Приложение

**Типовая форма Соглашения о конфиденциальности при предоставлении доступа к информационным ресурсам**

Соглашение о конфиденциальности

г. Москва «\_\_\_»\_\_\_\_\_\_\_\_\_\_20\_\_г.

ООО «Газпром страхование»), ИНН хххххххххххххх, в лице ˂\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_˃, действующего на основании ˂\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_˃, с одной стороны,
и ˂\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_˃, в лице ˂ \_\_\_\_\_\_\_\_\_\_\_\_\_\_˃, действующего на основании ˂\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_˃,
с другой стороны, совместно именуемые «Стороны», а по отдельности Сторона, заключили настоящее соглашение о конфиденциальности (далее – «Соглашение») о нижеследующем.

Стороны обязуются обеспечить конфиденциальность информации, необходимость Обработки которой определена существующими между Сторонами гражданско-правовыми отношениями или намерениями вступить в таковые, исключить ее Обработку и Разглашение в целях, противоречащих обязательствам, которые существуют между Сторонами.

1. ОПРЕДЕЛЕНИЯ

**«Информация»** – сведения (сообщения, данные) независимо от формы их представления, которые в соответствии с Федеральным законом «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ определены как информация ограниченного доступа и/или в отношении которых в соответствии с законодательством Российской Федерации для Стороны определена обязанность обеспечивать Конфиденциальность информации, включая, но не ограничиваясь сведения, составляющие Коммерческую тайну, персональные данные, тайну страхования, врачебную тайну, тайну следствия и др.;

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

**«Носитель информации»** – материальный объект, в котором информация отображается в виде символов, образов, сигналов, технических решений и процессов;

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

**«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 (обмен, предоставление, доступ), блокирование, удаление, уничтожение;

**«Персональные данные»** – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных), переданная Сторонами в письменном, электронном или любом другом виде или к которой Раскрывающая сторона предоставляет доступ работникам Принимающей стороны или лицам, привлекаемым Принимающей стороной (далее – третьим лицам) в рамках исполнения ими договорных обязанностей.

**«Раскрывающая сторона»** – Сторона, осуществляющую раскрытие информации и/или предоставляющая доступ к принадлежащим ей информационным ресурсам (информационным системам);

**«Принимающей стороной»** – Сторону, осуществляющую прием информации.

1. ОБЩИЕ ПОЛОЖЕНИЯ
	1. В рамках заключенного договора ˂\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_˃ (далее – Договор) Раскрывающая сторона намерена предоставить доступ Принимающей стороны к принадлежащей Раскрывающей Стороне конфиденциальной информации.
	2. Для надлежащего уровня защищенности Конфиденциальной информации Стороны согласовали нижеуказанный режим работы с Конфиденциальной информацией, способы ее защиты от Разглашения, ответственность за Разглашение Конфиденциальной информации.
2. ПРЕДМЕТ СОГЛАШЕНИЯ
	1. Принимающая Сторона обязуется обеспечить защиту Конфиденциальной информации от Разглашения в порядке, предусмотренном настоящим Соглашением на протяжении всего периода действия Соглашения и в течении 5 (пяти) лет после его окончания.
	2. Защите в соответствии с условиями настоящего Соглашения подлежит конфиденциальная информация:

(а) полученная Принимающей стороной от Раскрывающей стороны;

(б) ставшая доступна Принимающей стороне в результате доступа к информационным системам Раскрывающей стороны.

* 1. В рамках настоящего соглашения к Конфиденциальной информации относится информация Раскрывающей стороны согласно Перечня информации, составляющей коммерческую тайну и иной конфиденциальной информации ООО «Газпром страхование» (далее – Перечень конфиденциальной информации) (Приложение № 1), который является неотъемлемой частью настоящего Соглашения. Принадлежность информации к разряду Конфиденциальной не зависит от наличия или отсутствия на носителе информации, в реквизитах документа (файла), какой-либо маркировки (отметки, грифа).

Раскрывающая сторона вправе в одностороннем порядке вносить изменения в Перечень конфиденциальной информации. Информирование Принимающей стороны о внесении изменений в Перечень конфиденциальной информации, осуществляется путем размещения соответствующих сведений на официальном сайте ООО «Газпром страхование» <https://www.gazpromins.ru/>. Изменения в Перечне конфиденциальности вступают в силу с даты размещения указанных сведений на сайте. Принимающая сторона самостоятельно отслеживает размещение информации на сайте.

