**УТВЕРЖДАЮ**
**Генеральный директор**
**АО «ЧАК»**

**_____ Д.В. Крючков**

**«16» 11 2020 г.**

# ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В АО «ЧАК»

г. Новочебоксарск, 2020г.

## Содержание


1 Назначение и область применения ... 3
2 Нормативные ссылки ... 3
3 Термины и определения ... 3
4 Обозначения и сокращения ... 5
5 Ответственность ... 5
6 Участники процесса обеспечения информационной безопасности ... 5
7 Правовое обеспечение информационной безопасности ... 5
8 Соглашение о конфиденциальности ... 6
9 Классификация информации ... 6
10 Организация рабочего места ... 6
11 Организация дистанционной работы ... 7
12 Безопасность электронного документооборота ... 7
13 Антивирусная защита ... 7
14 Использование сети Интернет ... 8
15 Электронная почта ... 8
16 Программное обеспечение ... 9
17 Использование мобильных устройств ... 9
18 Ведение переговоров и использование средств связи ... 9
19 Физическая защита информационных ресурсов ... 10
20 Сетевая безопасность ... 10
21 Настройка оборудования и техническое обслуживание ... 11
22 Аудит информационной безопасности ... 12
23 Работа с третьими лицами ... 12
Приложение №1 ... 13
Лист регистрации изменений ... 14
Лист согласования и рассылки ... 15

## 1 Назначение и область применения

1.1 Настоящая Политика разработана с целью обеспечения защиты информационных ресурсов Акционерного общества «Чувашская автотранспортная компания» (далее –Общество) от различного вида угроз, внешних и внутренних, умышленных и непреднамеренных, минимизации ущерба, в результате реализации угроз.

1.2 Целью настоящей Политики является определение направлений обеспечения информационной безопасности, актуальных для Общества, ане детализация всех правил и мер, направленных на обеспечения информационной безопасности.

1.3 Настоящая Политика распространяется на все структурные подразделения Общества.

1.4 Требования Политики обязательны к исполнению всеми работниками Общества в части их касающейся.

## 2 Нормативные ссылки

В настоящей Политике использованы ссылки на следующие документы:

2.1 Федеральный закон от 29.07.2004 г. № 98-ФЗ «О коммерческой тайне» (с изменениями и дополнениями)

2.2 Федеральный закон от 27.07.2006г. №149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями и дополнениями)

2.3 Федеральный закон от 27.07.2006г. №152-ФЗ «О персональных данных» (с изменениями и дополнениями)

2.4 Федеральный закон от 30.12.2001г. №197-ФЗ «Трудовой Кодекс Российской Федерации» (с изменениями и дополнениями)

2.5 Федерального закона от 27.07.2010 г. №224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации»(с изменениями)

2.6 Гражданский кодекс Российской Федерации (с изменениями и дополнениями)

2.7 ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности»

## 3 Термины и определения

В настоящей Политике применены следующие термины с соответствующими определениями:

**Аудит информационной безопасности**– системный процесс получения объективных качественных и количественных оценок о текущем состоянии информационной безопасности в соответствии с определенными критериями и показателями безопасности.

**Инсайдерская информация** – точная и конкретная информация, которая не была распространена или предоставлена (в том числе сведения, составляющие коммерческую, служебную, банковскую тайну, тайну связи (в части информации о почтовых переводах денежных средств) и иную охраняемую законом тайну), распространение или предоставление которой может оказать существенное влияние на цены финансовых инструментов, товаров Общества, иностранной валюты и которая относится к информации, включенной в соответствующий перечень инсайдерской информации, утвержденный ФСФР России (в соответствии с ч. 1 ст. 2 Федерального закона от 27 июля 2010 года №224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации»).

**Информационная безопасность (ИБ)** – состояние защищенности технологических и бизнес-процессов, объединяющих в своем составе технические и программные средства обработки информации, информацию в условиях угроз в информационной сфере.

