СОГАЗ | Медицинский сервис

ПРИКАЗ

«07» 11 2022 года № 130/22

Москва

«Об утверждении Правил обеспечения информационной безопасности»

В целях обеспечения безопасности информации при работе пользователей с использованием средств вычислительной техники и информационных ресурсов ООО «СОГАЗ-Медсервис», а также внешних систем, ИТ-сервисов и личных устройств,

ПРИКАЗЫВАЮ:

1. Утвердить прилагаемые Правила обеспечения информационной безопасности.
2. В целях обеспечения оперативного и полного доведения положений Правил обеспечения информационной безопасности до сведения всех работников ООО «СОГАЗ-Медсервис» (далее – Общество), руководителям структурных подразделений Общества в течение пяти рабочих дней ознакомить подчиненных работников под расписку с Правилами информационной безопасности.
3. Руководителю направления Группы по административной, лицензионной деятельности и информационной поддержке, ответственному за обеспечение информационной безопасности в Обществе, в случае возникновения у работников вопросов по применению положений Правил информационной безопасности проводить соответствующую разъяснительную работу (включая обучающие тренинги, информационные собрания и т.д.).
4. Содержание настоящего приказа довести до сведения всех заинтересованных сотрудников Общества.
5. Контроль за исполнением настоящего приказа оставляю за собой.
6. Настоящий приказ вступает в силу со дня его подписания.

Генеральный директор **А.А. Низов**

Приложение № 1

УТВЕРЖДЕНЫ

приказом генерального директора
ООО «СОГАЗ-Медсервис»
от «07» 11 2022 года № 130/22

ПРАВИЛА

обеспечения информационной безопасности

Оглавление

1 Назначение и область применения 3
2 Термины и определения 3
3 Обозначения и сокращения 7
4 Общие положения 7
5 Доступ к информационным ресурсам 8
6 Требования к формированию пароля 8
7 Рабочее место пользователя 9
8 Защита учетных записей пользователей 9
9 Защита данных 10
10 Работа в сети Интернет 11
11 Ответственность 12
12 Контроль версий документа 12
13 Нормативные ссылки 13
Приложение 1 Дополнения к правилам обеспечения ИБ 14

1 Назначение и область применения

Ответственный за применение документа	Административно-правовое управление/Группа по административной, лицензионной деятельности и информационной поддержке /Руководитель направления (в должностные обязанности входит обеспечение информационной безопасности)
Назначение	Настоящий документ устанавливает правила и требования, необходимые для обеспечения безопасности информации при работе пользователей с использованием средств вычислительной техники и информационных ресурсов Общества, а также внешних систем, ИТ-сервисов и личных устройств
Область применения	Все подразделения

2 Термины и определения

Наименование термина	Определение термина
Авторизация	От англ. authorization «разрешение; уполномочивание» — предоставление определённому лицу или группе лиц прав на выполнение определённых действий; а также процесс проверки (подтверждения) данных прав при попытке выполнения этих действий
Аутентификация	Процедура проверки подлинности предъявленного Пользователем идентификатора (пароля или его аналога) при входе в информационную систему
Блокировка	Ограничение прав доступа на определенный срок. При этом учетная запись Пользователя информационного ресурса блокируются, но не удаляется, права доступа учетной записи в информационных ресурсах сохраняются
Владелец бизнес-процесса	Субъект, осуществляющий владение необходимыми для выполнения процесса ресурсами, обладающий полномочиями по распоряжению ими для получения результата процесса, устанавливающий правила, ограничения и требования к выполнению процесса, несущий ответственность, за ход его выполнения и удовлетворенность клиентов результатами процесса
Владелец информации	Субъект, осуществляющий владение информацией и/или ее обработку, а также реализующий полномочия распоряжения информацией в пределах прав, установленных законом – структурное подразделение Общества или Контрагент
Владелец информационного ресурса	Субъект, осуществляющий владение Информационным ресурсом, обладающий полномочиями по распоряжению им
Владелец информационной системы	Субъект (Работник Общества), осуществляющий владение и пользование Информационной системой и реализующий полномочия распоряжения Информационной системой
Внешние носители информации	Носители информации любого типа, предназначенные для записи/считывания информации с компьютера или любого аналогичного устройства. (USB-носители, оптические диски, внешние жесткие диски и др.)
Договор	Документ, определяющий основание предоставления Пользователю доступа к информационным ресурсам Общества (трудовой договор, гражданско-правовой договор, оферта)

Доступ в Интернет	Совокупность технических средств, направленных на обеспечение доступа Пользователей к ресурсам сети Интернет
Доступность	Состояние информации, при котором субъекты, имеющие Права доступа, могут реализовать их беспрепятственно
Законное основание	Договор, предписание на проведение аудита/проверки, приказ/внутренний нормативный документ (служебная записка, информационное письмо) о закреплении ответственности/назначении ответственного в рамках процесса, устанавливающие для Пользователя права и обязанности по использованию соответствующего информационного ресурса и т.п.), должностная инструкция Работника, Пользовательское соглашение, размещенное на сайте Общества
Защищаемая информация[1]	Информация ограниченного доступа, а также общедоступная информация, уничтожение, нарушение целостности и доступности которой, может нанести Обществу прямой или косвенный материальный ущерб
Информационная безопасность[2]	Состояние защищенности интересов (целей) Общества в условиях угроз нарушения свойств доступности, целостности, конфиденциальности и отслеживаемости информационных активов
Информационная система	Взаимосвязанная совокупность средств, методов и персонала, используемых для хранения, обработки и выдачи информации в интересах достижения поставленной цели
Информационный ресурс	Совокупность программного обеспечения и технических средств, используемых для хранения, обработки и передачи информации, с целью решения задач подразделений Общества
Информация ограниченного доступа	Информация, доступ к которой ограничен федеральными законами. Обладатель информации, если иное не предусмотрено федеральными законами, вправе: разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа, принимать меры по защите информации
Инцидент ИБ[3]	Одно или серия связанных нежелательных или неожиданных событий ИБ, которые могут привести (или привели) к риску появления негативных последствий[4] для Общества, включая значимый финансовый ущерб
Контрагент	Физическое или юридическое лицо, являющееся стороной по договору (соглашению) с Обществом
Конфиденциальность	Состояние информации, выраженное в обязательном для выполнения лицом, получившим доступ к

[1] Трактовка термина адаптирована применительно к специфике деятельности Общества на основе значения термина, приведенного в ГОСТ Р 50922-2006 (п.2.5.2).

[2] Трактовка термина адаптирована применительно к специфике деятельности Общества на основе значения термина, приведенного в ГОСТ Р 53114-2008 (3.2.1).

[3] Трактовка термина адаптирована применительно к специфике деятельности Общества на основе значений терминов, приведенных в ГОСТ 57580.1 2017; ГОСТ Р ИСО/МЭК ТО 18044-2007; РС БР ИББС-2.5-2014.

[4] К негативным последствиям в соответствии с РС БР ИББС-2.5-2014 «Менеджмент инцидентов ИБ» относятся: нарушения выполнения бизнес-процессов; технологических процессов; нарушение работы средств защиты информации; нарушение требований законодательства Российской Федерации, нормативных актов и предписаний регулирующих и надзорных органов; внутренних документов Общества; нанесение ущерба Обществу.

