Утверждено Протоколом Правления
Товарищество с Ограниченной Оответственностью
«Kazakhstan Petrochemical Industries Inc.»
(«Казахстан Петрокемикал Индастриз Инк.»)

№ 25/13 от 5 августа 2013 года

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Атырау 2013

История изменений			
Дата	**Версия**	**Комментарии**	**Автор**
18.03.2013	1	Создание документа	Иргалиев Ануар
12.06.2013	2	Изменение документа	Иргалиев Ануар

ОПРЕДЕЛЕНИЕ ТЕРМИНОВ

Товарищество – Товарищество с Ограниченной Ответственностью «Kazakhstan Petrochemical Industries Inc.» («Казахстан Петрокемикал Индастриз Инк.»)

Пользователи – штатные сотрудники Товарищества, а так же другие лица, осуществляющие использование ресурсов ИТ системы Товарищества в офисе Товарищества или за его пределами (напр., использование ноутбуков Товарищества, дистанционное подключение к серверам Товарищества и т.д.).

ИТ – Информационные Технологии

ИТ системы - все ресурсы корпоративной сети Товарищества, которые включают, но не ограничиваются следующим: персональные компьютеры, ноутбуки, сервера, устройства телефонной связи, сканеры, принтеры, копиры, активное и пассивное сетевое оборудование, программное обеспечение, установленное на персональных компьютерах, ноутбуках и серверах.

Межсетевой экран - комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами. Основной задачей сетевого экрана является защита компьютерных сетей или отдельных узлов от несанкционированного доступа

VPN – Virtual Private Network, Виртуальные Частные сети

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящий документ «Политика информационной безопасности» (далее - Политика) является частью системы управления информационными технологиями Товарищества.

Настоящая Политика определяет совокупность правил, требований и принципов в области обеспечения информационной безопасности (далее - ИБ),

которыми должны руководствоваться все пользователи ИТ сервисов Товарищества в своей деятельности.

Целью настоящей Политики является обеспечение защиты от угроз, связанных с:

- попытками проникновения в его информационно-телекоммуникационные сети и хищением конфиденциальной информации;
- нарушением защиты от несанкционированного доступа в информационных системах Товарищества;
- неправомерным использованием информации, утечки информации и ее искажением;
- нарушением конфиденциальности, доступности и целостности информации в результате программно-аппаратных сбоев и выхода из строя ИТ сервисов.

2. ОСНОВНЫЕ ПОЛОЖЕНИЯ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Область применения

Положения настоящей политики распространяются на следующий перечень объектов:

- работники структурных подразделений Товарищества;
- поставщики, третьи лица и стороны, имеющие договорные отношения с Товариществом;
- информационные ресурсы Товарищества, составляющие конфиденциальную информацию, иные чувствительные по отношению к случайным и несанкционированным воздействиям и нарушению их безопасности, информационные ресурсы (базы данных, файлы, системная документация, руководства пользователя, учебные материалы, политики и процедуры и т.п.), в том числе общедоступная информация, представленная в электронном виде;
- информационная инфраструктура Товарищества, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, носители информации, системы и средства защиты информации, объекты и помещения, в которых размещены элементы ИТ ресурсов.

Цели защиты

Основной целью настоящей Политики является защита Товарищества и субъектов его информационных отношений от возможного нанесения ущерба посредством случайного или преднамеренного несанкционированного вмешательства в процесс функционирования ИТ ресурсов Товарищества или несанкционированного доступа к обрабатываемой информации и ее незаконного использования.

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

- доступности обрабатываемой информации для пользователей (устойчивого функционирования ИТ ресурсов, при котором пользователи имеют

возможность получения необходимой информации тогда, когда им это необходимо);
- конфиденциальность (сохранения в тайне) информации, хранимой, обрабатываемой в ИТ ресурсах Товарищества и передаваемой по каналам связи;
- целостности и аутентичности (подтверждение авторства) информации, хранимой и обрабатываемой в ИТ ресурсах Товарищества и передаваемой по каналам связи.