**Информационная система (ИС)** – совокупность программно-аппаратных комплексов, применяемых для обеспечения бизнес – процессов.

**Инцидент информационной безопасности** – это появление одного или нескольких нежелательных рисковых событий информационной безопасности, с которыми связана значительная вероятность нарушения конфиденциальности, целостности или доступности информационных активов и инфраструктуры и создания угрозы информационной безопасности.

**Коммерческая тайна** – режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

**Конфиденциальная информация** – любая информация, независимо от формы ее предоставления и носителя, которая не является общеизвестной или широкодоступной из других источников на законном основании, не относится к государственной тайне, и доступ к которой третьим лицам ограничен или невозможен без согласия ее обладателя.

Виды конфиденциальной информации в АО «ЧАК»:

– персональные данные;
– информация, относящаяся к коммерческой тайне;

**Конфиденциальность информации** – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

**Модель угроз** – описательное представление свойств или характеристик угроз безопасности информации.

**Модель нарушителя** – описательное представление опыта, знаний, доступных ресурсов возможных нарушителей ИБ, необходимых им для реализации угрозы ИБ, и возможной мотивации действий.

**Персональные данные** – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).

**Подразделение по защите информации** – отдел защиты информации и информационно-аналитической работы Департамента безопасности ПАО «МРСК Волги».

**Пользователь информационной системы** – физическое лицо, обладающеевозможностью доступа к информационной системе.

**Правила информационной безопасности** – список разрешенных и/или запрещенных действий для пользователей информационной системы.

**Разглашение конфиденциальной информации** – действие или бездействие, в результате которых конфиденциальная информация в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору.

**Режим конфиденциальности информации** – организационно-техническиемероприятия по защите информации, позволяющие обладателю конфиденциальной информации при существующих иливозможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранитьположение на рынке товаров, работ, услуг или получить иную коммерческую выгоду, иреализующие меры по охране конфиденциальной информации.

**Структурное подразделение** – организационно-структурная единица Общества.

**Угроза информационной безопасности** – риск, влияющий на нарушение одного (или нескольких) свойств информации – целостности, конфиденциальности,доступности объектов Общества.

**Электронный документ** – документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием

электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах».

## 4 Обозначения и сокращения

**Общество** – Акционерное общество «Чувашская автотранспортная компания» (АО «ЧАК»).

## 5 Ответственность

5.1 Работники Общества несут персональную ответственность за выполнение требований настоящей Политики.

5.2 Каждый работник Общества должен быть проинформирован о правилах информационной безопасности и знать, какие санкции могут быть к нему применены в случае несоблюдения требований информационной безопасности. Работники Общества, третьи лица, участвующие в обработке информации Общества должны получать соответствующую и постоянно обновляемую информацию о требованиях информационной безопасности и средствах контроля.

5.3 Обязанность работников Общества по соблюдению правил обеспечения информационной безопасности, установленных в Обществе, должна быть в обязательном порядке отражена в их должностных инструкциях.

5.4 Работники Общества, нарушающие требования настоящей Политики, могут быть привлечены к дисциплинарной ответственности в соответствии с Трудовым кодексом Российской Федерации.

5.5 В случае нанесения ущерба Обществу, связанному с разглашением сведений, содержащих конфиденциальную информацию,работник несет ответственность в соответствии с законодательством Российской Федерации.

## 6 Участники процесса обеспечения информационной безопасности

6.1 Руководители структурных подразделений (отделов) в соответствии с функциями подразделения обеспечивают организацию в подразделении (отделе) контроль соблюдения норм и правил обеспечения информационной безопасности, информируют руководство Общества о любых подозрительных событиях и (или) о нарушениях действующих правил обеспечения информационной безопасности.

6.2 Работники, наделенные значительными техническими правами (системные администраторы, разработчики, администраторы баз данных и т.д.), должны применять необходимые меры по конфигурации систем для обеспечения необходимого уровня информационной безопасности.