	определенной информации, требовании не передавать такую информацию Третьим лицам без согласия ее обладателя
Межсетевой экран	Программный или программно-аппаратный элемент компьютерной сети, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами. Применяется как рекомендованная мера при использовании Мобильных устройств.
Мобильное устройство	Мобильный телефон (смартфон), планшет, ноутбук
Нецелевое использование	Действия, не предусмотренные функционалом ИР, Пользовательским Соглашением, Законным основанием и/или бизнес-процессом, а также не связанные с выполнением должностных/ функциональных обязанностей, распоряжений Руководителя, декларированными интересами Общества
Носители информации[5]	Материальный объект, машинные носители информации, Внешние носители информации, в том числе физическое поле, в котором информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин
Обработка информации	Любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без их использования с информацией, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), блокирование, удаление, уничтожение
Обязанности	Безусловные для выполнения действия Пользователя, предусмотренные Законным основанием и/или его должностными инструкциями, функциональными обязанностями
Отслеживаемость	Свойство, гарантирующее регистрацию и сохранность факта значимого (влияющего на результата бизнес-процесса) действия субъекта (Пользователя) по отношению к объекту (единице информации, Информационному ресурсу или Информационной системе) в соответствующий момент времени
Персональная учетная запись	Персонифицированная учётная запись пользователя (работника, работника), содержащая идентифицирующую информацию пользователя, используемая для аутентификации пользователя при доступе к информационному ресурсу
Персональные данные[6]	Любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных)
Персональный идентификатор[7]	Уникальный признак Пользователя, позволяющий отличать его от других Пользователей, т.е.

[5] Трактовка термина адаптирована применительно к специфике деятельности Общества на основе значений терминов, приведенных в ГОСТ Р 50922-2006 (Приложение А); Приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21.

[6] В Соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»

[7] В качестве персональных идентификаторов могут применяться отпечатки пальцев, радужная оболочка глаза и т.д. (биометрические персональные данные).

	идентифицировать. Для целей настоящего документа к Персональным идентификаторам относится: Персональная учетная запись (УЗ), Токен, Карта доступа
Пользователь	Субъект, участвующий в функционировании Информационного ресурса или использующий результаты его функционирования. Пользователем является Работник Общества или Контрагента, или иное лицо, действующие в рамках Законного основания, который в своей деятельности использует Информационные ресурсы, работают с Информационными системами и/или Средствами вычислительной техники Общества
Пользовательское соглашения	Документ Общества, устанавливающий правила использования Информационного ресурса, права и обязанности Пользователя и Общества, как Владельца Информационного ресурса
Права доступа	Набор полномочий, предоставленных учетной записи пользователя, или группе учетных записей пользователей к объектам информационной системы (информации, её носителям, процессам и другим ресурсам) установленных правовыми документами или владельцем информации. Права доступа определяют набор действий (например, чтение, запись, выполнение), разрешённых для выполнения пользователям системы над объектами данных
Предопределенные действия	Легитимные действия, выполняемые в рамках бизнес-процесса, предусмотренные/определенные Обязанностями Пользователя, Законным основанием или технологией обработки информации
Простая электронная подпись[8]	Электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом
Профиль пользователя	Набор прав доступа для работы с информационными системами и ресурсами, предоставляемый для выполнения обязанностей в рамках конкретной должности или функции
Служба поддержки пользователей	Структурное подразделение Уполномоченного ИТ подразделения, выполняющие функции по обеспечению работы Пользователей
Средство вычислительной техники	Разновидность технических средств Обработки информации, которым относятся персональные компьютеры, Мобильные устройства, сетевые рабочие станции, серверы и другие виды компьютеров, а также периферийные устройства (компьютерная оргтехника) и средства межкомпьютерной связи
Токен	Носитель ключевой информации — устройство с защищенной паролем памятью, на которой хранится информация для создания электронной подписи, а также предназначенное для идентификации его владельца, упрощения аутентификации, безопасного удалённого доступа к информационным ресурсам
Третьи лица	Физические или юридические лица, не имеющие Законного основания для доступа к Защищаемой информации и/или участия в бизнес-процессе

[8] В соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»

Уполномоченное по ИБ лицо	Работник Общества, в должностные обязанности которых входят функции по организации деятельности в области обеспечения информационной безопасности и контролю выполнения требований по обеспечению информационной безопасностью
Уполномоченное ИТ подразделение	Подразделение Общества, в составе которого находятся Работники, в должностные обязанности которых входит установка, настройка и администрирование программного обеспечения и аппаратной части персонального компьютера и/или администраторы серверного (коммуникационного) оборудования (администрирование и сопровождение аппаратной части и системного программного обеспечения серверного оборудования), создание и администрирование Информационных ресурсов, ИТ-сервисов, Информационных (автоматизированных) систем
Учетная запись	Хранимая в Информационном ресурсе совокупность данных о Пользователе, необходимая для его Аутентификации и Авторизации
Фишинговое письмо	Поддельное уведомление, направленное Пользователю, целью которого является получение несанкционированного доступа к Защищаемой информации Общества
Целостность	Состояние информации, характеризующее ее неизменность, либо то, что все изменения внесены уполномоченными на это лицами
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

3 Обозначения и сокращения

Сокращение	Расшифровка сокращения
SMS	от англ. Short Message Service — служба коротких сообщений») — технология приёма и передачи коротких текстовых сообщений с помощью сотового телефона. Входит в стандарты сотовой связи
ВНД	Внутренний нормативный документ
ИБ	Информационная безопасность
ИР	Информационный ресурс
ИС	Информационная система
ИТ	Информационные технологии
ОС	Операционная система
ПК	Персональный компьютер
ПО	Программное обеспечение
СВТ	Средство вычислительной техники
СПП	Служба поддержки пользователей
УЗ	Учетная запись
ЭП	Электронная подпись

4 Общие положения

4.1 Настоящий документ является нормативным документом Общества и регламентирует базовые требования, необходимые для выполнения Пользователями в части обеспечения ИБ (далее — Правила).

4.2 Пользователь при обработке информации в рамках Предопределенных действий имеет право, а в определённых случаях и обязанность, применять ЭП.

Обязательность применения ЭП установлена законодательством Российской Федерации и может быть детализирована в Пользовательском соглашении.

4.3 Все электронные документы, созданные или пересланные Пользователем под его УЗ (Персональным идентификатором), считаются подписанными им простой ЭП, и признаются равнозначными документам на бумажном носителе, подписанными собственноручной подписью Пользователя.

4.4 Действие Правил не распространяется на устанавливаемый государственными органами режим защиты сведений, составляющих государственную тайну Российской Федерации.

4.5 Правила обязательны для исполнения всеми Пользователями, использующими ИС, ИР и/или СВТ Общества.

4.6 Обеспечение ИБ в Обществе организуется в соответствии с требованиями законодательства Российской Федерации, требованиями регулирующих органов, внутренних нормативных документов Общества и контролируется Уполномоченным по ИБ лицом.

4.7 В Обществе при формировании правил использования СВТ и ИР Общества применяется принцип: «Что явно не разрешено – запрещено».

4.8 Общество вправе осуществить контроль информационных потоков и результатов деятельности Пользователя, исполнения им требований по обеспечению ИБ, соблюдения Пользователем порядка информационного взаимодействия (отправка/получение информации) и использования ИС и ИР. В случае выявления нарушений требований настоящих Правил Общество вправе прекратить доступ Пользователя к ИР/ИС и сервисам Общества, а также инициировать проверку законности действий Пользователя.

4.9 На Владельца информации, Пользователей возлагается обязанность осуществления мероприятий по безопасной обработке информации (обеспечение ИБ), в том числе и при использовании ИР.