1. ОБЯЗАННОСТИ СТОРОН ПО ОБЕСПЕЧЕНИЮ КОНФИДЕНЦИАЛЬНОСТИ
	1. Принимающая Сторона обязуется:
		1. Обеспечивать соблюдение Режима конфиденциальности в отношении Конфиденциальной информации Раскрывающей стороны которая была ей предоставлена, либо к которой она получила доступ, с обязательным соблюдением следующих минимальных требований:
2. Принимающей Стороной должен обеспечиваться достоверный учет Конфиденциальной информации, к которой она получила доступ, мест хранения такой Конфиденциальной информации, включая информационные системы, к которой Принимающая сторона имела доступ;
3. хранение Конфиденциальной информации на материальных носителях информации должно осуществляться Принимающей Стороной в служебных помещениях, обеспечивающих физическую сохранность носителей Конфиденциальной информации, а также соблюдение Режима конфиденциальности в соответствии с настоящим Соглашением, в том числе и вне рабочего времени;
4. на устройствах Принимающей Стороны, в которых осуществляется хранение Конфиденциальной информации в электронном виде, должны быть установлены пароли на доступ к ней. Такие пароли также не должны Разглашаться Принимающая Стороной Третьим лицам;
5. Принимающая Сторона обязана осуществлять обработку Конфиденциальной информации Раскрывающей стороны так, чтобы исключить возможность ознакомления с ней лиц, не уполномоченных на такое ознакомление;
6. Принимающая сторона обязуется предоставить Раскрывающей стороне список лиц, допущенных к работе с конфиденциальной информацией, предоставленной (доступ к которой предоставлен) Раскрывающей Стороной.
7. Принимающая Сторона имеет право создавать и/или сохранять только те копии Конфиденциальной информации, выписки из нее (и копии таких выписок), служебные записки (и их копии) и иные документы (и их копии), созданные с использованием Конфиденциальной информации, которые разумно и обоснованно необходимы Принимающей стороне для достижения цели Договора, при этом все другие копии Конфиденциальной информации и указанные документы (и их копии) подлежат обязательному уничтожению в разумно возможный срок.
	* 1. Не допускать Разглашения Конфиденциальной информации, за исключением случаев, когда предоставление Конфиденциальной информации происходит в соответствии с условиями Договора, данного Соглашения или после получения предварительного письменного согласия от Раскрывающей Стороны.
		2. Не предпринимать попытки обхода установленных Раскрывающей Стороной ограничений, направленных на предотвращение Разглашения Конфиденциальной информации, в том числе не осуществлять фото-, аудио-, видео- и иную фиксацию документов и материалов Раскрывающей Стороны, Конфиденциальной информации, отображаемой на экранах мониторов средств вычислительной техники и/или демонстрируемой на экранах в ходе проведения закрытых мероприятий, переговоров и совещаний, а также аудио- и видеофиксацию Конфиденциальной информации, предоставляемой Принимающей Стороне в устной форме, а также фото-, аудио- и видеофиксацию переговоров и совещаний, имеющих отношение к Сотрудничеству, без предварительного письменного согласия Раскрывающей Стороны.
		3. Не осуществлять передачу информации по открытым каналам связи, а также с использованием сети Интернет без принятия мер защиты, удовлетворяющих Стороны Соглашения. Для определения мер защиты, удовлетворяющих Стороны, Стороны выделяют уполномоченных специалистов, а в случае необходимости совместно создают рабочую группу, для определения решений по реализации мер защиты. Принятые решения фиксируются Сторонами в любой удовлетворяющей Стороны форме, принимаются ими к обязательному взаимному исполнению.
		4. Не допускать использование Конфиденциальной информации в иных целях, отличных от цели выполнения условий Договора с Раскрывающей стороной.
		5. Не допускать без письменного согласования Раскрывающей стороны публикации в средствах массовой информации, социальных сетях и прочих подобных им площадках информации о контрактах, договорах, соглашениях, заключенных (заключаемых) с Раскрывающей стороной,
		6. Незамедлительно сообщать в письменной форме (посредством электронной почты) Раскрывающей Стороне о фактах Разглашения (а также о попытках совершения Третьими лицами действий с целью неправомерного получения доступа к Конфиденциальной информации), но в любом случае не позднее чем в течение 1 (одного) рабочего дня с момента, когда Принимающей Стороне станет известно о таких фактах, и предпринимать обоснованно необходимые меры для минимизации негативных последствий Разглашения и защиты от таких инцидентов в будущем.

В случае, если раскрываемую информацию или ее часть по объективным причинам, не зависящим от Принимающей Стороны, невозможно предоставить в установленный данным пунктом срок, допускается ее предоставление в течение 10 (десяти) рабочих дней с даты, когда Принимающей Стороне станет известно о невозможности своевременного предоставления информации.

* + 1. Незамедлительно уведомлять Раскрывающую Сторону о факте возбуждения Третьими лицами исков или совершения ими иных юридически значимых действий, направленных на получение доступа к Конфиденциальной информации, но в любом случае не позднее 2 (двух) рабочих дней с момента, когда Принимающей Стороне станет известно о таких фактах, при условии, что направление такого уведомления не запрещено действующим законодательством Российский Федерации.
		2. Принимающая Сторона обязуется, по требованию Раскрывающей Стороны, продемонстрировать соблюдение условий настоящего Соглашения путем предоставления подтверждающих документов, при условии, что исполнение этой обязанности не будет противоречить обязательствам Принимающей стороны перед Третьими лицами по обеспечению конфиденциальности информации.
	1. Раскрывающая сторона обязуется:

