**УТВЕРЖДАЮ**

Генеральный директор
ООО «Сатурн»

_____ Соколов А.А

«____» _____ 20__ г.

# РЕГЛАМЕНТ

## ПО ИСПОЛЬЗОВАНИЮ ЭЛЕКТРОННОЙ ПОЧТЫ В ООО «САТУРН»

г. Москва

2018 г.

## 1 Область применения

1.1 Настоящий документ регламентирует порядок предоставления доступа к работам, связанным с использованием корпоративной электронной почты из локально-вычислительной сети Компании и глобальной сети Интернет, и устанавливает требования по безопасности с целью снижения рисков, связанных с передачей информации с использованием информационных средств и систем.

1.2 Настоящий документ является дополнением к действующей политике информационной безопасности ООО «Сатурн» и действующим нормативным документам, определяющим требования режима и информационной безопасности в Компании.

1.3 Настоящий документ предназначена для применения работниками Компании во всех структурных подразделениях, использующих в работе корпоративную электронную почту.

1.4 Настоящий документ предназначена для применения всеми сотрудниками сторонних организаций, использующих информационные средства и системы обществ Компании для доступа к работам с использованием электронной почты, в рамках выполнения договорных или иных обязательств.

## 2 Термины и определения

В настоящей инструкции применены следующие термины с соответствующими определениями:

2.1 **Интернет:** Всемирная система объединенных компьютерных систем для хранения и передачи информации.

2.2 **электронная почта (англ. email, e-mail, от англ. electronic mail):** Технология и предоставляемые ею услуги по пересылке и получению электронных сообщений (называемых «письма» или «электронные письма») по распределённой (в том числе глобальной) компьютерной сети.

2.3

**электронная подпись:** Информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

[Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи», статья 2]

2.4 **корпоративная защищённая электронная почта Компании:** Система, построенная в границах информационного пространства локальных сетей Компании посредством программ и сервисов с использованием центра сертификации, гарантирующих безопасность информационных и коммуникационных систем, использующих криптографические алгоритмы с

открытыми ключами, а также позволяющая получателю сообщений электронной почты убедиться в подлинности и целостности сообщения.

2.5 **информация общего пользования:** Информация, не относящаяся к коммерческой тайне обществ Компании и не являющаяся государственной тайной.

2.6 **конфиденциальная информация:**

– составляющая коммерческую тайну - научно-техническая, технологическая, производственная, финансово-экономическая или иная информация (в том числе, составляющая секреты производства (ноу-хау)), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой введен режим коммерческой тайны;

2.7 **спам:** Несанкционированная массовая рассылка электронной почты.

## 3 Обозначения и сокращения

В настоящей инструкции применены следующие обозначения и сокращения:

АС – автоматизированная система

Администратор ИБ – администратор информационной безопасности

ИБ – информационная безопасность

ИТ – информационные технологии

КЗЭП – корпоративная защищённая электронная почта Компании

ЛВС – локальная вычислительная сеть

ПК – персональный компьютер

ПО – программное обеспечение

ЭП – электронная почта

## 4 Общие положения

4.1 Корпоративная ЭП служит для осуществления деловой переписки между предприятиями и внутри обществ Компании, а также сторонними организациями, как российскими, так и зарубежными.

4.2 Адреса корпоративной ЭП, относящиеся к Компании, представляют собой связку персонифицированного идентификатора сотрудника (сокращения от имени и фамилии работника латинскими буквами) и имени домена почтового сервера @saturn**.ru (образец: ivan.ivanov@saturn**.ru).

4.3 Система ЭП построена на основе ПО с использованием средств электронной подписи корпоративного центра сертификации Компании.

4.4 Передача сведений, составляющих государственную тайну, средствами ЭП – **запрещена.**

4.4.1 Для передачи конфиденциальной информации внутри Компании предназначена КЗЭП Компании построенная на базе программного обеспечения ***.

4.5 Для осуществления сеанса работы с корпоративной ЭП и доступа к почтовым серверам Компании необходимо использовать только лицензионное ПО.

4.6 Изменение конфигурации ПО для работы с ЭП должно проводиться только сотрудниками подразделения, ответственно за ИТ и ИБ.

4.7 Предоставление доступа к работам с использованием корпоративной ЭП сотрудникам сторонних организаций может предоставляться в рамках выполняемых договорных или иных обязательств по решению руководства обществ Компании с соблюдением требований режима и информационной безопасности.

4.8 Перед предоставлением доступа к работам с использованием ЭП работник Компании должен быть ознакомлен с положениями настоящей инструкции.

4.9 Сервисы, предоставляемые при работе с корпоративной ЭП:

4.9.1 Отправка и получение электронных сообщений;

4.9.2 Календарь;

4.9.3 Адресная книга, которая включает глобальный список адресов работников обществ Компании.

4.10 Доступ работников обществ Компании к корпоративной ЭП предоставляется для ведения служебной переписки.