4.10 Пользователь, которому предоставляется санкционированный доступ к ИР Общества, в том числе с использованием личных Мобильных устройств, и/или к СВТ Общества получает допуск к Защищаемой информации, обрабатываемой Обществом в минимальном объеме, необходимом и достаточном для выполнения Предопределенных действий, предусмотренных комбинацией из следующего:

- правами Пользователя;
- Обязанностями Пользователя;
- предоставляемыми услугами.

4.11 Пользователю запрещается Нецелевое использование ИР, ИТ- сервисов и/или СВТ Общества.

4.12 По любым вопросам, связанным с обеспечением ИБ, Пользователь может обратиться в Общество любым доступным способом.

4.13 Пользователь, выявивший нарушение требований ИБ или имеющий подозрения на нарушение требований ИБ, определенных в настоящих Правилах, а также о полученных поручениях, выполнение которых явно ведет к нарушению правил ИБ, вправе уведомить Общество любым доступным способом.

5 Доступ к информационным ресурсам

5.1 Пользователю при наличии Законного основания, для выполнения Предопределенных действий предоставляется доступ к ИР Общества, в порядке, установленном ВНД Общества или описанном в Пользовательском соглашении.

5.2 Для работы с ИР, предусматривающими процедуры аутентификации, Пользователю выдается Персональный идентификатор, применимый для доступа к конкретному ИР.

5.3 Пользователь получает Права доступа к ИР в необходимом и достаточном объеме для выполнения Предопределенных действий.

5.4 Пользователю запрещается использовать для доступа к ИР/ИС Общества, не принадлежащие Пользователю Персональные идентификаторы, расширять Права доступа, в обход предусмотренных в Обществе процедур и/или Пользовательском соглашении.

6 Требования к формированию пароля

6.1 При использовании пароля в качестве мер защиты Пользователь обязан:

6.1.1 назначать уникальный пароль для каждого защищаемого объекта (УЗ, ИС, архив и пр.) удовлетворяющий требованиям безопасности, указанным далее длиной не менее 8 (Восьми) символов, кроме отдельно оговоренных случаев;

6.1.2 пароль должен содержать в себе следующие символы: буквы нижнего регистра, буквы верхнего регистра, цифры и спецсимволы (например, ~ @ # $ % ^ & _);

6.1.3 пароль не должен включать в себя осмысленные слова, словосочетания, общепринятые аббревиатуры, а также легко идентифицируемую с его владельцем информацию – имена, фамилии, названия учетных записей, номера телефонов, клички животных, наименования организаций и т. п.;

6.1.4 при смене пароля новый пароль не должен совпадать с двумя предыдущими.

7 Рабочее место пользователя

7.1 Пользователь обязан:

7.1.1 принимать меры для безопасной обработки информации и обеспечения ее сохранности при использовании ПК или Мобильного устройства и реагировать на уведомления средств защиты информации;

7.1.2 использовать средства антивирусной защиты с актуальными сигнатурами, Межсетевой экран (программный или аппаратный) при доступе в Интернет и иные недоверенные сети;

7.1.3 использовать на ПК и/или Мобильном устройстве отдельную УЗ, не обладающую правами администратора и защищенную паролем, или защитить Мобильное устройство от разблокировки встроенным средством аутентификации (паролем, графическим паролем, отпечатком пальца и т.п.). Наличие указанного функционала зависит от типа конкретного устройства;

7.1.4 контролировать действия иных Пользователей при выполнении операций и действий, выполняемых при непосредственном участии Пользователя и в его интересах с использованием Персональных идентификаторов;

7.1.5 завершать сеансы удаленного подключения к ИС Общества сразу после выполнения задачи, связанной с их использованием;

7.1.6 принимать меры для сохранности обрабатываемой информации, включая перевозку Мобильного устройства только в ручной клади;

7.1.7 осуществлять обновления ОС и прикладного ПО, установленного на ПК и/или Мобильном устройстве при появлении соответствующих уведомлений. Перед установкой обновлений рекомендуется убедиться, что их установка не приведет к блокировке Мобильного устройства.

7.2 обращать внимание на полномочия, которые запрашиваются при установке на Мобильное устройство приложений. Если приложению требуются излишние полномочия (например, доступ к SMS и их отправка, доступ к интернету, к телефонной книге, при том, что это не относится к основному функционалу приложения), его установка не рекомендуется.

7.3 Пользователь вправе, обратиться в Общество в случае выявления нарушений штатной работы ИР.

7.4 Пользователю запрещается:

7.4.1 вмешиваться в штатную работу антивирусного ПО, создавать предпосылки действием или бездействием для возникновения Инцидента ИБ;

7.4.2 создавать условия действием или бездействием для возникновения Инцидента ИБ;

7.4.3 оставлять без присмотра Мобильное устройство, подключенное к ИР/ИС Общества.

8 Защита учетных записей пользователей

8.1 Пользователь работает в ИР/ИС только под выделенными ему УЗ. Учетная запись Пользователя ИР/ИС, является уникальным Персональным идентификатором, индивидуализирующим его деятельность в рамках ИС. Все действия, совершаемые с использованием УЗ Пользователя, рассматриваются как совершаемые лично им.

8.2 К Персональному идентификатору (в зависимости от того что используется) Пользователю назначают и/или предлагают установить свой пароль в соответствии с правилами формирования пароля, установленными в Обществе.

8.3 Для защиты УЗ от компрометации Пользователь обязан:

8.3.1 при работе с ИС соблюдать требования к формированию пароля, установленные в разделе 6 Правил.

8.3.2 при первом входе в ИС самостоятельно провести смену пароля, при наличии такой возможности, даже если ИС сама не запросила смену пароля;

8.3.3 при вводе пароля соблюдать осмотрительность, чтобы не допустить его компрометацию (раскрытие) Третьими лицами;

8.3.4 изменять используемый пароль для каждой УЗ и каждой ИС с периодичностью не реже, чем один раз в год;

8.4 Пользователю запрещается:

8.4.1 действия до идентификации и аутентификации, не предусмотренные Пользовательским соглашением и/или Инструкцией Пользователя по эксплуатации ИС (если применимо);

8.4.2 сообщать, кому бы то ни было, свои пароли, в том числе представителям Общества;

8.4.3 хранить пароли в доступной для чтения форме в командных файлах, сценариях автоматической регистрации, программных макросах, функциональных клавишах терминала, на компьютерах с неконтролируемым доступом, а также в иных местах, где Третьи лица могут получить к ним доступ;

8.4.4 создавать действием или бездействием условия для компрометации/ разглашения пароля;

8.4.5 использовать пароли, предназначенные для первого входа в ИР/ИС или ПК (если применимо) в качестве постоянных паролей;

8.4.6 подбирать пароли (в том числе автоматизированными способами) или любыми другими средствами пытаться завладеть паролями других Пользователей.

8.5 При любых подозрениях на компрометацию пароля необходимо немедленно сменить его и проинформировать Общество любым доступным способом.

8.6 Если Пользователь забыл пароль, ему необходимо направить заявку на восстановление пароля (присвоение Пользователю пароля на первый вход). Способ подачи заявки определен в ВНД Общества или Пользовательском соглашении.

9 Защита данных

9.1 В Обществе к Защищаемой информации отнесены, включая, но не ограничиваясь:

- сведения, составляющие Коммерческую тайну Общества;
- сведения, отнесенные к врачебной тайне;
- сведения, отнесенные к персональным данным;
- сведения, не являющиеся Информацией ограниченного доступа, но уничтожение, нарушение целостности и доступности которой, может нанести Обществу прямой или косвенный материальный ущерб.

