная технология. Методы обеспечения безопасности. Руководящие указания по управлению информационной безопасностью в организациях телекоммуникаций»;

O'z DSt 2814:2014 «Информационная технология. Автоматизированные системы. Классификация по уровню защищённости от несанкционированного доступа к информации»;

O'zDSt 2815:2014 «Информационная технология. Межсетевые экраны. Классификация по уровню защищённости от несанкционированного доступа к информации»;

O'zDSt 2816:2014 «Информационная технология. Классификация программного обеспечения средств защиты информации по уровню контроля отсутствия не декларированных возможностей»;

O'z DSt 2817:2014 «Информационная технология. Средства вычислительной техники. Классификация по уровню защищённости от несанкционированного доступа к информации»;

O'z DSt ISO/IEC 27003:2014 «Информационная технология. Методы обеспечения безопасности. Руководство по внедрению системы управления информационной безопасностью»;

O‘z DSt ISO/IEC 27010:2015 «Информационная технология. Методы обеспечения безопасности. Руководство по управлению информационной безопасностью при коммуникациях между отраслями и организациями»;

O‘z DSt 2927:2015 «Информационная технология. Информационная безопасность. Термины и определения»;

O‘z DSt ISO/IEC 27001:2016 «Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования»;

O‘z DSt ISO/IEC 27002:2016 «Информационная технология. Методы обеспечения безопасности. Практические правила управления информационной безопасности»;

O‘z DSt ISO/IEC 15408-1,2,3:2016 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий;

O‘z DSt 3243:2017 «Информационная технология. Локальные и корпоративные вычислительные сети. Общие технические требования»;

O‘z DSt 3386:2019 (ISO/IEC 27035-1:2016, MOD) «Информационная технология. Методы обеспечения безопасности. Управление инцидентами информационной безопасности. Часть 1»;

O‘z DSt 3387:2019 (ISO/IEC 27035-2:2016, MOD) «Информационная технология. Методы обеспечения безопасности. Управление инцидентами информационной безопасности. Часть 2»;

O‘z DSt ISO/IEC 13335-1:2019 Информационная технология. Методы обеспечения безопасности. Управление безопасностью информационно-коммуникационных технологий. (Часть 1). Концепции и модели управления безопасностью информационно-коммуникационных технологий;

Методические пособия по разработке политики информационной безопасности на территории Республики Узбекистан (Приложение №10 к протоколу Республиканской комиссии по координации реализации Комплексной программы развития Национальной информационно-коммуникационной системы Республики Узбекистан на 2013-2020 годы от 23 февраля 2016 года № 7);

«Регламент взаимодействия между Министерством по развитию информационных технологий и коммуникаций Республики Узбекистан и органами государственного и хозяйственного управления по реагированию и расследованию, и предотвращению инцидентов информационной безопасности» (Приложение №1 и №2 к протоколу Технического совета по вопросам информационно коммуникационной безопасности Республики Узбекистан №7 от 17.11.2017 г.);

«Требования обеспечения информационной безопасности органов государственного и хозяйственного управления, государственной власти на местах» (Приложение №2 к протоколу Республиканской комиссии по координации

реализации Комплексной программы развития Национальной информационно-коммуникационной системы Республики Узбекистан на 2013-2020 годы от 11 ноября 2017 года №7).

3. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

- **Анализ рисков** – систематическое выполнение процедур идентификации ресурсов системы обработки данных, угроз этим ресурсам и уязвимостей системы к этим угрозам;
- **Антивирусная защита** – комплекс мер, направленных на предотвращение, обнаружение и обезвреживание действий компьютерного вируса при помощи антивирусных программ;
- **Антивирусная программа** – программа, предназначенная для обнаружения вирусов и, возможно, предлагающая удалить или удаляющая их;
- **Аутентификация** – процедура установления подлинности пользователя (абонента сети, отправителя сообщения), программы, устройства или данных (информации, получаемого сообщения, ключа);
- **База данных** – совокупность данных, организованных по определенным правилам, предусматривающим общие принципы описания, хранения и манипулирования данными, независимо от прикладных программ;
- **Доступ к информации** - ознакомление с информацией, её обработка, в частности, копирование, модификация или уничтожение информации;
- **Доступность** - состояние информации и её носителя, при котором обеспечивается беспрепятственное и своевременное получение пользователями предназначенной для них информации;
- **Для служебного пользования ДСП** – гриф ограничения доступа к документу, содержащему служебную информацию ограниченного распространения, не содержащую сведения, отнесенные к государственным секретам, разглашение (передача, утечка) которой может нанести материальный, моральный и иной ущерб интересам организации, предприятия, компании и обществу;
- **Защита информации** – комплекс правовых, организационных и технических (программно-аппаратных) мероприятий, направленных на предотвращение или затруднение нанесения ущерба интересам собственника информации (данных);
- **Злоумышленник (нарушитель)** – лицо или организация, заинтересованные в получении несанкционированного доступа к информационной системе и её ресурсам и совершившие преднамеренные действия для их несанкционированного получения или изменения;
- **Информационная безопасность** – защищённость информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений;