(а) предоставить Принимающей стороне информацию, обеспечивающую выполнение Договора;

(б) предоставить Принимающей стороне доступ к информационным системам в объеме, предусмотренном Договором;

1. ИСКЛЮЧЕНИЯ ИЗ ОБЯЗАННОСТЕЙ ПО ОБЕСПЕЧЕНИЮ КОНФИДЕНЦИАЛЬНОСТИ
	1. Обязанности Принимающей Стороны, предусмотренные разделом 4 Соглашения, не распространяются на Конфиденциальную информацию, которая:

(а) предоставляется Принимающей Стороной органам государственной и муниципальной власти в том объеме, в котором это необходимо для исполнения требований действующего законодательства, распоряжений суда или законных предписаний органов государственной и муниципальной власти, изданных в пределах их компетенции при предварительном уведомлении (если это не запрещено соответствующими нормативными правовыми актами) в трехдневный срок Раскрывающей Стороны о характере, причинах, целях, форме и сроках такого предоставления, и объеме предоставляемой Конфиденциальной информации;

(б) не может считаться конфиденциальной в соответствии с законодательством Российской Федерации;

(в) является или становится общеизвестной по причинам, не связанным с нарушением Принимающей Стороной положений настоящего Соглашения.

1. ВОЗВРАТ ИНФОРМАЦИИ И ДЕЙСТВИЕ УСЛОВИЙ СОГЛАШЕНИЯ ПОСЛЕ ЕГО ПРЕКРАЩЕНИЯ
	1. По требованию Раскрывающей Стороны, а также по окончанию срока действия Соглашения и при расторжении Соглашения Принимающая Сторона обязана, по письменному запросу Раскрывающей Стороны, в течение 10 (десяти) рабочих дней с даты получения такого запроса:
2. уничтожить/обеспечить уничтожение и/или вернуть/обеспечить возврат Раскрывающей Стороне всех предоставленных документов и иных материалов, а также переданных ей Раскрывающей Стороной материальных носителей, содержащих Конфиденциальную информацию (с составлением акта приема-передачи материальных носителей Конфиденциальной информации, скрепленного печатями Сторон, при их наличии, и подписями уполномоченных представителей Сторон), включая все копии и выписки, сделанные Принимающей Стороной, за исключением документов и материалов, которые могут потребоваться Принимающей стороне для защиты своих интересов в случае возникновения между Сторонами споров в рамках и в связи с Соглашением и/или Сотрудничеством;
3. удалить или обеспечить удаление всех электронных копий Конфиденциальной информации из информационных систем Принимающей Стороны;
4. прекратить доступ к информационным системам Раскрывающей Стороны;
5. предоставить Раскрывающей Стороне документ с печатью Принимающей Стороны (при ее наличии) и подписью уполномоченного представителя Принимающей Стороны, подтверждающий исполнение обязанностей, указанных в данном пункте, в течение двух рабочих дней после даты такого исполнения.
6. ОТВЕТСТВЕННОСТЬ СТОРОН
	1. Принимающая Сторона обязана возместить Раскрывающей Стороне документально подтвержденные убытки, возникшие в результате нарушения ей условий данного Соглашения в полном объеме. Обоснованное письменное требование о возмещении убытков подлежит удовлетворению в течение десяти рабочих дней с даты получения такого требования Принимающей Стороной.
	2. За каждый случай нарушения условий настоящего Соглашения нарушившая Сторона выплачивает другой Стороне неустойку в размере ˂ *указать сумму[[1]](#footnote-1)*˃ рублей). Обоснованное письменное требование об уплате неустойки подлежит удовлетворению в течение десяти рабочих дней с момента получения такого требования Стороной.
	3. Кроме того, в случае доказанного факта утечки персональных данных Принимающая Сторона обязуется уплатить неустойку в размере 100 000 (сто) тысяч рублей, за каждый субъект персональных данных в отношении персональных данных которого произошла утечка информации.