9.2 Пользователь обязан соблюдать правила обращения с Защищаемой информацией при ее Обработке, вне зависимости от вида ее носителя и формы представления.

9.3 При обработке Защищаемой информации в ИС Пользователь не предпринимает дополнительных действий по обеспечению ее конфиденциальности, целостности и доступности, отслеживаемости, если Защищаемая информация обрабатывается согласно Предопределенным действиями, не покидает границы ИР/ИС или Общества.

9.4 При обработке Защищаемой информации, вне зависимости от формы ее представления, Пользователь обязан:

9.4.1 выполнять требования действующего законодательства Российской Федерации (применимого законодательства);

9.4.2 предпринимать действия (меры) для обеспечения конфиденциальности, целостности и доступности (защиты), ставшей ему известной информации;

9.4.3 обрабатывать Защищаемую информацию, с соблюдением требований по разграничению доступа;

9.4.4 проводить перед началом использования Внешнего носителя информации на Мобильном устройстве или ПК его сканирование антивирусным ПО;

9.4.5 производить отправку почтовых сообщений только в адрес заинтересованных лиц. При необходимости пересылки Защищаемой информации, в том числе Пользователям Общества, необходимо максимально ограничивать перечень получателей;

9.5 При Обработке Защищаемой информации Пользователю запрещается:

9.5.1 создавать условия для доступа к Защищаемой информации Пользователям (Работникам, Третьим лицам), которым такая информация не предназначена в рамках исполнения Обязанностей или Законного основания.

9.5.2 создавать действием или бездействием предпосылки для нарушения конфиденциальности, целостности, доступности и отслеживаемости при обработке Защищаемой информации или условия появления инцидента ИБ;

9.5.3 совершать действия, связанные с Обработкой Защищаемой информации, не предусмотренные Предопределенными действиями.

9.6 В случае использования архива с паролем, в качестве мер защиты информации при пересылке, пароль должен соответствовать требованиям, указанным в разделе 6 Правил, а сам пароль должен быть передан адресату по альтернативным каналам коммуникаций.

9.7 При получении фишингового письма, письма, полученного от неустановленного отправителя, и/или письма, содержащего спам (включая письма, содержащие информацию развлекательного характера), письма, содержащего подозрительное вложение, такое письмо, не открывая, необходимо удалить.

9.8 Признаки того, что сообщение является мошенническим:

- замаскировано под официальное письмо сторонней организации и требует каких-либо быстрых действий или ответа;
- содержит ссылки на Интернет-ресурсы, визуально похожие на настоящие ресурсы сторонней Общества, однако в отношении которых возникают сомнения, а также ссылки, оформленные в виде «коротких ссылок» (наподобие bit.ly или goo.gl);
- к сообщению прикреплен файл-вложение, который настойчиво предлагают открыть;
- в тексте содержатся опечатки, ошибки, избыточные знаки препинания (идущие подряд восклицательные или вопросительные знаки и т.п.).

9.8.1 Пользователю при взаимодействии с ИР/ИС Общества запрещается открывать/запускать исполняемые файлы и файлы сценариев (например, с расширением: exe, com, cmd, bat, js, msi и др.), в том числе полученные в виде вложений к почтовым сообщениям.

10 Работа в сети Интернет

10.1 При работе с ресурсами сети Интернет Пользователю запрещается:

10.1.1 сохранять учетные данные для доступа к ИР/ИС Общества в настройках браузера;

10.1.2 осуществлять действия, предлагаемые в рекламных объявлениях (баннерах, всплывающих окнах и т.д.), т.е. переходить по указанным ссылкам;

10.1.3 осуществлять публикацию, загрузку и распространение материалов (контента), запрещенных законодательством Российской Федерации, содержащих вирусы (или другие компьютерные коды), файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования;

10.1.4 использование логотипов, товарных знаков и символики Общества в личной электронной почте, на публичных Интернет-ресурсах, размещение на них фото- и видеоизображений, не соответствующих действительности и (или) порочащих деловую

репутацию Общества, в коммерческих целях или в целях личного обогащения, иными злонамеренными умыслами.

10.2 Пользователю необходимо помнить:

10.2.1 опубликованная в сети Интернет информация остается в ней навсегда. Удаление поста, сообщения или любого другого материала не гарантирует его уничтожения — его копия может остаться у других пользователей сети Интернет, либо на серверах социальных медиа[9], поисковых систем, сервисов архивирования Интернет-контента (например, web.archive.org);

10.2.2 опубликование информации о себе или Обществе может быть использована Третьими лицами (злоумышленниками) для атаки на Общество или Пользователя;

10.2.3 информация, публикуемая Пользователем в сети Интернет, с использованием методов социальной инженерии (человеческих слабостей) может быть использована Третьими лицами (мошенниками) в качестве «болевой точки» Пользователя для последующего его шантажа и манипуляции им в целях проникновения в корпоративную сеть Общества, получения доступа к Защищаемой информации и нанесения ущерба Обществу.

11 Ответственность

11.1 Пользователь несет персональную ответственность за:

11.1.1 соблюдение правил обеспечения ИБ, определенных настоящим документом, независимо от причин такого нарушения;

11.1.2 все действия, выполненные от имени его Персональных идентификаторов;

11.1.3 обработку информации с нарушениями требований по обеспечению ИБ;

11.2 Пользователи, не обеспечившие выполнение правил ИБ или создающие условия, ведущие к их нарушению, несут гражданскую, административную и уголовную ответственность в соответствии с действующим законодательством Российской Федерации. Общество вправе для взыскания ущерба, причинённого Пользователем или в целях его привлечения к административной, гражданско-правовой или уголовной ответственности, обратиться в правоохранительные органы или суд.

12 Контроль версий документа

Номер версии	Краткое описание изменений документа
1.	Разработка нового ВНД
2.	Добавление уточнений по получению прав доступа, в т.ч. в выходной день.

[9] Социальные сети, блоги, форумы, группы в мессенджерах, wiki-платформах, и другие интернет-сервисы межличностного взаимодействия.

13 Нормативные ссылки

№	Наименование документа
1.	Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
2.	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»
3.	Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне»
4.	Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи»
5.	Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»
6.	Приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»
7.	Положение ЦБ РФ от 20.04.2021 № 757-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций»
8.	РС БР ИББС-2.0-2007. «Методические рекомендации по документации в области обеспечения информационной безопасности в соответствие с требованиями СТО БР ИББС-1.0»
9.	РС БР ИББС-2.1-2007. «Руководство по самооценке соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0»
10.	РС БР ИББС-2.2-2009. «Методика оценки рисков нарушения информационной безопасности»
11.	РС БР ИББС-2.5-2014. «Менеджмент инцидентов информационной безопасности»
12.	РС БР ИББС-2.6-2014. «Обеспечение информационной безопасности на стадиях жизненного цикла автоматизированных банковских систем»
13.	РС БР ИББС-2.7-2015. «Ресурсное обеспечение информационной безопасности»
14.	РС БР ИББС-2.8-2015. «Обеспечение информационной безопасности при использовании технологии виртуализации»
15.	РС БР ИББС-2.9-2016. «Предотвращение утечек информации»
16.	ГОСТ Р 57580.1-2017 Национальный стандарт Российской Федерации. «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер»
17.	ГОСТ Р ИСО/МЭК 27001-2021 Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования
18.	ГОСТ Р ИСО/МЭК 27002-2021 Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности
19.	ГОСТ Р 50922-2006 Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения
20.	ГОСТ Р 53114-2008 Национальный стандарт Российской Федерации. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения

Приложение 1 Дополнения к правилам обеспечения ИБ

1 Общие положения

1.1 Перечисленные далее требования, обязанности и ограничения являются дополнением к Правилам обеспечения информационной безопасности, применяются как меры усиления Правил, имеют приоритет в случаях разночтения, противоречия или определенные выше действия Пользователя определены как право.