Основные задачи

Для достижения основной цели защиты и обеспечения свойств информации Политика ИБ должна обеспечивать эффективное решение следующих задач:
- защита от вмешательства в процесс функционирования ИТ ресурсов посторонних лиц;
- разграничение доступа (определение минимального уровня доступа) зарегистрированных пользователей ИТ ресурсов Товарищества;
- обеспечение аутентификации пользователей, участвующих в информационном обмене;
- регистрация в системных журналах действий пользователей при использовании ими ИТ ресурсов Товарищества;
- периодический мониторинг и контроль корректности действий пользователей путем анализа содержимого системных журналов;
- защита от несанкционированной модификации и контроль целостности используемых ИТ ресурсов;
- защита ИТ ресурсов от внедрения вредоносного программного обеспечения;
- защита информации ограниченного доступа, хранимой, обрабатываемой и передаваемой по каналам связи, от разглашения и искажения;
- обеспечение работоспособности криптографических средств защиты информации;
- своевременное выявление источников угроз безопасности информации, причин и условий, способствующих нанесению ущерба заинтересованным субъектам информационных отношений, 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.

3. ТРЕБОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Настоящая Политика определяет требования в следующих областях обеспечения информационной безопасности:
- Обучение и информированность персонала.
- Парольная Политика.
- Политика резервного копирования.
- Антивирусная Политика.
- Политика управления инцидентами по ИБ.

- Политика использования не корпоративных почтовых адресов для обмена служебными сообщениями по электронной почте.
- Политика по физической безопасности в Товарищества.
- Политика использования и управления внешними съемными носителями информации (все виды носителей) и регламент эксплуатации данных носителей.
- Правила защиты при хранении и передаче данных Товарищества.
- Правила доступа к сети Интернет.
- Политика удаленного доступа.
- Политика межсетевого экранирования.

Обучение и информированность персонала

Для обеспечения должного уровня ИБ, работники структурных подразделений Товарищества должны быть хорошо информированы в данных вопросах и при необходимости дополнительно обучены. Для этого в Товарищества должна быть организована эффективная система обучения и контроля знаний работников в области ИБ, включающая:

- обучение вопросам обеспечения ИБ в Товарищества при найме на работу;
- ознакомление с действующими нормативными документами по вопросам ИБ;
- при необходимости периодический контроль знаний по вопросам ИБ, в части касающейся выполняемых работниками Товарищества функций по защите информационных активов;
- при необходимости повышение квалификации лиц, выполняющих функции менеджера ИБ, сетевых администраторов, системных администраторов, путем обучения их на специализированных курсах по вопросам ИБ;
- организацию доступа работников Товарищества к нормативным документам по вопросам ИБ для самостоятельного изучения.

Парольная Политика

Основным инструментом защиты информационных систем Товарищества и информации хранящейся в них (далее - ИС), является персонализированная учетная запись, состоящая из идентификатора и пароля. Пароль должен выбираться пользователем ИС самостоятельно.

Пароли должны соответствовать следующим требованиям:

- минимальная длина пароля пользователя должна быть не менее 7 символов;
- при смене пароля пользователь не должен повторно использовать предыдущие три пароля;
- минимальная длина пароля службы администрирования и системных учетных записей (root, administrator и т.п.) должна быть не менее 12 символов, история паролей при смене не менее 20 паролей;
- пароли должны быть сложными, состоять из комбинации цифр, букв в верхнем и нижнем регистре;
- пароли не должны включать в себя легко вычисляемые сочетания символов (имена, фамилии, номера телефонов, словарные слова и т.п.) и какие либо сокращения;

- после 10 последовательных неудачных попыток авторизации в ИС в течении 30 минут, учетная запись пользователя должна блокироваться на полчаса;
- имена учетных записей запрещено использовать в качестве паролей.

Пользователь должен обеспечить конфиденциальность личного пароля. Передача пароля другим работникам Товарищества, работникам Службы ИТ, Руководству Товарищества или другим третьим лицам строго запрещена.