6.3 Работники Общества должны соблюдать правила информационной безопасности, действовать осторожно и проявлять осмотрительность в отношении любых действий, которые могут повлечь за собой снижение уровня информационной безопасности, информировать своих непосредственных руководителей обо всех подозрительных событиях информационной безопасности.

## 7 Правовое обеспечение информационной безопасности

Обеспечение информационной безопасности должно осуществляться в соответствии с требованиями законодательства Российской Федерации, подзаконных актов в области

информационной безопасности, нормативно-методических и руководящих документов ФСБ России и ФСТЭК России, организационно-распорядительных документов Общества по вопросам обеспечения информационной безопасности, а также с учетом лучших отечественных и зарубежных практик.

## 8 Соглашение о конфиденциальности

Перед предоставлением работникам доступа к информационным ресурсам Общества и конфиденциальной информации работники Общества подписывают соглашение о конфиденциальности.

## 9 Классификация информации

9.1 Для обеспечения адекватного потребностям Общества уровня защиты информационных ресурсов, содержащаяся в них информация классифицируется в соответствии со степенью ее важности для Общества.

9.2 К информации с повышенными требованиями к обеспечению конфиденциальности, целостности и/или доступности относятся: персональные данные, коммерческая тайна, а также иная информация, в отношении которой требования к обеспечению конфиденциальности, целостности и/или доступности установлены действующим законодательством, организационно-распорядительными документами Общества, условиями соглашений с третьими сторонами.

9.3 К информации с минимально достаточными требованиями к обеспечению конфиденциальности относится внутренняя информация, являющаяся собственностью Общества, не являющаяся открытой информацией, не отнесенная к информации с повышенными требованиями к обеспечению конфиденциальности, целостности и/или доступности, включая любые служебные документы.

9.4 К информации без предъявления требований к обеспечению конфиденциальности относится открытая информация и информация, предназначенная для опубликования в открытых источниках.

9.5 В отношении информационных ресурсов, содержащих конфиденциальную информацию, должен быть установлен соответствующий режим обработки информации, подразумевающий проведение организационно-технических мероприятий по защите.

9.6 Конфиденциальная информация не подлежит передаче по открытым каналам передачи данных и в открытой переписке, в личных и деловых переговорах по открытым каналам связи и средствах массовой информации.

## 10 Организация рабочего места

10.1 Организация нового рабочего места пользователя информационных ресурсов Общества должна быть санкционирована руководителем работника и согласована с руководителем отдела безопасности.

10.2 Учетная запись пользователя включается в группу пользователей. Назначение пользователю привилегий администратора в общем случае не допускается.

10.3 Средства обработки информации должны быть размещены таким образом, чтобы исключить возможность несанкционированного ознакомления посторонних лиц с обрабатываемой информацией.

10.4 Оборудование должно быть защищено от хищения или порчи, а также от воздействия окружающей среды, способного привести к его повреждению или преждевременному выходу из строя.

10.5 Запрещается использовать на рабочем месте оборудование и программное обеспечение, не принадлежащие Обществу или не предназначенные для выполнения пользователем своих должностных обязанностей.

10.6 При оставлении, даже на непродолжительное время, своего рабочего места, пользователь должен заблокировать доступ к своему компьютеру и предпринять соответствующие меры по защите конфиденциальной информации на физических носителях.

## 11 Организация дистанционной работы

11.1 Предоставление пользователю дистанционного доступа к информационным ресурсам Общества должно быть согласовано с руководителем отдела безопасности.

11.2 Для контроля доступа пользователя в дистанционном режиме должны использоваться надежные методы аутентификации.

11.3 Доступ в дистанционном режиме в обязательном порядке организуется с использованием средств шифрования трафика.

11.4 Дистанционный доступ к используемым диагностическим и конфигурационным портам оборудования запрещается.

11.5 Для сеансов дистанционного доступа должно быть установлено время бездействия, по истечении которого сеанс автоматически завершается.