- **Идентификация** – присвоение субъектам и объектам доступа идентификатора и/или сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов;
- **Информация** – 1. Сведение о лицах, предметах, фактах, событиях, явлениях и процессах независимо от источников и формы их представления. 2. Совокупность знаний, фактов, сведений, представляющих интерес и подлежащих хранению и обработке;
- **Информационная система** – организационно упорядоченная совокупность информационных ресурсов, информационных технологий и средств связи, позволяющая осуществлять сбор, хранение, поиск, обработку и пользование информацией;
- **Интернет, сеть интернет** – глобальная информационная система, которая: логически связанна унитарным адресным пространством, основанном на IP-протоколе или на его перспективных расширениях/последователях. Может поддерживать коммуникации, используя TCP/IP или его расширения/последователи и/или IP – совместимые протоколы. Предоставляет, использует или делает доступным (для всех или конфиденциально) сервисы высокого уровня, основанные на коммуникациях и связанной с ними инфраструктуры. Глобальное (всемирное) множество независимых компьютерных сетей, соединённых между собой для обмена информацией по стандартным открытым протоколам;
- **Конфиденциальность –** состояние информации и её носителя, при котором обеспечиваются предотвращение несанкционированного ознакомления с ней или несанкционированного документирования (снятия копий);
- **Контролируемая зона** – территория объекта, на которой исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового доступа. Границами контролируемой зоны являются ограждающие конструкции помещений (стены, окна, двери, потолок) и территорий (ограждения, проходные);
- **Политика информационной безопасности** – совокупность правил, определяющих и ограничивающих виды деятельности объектов и участников, системы информационной безопасности;
- **Программное обеспечение** – совокупность программ системы обработки информации и программных документов, необходимых для эксплуатации этих программ;
- **Рабочая станция (PC)** – полноценный персональный компьютер или компьютерный терминал (устройства ввода-вывода, отдельные или удаленные от управляющего компьютера), набор необходимого ПО, по необходимости, дополняемые вспомогательным оборудованием: печатающее устройство,

внешнее устройства хранения данных на магнитных и/или оптических носителях, сканеры и т.п.;

- **Ресурсы информационные (информационные ресурсы)** – 1. Отдельные документы, отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных и других). 2. Информация, банк данных, база данных в электронной форме в составе информационной системы;
- **Риск** – возможность использования конкретной уязвимости системы обработки данных при реализации конкретной угрозы;
- **Сервер** – совокупность аппаратного и программного обеспечения (программа-сервер), позволяющая РС предоставлять услуги другой РС. РС работают с программой-сервером с помощью программ-клиентов;
- **Система информационная** – система для подготовки, отправления, получения, хранения или иной обработки данных. Организационно-упорядоченная совокупность информационных ресурсов, информационных технологий и средств связи, позволяющая осуществлять сбор, хранение, поиск, обработку и пользование информацией. Любая система, связанная с накапливанием, хранением или обработкой информации;
- **Системный администратор** – должностное лицо, назначенное в установленном порядке ответственным за эксплуатацию службы каталога, системы управления базами данных, СЭП и прочих систем или серверов, их ведение, настройку, изменения полномочий пользователей, информационную безопасность;
- **Среда информационная общества** (**информационная среда**) - совокупность информационных ресурсов системы формирования, распространения и использования информации, информационной инфраструктуры;
- **Средства технической защиты (СТЗИ)** – аппаратные, программные или аппаратно-программные средства, осуществляющие защиту информации и обеспечивающие безопасность информации на всех стадиях ее жизненного цикла (формирования, передачи, приема, преобразования, отображения и хранения информации);
- **Средства криптографической защиты информации (СКЗИ)** – аппаратные, программные или аппаратно-программные средства, осуществляющие криптографические преобразования информации для обеспечения ее безопасности, в том числе:

  а) средства шифрования – аппаратные, программные и аппаратно-программные средства, реализующие криптографические алгоритмы преобразования информации и предназначенные для защиты информации от несанкционированного доступа при ее обработке, хранении и передаче по каналам связи.

б) средства имитозащиты - аппаратные, программные и аппаратно-программные средства, реализующие криптографические алгоритмы преобразования информации и предназначенные для защиты от навязывания ложной информации.

в) средства электронной цифровой подписи – совокупность технических и программных средств, обеспечивающих создание электронной цифровой подписи в электронном документе, подтверждение подлинности электронной цифровой подписи, создание открытых и закрытых ключей электронной цифровой подписи.

г) средства изготовления ключевых документов и сами ключевые документы (независимо от вида носителя ключевой информации);

- **Субъект** - активный логический объект, имеющий доступ к объектам;
- **Субъект информационных отношений** – физическое и юридическое лицо, обладающее определенным правом по отношению к субъекту информационному ресурсу;
- **Угроза** - потенциальная возможность нарушения компьютерной безопасности;
- **Уязвимость информации** - подверженность информации воздействию различных дестабилизирующих факторов, которые могут привести к нарушению её конфиденциальности, целостности, доступности или неправомерному тиражированию;
- **Целостность** - состояние информации и её носителя, при котором обеспечиваются неделимость и предотвращение несанкционированного или преднамеренного уничтожения, искажения, утечки, хищения, подделки, подмены в целом и её отдельных составных частей.
- **Шифрование** – совокупность обратимых преобразований информации (данных) в соответствии с криптографическим алгоритмом и ключом для надежного сокрытия ее истинного содержания;

4. ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

ИБ - информационная безопасность;
ИР - информационный ресурс;
ИС – информационная система;
ИТ - информационная технология;
ПО - программное обеспечение;
СУИБ - Система управления информационной безопасностью;
УАП - Управление автоматизации производства;
ЭЦП - электронная цифровая подпись.

5. ОБЛАСТЬ ПРИМЕНЕНИЯ

Настоящая Политика ИБ распространяется на всех сотрудников Комбината (штатных, временных, практикантов, работающих по контракту и др.) вне зависимости от их места работы и занимаемой должности, на третьих лиц (подрядчики, аудиторы, посетители, обслуживающий персонал и т.п.), получивших легитимный доступ к информационным системам и ресурсам Комбината.

Политика распространяется на информационные системы и ресурсы, предназначенные исключительно для передачи, обработки, хранения открытой и конфиденциальной информации.

Защита информации, содержащей сведения, отнесенные к государственным секретам Республики Узбекистан, обеспечивается в соответствии с законодательством.