4.11 В качестве дополнительных сервисов, работникам может быть предоставлен доступ к ресурсам корпоративной ЭП посредством web интерфейса, а также приложений на устройствах мобильной связи (планшеты, смартфоны и пр.). Установка приложений на устройствах мобильной связи осуществляется работником самостоятельно. Настройка приложений на устройствах мобильной связи производится работником в соответствии с инструкцией, полученной от подразделения ИТ. Доступ к ресурсам корпоративной электронной почты посредством web интерфейса и приложений на устройствах мобильной связи ограничен. Для подключения дополнительных сервисов доступа к корпоративной ЭП в подразделение ИТ направляется письменный запрос, согласованный с непосредственным руководителем работника и руководителем безопасности Компании.

4.12 В соответствии частью 4 статьи 10 Федерального Закона «О коммерческой тайне» № 98-ФЗ от 29 июля 2004 года в информационных системах Компании применяются средства и методы технической защиты конфиденциальной информации.

4.13 Выполнение Работниками обществ Компании требований настоящей инструкции контролируется работниками ИТ и ИБ с применением средств управления и технической защиты ЛВС.

## 5 Подключение ЭП

5.1 Для выполнения служебных обязанностей работника Компании с использование ЭП, при приеме на работу такого работника, отдел кадров направляет в подразделение ИТ уведомление о приеме нового работника с указанием фамилии, имени и отчества сотрудника, занимаемой должности, помещения (№ кабинета, комнаты), контактного номера телефона, публичного (личного) адреса электронной почты и обоснования производственной необходимости подключения к КЭЭП.

5.2 Для выполнения работ по предоставлению доступа к работам с использованием корпоративной ЭП, ПК сотрудника должен быть предварительно настроен и подключен к ЛВС Компании сотрудниками ИТ.

5.3 Сотрудниками ИТ, средствами администрирования системы электронной почты, должна быть создана персонифицированная учетная запись работника и создан электронный почтовый ящик.

5.4 Установка, настройка и проверка работоспособности программных средств, необходимых для доступа сотруднику на рабочем месте с ПК к ЭП, средств электронной подписи и средств шифрования проводится работниками ИТ.

5.5 Перед началом выполнения служебных обязанностей с использованием корпоративной ЭП работник проходит инструктаж по соблюдению правил информационной безопасности при работе с использованием ЭП.

5.6 При необходимости, с сотрудником, допущенным до работ с использованием ЭП, сотрудником ИТ проводится обучение по работе с ПО, предназначенным для отправки и получения корреспонденции.

## 6 Прекращение доступа к работам с использованием ЭП

6.1 Доступ к корпоративной ЭП может быть ограничен или прекращен при переводе работника в другое структурное подразделение Компании, а также при нарушении требований настоящей инструкции.

6.2 Ограничение доступа к корпоративной ЭП осуществляется сотрудниками ОИБ по решению руководства Компании.

## 7 Права сотрудника при работе с ЭП

Сотрудник при работе с использование ЭП имеет право:

7.1 Доступа к электронному почтовому ящику на рабочем месте для отправки и получения корреспонденции.

7.2 Доступа к календарю и событиям календаря. Назначать и отменять рабочие встречи, в рамках выполняемых должностных обязанностей.

7.3 Сохранять электронные документы и файлы, полученные посредством ЭП, на локальном диске ПК, сетевых директориях и вложенных подпапках, если содержание корреспонденции не противоречит

законодательству Российской Федерации и нормативным документам, определяющим требования режима и информационной безопасности Компании.

7.4 Запрашивать в подразделениях ИТ и ИБ информацию о работоспособности систем, связанных с работой корпоративной ЭП.

## 8 Обязанности сотрудника при работе с ЭП

Сотрудник при работе с корпоративной ЭП обязан:

8.1 Своевременно устанавливать или контролировать установку обновления операционной системы, браузера, антивирусных средств ПК.

8.2 Использовать на ПК с доступом к ЭП только лицензионное ПО.

8.3 По необходимости, производить резервное копирование корреспонденции встроенными и доступными средствами корпоративной ЭП.

8.4 При отправке сообщений следить за правильностью указания адресата и отправителя для предотвращения доставки информации лицам, которым она не предназначена.

8.5 Самостоятельно принимать решение об использовании средств электронной подписи и шифрования при отправке корреспонденции.

8.6 Своевременно удалять или перемещать на локальный диск ПК или сетевые директории сообщения, полученные посредством ЭП. При превышении максимального объема почтового ящика пользователя отключается и выводится сообщение о необходимости очистить почтовый ящик.

8.7 Обеспечить беспрепятственный доступ работников ИБ и ИТ к ПК во время проведения работ по организации доступа к ЭП, а также во время проведения служебных проверок и расследований.

8.8 Контролировать работу средств электронной подписи и шифрования при отправке и получении корреспонденции.