11.6 Обязательными условиями предоставления дистанционного доступа к информационным ресурсам являются:

– установка и своевременное обновление на компьютере пользователя средств антивирусной защиты;

– установка и надлежащая настройка на компьютере пользователя применяемых средств предотвращения атак;

– настройка локальных параметров безопасности на компьютере пользователя в соответствии с применяемыми групповыми политиками.

## 12 Безопасность электронного документооборота

12.1 Электронные документы должны быть представлены в формате, позволяющем указывать дополнительные идентифицирующие атрибуты, в том числе автора, дату создания и последнего изменения, права доступа и т. д.

12.2 При хранении электронных документов в файловых архивах в сети, доступ к ним должен быть разграничен и предоставляться только пользователям, имеющим соответствующие права.

12.3 Локальное хранение электронных документов на компьютере пользователя запрещено.

12.4 При передаче электронных документов, содержащих конфиденциальную информацию, по незащищенным каналам или на сменных носителях, в том числе за пределы Общества, должны применяться средства криптографической защиты информации.

12.5 Выведенный на бумажный носитель электронный документ, содержащий конфиденциальную информацию, должен незамедлительно изыматься из лотка принтера общего пользования для его защиты от неавторизованного прочтения.

## 13 Антивирусная защита

13.1 Средства антивирусной защиты должны быть установлены, настроены и активизированы на всех допускающих такую установку программно-технических средствах до начала их использования в составе сети Общества.

13.2 Средства антивирусной защиты должны иметь все последние обновления, полученные из доверенных источников.

13.3 Контролю на предмет обнаружения вредоносных программ должна подвергаться вся информация, создаваемая и/или обрабатываемая программно-техническими средствами, а также принимаемая и/или передаваемая с помощью машинных носителей или средств телекоммуникаций.

13.4 Эксплуатация средств антивирусной защиты должна осуществляться только на основании лицензионных соглашений с их правообладателями.

13.5 Состав, архитектура и конфигурация средств антивирусной защиты должны быть стандартизованы, а процессы их установки, настройки, обеспечения ресурсами, эксплуатации и обновления регламентированы, протоколироваться и контролироваться.

13.6 Пользователям запрещается деактивировать установленные на рабочих станциях средства антивирусной защиты. Администраторам запрещается деактивировать установленные средства защиты, кроме случаев, связанных с проведением регламентированных восстановительных работ, согласованных с руководителем отдела безопасности.

## 14 Использование сети Интернет

14.1 Доступ работников Общества к сети Интернет должен быть санкционирован непосредственным руководителем, и согласован с руководителем отдела безопасности.

14.2 Доступ работников Общества к сети Интернет должен быть разрешен только для выполнения должностных обязанностей и не может использоваться для ненадлежащей или незаконной деятельности. Запрещается посещение любого сайта в сети Интернет, который считается оскорбительным для общественного мнения или содержит информацию сексуального характера, пропаганду расовой ненависти, дискредитирующие заявления или иные материалы с оскорбительными высказываниями, религиозных или политических убеждений, национального происхождения или недееспособности.

14.3 Информация, принимаемая и передаваемая посредством сети Интернет, должна подвергаться мониторингу и анализу на предмет соответствия информационного обмена установленным ограничениям.

14.4 Информация, полученная из сети Интернет, должна использоваться с учетом прав на интеллектуальную собственность, а также прав на использование программных продуктов, являющихся предметом собственности третьих лиц.

14.5 Информация, передаваемая посредством сети Интернет, должна быть защищена в соответствии с ее категорией.

## 15 Электронная почта

15.1 Электронная почта должна использоваться сотрудниками только для выполнения должностных обязанностей. Использование корпоративной электронной почты в личных целях не допускается.

15.2 Служебная переписка должна вестись только через корпоративный сервер электронной почты. Использование внешних серверов и сервисов электронной почты, кроме случаев, связанных с отказом корпоративного сервера электронной почты, запрещено. Использование внешних серверов и сервисов электронной почты должно быть согласовано с руководителем отдела безопасности.