	4. Прекращение Соглашения не освобождает Стороны от ответственности за нарушение его условий, имевшее место в период действия Соглашения.
7. ПЕРЕДАЧА ПРАВ
	1. Ни одна из Сторон не может передавать или иным образом уступать, полностью или частично, свои права и обязанности по данному Соглашению без предварительного письменного согласия на это другой Стороны.
	2. Права и обязанности Сторон по настоящему Соглашению в случае реорганизации какой-либо из Сторон переходят к соответствующему правопреемнику (правопреемникам). В случае ликвидации какой-либо Стороны или по прекращению действия настоящего Соглашения Принимающая сторона обязуется до завершения ликвидации (до прекращения действия настоящего соглашения) уничтожить информацию, переданную в рамках Договора и составить акт об уничтожении такой информации.
8. ДОПОЛНИТЕЛЬНЫЕ ОБЯЗАННОСТИ СТОРОН И ЗАВЕРЕНИЯ ОБ ОБСТОЯТЕЛЬСТВАХ, ИМЕЮЩИХ ЗНАЧЕНИЕ ДЛЯ ЗАКЛЮЧЕНИЯ И ИСПОЛНЕНИЯ СОГЛАШЕНИЯ
	1. Стороны заверяют друг друга в том, что они (их работники и уполномоченные представители) имеют право и необходимые полномочия, в соответствии с соответствующим применимым правом, заключать и исполнять настоящее Соглашение, и что на момент заключения настоящего Соглашения они не связаны никакими обязательствами, которые могут воспрепятствовать каким-либо образом заключению Соглашения и надлежащему исполнению принятых ими на себя обязательств по Соглашению.
	2. Раскрывающая Сторона гарантирует и заверяет Принимающую Сторону в том, что она обладает всеми необходимыми правами и полномочиями на предоставление Принимающей Стороне информации для выполнения Договора и в том, что такое предоставление и использование не нарушает требования применимого к Раскрывающей Стороне права, авторские, смежные, патентные права, права на секреты производства (ноу-хау) и любые иные права третьих лиц.
	3. Передавая Принимающей Стороне информацию, составляющую персональные данные Раскрывающая сторона гарантирует наличие всех необходимых согласий со стороны субъектов персональных данных на такую передачу.
	4. Заключая настоящее Соглашение, Стороны заключают Соглашение о кибербезопасности (Приложение № 2), которое является неотъемлемой частью настоящего Соглашения.
	5. Если по условиям Договора Принимающая сторона осуществляет разработку web-сервисов и программного обеспечения, создаваемых в интересах Раскрывающей стороны, Стороны заключают Соглашение о безопасной разработке (Приложение № 3)[[2]](#footnote-2), которое является неотъемлемой частью настоящего Соглашения.
9. РАЗРЕШЕНИЕ СПОРОВ И ПРИМЕНИМОЕ ПРАВО
	1. Настоящее Соглашение толкуется и регулируется в соответствии с законодательством Российской Федерации.
	2. Споры и разногласия, вытекающие из настоящего Соглашения, должны разрешаться Сторонами путем переговоров. При невозможности урегулирования споров и разногласий путем переговоров спорные вопросы подлежат передаче на разрешение в Арбитражный суд г. Москвы в соответствии с законодательством Российской Федерации.
10. ПРОЧИЕ УСЛОВИЯ
	1. Дополнения и изменения в настоящее Соглашение могут быть внесены только на основании письменного соглашения, подписанного должным образом уполномоченными представителями Сторон.
	2. Настоящее Соглашение вступает в силу с даты его подписания и действует по «\_\_\_» \_\_\_\_\_\_\_\_\_\_20\_\_ г.
	3. Стороны подписали настоящее Соглашение в 2 (двух) экземплярах, имеющих равную юридическую силу, по одному для каждой из Сторон.
	4. Подписи представителей Сторон:

