Приложение № 1
к Приказу от 13.02.2023 №11 – од

УТВЕРЖДАЮ
И.о. Генерального директора
ООО СК «Газпром страхование»

_____В.М. Носов
(личная подпись)
«13» 02 2023 г.

ПРАВИЛА

обеспечения информационной безопасности

ОГЛАВЛЕНИЕ

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

1. Назначение и область применения

Ответственный за применение документа	Головной офис/Дирекция информационной безопасности/Директор дирекции 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	Головной офис/все подразделения Филиалы/все подразделения Территориальные дирекции/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

[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.

	для выполнения лицом, получившим доступ к 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»

	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

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

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

Третьи лица	Физические или юридические лица, не имеющие Законного основания для доступа к Защищаемой информации и/или участия в бизнес-процессе
Уполномоченное ИБ подразделение	Подразделение Общества, выполняющие 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 ИБ подразделением.

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 объеме необходимом (достаточном) 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 Пользователь 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, непредусмотренные 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, отнесенные к тайне страхования;
- 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 публикуя информацию о себе или Обществе она 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	

[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