8.9 Ответственно относиться к хранению информации об учетной записи для доступа к ПК и сервисам ЛВС (идентификатор пользователя, пароль).

8.10 В случае компрометации пароля или подозрении на компрометацию немедленно сообщить в ИБ и ИТ.

8.11 Обеспечить невозможность использования ПК другими лицами на период своего отсутствия на рабочем месте (временная блокировка ПК, изъятие из ПК индивидуального устройства идентификации).

8.12 Немедленно докладывать обо всех нештатных ситуациях и их последствиях руководителю структурного подразделения и ставить в известность ИБ и ИТ.

## 9 Безопасность при работе с ЭП

9.1 ПК, сервера и устройства, подключенные к ЛВС Компании, являются критически важными устройствами, с которых возможна утечка конфиденциальной информации. Некоторые из них являются технологическими

устройствами, выход из строя которых может повлечь за собой сбой в работе информационных систем Компании.

9.2 Сотруднику, использующему доступ к работам с использованием ЭП запрещается:

9.2.1 Передавать информацию о своей учетной записи (идентификатор пользователя, пароль) третьим лицам.

9.2.2 Использовать предоставленный к корпоративной ЭП доступ в личных целях.

9.2.3 Использовать специализированные аппаратные и программные средства, позволяющие получить несанкционированный доступ к корпоративной ЭП Компании, а также общедоступной (в сети Интернет) ЭП из информационных систем Компании.

9.2.4 Игнорировать предупреждения о возможном наличии вредоносного содержания от систем контентного анализа и антивирусных средств при работе с корпоративной ЭП.

9.2.5 Включать не принадлежащие работнику адреса ЭП в различные списки рассылки (единичной или регулярной).

9.2.6 Выдавать себя и действовать от имени Компании или его филиала (обособленного подразделения) при работах с использованием ресурсов корпоративной ЭП.

9.2.7 Использовать учетную информацию (идентификатор пользователя, пароль) третьих лиц при работе с использованием ресурсов корпоративной ЭП.

9.2.8 Использовать ресурсы публичных, общедоступных почтовых серверов в сети Интернет.

9.2.9 Рассылать информацию, носящую рекламный характер (несанкционированная массовая рассылка – спам).

9.2.10 Выполнять любые попытки несанкционированного использования компьютерных систем, неправомерного доступа к компьютерной информации, допускать нарушение правил эксплуатации ПК, систем и их сетей, а также создание, использование и распространение вредоносных программ для ПК.

9.3 Корпоративную ЭП запрещается использовать для:

9.3.1 Нужд частного бизнеса и личных целей, а также любого рода коммерческой рекламы.

9.3.2 Несанкционированного доступа или получения несанкционированного доступа к информационно-вычислительным и сетевым ресурсам, принадлежащим другим пользователям и сетям.

9.3.3 Совершения действий, запрещенных законодательством Российской Федерации.

## 10 Ответственность при работе с ЭП

10.1 Работник Компании, осуществляющий работы с информационными ресурсами, несет персональную ответственность за свои действия и за невыполнение требований положений данной инструкции.

10.2 При работе с использованием корпоративной ЭП сотрудник несет персональную ответственность за:

10.2.1 Содержание и целостность передаваемой информации.

10.2.2 Разглашение паролей и другой конфиденциальной информации.

10.2.3 Несанкционированное использование ПК и компьютерных систем, неправомерный доступ к компьютерной информации, нарушение правил эксплуатации ПК, систем и их сетей, а также создание, использование и распространение вредоносных программ.

10.3 В случае выявления нарушений и злоупотреблений при выполнении работ с использованием ЭП могут быть применены нижеуказанные меры на установленный период или до устранения причин, повлекших за собой принятие настоящих мер:

10.3.1 Персонально к нарушителю:

10.3.1.1 Прекращение доступа к работам с использованием корпоративной ЭП.

10.3.1.2 Ограничение доступа к информационным ресурсам ЛВС Компании.

10.3.1.3 Принятие административных мер.

10.3.2 К ПК или серверу:

10.3.2.1 Отключение доступа к ЛВС и/или сервисам ЭП.

10.4 В случаях, когда нарушения требований настоящей инструкции повлекли за собой несанкционированный доступ, несанкционированное копирование, модификацию, блокирование или уничтожение информации, необходимой структурным подразделениям обществ Компании для выполнения своих функциональных задач, а также в случаях создания ситуаций, которые потенциально могли бы привести к таким последствиям, проводится служебное расследование с привлечением работников подразделений ИТ и ИБ.

10.5 На руководителей подразделений обществ Компании возлагается ответственность за организацию работы подчиненных, использующих ресурсы корпоративной ЭП и контроль за исполнением работниками требований настоящей инструкции.

**Разработчик**

Начальник отдела информационной безопасности

«____» _____ 20__ г. _____ Смирнов В.В.