1.2 Исключительное право на служебное произведение, созданное Пользователем с использованием СВТ и ИР Общества в пределах, установленных для его трудовых обязанностей, принадлежит Обществу.

1.3 Пользователь при обработке информации в рамках бизнес-процесса имеет право, а в определённых случаях и обязанность, применять СКЗИ. Обязательность применения СКЗИ установлена законодательством Российской Федерации и может быть детализирована в ВНД Общества.

1.4 Пользователь вправе использовать ЭП в бизнес-процессах Общества при условии, что он принял установленные Обществом правила работы с ЭП. Вид ЭП, доступной/обязательной к использованию, определен требованиями к бизнес-процессу.
ЭП не применяется Пользователем ИР в случае, когда ВНД Общества введен прямой запрет на ее использование.

2 Доступ на объекты Общества

2.1 Доступ на территорию и в помещения Общества, за исключением общедоступных мест, ограничен. Порядок доступа на территорию и в помещения Общества регламентируется действующими ВНД Общества.

2.2 Для прохода на территорию Общества Пользователю выдается Персональный идентификатор (далее – пропуск) и предоставляется доступ только в помещения Общества, необходимые ему для выполнения должностных/функциональных обязанностей или обязанностей, предусмотренных Законным основанием (далее – Обязанности). В случае изменения Обязанностей производится пересмотр и уточнение прав доступа Пользователя в помещения Общества.

2.3 При прекращении действия Законного основания пропуск подлежит сдаче в установленном порядке в Уполномоченное подразделение по режиму Общества.

2.4 Пользователь обязан запирать входные двери рабочего помещения (если применимо), оставляя рабочее место в случае отсутствии в нем других Работников.

2.5 Пользователю запрещается:

2.5.1 создавать действием или бездействием условия, способствующие несанкционированному проникновению на территорию и в помещения Общества посторонних лиц;

2.5.2 предпринимать попытки использования для прохода на территорию (в помещения) Общества чужого пропуска;

2.5.3 производить на территории Общества, не являющейся общедоступной, несанкционированную фото-, киносъемку, а также видео-, аудиозапись.

3 Логический доступ к информационным ресурсам

3.1 Набор Прав доступа и/или Профиль Пользователя определяет руководитель работника Общества в зависимости от состава Обязанностей Пользователя.

3.2 При изменении Обязанностей Пользователя осуществляется пересмотр его Прав доступа к ИР. В случаях, предусмотренных ВНД Общества или Договором с Обществом, доступ Пользователя к ИР может быть прекращен или приостановлен.

3.3 Работник, являющийся ответственным за исполнение договора с Контрагентом или коммуникации с Третьими лицами, в рамках исполнения которых требуется предоставить доступ к ИР Общества, обязан:

3.3.1 обеспечить актуальность соответствия перечня ИР/ИС, к которым необходим доступ Работникам Контрагента и перечня их Пользователей со стороны Контрагента;

3.3.2 информировать Администратора доступа и Уполномоченное по ИБ лицо об изменении Обязанностей и/или состава Пользователей со стороны Контрагента, Третьих лиц, а также о прекращении действия Законного основания (потребности в доступе).

3.4 Для запроса пользователям Общества прав доступа к информационным системам Общества предусмотрено предоставление следующих видов прав доступа:

- первичный;
- стандартный;
- расширенный.

3.5 В Заявке на предоставление первичного доступа в обязательном порядке указывается правовое основание, развернутое объяснение и сроки предоставления доступа. Для предоставления доступа Пользователю, являющемуся представителем Контрагента Общества, необходимо приложить перечень ответственных лиц (предоставляется Контрагентом на бланке организации.)

3.6 Первичный доступ предоставляется работнику Общества автоматически при заключении трудового договора, иному Пользователю при наличии Законного основания.

3.7 В права первичного доступа входят:

- внутренняя переписка по электронной почте;
- использование корпоративной сети, корпоративного портала;
- другие сервисы Общества, для которых предусмотрен общий доступ.

3.8 В права первичного доступа не входят:

- внешняя переписка по электронной почте;
- использование внешних носителей информации.

3.9 Для предоставления первичного доступа Пользователю, не являющемуся работником Общества, Инициатор, например, представитель заинтересованного подразделения, подает Заявку на предоставление первичного доступа (с указанием, что Пользователь не является работником Общества).

3.10 Стандартный доступ представляет собой совокупность Доступов, необходимых для выполнения Пользователю его непосредственных обязанностей, предусмотренных должностной инструкцией работника Общества или иным документом, регламентирующим его трудовую деятельность в Обществе (Законным основанием).

3.11 Стандартный доступ предоставляется работнику Общества автоматически за исключением случаев, когда должность вводится в штатное расписание впервые и для нее нет аналогов в существующем штатном расписании и сохраняется за работником на все время работы в Обществе.

3.12 Расширенный доступ подразумевает под собой совокупность прав, которые выдаются Пользователю вне первичного и стандартного доступов. Необходимость выдачи прав расширенного доступа подтверждает руководитель Пользователя (работника Общества).

3.13 В выходные или праздничные дни работнику Общества доступны к запросу следующие виды доступа:

- Удаленный доступ к рабочему месту;
- Удаленный доступ к электронной почте.

3.14 Запрос прав доступа в выходные и праздничные дни формирует руководитель Пользователя (работника Общества) и направляет срочную (в выходной/праздничный день) заявку по электронной почте Уполномоченному по ИБ лицу.

3.15 Запрос прав доступа в выходные и праздничные дни формирует исключительно руководитель Пользователя (работника Общества). Запрос прав доступа от работника Общества не принимается к обработке. В Заявке в обязательном порядке указывается ФИО работника Общества, его должность, обозначение нужных прав доступа и развернутое объяснение срочности предоставления прав доступа.

3.16 При представлении работником Общества в кадровую службу заявления на увольнение осуществляется отзыв критичных доступов (внешняя переписка по электронной почте, использование внешних носителей информации). Прочие доступы для работника Общества активны до последнего рабочего дня.

3.17 Критичные доступы (внешняя переписка по электронной почте, использование внешних носителей информации) для увольняемого работника могут быть запрошены вновь в установленном порядке. Заявку на возврат критичных доступов может направить только

руководитель работника Общества. Ответственность за последствия возможного инцидента ИБ, возникшего в результате принятого руководителем решения о возврате прав, лежит на руководителе Пользователя.

3.18 Отзыв прав доступа работнику по договору гражданско-правового характера, работнику подрядной организации, иному лицу производится автоматически по истечению срока, на который ему были предоставлены права по заявке или ранее при наличии мотивированного основания.

3.19 При изменении должностных обязанностей работника Общества, условий доступа Пользователя, содержащихся в Законном основании, предусматривающих расширенный или стандартный доступ работника Общества к информационным ресурсам Общества, в иных случаях, при наличии мотивированного решения руководителя, для исполнения которых Пользователю частично или полностью более не требуется предоставленный доступ, осуществляется пересмотр или отзыв предоставленных Пользователю прав доступа. Для этого Инициатор — непосредственный руководитель работника Общества или работник/руководитель структурного подразделения, являющийся ответственным за исполнение договора с Контрагентом или коммуникации с Третьими лицами, в рамках исполнения которых предоставлен доступ к ИР Общества, подает Заявку Уполномоченному по ИБ лицу на отзыв/изменение прав доступа.