|  |  |
| --- | --- |
| * **От**
 | * **От Контрагента**
 |
| * <Должность>
 | * <Должность>
 |
| * \_\_\_\_\_\_\_\_\_\_\_\_\_\_ / \_\_\_\_\_(указать ФИО) /
 | * \_\_\_\_\_\_\_\_\_\_\_\_\_\_ / \_\_\_\_\_(указать ФИО) /
 |
| * м.п.
 | * м.п.
 |

Приложение № 1

К Соглашению о конфиденциальности

ПЕРЕЧЕНЬ

информации, составляющей коммерческую тайну и иной конфиденциальной информации

| № п/п | Содержание информации |
| --- | --- |
|
|  | Планово-бюджетная информация и бюджеты Общества |
|  | Сведения о ценообразовании на страховые продукты (за исключением коммерческих переговоров с партнерами) |
|  | Данные о движении денежных средств по инвестиционным договорам, в том числе о суммах и сроках уплаты процентного дохода за исключением сведений, подлежащих раскрытию в соответствии с действующим законодательством. Сводные сведения о планируемых поступлениях и выплатах денежных средств. |
|  | Коммерческие предложения, котировки, документы по участию в тендерах и конкурсах по страхованию |
|  | Сведения о формах, содержании и условиях (как в отдельности, так и в совокупности) заключения коммерческих сделок, договоров |
|  | Материалы о работе со страховыми посредниками для согласования ставок комиссионного вознаграждения |
|  | Информация других организаций, отнесенная ими к коммерческой тайне |
|  | Сведения о страхователе, о застрахованном лице и выгодоприобретателе  |
|  | Сведения о состоянии здоровья страхователя, застрахованного лица и выгодоприобретателя  |
|  | Сведения об имущественном положении страхователя, застрахованного лица и выгодоприобретателя  |
|  | Сведения об объектах страхования  |
|  | Сведения о факте обращения лица за оказанием медицинской помощи, состоянии его здоровья, диагнозе и иные сведения, полученные при его медицинском обследовании и лечении  |
|  | Данные работников Общества |
|  | Данные физических лиц - представителей контрагентов Общества и иных юридических лиц |
|  | Хранящаяся в базе данных сводная информация о партнерах и клиентах ООО «Газпром страхование» |
|  | Информация других организаций, отнесенная ими к разряду конфиденциальной  |
|  | Значение кодов, паролей и иных идентификаторов, используемых для подтверждения полномочий при установлении связи, разблокировки средств вычислительной техники и (или) доступа к информационным ресурсам  |
|  | Ключевая информация средств криптографической защиты  |
|  | Сведения о технической укрепленности и системе охраны учреждений и объектов Общества |
|  | Сведения, связанные с обеспечением корпоративной безопасности в Обществе, полученные в результате служебной деятельности |
|  | Сведения об архитектуре, составу, топологии, конфигурации и параметрам средств и систем вычислительной техники, программно-технических комплексов и технических средств связи и коммуникаций |
|  | Техническая документация на программные компоненты, используемые в Обществе, включая исходные коды программных компонентов |
|  | Сведения об убытках общества по договорам страхования |
|  | Сведения по расчету заработной платы и иных выплат работникам Общества |
|  | Информация о конкретных методах или способах обеспечения безопасности и защиты информации  |
|  | Сведения об имущественных интересах граждан и организаций Российской Федерации, находящихся под действием иностранных санкций  |
|  | Сведения о вооружении, военной технике, объектах военно-промышленного комплекса Российской Федерации и государственного оборонного заказа, о воинских перевозках и транспортировке особо опасных грузов, включая наименование, количество, стоимость, дислокацию, маршруты и способы транспортировки  |
|  | Сведения об ущербе и происшествиях, которые произошли в отношении имущественных интересов граждан и организаций Российской Федерации, находящихсяпод действием иностранных санкций  |
|  | Сведения об ущербе и происшествиях, которые произошли в отношении вооружения, военной техники, объектов военно-промышленного комплекса Российской Федерации и государственного оборонного заказа, воинских перевозок и транспортировок особо опасных грузов  |

Подписи представителей Сторон:

|  |  |
| --- | --- |
|  | * **От Контрагента**
 |
| * <Должность>
 | * <Должность>
 |
| * \_\_\_\_\_\_\_\_\_\_\_\_\_\_ / \_\_\_(указать ФИО) /
 | * \_\_\_\_\_\_\_\_\_\_\_\_\_\_ / \_\_\_\_\_(указать ФИО)/
 |
| * м.п.
 | * м.п.
 |

Приложение № 2

К Соглашению о конфиденциальности

СОГЛАШЕНИЕ

О КИБЕРБЕЗОПАСНОСТИ

|  |  |  |
| --- | --- | --- |
| г. Москва |  | «\_\_\_\_\_» \_\_\_ 20\_\_ г. |

ООО «Газпром страхование», далее именуемое «Общество» в лице ˂\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_˃, действующего на основании ˂\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_˃, с одной стороны,
и˂ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_˃, далее именуемое «Компания» в лице ˂\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_˃, действующего на основании ˂\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_˃,
с другой стороны, совместно именуемые «Стороны», заключили настоящее соглашение о кибербезопасности (далее – «Соглашение») о нижеследующем.

# ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

**Информационная система** – совокупность взаимосогласованных компонентов программного, технического, информационного, организационного, методического, правового обеспечения, используемая пользователями для реализации заданной информационной технологии.

**Безопасность информации** – сохранение конфиденциальности, целостности и доступности информации; кроме того, также могут охватываться другие свойства информации, такие как аутентичность, учетность, неотказуемость и надежность.

**Вредоносное программное обеспечение** – программное обеспечение, предназначенное для получения несанкционированного доступа к устройству пользователя или к информации, хранимой на нем, с целью несанкционированного использования информационных ресурсов или причинения вреда.

**Доступность** – гарантия того, что авторизованные пользователи могут иметь доступ и работать с необходимыми информационными активами, ресурсами и системами с требуемой производительностью.

**Информационный актив –** информация с реквизитами, позволяющими ее идентифицировать, имеющая ценность для Общества, находящаяся в его распоряжении и представленная на любом материальном носителе в форме, пригодной для ее обработки, хранения или передачи.

**Информационный ресурс** – отдельный документ или отдельный массив документов, документ или массив документов в автоматизированной системе (библиотеке, архиве, фонде, банке/базе данных и т.д.).

**Инцидент кибербезопасности –** одно или несколько событий кибербезопасности, приводящих с высокой вероятностью к угрозе проведения бизнес-операций и/или угрозе кибербезопасности.

**Оборудование** - любые устройства, обладающие функционалом по обработке информации (включая ввод, хранение, отображение, поиск, передачу, коммутацию, управление), которые могут быть подключены к СВТ Общества по интерфейсам (включая беспроводные), предназначенным для передачи данных.

**Кибербезопасность –** состояние защищенности киберпространства (сохранение конфиденциальности, целостности, доступности), достигающееся применением набора средств, методик и принципов, направленных на противодействие угрозам в киберпространстве и минимизацию последствий их реализации.

**Киберпространство** – информационное пространство, образованное совокупностью телекоммуникационных сетей и оборудования, средств вычислительной техники и программного обеспечения, а также деятельностью человека по его информационному наполнению.