При предоставлении доступа к информационным ресурсам Комбината внешним пользователям, последние в обязательном порядке должны быть ознакомлены с требованиями Политики, в части касающейся.

6. ЦЕЛИ И ЗАДАЧИ

6.1. Цели

Основной целью, на достижение которой направлены все положения настоящей Политики, является защита субъектов информационных отношений Комбината от возможного нанесения им материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на информацию, её носители, процессы обработки и передачи, а также минимизация уровня операционных и других рисков (риск нанесения урона деловой репутации Комбината, правовой риск и т.д.).

Указанная цель достигается посредством обеспечения и постоянного поддержания следующих свойств информации:

- доступности информации для легальных пользователей (устойчивого функционирования информационных систем Комбината, при котором пользователи имеют возможность получения необходимой информации и результатов решения задач за приемлемое для них время);
- целостности и аутентичности (подтверждение авторства) информации, хранимой и обрабатываемой в информационных системах Комбината и передаваемой по каналам связи;
- конфиденциальности - сохранения в тайне определённой части информации, хранимой, обрабатываемой и передаваемой по каналам связи;
- создание условий для максимально возможного возмещения и локализации наносимого ущерба неправомерными действиями пользователей на объектах информатизации.

Необходимый уровень доступности, целостности и конфиденциальности информации обеспечивается соответствующими множеству значимых угроз методами и средствами.

6.2. Задачи

Для достижения основной цели защиты и обеспечения указанных свойств информации система обеспечения информационной безопасности Комбината должна обеспечивать эффективное решение следующих задач:

- защита информационных активов от угроз, исходящих от противоправных действий злоумышленника;
- управление непрерывной работой системы;
- уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий персонала, технических сбоев, неправильных технологических и организационных решений в процессах обработки, передачи и хранения информации, обеспечение нормального функционирования технологических процессов;
- обеспечение информационной безопасности информационных ресурсов и систем, а также персонала Комбината;
- разработка модели нарушителя информационной безопасности Комбината;
- разработка перечня потенциальных угроз информационной безопасности Комбината и их анализ;
- классификация информационных ресурсов объекта и их контроль;
- формирование требований к СУИБ;
- определение обязанностей персонала по обеспечению информационной безопасности;
- своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба заинтересованным субъектам информационных отношений, нарушению нормального функционирования информационных систем Комбината;
- создание механизма оперативного реагирования на угрозы безопасности информации и негативные тенденции;
- создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации;
- защиту от вмешательства в процесс функционирования информационных систем Комбината посторонних лиц (доступ к информационным ресурсам должны иметь только зарегистрированные в установленном порядке пользователи);

- разграничение доступа пользователей к информационным, аппаратным, программным и иным ресурсам Комбината (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям для выполнения своих служебных обязанностей), то есть защиту от несанкционированного доступа;
- обеспечение аутентификации пользователей, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации);
- защиту от несанкционированной модификации, используемых в корпоративных информационных системах Комбината программных средств, а также защиту систем от внедрения несанкционированных программ, включая компьютерные вирусы;
- защиту информации ограниченного пользования от утечки по техническим каналам при её обработке, хранении и передаче по каналам связи;
- обеспечение живучести криптографических средств защиты информации.

7. ОСНОВНЫЕ ПОЛОЖЕНИЯ

Информационная безопасность состоит из трёх основных компонентов:

- конфиденциальность: защита конфиденциальной информации от несанкционированного раскрытия или перехвата;
- целостность: обеспечение точности и полноты информации и компьютерных программ;
- доступность: обеспечение доступности информации и жизненно важных сервисов для пользователей, когда это требуется.

Политика предусматривает обеспечение информационной безопасности на основе использования совокупности организационных, режимных, криптографических, технических, программных и других методов и средств защиты информации, а также осуществления всестороннего непрерывного контроля за эффективностью реализованных мер по обеспечению информационной безопасности.

Информационная безопасность Комбината и её построение должны соответствовать требованиям политики безопасности национального и международного законодательства.

В процессе реализации Политики с целью приведения в соответствие её реальным условиям, а также с учётом возникновения новых угроз ИБ, в Политику могут вноситься изменения и дополнения.

Ответственность за применение данного документа, исполнение, сохранность, доведение до сотрудников предприятия возлагается на лицо ответственное за ИБ,

руководителей структурных подразделений, отделов, служб, управлений Исполнительного аппарата Комбината. Настоящая политика утверждается руководителем Комбината. Инициатором планового и внепланово пересмотра политики является лицо ответственное за ИБ, а также по результату внешнего аудита ИБ.

8. ОБЪЕКТЫ ЗАЩИТЫ

Основными объектами информационной безопасности на Комбинате являются:

- информационные ресурсы с ограниченным доступом, информационные ресурсы составляющие коммерческую тайну или иные чувствительные по отношению к случайным и несанкционированным воздействиям и нарушению их безопасности, а также открытая (общедоступная) информация, необходимая для работы Комбината, независимо от формы и вида её представления;
- процессы обработки информации в информационных системах Комбината, регламенты и процедуры сбора, обработки, хранения и передачи информации, персонал разработчиков и пользователей систем и обслуживающий их персонал;
- информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства её обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены чувствительные элементы информационной среды.
- программные ресурсы – операционные системы и прикладное ПО, ПС, средства разработки и утилиты, серверные приложения и сервисы.
- физические ресурсы – компьютерное и коммуникационное оборудование, оргтехника, носители данных, помещения и др.

8.1. Структура, состав и размещение основных объектов защиты, информационные связи

Информационная среда Комбината является распределённой структурой, объединяющей информационные подсистемы Исполнительного аппарата и структурных подразделений Комбината.