3.20 Права доступа могут быть отозваны в частичном или полном объеме (вплоть до блокировки учетной записи) незамедлительно по инициативе:

- Уполномоченного по ИБ лица;
- Работника Уполномоченного ИТ подразделения;
- Руководителя направления экономической и корпоративной защиты;
- Уполномоченных подразделений по работе с кадрами;
- Руководителя Работника,

Отзыв прав доступа инициируется заявкой на электронный адрес Уполномоченного по ИБ лица.

3.21 Для обеспечения информационного взаимодействия Пользователей в Обществе реализован механизм Файловых ресурсов, которые предназначены для передачи и хранения файлов, необходимых для работы различным Пользователям, подразделениям и т.п.

3.22 Пользователю запрещается:

3.22.1 предпринимать попытки/размещать на ИР файлы, содержащие Защищаемую информацию, если данные ресурсы не предназначены для этого, включая общедоступные внешние сервисы (DropBox, Яндекс.Диск и т.д.);

3.22.2 создавать самостоятельно на выделенном для исполнения Обязанностей ПК Файловые ресурсы для доступа других Пользователей, предоставлять часть собственного дискового пространства для совместного доступа к файлам (eDonkey, Gnutella, BitTorrent и другие), и размещать файлы для последующей их передачи другим пользователям сети Интернет (RapidShare, Depositfiles и другие).

4 Рабочее место пользователя

4.1 Установка, подключение и настройка, принадлежащих Обществу, СВТ, включая предоставление Прав доступа к ИР и иные операции с СВТ, не предусмотренные Обязанностями Пользователя, производится исключительно Работниками Уполномоченного ИТ подразделения, в соответствии с установленной в Обществе процедурой.

4.2 На СВТ, принадлежащих Обществу, должно использоваться только разрешенное к эксплуатации в Обществе ПО, установленное Работниками Уполномоченного ИТ подразделения. Запрещено несанкционированное использование коммерческого ПО без лицензий, приобретенных Обществом, а также прошедшего процедуру активации на условиях, не предусмотренных правообладателем или лицензиатом (взломанного).

4.3 Пользователь обязан:

4.3.1 обратиться в Уполномоченное ИТ подразделение в случае выявления нарушений штатной работы СВТ или ПО;

4.3.2 принимать меры для безопасной обработки информации и обеспечения ее сохранности при использовании СВТ и реагировать на уведомления средств защиты информации;

4.4 При эксплуатации принадлежащих Обществу СВТ Пользователю, в случае, если отдельные нижеперечисленные действия прямо не предусмотрены его Обязанностями, запрещается:

4.4.1 вскрывать самостоятельно корпус СВТ, срывать защитные наклейки (стикеры);

4.4.2 вмешиваться в штатную работу СВТ/предпринимать попытки по изменению настроек ПК в том числе: производить загрузку ПК с Внешних носителей информации, изменять пароль BIOS/UEFI и ее настройки, устанавливать самостоятельно/ запускать дополнительные экземпляры ОС, изменять настройки ОС и системного ПО, включать СВТ в домен Общества;

4.4.3 вмешиваться в штатную работу средств защиты информации Общества;

4.4.4 использовать аппаратные и программные средства съема нажатий клавиатуры (кейлогеры), не предусмотренные бизнес-процессами Portable версии ПО, несанкционированно устанавливать самостоятельно/запускать виртуальные машины (vmware, vbox, и аналоги), платформы контейнеризации (docker и аналоги);

4.4.5 производить любые действия с сетевым коммуникационным оборудованием, сетевыми розетками, проводами локальной вычислительной сети Общества; несанкционированно организовывать беспроводные точки доступа, изменять настройки сетевых интерфейсов,

4.4.6 подключать к ПК, находящемуся в корпоративной сети Общества, корпоративные и личные Мобильные устройства, любое оборудование, если указанное оборудование содержит дополнительные порты для подключения периферийного оборудования и внешних носителей информации, в том числе, позволяющее выходить в Интернет в обход установленных в Обществе правил и технологий

5 Мобильные устройства и удаленная работа

5.1 Пользователь обязан использовать принятые в Обществе правила и технологии удаленного подключения к корпоративной сети Общества.

5.2 При использовании личного ПК или Мобильного устройства для доступа в корпоративную сеть Общества Пользователь обязан согласовывать его использование для исполнения Обязанностей;

5.3 При использовании личного Мобильного устройства для доступа в корпоративную сеть Общества Пользователю запрещается:

5.3.1 использовать Wares, устройство прошедшее процедуру jailbreak/root;

5.3.2 передавать/оставлять без присмотра Токен, Мобильное устройство, подключенное к корпоративной сети Общества;

5.3.3 хранить Токен вместе с Мобильным устройством;

5.4 Пользователь, допустивший утрату Мобильного устройства, используемого для доступа к ИС Общества, обязан в течение одного рабочего дня проинформировать о данном факте любым доступным способом Уполномоченное по ИБ лицо и своего непосредственного Руководителя.

6 Защита учетных записей пользователей

6.1 Пользователь работает только под выделенными ему УЗ, и не вправе использовать групповые и технологические УЗ, если их использование не предусмотрено бизнес-процессом и ВНД Общества.

6.2 Для защиты УЗ от компрометации Пользователь, кроме случаев Аутентификации только по Токену, обязан:

6.2.1 работать под административной УЗ только при выполнении задач, требующих полномочий административной УЗ и использовать механизмы двухфакторной Аутентификации в случаях, предусмотренных бизнес-процессом;

6.2.2 назначать для административных УЗ уникальный пароль – не менее 16 (Шестнадцать) символов, удовлетворяющих требованиям безопасности, определенных в разделе 6 Правил.

6.2.3 изменять для административных УЗ используемый пароль для каждой УЗ и каждой ИС с периодичностью не реже, чем один раз в 90 (Девяносто) дней.

6.3 Пользователю запрещается:

6.3.1 сообщать свои пароли Руководителю, специалистам СПП, Уполномоченному по ИБ лицу и т.д.;

6.3.2 использовать общие пароли совместно с другими Пользователями, пароли, предназначенные для первого входа в ИР/ИС или ПК (если применимо) в качестве постоянных паролей;

6.3.3 подбирать пароли (в том числе автоматизированными способами) или любыми другими средствами пытаться завладеть паролями других Пользователей.

6.4 При любых подозрениях на компрометацию пароля необходимо проинформировать Уполномоченное по ИБ лицо.

6.5 Если Пользователь забыл пароль, ему необходимо направить заявку на восстановление пароля (присвоение Пользователю пароля на первый вход) в Уполномоченное ИТ подразделение.

6.6 Для хранения парольной информацией Пользователь может использовать менеджер паролей, предоставляемый Обществом.

7 Защита данных

7.1 При обработке информации, вне зависимости от формы ее представления, Пользователь самостоятельно принимает решение о ее принадлежности к Защищаемой информации.

7.2 Правила обращения с Защищаемой информацией, обрабатываемой в Обществе, определены нормативными документами Общества.

7.3 Отнесение сведений к категории Защищаемой информации осуществляет Владелец информации, если нарушение хотя бы одного из состояний информации (конфиденциальности, целостности, доступности), может нанести Владельцу информации вред и/или прямой или косвенный материальный ущерб.