15.3 Электронная почта не должна использоваться для передачи или получения материалов, защищенных авторским правом, без разрешения правообладателя.

15.4 Информация, принимаемая и передаваемая посредством электронной почты с использованием информационных ресурсов Общества, должна подвергаться мониторингу и анализу на предмет соответствия информационного обмена установленным ограничениям.

15.5 Все входящие и исходящие сообщения электронной почты должны быть проверены на наличие в них вредоносного кода.

15.6 Передача конфиденциальной информации в незащищенном виде средствами электронной почты не допускается.

15.7 При передаче по электронной почте сообщений, содержащих конфиденциальную информацию, должны использоваться средства криптографической защиты.

15.8 Электронные сообщения от неизвестных отправителей, или содержащие неизвестные вложения, должны удаляться без прочтения.

15.9 Все факты отправки, приема и обработки электронных сообщений должны регистрироваться.

15.10 Входящие и/или исходящие сообщения электронной почты могут быть задержаныв случае их несоответствия установленным ограничениям.

## 16 Программное обеспечение

16.1 Во всех информационных системах Общества разрешается использовать только лицензионное программное обеспечение в соответствии с требованиями действующего законодательства и соответствующих лицензионных соглашений.

16.2 Перечень устанавливаемого программного обеспечения формируется исходя из функций информационной системы и в соответствии с паспортом информационной системы.

16.3 Пользователям запрещается самовольно устанавливать программное обеспечение на компьютеры и другие средства обработки информации.

16.4 Пользователям запрещается использовать установленное программное обеспечение, не предназначенное для исполнения ими функциональных обязанностей, в том числе системные утилиты и программы.

16.5 При внесении изменений в операционные системы, в том числе после установки обновлений, должна быть проведена проверка корректности работы критичных приложений.

## 17 Использование мобильных устройств

17.1 Использование мобильных устройств для работы с информационными ресурсами Общества и хранения конфиденциальной информации Общества запрещено.

## 18 Ведение переговоров и использование средств связи

18.1 Запрещается обсуждать конфиденциальную информацию,не приняв достаточных мер по недопущениюее утечки и (или) разглашения.

18.2 Запрещается передавать конфиденциальную информацию по открытым каналам связи, не приняв достаточных мер по ее технической защите.

18.3 Запрещается оставлять сообщения, содержащие конфиденциальную информацию, на автоответчиках и в системах голосовой почты.

18.4 При использовании средств связи следует учитывать, что незащищенная передаваемая информация может быть перехвачена, подслушана или подсмотрена посторонними лицами, и принимать разумные меры предосторожности по недопущению этого.

18.5 При проведении совещаний, на которых обсуждается конфиденциальная информация, использование средств мобильной сотовой связи запрещается.

## 19 Физическая защита информационных ресурсов

19.1 Доступ в помещения Общества, где размещаются информационные ресурсы, средства обработки информации и вспомогательное оборудование (устройства электропитания, кондиционирования, коммуникации и др.) должен контролироваться при помощи технических средств управления доступом, систем видеонаблюдения или уполномоченными лицами.

19.2 При размещении оборудования в местах доступа посторонних лиц оно должно быть размещено таким образом, чтобы исключить возможность неавторизованного доступа, хищения или повреждения. При невозможности такого размещения должны быть приняты меры к тому, чтобы оборудование не оставалось без присмотра авторизованного персонала.

19.3 В помещениях, где размещено оборудование, должны быть предусмотрены меры защиты от пожара, затопления, взрыва и других разрушающих природных и антропогенных воздействий.

19.4 Помещения серверных комнат должны быть оборудованы средствами наблюдения и регистрации.

19.5 Должны быть предусмотрены меры по обеспечению приемлемого эксплуатационного режима работы оборудования (температуры, влажности, освещенности, уровня электромагнитных излучений и др.) согласно требованиям соответствующих стандартов и нормативных документов.