При работе с паролями должны выполняться следующие требования:

- новой учетной записи назначается временный пароль;
- первый вход в ИС пользователь должен осуществить с временным паролем;
- после аутентификации в ИС, пользователю должна быть предоставлена возможность смены пароля;
- пользователь должен сменить временный пароль после первого входа в ИС;
- пароли стандартных «по умолчанию» учетных записей ИС Товарищества должны быть изменены;
- пароли не должны передаваться кому либо, а также не должны включаться в сообщения, передаваемые по системам мгновенного обмена сообщениями, электронной почте или через другие виды связи;
- при вводе пароль не должен отображаться на экране в открытом виде;
- необходимо убедиться в том, что при вводе пароля, он не был подсмотрен;
- пользователь должен блокировать сеанс работы, если оставляет свое рабочее место на длительное время;
- сеансы работы, оставленные пользователем без присмотра, должны автоматически блокироваться по истечению 15 минут;
- записи о паролях в ИС Товарищества должны храниться в зашифрованном виде и быть доступны только их владельцу;
- пользователям запрещено записывать, хранить свои пароли на бумажном носителе;
- пароли службы администрирования должны храниться в запечатанном конверте в сейфе на случай замещения работника ответственного за администрирование информационных систем или аварийной ситуаций. Ключи от сейфа должен иметь только Руководитель Службы ИТ Товарищества. После смены паролей служба администрирования должна передать в запечатанном конверте новые значения паролей Руководителю Службы ИТ Товарищества на хранение;
- изъятие и вскрытие конвертов с паролями службы администрирования должно производится только Руководителем Службы ИТ Товарищества или лицом исполняющим его обязанности;
- Руководитель Службы ИТ имеет право сообщить пароли службы администрирования только лицу выполняющему функции администратора информационных систем;
- выдача пользователям временного пароля или активация заблокированной учетной записи (включая учетные записи пользователей временно не имеющих доступа к ИС Товарищества) выполнятся только по заявке утвержденной Руководителем структурного подразделения, в котором работает пользователь.

В следующих случаях требуется немедленная смена пароля, независимо от предписанных выше интервалов смены:

- имеется подозрение, что учетная запись была скомпрометирована;
- пароль был сообщен кому-либо непреднамеренно;
- пароль был использован другим лицом при аварийных ситуациях.

Политика резервного копирования

В целях защиты информации Товарищества от преднамеренного или непреднамеренного ее уничтожения и фальсификации должно быть обеспечено обязательное резервирование всей информации, являющейся важной для Товарищества.

При взаимодействии и по согласованию с владельцами информации должны быть выполнены следующие работы:

- классификация информации, подлежащей резервному копированию и/или архивированию;
- расчет объема информации, подлежащей резервному копированию и/или архивированию;
- составление расписания для системы резервного копирования;
- определение методов резервного копирования;
- определение ответственных лиц за хранение и резервирование информации;
- определение и согласование сроков хранения резервных и/или архивных копий, схемы ротации носителей и их количество;
- определение требований к восстановлению и тестированию резервных копий ИС.

Антивирусная Политика

Для защиты ИС и своевременного блокирования вредоносных программ (далее - Вирусов), в Товарищества должна применяться Система Антивирусной Защиты (САЗ).

САЗ должна основываться на клиент-серверной технологии. Клиентская часть должна быть установлена на всех рабочих станциях и ноутбуках Товарищества. Серверная часть должна предоставлять возможность централизованного управления и обновления антивирусного приложения, установленного на рабочих станциях и ноутбуках, а также обеспечивать возможность мониторинга состояния антивирусного приложения и оповещения об этих событиях ответственных лиц.

САЗ должна отвечать следующим требованиям:

- мониторинг возможных каналов проникновения Вирусов на всех средствах обработки информации, должен производиться в режиме реального времени;
- не реже одного раза в неделю должна производиться полная проверка средств обработки информации на предмет наличия Вирусов;
- пользователи средств обработки информации не должны иметь возможность отключения или изменения настроек антивирусного приложения;
- пользователи должны иметь возможность инициировать частичную или полную проверку средства обработки информации на предмет наличия Вирусов;

- обновление баз Вирусных сигнатур должно производиться регулярно, но не реже одного раза в сутки;
- обновление клиентских баз Вирусных сигнатур и приложения должно производиться незамедлительно после получения данных обновлений серверной частью САЗ.

Политика управления инцидентами в области ИБ

Для инцидентов в области ИБ должны выполнятся следующие мероприятия:

- немедленное реагирование на инцидент (защита системы);
- предоставление информации об инциденте;
- анализ инцидента;
- восстановление работоспособности ИС, возобновление бизнес-деятельности Товарищества (при необходимости);
- расследование причин инцидента, установление виновных;
- выработка корректирующих шагов (при необходимости) направленных на улучшение системы обеспечения ИБ;
- документирование инцидента.