К основным особенностям информационной среды Комбината, относятся:

- широкая территориальная распределённость компонентов информационной системы;
- объединение в единую систему большого количества разнообразных технических средств обработки и передачи информации;

- значительное расширение сферы использования автоматизированных систем обработки информации, широкое многообразие и повсеместное распространение информационно-управляющих систем на Комбинате;
- большое разнообразие решаемых задач и типов, обрабатываемых данных, сложные режимы автоматизированной обработки информации с широким совмещением выполнения информационных запросов различных пользователей;
- значительная важность и ответственность решений, принимаемых на основе автоматизированной обработки данных;
- наличие баз данных информации различного назначения, принадлежности и уровней конфиденциальности;
- абстрагирование владельцев данных от физических структур и места размещения данных (информации);
- наличие информационных каналов взаимодействия с «внешним миром» (источниками и потребителями информации);
- высокая интенсивность информационных потоков;
- разнообразие категорий пользователей и обслуживающего персонала систем.

В этих условиях резко возрастает уязвимость информации и одним из важнейших элементов информационной среды Комбината становятся корпоративные информационные системы, в которых обрабатываются и накапливаются значительные объёмы информации, совместно используемой различными пользователями, различной организационной принадлежности.

8.2. Категории информационных ресурсов, подлежащих защите

На Комбинате циркулирует информация различных уровней конфиденциальности, содержащая сведения ограниченного распространения (служебная, коммерческая, персональные данные) и открытые сведения.

Защите подлежит вся информация и информационные ресурсы Комбината, независимо от её представления и местонахождения в информационной среде Комбината:

- сведения, составляющие коммерческую тайну, доступ к которым ограничен собственником информации;
- сведения, составляющие служебную информацию, доступ к которым ограничен собственником информации;
- сведения о частной жизни граждан (персональные данные), доступ к которым ограничен;
- открытая информация, необходимая для обеспечения нормального функционирования Комбината.

9. РИСК И МОДЕЛЬ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

9.1. Риски информационной безопасности

Риск ИБ – это потенциальная возможность использования уязвимостей актива или группы активов с конкретной угрозой для причинения ущерба. Для управления рисками ИБ необходимы соответствующие методы определения и обработки рисков, которые могут включать расчёт затрат и экономического эффекта, требования законодательных актов, интересы заинтересованных сторон и другие соответствующие данные.

Процесс определения рисков, включает идентификацию, сравнительную оценку риска, и назначение им приоритетов в соответствии с критериями принятия риска и важностью целей. Результаты определения рисков ИБ помогут руководству Комбината принять решения относительно управления рисками ИБ, назначения приоритетов при управлении рисками ИБ и внедрения соответствующих средств управления безопасностью для защиты от этих рисков.

Процесс определения рисков включает систематический метод оценки величины риска (анализ риска) и процесс сравнения предполагаемого риска с соответствующими критериями риска. Определение риска должно выполняться периодически, это позволит своевременно учитывать изменения требований ИБ и возникновение рискованных ситуаций, а также произошедшие существенные изменения. Для определения риска следует использовать методы, обеспечивающие сопоставимые и воспроизводимые результаты.

Для эффективного определения риска ИБ чётко определяется область его действия. Определение риска ИБ будет взаимосвязано с определениями рисков для других областей деятельности (при необходимости). До начала обработки рисков устанавливается критерии принятия рисков. Риск принимается, если определено, что его уровень низкий или стоимость его обработки экономически невыгодна, эти критерии документируются.

После определения риска для каждого идентифицированного риска должно быть принято решение об его обработке. К возможным опциям обработки рисков относятся:

- применение соответствующих средств управления для снижения рисков;
- осознанное и объективное принятие рисков, если они однозначно удовлетворяют требованиям и критериям принятия рисков;
- разделение совместных рисков с другими сторонами, например, страховщиками или поставщиками.

После принятия решения об обработке рисков используются соответствующие средства управления, которые прежде были выбраны и внедрены. При случаях

доступа сторонних организаций к информационным активам Комбината и средствам обработки информации необходимого по производственным причинам, а также, в случае получения товаров и услуг от сторонних организаций, проводится анализ рисков для определения возможных последствий для безопасности информации и требований к средствам управления. Такие мероприятия следует согласовывать и определять в договорах со сторонней организацией.

Все действия по определению, обработке и принятию рисков, обмену информацией относительно рисков, мониторингу рисков, должны выполняться в соответствии со стандартом O‘z DSt ISO/IEC 27005:2013.

9.2. Угрозы информационной безопасности и их источники

Всё множество потенциальных угроз безопасности информации по природе их возникновения разделяются на два класса: естественные (объективные) и искусственные (субъективные).

- Естественные угрозы - это угрозы, вызванные воздействиями на информационную систему и её компоненты объективных физических процессов техногенного характера или стихийных природных явлений, независящих от человека;
- Искусственные угрозы - это угрозы, вызванные деятельностью человека.

Среди них, исходя из мотивации действий, можно выделить:

- непреднамеренные (неумышленные, случайные) угрозы, вызванные ошибками в проектировании информационной системы и её элементов, ошибками в действиях персонала и т.п.;
- преднамеренные (умышленные) угрозы, связанные с корыстными, идейными или иными устремлениями людей (злоумышленников).

Источники угроз по отношению к самой информационной системе могут быть как внешними, так и внутренними.