19.6 Должны быть предусмотрены меры защиты оборудования от перебоев электропитания или других поддерживающих услуг.

19.7 Кабельные линии должны быть проложены в соответствии с требованиями нормативных документов для обеспечения их надлежащей защиты от непреднамеренного повреждения. При прокладке кабельных линий в неконтролируемых зонах должны быть приняты разумные дополнительные меры по защите от несанкционированного подключения.

19.8 Все оборудование, обеспечивающее функционирование информационного ресурса, в том числе вспомогательное оборудование, подлежит техническому обслуживанию в соответствии с правилами технического обслуживания.

19.9 При утилизации (списании) оборудования все его компоненты, содержащие носители данных, должны быть проверены с целью безопасного сохранения или удалениялюбых чувствительных данных и лицензионного программного обеспечения.

19.10 Не контролируемый вынос (внос) оборудования и носителей информации с (на) территории (ю) Общества запрещен.

19.11 При организации работы оборудования вне контролируемых зон, а также при транспортировке носителей информации за пределами территории Общества должны предприниматься все меры защиты для предотвращения неавторизованного доступа, повреждения или утери оборудования и носителей информации.

19.12 Все коммуникационные порты средств обработки информации должны быть защищены от неавторизованного доступа надежными программно-аппаратными способами. При невозможности применения таких способов порты должны быть опечатаны защитными пломбами.

19.13 Допускается не опечатывать коммуникационные порты устройств обработки информации в запирающихся шкафах, при условии опечатывания шкафа.

## 20 Сетевая безопасность

20.1 В корпоративной сети Общества выделяются следующие сегменты:

- внутренние;
- закрытые;
- демилитаризованные зоны;
- удаленные сегменты и пользователи.

20.2 Сопряжение сегментов осуществляется при помощи средств межсетевого экранирования (межсетевых экранов или маршрутизаторов с возможностью фильтрации трафика).

20.3 Количество точек сопряжения сегментов должно быть ограничено и минимально необходимо.

20.4 Правила фильтрации трафика для средств межсетевого экранирования должны быть надлежащим образом определены и настроены, и должны позволять сетевое взаимодействие, минимально достаточное для корректного функционирования систем.

20.5 Закрытые сегменты могут сопрягаться только с внутренними сегментами сети.

20.6 Внутренние сегменты сопрягаются только с закрытыми сегментами и демилитаризованными зонами.

20.7 Системы (ftp, e-mail, www), участвующие во взаимодействии с глобальными сетями, в том числе с сетью Интернет, размещаются в демилитаризованных зонах.

20.8 Демилитаризованные зоны отделяются от глобальных сетей средствами межсетевого экранирования.

20.9 Удаленные сегменты сопрягаются с демилитаризованными зонами, обособленными от зон, в которых размещены взаимодействующие с глобальными сетями системы. Допускается сопряжение удаленных сегментов и пользователей к внутренним сегментам по выделенным каналам связи при условии соблюдения необходимых мер безопасности.

20.10 При заключении любых договоров по разработке и развитию информационных и телекоммуникационных систем должны быть определены требования к информационной безопасности.

20.11 Использование беспроводных сетей и точек доступа в общем случае запрещено.

20.12 При необходимости использования беспроводного доступа такое решение должно быть согласовано с руководителем отдела безопасности. При этом должны быть приняты адекватные меры защиты, исключающие возможность несанкционированного подключения, перехвата и внедрения трафика, включая автоматическую идентификацию беспроводного оборудования по физическим адресам и шифрование сетевого трафика.

## 21 Настройка оборудования и техническое обслуживание

21.1 Настройка, конфигурирование, техническое обслуживание и ремонт оборудования и кабельных линий производится только уполномоченными на то работниками Общества или обслуживающих организаций и документируется. Выполнение этих работ неуполномоченными на то лицами запрещена.

21.2 Техническое обслуживание оборудования и кабельных линий проводится регулярно в соответствии с процедурами технического обслуживания, с учетом требований страхования (при его наличии) и гарантийного обслуживания.