**Конфиденциальность** – характеристика, определяющая, что информация не может быть доступной и раскрытой неавторизованным лицом, логическим объектом или процессом.

**Подключение** – действие, последствием которого является передача информации между Оборудованием Компании и инфраструктурой или СВТ Общества.

**Средства вычислительной техники** – автоматизированные рабочие места и оргтехника (средства печати, копирования и сканирования и т.д.), а также серверное и сетевое оборудование.

**Уязвимость** – недостаток в компьютерной системе, использование которого приводит к нарушению целостности системы и некорректной работе.

**Целостность** - свойство сохранения правильности и полноты информационных активов.

1. ПРЕДМЕТ СОГЛАШЕНИЯ

## Компания, получая доступ к информационным ресурсам Общества обязуется соблюдать требования законодательства Российской Федерации.

## Компания обязуется применять защитные меры и проводить мероприятия, перечисленные в настоящем Соглашении. Технические требования, предъявляемые к ИТ-инфраструктуре Компании изложены в Приложении к настоящему Соглашению. Условия Соглашения являются обязательными для Компании и распространяются на любые действия Компании и ее работников, а также подрядных организаций, привлекаемых Компанией к выполнению договора, связанные с доступом к информационным ресурсам Общества.

## В случае заключения договоров, на которые распространяется действие Соглашения, Стороны включают в такие договоры нормы о том, что к отношениям в рамках этих договоров применяются положения Соглашения. При наличии между Сторонами договорных отношений, на которые распространяется Соглашение, Стороны признают, что при неисполнении Компанией обязательств по Соглашению Общество имеет право приостановить доступ к информационным ресурсам в рамках соответствующего Договора до момента устранения Компанией нарушений условий настоящего Соглашения.

## Стороны признают, что при наличии между Сторонами договоров, на которые распространяется Соглашение, обязательство Компании по исполнению требований по кибербезопасности, применению защитных мер, проведению мероприятий и иных условий, установленных Соглашением, является обстоятельством, имеющим существенное значение для Общества для исполнения, а также при принятии Обществом решения о заключении или прекращении действия таких договоров (в порядке, предусмотренном ст. 431.2 Гражданского кодекса РФ).

# ТРЕБОВАНИЯ ПО КИБЕРБЕЗОПАСНОСТИ

* 1. Соглашение является неотъемлемой частью действующего соглашения о конфиденциальности.
	2. Средства вычислительной техники (далее – СВТ) Компании, посредством которых осуществляется взаимодействие с объектами ИТ-инфраструктуры Общества, должны быть размещены в выделенных сетевых сегментах Компании, изолированных от сети Интернет, взаимодействие указанных СВТ с внутренней сетью Компании должно осуществляться только в рамках схемы взаимодействия, согласованной с Обществом.
	3. Запрещается организация информационного взаимодействия между Компанией и Обществом по сетевым протоколам без использования шифрования трафика.
	4. Способ организации защищенного удаленного доступа к информационным ресурсам Общества, технические параметры подключения, тип и настройки оборудования, используемого для удаленного доступа, определяются Обществом.
	5. Почтовый трафик между Обществом и Компанией должен передаваться внутри VPN-туннеля или с использованием средств защиты сетевых подключений; при использовании протокола TLS должна использоваться версия не ниже 1.1;
	6. Подключение Компании к ИТ-инфраструктуре Общества осуществляется путем установки сетевого соединения СВТ Компании с СВТ внешней сети Общества с обязательной трансляцией IP-адресов на сетевом оборудовании Компании в диапазон адресов, выданный Обществом и закрепленным за Компанией. Соединение должно осуществляться с использованием средств защиты сетевых соединений
	7. При возникновении необходимости подключения любого оборудования Компании к ИТ-инфраструктуре Общества такое подключение осуществляется после согласования Сторонами схемы подключения и описания условий данного подключения в договоре (дополнительном соглашении к договору).
	8. В случае, если работнику Компании потребуется доступ к СВТ, оборудованию, информационным системам Общества или в помещения Общества, работник Компании обязан выполнять требования Правил Обеспечения информационной безопасности, размещенных на сайте Общества по адресу https://www.sogaz.ru/info/#privacy. Компания и ее представители заверяют, что Правила Обеспечения информационной безопасности Общества им понятны. Контрагент обязуется их выполнять.

 Общество вправе в одностороннем порядке вносить изменения в вышеупомянутые Правила обеспечения информационной безопасности путем размещения в информационно телекоммуникационной сети Интернет на официальном сайте ООО «Газпром страхование» по адресу https://www.gazpromins.ru/. Контрагент обязуется самостоятельно отслеживать изменения Правил обеспечения информационной безопасности Общества.