Основными источниками угроз безопасности информации Комбината являются:

- непреднамеренные (ошибочные, случайные, без злого умысла и корыстных целей) нарушения установленных регламентов сбора, обработки и передачи информации, а также требований безопасности информации и другие действия пользователей информационных систем Комбината (в том числе сотрудников, отвечающих за обслуживание и администрирование компонентов информационных систем), приводящие к непроизводительным затратам времени и ресурсов, разглашению сведений ограниченного распространения, потере ценной информации или нарушению работоспособности компонентов информационной системы;

- преднамеренные (в корыстных целях, по принуждению третьими лицами, со злым умыслом и т.п.) действия легально допущенных к информационным ресурсам Комбината пользователей (в том числе сотрудников, отвечающих за обслуживание и администрирование компонентов информационных систем), которые приводят к непроизводительным затратам времени и ресурсов, разглашению сведений ограниченного распространения, потере ценной информации или нарушению работоспособности компонентов информационных систем Комбината;
- деятельность преступных групп и формирований, политических и экономических структур, а также отдельных лиц по добыванию информации, навязыванию ложной информации, нарушению работоспособности информационных систем Комбината в целом и её отдельных компонентов;
- удалённое несанкционированное вмешательство посторонних лиц из внешних сетей общего назначения (прежде всего сеть Интернет) через легальные и несанкционированные каналы подключения к таким сетям, используя недостатки протоколов обмена, средств защиты и разграничения удалённого доступа к ресурсам;
- ошибки, допущенные при разработке компонентов информационных систем Комбината и их систем защиты, ошибки в программном обеспечении, отказы и сбои технических средств (в том числе средств защиты информации и контроля эффективности защиты);
- нарушение правил эксплуатации ИС;
- аварии, стихийные бедствия.

Наиболее значимыми угрозами безопасности информации Комбината (способами нанесения ущерба субъектам информационных отношений) являются:

- действия, приводящие к частичному или полному отказу работы сети, разрушению аппаратных, программных и информационных ресурсов (порча оборудования, удаление и/или искажение файлов с важной информацией);
- неправомерное отключение оборудования или изменение режимов работы систем электропитания, охлаждения, вентиляции, видеонаблюдения и т.п.;
- нелегальная установка и использование неучтённых программ (игровых, обучающих, технологических и других, не являющихся необходимыми для выполнения сотрудником своих служебных обязанностей);
- нарушение конфиденциальности (разглашение, утечка) сведений, составляющих служебную или коммерческую тайну, а также персональных данных;

- порча и/или умышленное уничтожение электронных и бумажных носителей информации;
- заражение сети и/или рабочей станции вредоносными программами;
- недоступность ИС/ИР в результате несанкционированного вмешательства в их работу;
- несанкционированное изменение главной страницы веб-сайта;
- несанкционированный доступ в файловую систему ИР с последующим размещением вредоносного контента;
- DoS и DDoS-атаки на ИС/ИР;
- несанкционированный доступ в ИС;
- взлом защиты ИС/ИР;
- введение специальных программных или аппаратных средств для получения несанкционированного доступа к защищенной ИС;
- изменение, повреждение, удаление информации, хранящейся в ИС, а равно внесении в нее заведомо ложной информации без разрешения собственника или законного владельца этой информации;
- несанкционированное вмешательство в работу серверного оборудования или ИС/ИР;
- несанкционированное уничтожение, блокирование, модификация, копирование или перехват информации, хранящейся или передаваемой, в ИС/ИР путём внесения изменений в существующие программы;
- разработка, использование и распространение специальных вирусных программ;
- другие инциденты ИБ, связанные с нарушением нормальной работоспособности ИС/ИР и имеющие преднамеренный или злоумышленный характер.

10. МОДЕЛЬ НАРУШИТЕЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Нарушители информационной безопасности по своей принадлежности разделяются на две группы: внутренние и внешние.

- внутренний потенциальный нарушитель – персонал организации, имеющие санкционированный доступ на территорию объектов информатизации;
- внешний потенциальный нарушитель – все остальные лица.

10.1. Неформальная модель возможных нарушителей

Нарушитель — это лицо, которое предприняло попытку выполнения запрещённых операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, с целью самоутверждения и т.п.) и использующее для этого различные возможности, методы и средства.

Злоумышленник - нарушитель, действующий намеренно из корыстных, идейных или иных побуждений.

Система обеспечения информационной безопасности Комбината должна строиться исходя из предположений о следующих возможных типах нарушителей в системе (с учётом категории лиц, мотивации, квалификации, наличия специальных средств и др.):

- **Некомпетентный** (невнимательный) пользователь - сотрудник Комбината (или другой организации, являющийся легальным пользователем информационной системы Комбината), который может предпринимать попытки выполнения запрещённых действий, доступа к защищаемым ресурсам информационной системы с превышением своих полномочий, ввода некорректных данных, нарушения правил и регламентов работы с информацией и т.п., действуя по ошибке, некомпетентности или халатности без злого умысла и использующий при этом только штатные (предоставленные) средства.
- **Любитель** - сотрудник Комбината (или другой организации, являющийся зарегистрированным пользователем информационной системы Комбината), пытающийся нарушить систему защиты без корыстных целей или злого умысла для самоутверждения. Для преодоления системы защиты и совершения запрещённых действий он может использовать различные методы получения дополнительных полномочий доступа к ресурсам, недостатки в построении системы защиты и доступные ему штатные средства (несанкционированные действия посредством превышения своих полномочий на использование разрешённых средств). Помимо этого, он может пытаться использовать дополнительно нештатные инструментальные и технологические программные средства, самостоятельно разработанные программы или стандартные дополнительные технические средства.
- **Внутренний злоумышленник** - сотрудник Комбината (или другой организации, являющийся зарегистрированным пользователем информационной системы Комбината), действующий целенаправленно из корыстных интересов или мести за нанесённую обиду, возможно в сговоре с лицами, не являющимися сотрудниками Комбината. Он может использовать весь набор методов и средств взлома системы защиты, включая агентурные методы, пассивные средства (технические средства перехвата), методы и средства активного воздействия (модификация технических средств, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ), а также комбинации воздействий, как изнутри, так и извне Комбината.