21.3 Техническое обслуживание и ремонт оборудования и кабельных линий проводится таким образом, чтобы исключить или минимизировать риски потери функциональности сети Общества.

21.4 В программно-технических средствах, предъявляемых для технического обслуживания и ремонта или возвращаемых в резерв по окончании технического обслуживания, вся конфиденциальная информация (данные и программы) после переноса на другие носители уничтожается способом, обеспечивающим невозможность ее восстановления, с соответствующей регистрацией.

21.5 Все устройства хранения информации перед утилизацией проверяются на наличие конфиденциальной информации. При наличии таковой они уничтожаются по акту способом, гарантирующим невозможность ее восстановления.

## 22 Аудит информационной безопасности

22.1 Аудит информационной безопасности проводится с санкции руководства Общества.

22.2 Аудит информационной безопасности проводится Аудитором - Подразделением по защите информации или внешней организацией, в том числе с привлечением экспертов из других структурных подразделений или специализированных организаций.

22.3 Проверяемые подразделения обязаны предоставлять Аудитору доступ к объектам аудита, сообщать необходимые сведения и оказывать иное содействие в объеме, достаточном для достижения целей аудита.

22.4 Аудит автоматизированных систем должен проводиться в режиме чтения или на копии автоматизированной системы, а производимые действия протоколироваться.

22.5 Отчет об аудите и предложения по устранению выявленных недостатков согласовываются с проверяемыми структурными подразделениямии представляются руководству для утверждения и назначения ответственного за реализацию корректирующих мероприятийи сроков повторной проверки.

22.6 Доступ к инструментальным средствам аудита должен быть ограничен для предотвращения их неправильного использования или компрометации.

## 23 Работа с третьими лицами

23.1 Исполнение договоров, несущих в себе риски информационной безопасности должно быть обеспечено необходимыми мерами по выполнению требований информационной безопасности, установлению режима конфиденциальности в отношении обрабатываемой в рамках исполнения договоров конфиденциальной информации.

23.2 В договорах на оказание третьей стороной услуг, обеспечивающих критически важные процессы, должны быть определены параметры безопасности услуг и учтены требования по реализации средств контроля безопасности.

23.3 Информационные и коммуникационные услуги, предоставляемые третьими сторонами, обеспечивающие критически важные процессы, должны подвергаться регулярному мониторингу и аудиту информационной безопасности.

**ОБЯЗАТЕЛЬСТВО**
**о неразглашении персональных данных**

Я, _____, паспорт серии _____, № _____, _____,

_____, что приступая к работе, получаю доступ к персональным данным работников АО «ЧАК»
(должность)

В связи с этим я добровольно принимаю на себя следующие обязательства:

- не разглашать и не передавать третьим лицам конфиденциальные сведения о персональных данных работников, которые мне доверены (будут доверены) или известны (станут известны) в связи с выполнением моих должностных обязанностей.
- не использовать конфиденциальные сведения о работниках АО «ЧАК» с целью получения выгоды.
- в случае попытки третьих лиц получить у меня конфиденциальные сведения сообщать непосредственному руководителю – главному инженеру, а в его отсутствие заменяющему его лицу.
- выполнять требования нормативных правовых актов, регламентирующих вопросы защиты персональных данных.

Мне известно, что в случае нарушения данного обязательства я буду привлечен к ответственности в соответствии с законодательством РФ.

Должность Подпись /ФИО/

## Лист регистрации изменений

| № п/п | Номер пункта | Номер листа | Номер и дата извещения | Дата внесения изменений | Ф.И.О., подпись |
|---|---|---|---|---|---|
| 1 | | | | | |
| 2 | | | | | |
| 3 | | | | | |
| 4 | | | | | |
| 5 | | | | | |
| 6 | | | | | |
| 7 | | | | | |
| 8 | | | | | |
| 9 | | | | | |
| 10 | | | | | |