7.4 В строго определенных случаях, носители Информации ограниченного доступа (Защищаемая информация) имеют особенные отличительные реквизиты, например, гриф «Коммерческая тайна», отметка «Конфиденциально» либо иные отметки, определяемые решением Владельца информации.

7.5 Отсутствие на носителе информации особенных отличительных реквизитов, указанных в п. 8.4, не отменяет ее отнесение к Защищаемой информации.

7.6 Решение о принадлежности обрабатываемой информации к Защищаемой информации Пользователь принимает с учетом требований ВНД Общества.

7.7 К видам прямого материального ущерба, включая, но не ограничиваясь, относится:

7.7.1 расходы, связанные с утратой оборудования/имущества Общества или ухудшение его состояния;

7.7.2 расходы, связанные с незапланированной модернизацией оборудования, или его ремонтом;

7.7.3 расходы на приобретение имущества, либо на возмещение причиненного Пользователем ущерба субъекту персональных данных и/или Третьим лицам;

7.7.4 расходы на уплату штрафных санкций.

7.8 К видам косвенного материального ущерба, включая, но не ограничиваясь, относится недополученная прибыль в результате:

7.8.1 увеличения/изменения сроков выхода продуктов и услуг Общества на рынок.

7.8.2 недоступности сервисов Общества для клиентов;

7.8.3 отток клиентов, в следствии реализации репутационных рисков;

7.8.4 необходимости проведения организационных изменений;

7.8.5 необходимости привлечения дополнительных сил и средств (Работников, Контрагентов, финансовых вложений) для минимизации технологического отставания Общества или последствий Инцидента ИБ.

7.9 Входящие документы (полученные от Контрагента или Третьих лиц), вне зависимости от вида их носителя и формы представления, имеющие особенные отличительные реквизиты (ограничительный гриф или пометку), подлежат защите как Защищаемая информация Общества.

7.10 При обработке Защищаемой информации, вне зависимости от формы ее представления, Пользователь обязан:

7.10.1 предпринимать действия (меры) для обеспечения конфиденциальности, целостности и доступности (защиты), ставшей ему известной информации;

7.10.2 обрабатывать Защищаемую информацию с использованием ИР и ИС, выделенных и расположенных в пределах корпоративной сети Общества, с соблюдением требований по разграничению доступа;

7.10.3 немедленно информировать любым доступным способом Уполномоченное ИБ подразделение о всех случаях попыток получения несанкционированного доступа к Защищаемой информации, ставших известными Пользователю;

7.10.4 в ответе на обращение, поступившее в адрес Общества от клиентов Общества, передавать информацию, полученную от контрагента, органа государственной власти, иного юридического или физического лица при соблюдении следующих условий:

- информация предоставляется прикреплением (приложением к письму) в формате скан-копии, скриншота и пр.;
- в теле письма содержится комментарий о передаче информации с указанием источника информации и реквизитов письма, в котором предоставлена передаваемая информация;
- передача информации согласована юридическим подразделением, подразделением информационной безопасности.

7.11 При Обработке Защищаемой информации, в отношении которой осуществляется ее передача за границы Общества, Пользователь обязан руководствоваться положениями заключенного соглашения о конфиденциальности (NDA).

7.12 При Обработке Защищаемой информации Пользователю запрещается:

7.12.1 использовать Защищаемую информацию в несвязанных с выполнением Обязанностями, в том числе личных целях, для получения выгоды, в том числе Аффилированными лицами;

7.12.2 создавать условия для доступа к Защищаемой информации Пользователям (Работникам, Третьим лицам), которым такая информация не предназначена в рамках исполнения бизнес-процесса, Обязанностей или Законного основания.

7.12.3 использовать не предусмотренные бизнес-процессом технологии и ИТ-сервисы, ИС, общедоступные интернет-мессенджеры (Viber, WhatsApp, Telegram и т.д.);

7.12.4 передавать Защищаемую информацию за пределы корпоративной сети Общества без применения мер защиты, определенных бизнес-процессом или ВНД Общества (в открытом виде);

7.12.5 при ответе на обращения, поступившие в адрес Общества от клиентов Общества, передавать информацию следующего рода:

- сведения о внутренних процессах Общества, об их специфике и особенностях;
- сведения о работниках и подразделениях Общества;
- сведения о внутренних коммуникациях и взаимодействиях в Обществе;
- сведения, передача которых может повлиять на бизнес-процессы Общества и деловую репутацию Общества (за исключением особых случаев при условии, что такая передача согласована начальником Административно-правового управления);
- сведения о технических сбоях и ошибках информационных систем Общества, возникших в том числе под воздействием человеческого фактора;

- информация о внутренней оценке качества выполнения предоставляемых услуг и выполнения должностных обязанностей работником;
- информация о проведении служебных расследований в Обществе, разрешении спорных вопросов с участием третьих сторон;
- данные, распространение которых может повлечь за собой нарушение законодательства РФ в сфере работы с персональными данными и в иных сферах (такие, как персональные данные лиц, согласие которых на обработку персональных данных Обществом отсутствует, работников Общества или третьих лиц и др.).

7.12.6 пересылать Защищаемую информацию на почтовые ящики (в том числе личные) вне доменных зон компаний, входящих в Группу СОГАЗ, если такое действие не предусмотрено бизнес-процессом и/или ВНД Общества, данные не принадлежат самому Пользователю или его родственникам, и направлены на его личный ящик, за исключением случаев, согласованных с Уполномоченным по ИБ лицом;

7.12.7 оставлять подключенными к ПК внешние носители информации, в том числе содержащие Персональные идентификаторы (Токен, ключ ЭП) по завершению операций, предусматривающих использование таких носителей информации.

8 Использование Внешних носителей информации при обработке Защищаемой информации

8.1 Обработка Защищаемой информации с использованием Внешних носителей информации допускается в случаях, предусмотренных бизнес процессом и/или технологией обработки информации, требованиями регуляторов. В иных случаях использование Внешних носителей информации должно быть согласовано Уполномоченным по ИБ лицом.

8.2 В Обществе определены следующие способы использования Внешних носителей информации: использование для передачи информации адресату за пределы периметра Общества. Иные способы использования Внешних носителей информации должны быть согласованы с Уполномоченным по ИБ лицом.

8.3 При необходимости использовать Внешние носители информации для обработки Защищаемой информации допускается использовать только носители информации, выданные и установленным образом зарегистрированные Обществом.

8.4 В случае нарушения Пользователем вышеуказанных требований, выданный Внешний носитель информации подлежит изъятию у Пользователя.

8.5 В случае утери Внешнего носителя информации, Пользователь незамедлительно уведомляет о факте его утери Уполномоченное по ИБ лицо.

8.6 При использовании Внешних носителей информации Пользователь обязан:

8.6.1 обеспечивать сохранность и контроль местонахождения носителей информации, хранить носители информации, содержащие Защищаемую информацию в сейфах (металлических шкафах), оборудованных внутренними замками с двумя или более дубликатами ключей и приспособлениями для опечатывания замочных скважин или кодовыми замками. В случае, если на Внешнем носителе информации Защищаемая информация размещена в зашифрованном с использованием СКЗИ виде, то допускается хранение таких носителей вне сейфов (металлических шкафов);

8.6.2 убирать носители информации (как бумажные, так и электронные), в места их постоянного или оперативного хранения: ящик стола или запирающийся шкаф; сейф; специализированные системы хранения (при наличии); при отсутствии потребности в данный момент времени работать с размещенной на них Защищаемой информацией или покидая рабочее место;

8.6.3 предъявлять (незамедлительно) по запросу Уполномоченного по ИБ лица для проверки Внешний носитель информации и обеспечить возможность просмотра и анализа размещенной на нем информации (запрашиваемой информации);

8.6.4 передать в случае обнаружения на территории Общества оставленные без присмотра носители информации (документы) Уполномоченному по ИБ лицу.