- **Внешний злоумышленник** - постороннее лицо, действующее целенаправленно из корыстных интересов, мести или из любопытства, возможно в сговоре с другими лицами. Он может использовать весь набор методов и средств взлома системы защиты, включая агентурные методы, пассивные средства (технические средства перехвата), методы и средства активного воздействия (модификация технических средств, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ), а также комбинации воздействий, как изнутри, так и извне Комбината.

Внутренним нарушителем может быть лицо из следующих категорий сотрудников Комбината:

- зарегистрированные пользователи информационных систем Комбината;
- сотрудники Комбината, не являющиеся зарегистрированными пользователями и не допущенные к ресурсам информационных систем Комбината, но имеющие доступ в здания и помещения;
- персонал, обслуживающий технические средства информационных систем Комбината;
- сотрудники подразделений Комбината, задействованные в разработке и сопровождении того или иного программного обеспечения;
- сотрудники подразделений обеспечения безопасности Комбината;
- руководители различных уровней.

Категории лиц, которые могут быть внешними нарушителями:

- уволенные сотрудники Комбината;
- представители организаций, взаимодействующих по вопросам технического сопровождения информационных систем и ресурсов Комбината;
- посетители (представители компаний, поставляющих технику, программное обеспечение, услуги и т.п.);
- представители конкурирующих организаций;
- члены преступных организаций, сотрудники спецслужб или лица, действующие по их заданию;
- лица, случайно или умышленно проникшие в информационные системы Комбината из внешних телекоммуникационных сетей (хакеры).

Пользователи и обслуживающий персонал из числа сотрудников Комбината потенциально имеют широкие возможности по осуществлению несанкционированных действий, вследствие наличия у них определённых

полномочий по доступу к информационным ресурсам и хорошего знания технологии обработки информации и защитных мер.

Особую категорию составляют администраторы различных автоматизированных систем, имеющие практически неограниченный доступ к информационным ресурсам информационных систем и компонентов локальной сети. Численность данной категории пользователей должна быть минимальной, а их действия должны находиться под обязательным контролем со стороны ответственных за обеспечение ИБ.

Уволенные сотрудники могут использовать для достижения целей свои знания о технологии работы, защитных мерах и правах доступа. Полученные во время работы на Комбинате знания и опыт выделяют их среди других источников внешних угроз.

Профессиональные хакеры имеют наиболее высокую техническую квалификацию и знания о слабостях программных средств, используемых в автоматизированных системах обработки информации. Они представляют наибольшую угрозу при взаимодействии с работающими или уволенными сотрудниками.

Организации, занимающиеся разработкой, поставкой, ремонтом и обслуживанием оборудования, представляют внешнюю угрозу в силу того, что эпизодически имеют непосредственный доступ к информационным ресурсам Комбината.

Принимаются следующие ограничения и предположения о характере действий возможных нарушителей:

- нарушитель скрывает свои несанкционированные действия от других сотрудников;
- несанкционированные действия могут быть следствием ошибок пользователей, эксплуатирующего и обслуживающего персонала, а также недостатков принятой технологии обработки, хранения и передачи информации;
- в своей деятельности вероятный нарушитель может использовать любые имеющиеся средства перехвата информации, воздействия на информацию и ИР, адекватные финансовые средства для подкупа сотрудников, шантаж и другие средства и методы для достижения стоящих перед ним целей.

11. МЕРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Меры обеспечения информационной безопасности

Основные меры обеспечения информационной безопасности Комбината подразделяются на:

- правовые меры;
- морально-этические меры;
- организационные меры;
- технологические меры;
- инженерно-технические меры;
- программно-аппаратные меры;
- физические меры;
- меры в отношениях с внешними пользователями.

Правовые (законодательные) меры защиты - к правовым мерам защиты, применяемым на Комбинате относятся действующие в Республике Узбекистан законы, указы и нормативные акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе её обработки и использования, а также устанавливающие ответственность за нарушения этих правил которые в свою очередь оперативно распространяются (доносятся до сотрудников) Комбината в виде внутренних руководящих документов (приказов, положений, распоряжений, рекомендаций) через службу офис-менеджера по представлению руководства УАП.

Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом информационных ресурсов Комбината.

Сотрудники Комбината, включая практикантов, контрактников и стажёров должны ознакомиться с требованиями настоящей Политики ИБ под роспись в Журнале ознакомления сотрудников, который приведён в **Приложении № 1** к настоящей Политике ИБ.

Морально-этические меры защиты - к морально-этическим мерам, применяемым на Комбинате относятся нормы поведения, которые традиционно сложились или складываются по мере распространения информационных технологий в обществе. Эти нормы большей частью не являются обязательными, как законодательно утверждённые нормативные акты, однако, их несоблюдение может привести к падению авторитета, престижа человека, группы лиц или Комбината в целом. Морально-этические нормы бывают как неписаные, так и писаные, то есть оформленные в некоторый свод (устав) правил или предписаний. Всем сотрудникам

необходимо ограничить себя от действий, порочащих деловую репутацию Комбината, так же, соблюдать правила этикета.

Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективах подразделений и снижают вероятность возникновения негативных действий, связанных с человеческим фактором.

Организационные (административные) меры защиты - это меры административного характера, применяемые на Комбинате в виде разработанных и утвержденных инструкций, регламентов, правил использования информационных ресурсов а так же информационных систем Комбината, положений и должностных инструкций сотрудников ИТ, регламентирующие процессы функционирования системы обработки данных, использование её ресурсов, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

Принимая во внимание вышесказанное на Комбинате назначается ответственный сотрудник по обеспечению ИБ, который осуществляет организацию и координацию работ по комплексной защите информации, контроль эффективности принятых мер по обеспечению ИБ, он является главным лицом, контролирующим состояние ИБ. Ответственный сотрудник по обеспечению ИБ проводит соответствующую работу по обеспечению ИБ, путём принятия необходимых мер и адекватного распределения ресурсов.