Политика использования не корпоративных почтовых адресов для обмена служебными сообщениями по электронной почте

Работники Товарищества не должны использовать внешнюю электронную почту как официальное средство связи. В тех случаях, когда нарушение настоящего положения повлекли за собой утечку конфиденциальной информации, несанкционированное копирование, модификацию, блокирование или уничтожение информации, а также в случаях создания ситуаций, которые потенциально могли бы привести к таким последствиям, необходимо выполнить мероприятия по управлению инцидентами в области ИБ, согласно положениям настоящей Политики.

Политика по физической безопасности в Товарищества

Все объекты критичные с точки зрения информационной безопасности (все сервера баз данных, телефонная станция, маршрутизатор, файервол) должны находиться в отдельном помещении, доступ в которое разрешен только работникам, имеющими соответствующее разрешение от Руководителя ИТ.

Помещение должно быть оборудовано принудительной вентиляцией, пожарной сигнализацией и системой автоматического пожаротушения. Вход в помещение должен контролироваться карточной системой доступа и системой видео наблюдения с выходом на мониторы службы охраны здания.

Доступ в помещение посторонним лицам запрещен. Технический персонал, осуществляющий уборку помещения, ремонт оборудования, обслуживание кондиционера и т.п. может находится в помещении только в присутствии работников, имеющих право находится в помещении для выполнения своих должностных обязанностей.

Политика использования и управления внешними съемными носителями информации (все виды носителей) и регламент эксплуатации данных носителей

Внешние носители информации (USB флэш накопители, внешние жесткие диски, коммуникаторы, портативные компьютеры и т.д.) могут быть использованы с учетом следующих исключений:

- рекомендуется хранить информацию на зашифрованном внешнем съемном носителе;
- хранение служебной информации на личных внешних съемных носителях запрещено;
- запрещено передавать внешние съемные носители информации третьим лицам;
- запрещено оставлять внешние съемные носители информации без присмотра;

Правила защиты при хранении и передаче данных Товарищества

Процедуры, применяемые в Товарищества для хранения и передачи данных должны обеспечивать их конфиденциальность и целостность. Достижение данных требований при хранении данных обеспечивается путем реализации следующих мер безопасности:

- аутентификация и авторизация пользователей;
- шифрование данных;
- использование электронно-цифровой подписи;
- мониторинг использования (копирования, удаления, перемещения) информации.

При передаче данных, достижение данных требований обеспечивается путем реализации следующих мер:

- шифрование данных;
- использование электронно-цифровой подписи.

Правила доступа к сети Интернет

Доступ к развлекательным, вредоносным сайтам, а также к социальным сетям может быть заблокирован по инициативе Службы ИТ. Службой ИТ определяются группы пользователей и список запрещенных им ресурсов сети Интернет.

При работе в корпоративной сети Товарищества и сети Интернет работникам запрещается:

- рассылать информацию коммерческого характера (SPAM);
- скачивать и устанавливать на компьютер программное обеспечение не входящее в список разрешенного к использованию;
- посещать интернет-ресурсы, не имеющие непосредственного отношения к работе и выполнению служебных обязанностей;
- осуществлять подписку на рассылку информации непроизводственного характера;
- сообщать адрес электронной почты в непроизводственных целях;
- использовать Интернет для получения материальной выгоды или непроизводственных целей, в том числе осуществляя торговлю через Интернет.

Политика удаленного доступа

Удаленный доступ к ИС Товарищества через сеть Интернет или каналы связи, не находящиеся под контролем Товарищества, должен быть защищен посредством использования технологии VPN.

Используемые в Товарищества средства реализации технологии VPN должны обеспечивать выполнение следующих требований:

- наличие уникального идентификатора у каждого пользователя;
- шифрование среды передачи данных;
- при необходимости проверка соответствия конфигурации пользовательских устройств, требованиям корпоративных политик;
- ведение аудиторского следа удачных и неудачных попыток авторизации в процессе подключения;
- использование защищенных протоколов передачи данных.

Политика межсетевого экранирования

В Товарищества должны быть реализованы межсетевые экраны, которые классифицируются по следующим признакам:

- по исполнению (аппаратно-программный и программный);
- по используемой технологии (контроль состояния протокола, на основе модулей посредников (proxy)).

Конфигурация межсетевого экрана должна быть полностью формализована. Межсетевые экраны должны управлять всем входящим и исходящим трафиком.