9 Работа с системами электронного документооборота

9.1 Пользователь для реализации бизнес-процессов Общества использует как внутренние, так и внешние ИС, образующие систему электронного документооборота.

9.2 Для выполнения Обязанностей, связанных с электронным документооборотом, отправкой/получением электронной почты, в Обществе разрешается использовать только корпоративную Систему электронного документооборота и/или предоставленную Контрагентами.

9.3 Для ведения служебной переписки между Работниками Общества, Контрагентами и Третьими лицами следует использовать только корпоративные адреса электронной почты.

9.4 В случае использования архива с паролем, в качестве мер защиты пароль для проверки содержания отправленных файлов должен быть представлен Уполномоченному по ИБ лицу по его требованию.

9.5 При получении фишингового письма, письма, полученного от неустановленного отправителя, и/или письма, содержащего спам (включая письма, содержащие информацию развлекательного характера), письма, содержащего подозрительное вложение, такое письмо перед удалением необходимо пересылать для дальнейшего анализа на почтовый адрес Уполномоченного по ИБ лица.

9.6 При работе с корпоративной электронной почтой Пользователю запрещается открывать/запускать исполняемые файлы и файлы сценариев (например, с расширением: exe, com, cmd, bat, js, msi и др), полученные в виде вложений к почтовым сообщениям в случаях, не определенных Обязанностями и/или ВНД Общества.

9.7 При работе с корпоративной электронной почтой Пользователь обязан:

9.7.1 производить отправку почтовых сообщений только в адрес заинтересованных лиц. При необходимости пересылки Защищаемой информации, в том числе Пользователям внутри Общества, по корпоративной электронной почте необходимо максимально ограничивать перечень получателей;

9.7.2 осуществлять обработку сообщений, поступивших по каналам корпоративной электронной почты;

9.7.3 контролировать наличие и при необходимости исключать Защищаемую информацию из «тела» письма (переписки) при ответе или пересылке сообщения на адреса внешних почтовых систем.

10 Работа в сети Интернет

10.1 Доступ в Интернет Пользователям Общества предоставляется с использованием ПК, подключенных к корпоративной сети Общества.

10.2 Допускается подключение Мобильных устройств Пользователей к корпоративной сети Общества по корпоративному сегменту беспроводной сети Wi-Fi.

10.3 При работе с ресурсами сети Интернет Пользователю запрещается:

10.3.1 использовать средства обхода ограничений, средства сокрытия следов деятельности, средств сокрытия информации и Пользователя при работе в сети Интернет;

10.3.2 изменять настройки веб-обозревателя (браузера), сохранять учетные данные для доступа к ресурсам сети Интернет в настройках браузера;

10.3.3 осуществлять действия, предлагаемые в рекламных объявлениях (баннерах, всплывающих окнах и т.д.), т.е. отвечать на задаваемые вопросы, участвовать в массовых рассылках;

10.3.4 указывать адрес рабочей электронной почты при регистрации, кроме электронных почтовых адресов, официальных контактов, специально для этого предназначенных;

10.4 распространение или обсуждение информации, связанной с деятельностью Общества, если перечисленные действия не определены Обязанностями пользователя.

11 Участие работников во внутренних чатах, системах управления проектами и базах знаний

11.1 Пользователь для реализации бизнес-процессов Общества использует корпоративные средствах коммуникации — внутренние вики-системы, системы управления

проектами и задачами (Jira), внутренние базы знаний, внутренние разрешенные чаты и мессенджеры, их закрытые каналы.

11.2 Пользователю при использовании указанных в п. 11.1 средств коммуникации запрещается публиковать в них Защищаемую информацию, необезличенные персональные данные или данные полученные из ИС.

12 Использование средств криптографической защиты информации

12.1.1 Допуск (право использования) Пользователя к средствам криптографической защиты информации (далее — СКЗИ) и в помещение, где расположены и эксплуатируются СКЗИ, регулируется отдельными ВНД Общества, на основании комиссионного решения о допуске к СКЗИ после прохождения Пользователем обучения и сдачи зачета.

12.2 При использовании СКЗИ Пользователь обязан:

12.2.1 соблюдать требования эксплуатации СКЗИ;

12.2.2 передавать применяя СКЗИ (при необходимости передачи по техническим средствам связи) служебные сообщения и соответствующие указания, касающихся организации и обеспечения безопасности хранения, обработки и передачи по каналам связи Информации ограниченного доступа;

12.2.3 обеспечивать сохранность и конфиденциальность ключевых документов и ключевых носителей;

12.2.4 вернуть Уполномоченному по ИБ лицу неиспользованные или выведенные из действия ключевые документы.

12.3 Передача по техническим средствам связи криптоключей не допускается.

13 Действия при выявлении нарушений требований информационной безопасности и обнаружении изменений, влияющих на процессы обеспечения информационной безопасности

13.1 Пользователь, выявивший нарушение требований ИБ или имеющий подозрения на нарушение требований ИБ, определенных в настоящем документе, а также о полученных поручениях, выполнение которых явно ведет к нарушению правил ИБ, а также о конфликтных ситуациях, последствия которых могут привести к нелояльным действиям работника, обязан немедленно уведомлять Уполномоченное по ИБ лицо, направив информацию на его почтовый адрес.

13.2 Пользователь обязан оказывать содействие и незамедлительно выполнять требования/рекомендации или указания, которые поступили от Руководителя или Уполномоченного по ИБ лица в рамках работ по локализации инцидента ИБ или обратной связи при выполнении действий, предусмотренных п. 13.1 настоящего документа.

13.3 Пользователю запрещено предпринимать действия, включая удаление/модификацию информации, влекущие (направленные на) изменение состояния СВТ в котором оно находилось в момент выявлении факта его Нецелевого использования, нарушения штатной работы, инцидента ИБ или подозрении на таковой.

13.4 Пользователь, при обнаружении изменений, в том числе в бизнес-процессах, влияющих на деятельность по обеспечению ИБ Общества, или формирующих условия, при котором выполнение бизнес-процесса без нарушения требований по обеспечению ИБ невозможно, обязан уведомлять Уполномоченное по ИБ лицо о таком факте, направив информацию на его почтовый адрес. Таковыми изменениями могут быть:

13.4.1 выявление угроз, рисков и уязвимостей (или подозрений на них) в обеспечении защиты информации при реализации бизнес-процессов или бизнес инициатив;

13.4.2 нарушение целостности защитной наклейки (стикера) на ПК.

13.5 Уполномоченное по ИБ лицо вправе отстранить Пользователя от выполнения работ с использованием СВТ в случае подозрения на нарушение им требований ИБ.

14 Ответственность

14.1 Пользователь несет персональную ответственность за обработку информации с нарушениями требований по обеспечению ИБ, включая корректность отнесения информации к Защищаемой информации и простановку грифа «Коммерческая тайна» в случаях, предусмотренных ВНД Общества.

14.2 Пользователи, в том числе и Руководители, не обеспечивающие выполнение, правил ИБ или создающие условия, ведущие к их нарушению, могут быть привлечены Обществом к дисциплинарной и иной ответственности в соответствии с действующим законодательством Российской Федерации.