Кроме того, любые изменения локальной сети и ИР Комбината должны быть предварительно согласованы с ответственным сотрудником по обеспечению ИБ.

Всем сотрудникам и пользователям, использующим ИР Комбината при окончании срока действия их трудового договора, контракта или соглашения следует возвратить все находящиеся у них материальные ценности Комбината (ключи ЭЦП, ноутбуки, жетоны для входа/выхода, личные удостоверения, документацию, содержащую конфиденциальную информацию и т.д.). Также удаляются права доступа данных сотрудников к локальной сети (удаляются данные об учётных записях корпоративной электронной почты, домена и т.д.).

Руководство Комбината должно регулярно следить за обучением и повышением уровня квалификации сотрудников в области обеспечения ИБ.

Технологические меры защиты - к данному виду мер защиты применяемых на Комбинате относятся разного рода технологические решения и приёмы, основанные на использовании некоторых видов избыточности (структурной,

функциональной, информационной, временной и т.п.) и направленные на уменьшение возможности совершения сотрудниками ошибок и нарушений в рамках предоставленных им прав и полномочий. Примером таких мер являются: использование процедур двойного ввода ответственной информации, инициализация ответственных операций только при наличии согласования нескольких лиц, процедура проверки реквизитов исходящих и входящих сообщений, периодическое подведение общего баланса всех счетов, резервное копирование критически важных массивов данных и т.п.

Инженерно-технические меры – эти методы, применяемые на Комбинате ориентированы на оптимальное построение зданий, сооружений, инженерных сетей и транспортных коммуникаций с учётом требований обеспечения информационной безопасности.

К инженерно-техническим мерам относятся:

- обеспечение электрозащиты оборудования и зданий;
- экранирование помещений;
- защита помещений от разрушений;
- оптимальное размещение оборудования;
- оптимальное размещение инженерных коммуникаций;
- применение средств визуальной защиты (видеонаблюдение);
- акустическая обработка помещений;
- применение систем кондиционирования;
- применение систем пожаротушения;
- применение систем контроля удаленного доступа.

Программно-аппаратные меры - меры защиты, применяемые на Комбинате основаны на использовании различных электронных устройств и специальных программ и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации, централизованное управление антивирусной защитой и доступом к интернет сетям и т.д.).

Физические меры - меры защиты, применяемые на Комбинате основаны на применении различного рода механических, электронных или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также средств визуального наблюдения, связи и охранной сигнализации. К данному типу относятся также меры и средства контроля физической целостности компонентов (пломбы, наклейки и т.п.).

Меры в отношениях с внешними пользователями - в случаях предоставления сторонним лицам доступ к информации и активам Комбината, внимание обращается на все установленные требования ИБ и принимаются меры безопасности в отношениях с внешними пользователями. Перед предоставлением доступа сторонним лицам к любым активам Комбината учитываются следующие условия, относящиеся к ИБ:

Защита активов, включающая:

- процедуры по защите активов, в том числе информации и ПО, а также управление известными уязвимостями;
- процедуры определения факта компрометации активов, например, вследствие потери или модификации данных;
- целостность активов;
- ограничения на копирование и раскрытие информации;
- описание предоставляемых услуг;
- различные предпосылки, требования и выгоды от доступа клиентов;
- процедура ознакомления с правилами политики информационной безопасности Комбината.

Соглашения по управлению доступом, охватывающие:

- разрешённые методы доступа, а также управление и использование уникальных идентификаторов пользователей и паролей;
- процесс предоставления привилегий и полномочий на доступ;
- принцип запрета любого доступа, явно неразрешённого;
- процесс отзыва прав доступа пользователей или блокирование доступа;
- процедуры отчётности, уведомления и расследования инцидентов нарушения ИБ и выявления слабых звеньев системы безопасности;
- описание каждого сервиса, предназначенного для доступа;
- плановый уровень сервиса и недопустимые уровни сервиса;
- право мониторинга и отмены любой деятельности, связанной с активами Комбината;
- соответствующие обязательства Комбината и внешнего пользователя;
- обязанности, касающиеся юридических вопросов и способов обеспечения соответствия требованиям законодательства, например, законов о защите данных, принимая во внимание различные национальные законодательные системы, в случае, если соглашение включает сотрудничество с клиентами за рубежом;
- права на интеллектуальную собственность и авторские права, а также защита любой совместной работы.

Требования ИБ, относящиеся к сотрудникам сторонних организаций, получающим доступ к активам Комбината, могут значительно различаться в

зависимости от классификации предоставляемой информации и средств её обработки. Данные требования безопасности могут быть отражены в контракте (договоре), заключаемом с сотрудником сторонней организации, который содержит все определённые риски и требования ИБ.

Контракт со сторонними организациями также может содержать и другие требования безопасности. В контракте на предоставление доступа сторонней организации, необходимо указывать разрешение на привлечение других приемлемых сторон, а также условия их доступа и участия.

12. РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

При возникновении инцидента ИБ сотрудники должны действовать в соответствии с «Регламентом реагирования на инциденты информационной безопасности в отношении информационных ресурсов и корпоративной сети» Комбината, который приведён в **Приложении № 2** к настоящей Политике ИБ.

К инцидентам, в частности, относятся вирусные атаки, взлом электронной почты, уничтожение или искажение информации, утечка конфиденциальной информации, в т.ч. утеря или кража носителей информации, срыв пломбы системного блока, а также любые другие нарушения безопасности, угрозы или сбои сети.