* 1. Для организации доступа работникам Компании к информационным ресурсам Общества Компания должна направить в Общество список таких работников. Список работников направляется письмом на имя лица, подписавшего договор с Компанией и подлежит актуализации в случае изменения персонального состава лиц, допущенных к информационным ресурсам Общества.
	2. Для доступа к информационным ресурсам Общества, работникам Компании предоставляются персонифицированные учетные записи.
		1. Работники Компании обязаны обеспечить конфиденциальность предоставленных им учетных записей, не допуская их раскрытия перед третьими лицами, включая других работников Компании, в том числе своих руководителей.
		2. При первом подключении к информационным ресурсам Общества работник Компании обязан поменять пароль учетной записи.
		3. При использовании пароля учетной записи:

(а) необходимо назначать уникальный пароль для каждого информационного ресурса;

(б) пароль должен быть длиной не менее 14 (четырнадцати) символов и должен содержать в себе следующие буквы нижнего регистра, буквы верхнего регистра, цифры и спецсимволы (например, ~ @ # $ % ^ &);

(в) 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.;

(г) пароль подлежит смене не реже одного раза в 30 (тридцать) дней;

(д) при смене пароля новый пароль не должен совпадать с двумя предыдущими. Общество вправе отказать работнику Компании в запрошенном доступе.

* 1. Компания в полном объеме несет ответственность за действия своих работников, выполняющих работы (оказывающих услуги) в информационных системах, на оборудовании, СВТ или в помещениях Общества.
	2. Общество в праве осуществлять проверку условий обеспечения безопасности обработки Контрагентом информации, доступ к которой предоставлен Обществом и порядка выполнения требований настоящего соглашения по кибербезопасности.
	3. Компания на постоянной основе, не реже одного раза в квартал, должна проводить сканирование защищенности внешнего периметра локальной вычислительной сети, при этом область сканирования должна включать, как минимум, СВТ и сетевое оборудование:
* взаимодействующее с инфраструктурой Общества;
* сетевой траффик с которыми разрешен для информационных систем и СВТ, обрабатывающих данные клиентов или партнеров Общества.

О результатах сканирования Компания должна информировать Общество.

* 1. В случае выявления по результатам сканирования уязвимостей, эксплуатация которых потенциально несет угрозу данным клиентов Общества, Компания обязана в течение максимально короткого срока устранить данные уязвимости, а в случае невозможности устранения – незамедлительно информировать об этом Общество.
	2. Компания обязуется на постоянной основе, не реже одного раза в год, проводить аудиты кибербезопасности Компании с привлечением внешних организаций, обладающих правом проведения таких аудитов на законном основании. О результатах таких аудитов Компания должна информировать Общество.

# ОБМЕН ИНФОРМАЦИЕЙ ОБ ИНЦИДЕНТАХ КИБЕРБЕЗОПАСНОСТИ

* 1. При возникновении в инфраструктуре Компании значимого инцидента КБ, последствия которого могут затронуть интересы Общества (в том числе клиентов или партнеров Общества), Компания обязана известить об этом Общество в максимально возможный короткий срок, но не позднее 3-х (трех) часов с момента обнаружения такого инцидента (подозрения на инцидент).
	2. Значимым считается инцидент КБ, удовлетворяющий одному из следующих критериев:

- невозможность выполнения Обществом бизнес-операций, в соответствии с установленными сроками для структурного подразделения, или ограничение функциональности ИТ-услуги или ИС;

- разглашение аутентификационных данных или конфиденциальной информации (коммерческая тайна, персональные данные, врачебная тайна, тайна страхования и др.);

- воздействие вредоносного ПО, массовые блокировки учетных записей, несанкционированное создание учетных записей;

- выявленные признаки несанкционированного доступа или неудачных попыток получения несанкционированного доступа, а также злоупотребление привилегиями.

* 1. В перечень инцидентов КБ Стороны включают инциденты, несущие риски потери конфиденциальности, целостности, доступности информации, в том числе:

- фишинговая атака якобы от имени Стороны;

- эксплуатация выявленной уязвимости на ресурсе, принадлежащем Стороне;

- эксплуатация выявленной уязвимости в программное обеспечение, предоставляемом/эксплуатируемом Стороной;

- заражение вредоносным программным обеспечением;

- несанкционированный доступ к ресурсам Стороны;

- DDOS-атака на ресурсы Стороны – выявленная, закончившаяся или планируемая.

* 1. В случае устранения значимого инцидента КБ Компания обязана уведомить Общество о мерах, предпринятых для управления инцидентом в течение 24 часов.
	2. Компания уведомляет об инцидентах в свободном формате. Для повышения оперативности при передаче технической информации Стороны вправе использовать телефонную связь и иные каналы передачи информации.
	3. В рамках обмена информацией об инцидентах КБ Стороны не обмениваются информацией, содержащей конфиденциальную информацию.