В обязательном порядке инженер по информационной безопасности при возникновении инцидента ИБ в случаи невозможности решить его своими силами должен обратится в соответствующий органы согласно «Регламенту взаимодействия между Министерством по развитию информационных технологий и коммуникаций Республики Узбекистан и органами государственного и хозяйственного управления по реагированию, расследованию и предотвращению инцидентов информационной безопасности» (Приложение №1 к протоколу Технического совета по вопросам информационно-коммуникационной безопасности Республики Узбекистан от 17 ноября 2017г. №7) (Далее- Регламент взаимодействия).

13. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ КАНАЛОВ СВЯЗИ

За защиту и безопасность кабельной системы в структурных подразделениях несет ответственный сотрудник, назначенный руководителем структурного подразделения.

Защита кабельной системы направлена на снижение вероятности несанкционированного доступа к информации путём гальванического подключения к информационным кабелям или снятия информации через побочные электромагнитные излучения и наводки на другие кабели, а также на обеспечение

защиты оборудования от электромагнитных помех и механического повреждения. Вся кабельная система должна быть проложена в специальных защитных коробах.

Защита беспроводных каналов связи должна быть направлена на снижение таких атак, как прослушивание трафика, отказ в обслуживании, несанкционированное подключение.

При передаче конфиденциальной информации по каналам связи, выходящими за пределы контролируемой зоны, должно обеспечиваться шифрование информации сертифицированными в Республике Узбекистан средствами криптографической защиты информации.

Для защиты данных, передаваемых по указанным каналам связи, необходимо:

- кабели электропитания и линии связи, идущие к ИС, должны быть проведены (по возможности) под землей или защищены надлежащим образом;
- для защиты сетевых кабелей от их несанкционированного вскрытия для целей перехвата данных и от повреждения, используются экраны или кабели прокладываются так, чтобы они не проходили через общедоступные места;
- кабели электропитания должны быть отделены от кабелей телекоммуникаций, чтобы исключить помехи;
- незадействованные разъемы информационных кабелей, предназначенные для подключения рабочих станции, должны быть опечатаны или заклеены специальной маркой для исключения возможного несанкционированного подключения нештатных технических средств обработки информации;
- использовать соответствующие средства криптографической защиты;
- установка камер видеонаблюдения, с круглосуточным наблюдением за шлюзами магистральных каналов связи;
- использование защищенных волоконно-оптических линий связи;
- в пределах территорий и зданий запечатывание комнат с распределительными шкафами, например, с сургучной печатью;
- на этажных коммутационных шкафах установить сигнализацию с передачей сигналов на рабочее место поста охраны.

14. РАСПРЕДЕЛЕНИЕ ОТВЕТСТВЕННОСТИ

Настоящая Политика устанавливает следующие основы распределения ответственности за обеспечение безопасности ресурсов Комбината:

- за всю деятельность по обеспечению безопасности в том числе информационную несёт ответственность заместитель председателя правления по безопасности;
- за хранение доверенной сотруднику информации (в любом её виде) и обеспечение должного уровня её защиты сотрудник несёт персональную ответственность;
- за безопасность рабочих станций (в т.ч. физическую) несёт ответственность сотрудник, которому данная рабочая станция предоставлена для исполнения его служебных обязанностей;
- за безопасность локальных серверов и других важных ресурсов с ограниченным доступом, физически находящимся на территории Комбината, несут ответственность лица, за кем данное оборудование закреплено;
- за целостность корпоративной сети Комбината, её доступность и конфиденциальность циркулирующей в ней информации, несёт ответственность группа по обслуживанию сетей передачи данных службы ИТ УАП и все сотрудники Комбината, в части своей рабочей зоны (зоны доступа);
- за физическую безопасность и несанкционированное проникновение посторонних лиц на территорию Комбината, несут ответственность сотрудники ведомственной военизированной охраны;
- за пожарно-техническую безопасность и сохранность оборудования внутри каждого помещения несёт ответственность, назначенный соответствующим приказом сотрудник Комбината;
- за безопасность внешних информационных ресурсов (сайтов, баз данных и т.п.) несут ответственность сотрудники, за которыми эти ресурсы закреплены, а также руководители соответствующего подразделения.

Ответственность за отдельные ресурсы определяется в должностных функциональных обязанностях работников и других локальных нормативных документах Комбината.

Владелец ресурса может частично или полностью передавать полномочия по обеспечению защиты ресурса, однако, ответственность за данный ресурс продолжает оставаться за владельцем.

15. ПОРЯДОК ПЕРЕСМОТРА И АКТУАЛИЗАЦИИ ПОЛИТИКИ

Пересмотр Политики ИБ осуществляется один раз в год, а также в следующих случаях, в частности при:

- изменении и утверждении новых нормативно-правовых и нормативно-технических актов, касающихся ИБ;

- изменении конфигурации, добавления или удаления программных и технических средств объекта, не изменяющих технологию информационных процессов;
- изменении конфигурации и настроек технических средств защиты информации объекта;
- изменении состава и обязанностей должностных лиц пользователей и обслуживающего персонала объекта и сотрудников, отвечающих за ИБ.

Политика ИБ подлежит полному пересмотру в случае изменения технологии информационных процессов или использовании новых технических средств защиты информации. Проводимые мероприятия по ИБ следует регулярно проверять на соответствие настоящей Политике ИБ.

Новая редакция Политики ИБ подлежит повторному согласованию со Службой государственной безопасности Республики Узбекистан и министерством по развитию информационных технологий и коммуникаций Республики Узбекистан.

В случае вступления отдельных пунктов настоящей Политики в противоречие с новыми законодательными актами республики в области защиты информации, а также иными руководящими и нормативными документами Комбината, данные пункты утрачивают юридическую силу после внесения дополнений и изменений в Политику.