# ПЕРСОНАЛЬНЫЕ ДАННЫЕ

* 1. Если по условиям договора, заключаемого между Обществом и Компанией, осуществляется обработка персональных данных, условия обработки и защиты таких данных должны определяться в соответствии с условиями такого договора.
	2. В случае, если по условиям договора, заключаемого между Обществом и Компанией, одна из Сторон осуществляет обработку персональных данных по поручению другой Стороны, в содержание соответствующего договора должно быть включено поручение на обработку персональных данных, соответствующее требованиям части 3 статьи 6 Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
	3. Стороны принимают на себя обязательства обеспечить конфиденциальность и безопасность персональных данных, ставших известными Сторонам в ходе исполнения договора. Меры, принимаемые для обеспечения безопасности персональных данных и защиты прав субъектов персональных данных, должны соответствовать требованиям законодательства Российской Федерации.
	4. При обработке персональных данных стороны обязуются принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных в соответствии с требованиями к защите обрабатываемых персональных данных, установленными статьей 19 Федерального закона № 152-ФЗ «О персональных данных» от 27.07.2006.

# ДОПОЛНИТЕЛЬНЫЕ ОБЯЗАТЕЛЬСТВА

## Компания гарантирует, что во время действия Соглашения её действия (бездействие) в рамках информационного обмена не приведут к появлению скрытых функциональных возможностей (недокументированных изменений, операций, либо внедренных «программных закладок»), а также компьютерных вирусов, самоликвидирующихся механизмов, механизмов защиты от копирования и других подобных машинных команд, которые могут деактивировать, уничтожить или изменить иным образом данные, программное или аппаратное обеспечение Компаний группы СОГАЗ и Общества в частности.

## В случае выявления Обществом нарушения гарантий, предусмотренных настоящим Соглашением (далее – Нарушение),

* + 1. Общество:

(а) до устранения Нарушения вправе ограничить или полностью прекратить возможность доступа работников Компании к информационным активам Общества;

(б) направить уведомление Компании с приложением подтверждений Нарушения, после чего Компания в течение максимально возможного, с учетом обстоятельств, короткого срока обязана провести расследование, устранить причину Нарушения и предоставить Обществу отчет об устранении Нарушения.

* + 1. Компания:

(а) обязуется компенсировать ущерб, причиненный Обществу Нарушением;

(б) дополнительно выплатить неустойку в сумме:

- 50% от общей суммы Договора, в случае если Нарушение связано с умышленным созданием работниками Компании скрытых функциональных возможностей (недокументированных изменений, операций, либо внедренных «программных закладок»), а также внесением в информационные системы Общества вредоносного программного обеспечения и/ или повлекло за собой значимый инцидент КБ, согласно п. 5.2. настоящего соглашения.

- 20% от общей суммы Договора, в случае если Нарушение связано с непредумышленным созданием работниками Компании скрытых функциональных возможностей (недокументированных изменений, операций, либо внедренных «программных закладок»), а также внесением в информационные системы Общества вредоносного программного обеспечения.

- 10 % от общей суммы Договора, в случае компрометации учетной записи для подключения к информационным системам Раскрывающей стороны.

- 5% от общей суммы Договора, в случае иных нарушений настоящего Соглашения.

## В случае если Компании в рамках исполнения обязательств перед Обществом будет предоставлено право привлекать субподрядчиков, то условия привлечения субподрядчиков подлежат согласованию с Обществом и Компанией в договорах между Обществом и Компанией (для исполнения обязательств, по которым привлекаются субподрядчики). При этом:

### запрещено самостоятельное подключение Компанией субподрядчика к ИТ- инфраструктуре Общества и/или предоставление доступа к СВТ и информационным системам Общества без письменного согласования с Обществом;

### в случае необходимости передачи субподрядчику Компании Конфиденциальной информации Общества, порядок такой передачи, условия передачи и обработки, требования к защите информации определяются отдельным договором между Обществом и субподрядчиком;

### Компания несет ответственность за все действия и/или бездействие привлекаемых ими субподрядчиков в соответствии с законодательством Российской Федерации.

# ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

## Соглашение вступает в силу с момента его подписания Сторонами и действует до полного исполнения Сторонами обязательств, принятых по договорам, заключенным между Сторонами, включая, но не ограничиваясь, по договорам поставки, предоставления Компанией Обществу услуг по Разработке, доработке (модификации, адаптации), настройке программного обеспечения и автоматизированных систем, а также договоры информационного и технологического взаимодействия.

## Общество вправе инициировать пересмотр условий Соглашения по своей инициативе в следующих случаях:

### наличие у Общества необходимости сохранить надлежащий уровень контроля и управления в отношении риска нарушения информационной безопасности Компанией;

### наличие у Общества необходимости принять соответствующие меры для выполнения своих обязательств перед клиентами и контрагентами, а также перед Обществом России и уполномоченными государственными органами.

## Стороны пришли к соглашению, что в течение действия Соглашения Общество вправе осуществить контроль за соблюдением Компанией требований кибер безопасности.

## Все споры, разногласия и требования, возникающие из Соглашения или в связи с ним, в том числе касающиеся его исполнения, нарушения, прекращения или недействительности, будут разрешаться сторонами претензионным путем. В случае если одна Сторона посчитает, что ее право нарушено, она должна направить другой Стороне обоснованную претензию.

## Сторона, получившая претензию, обязана удовлетворить ее, либо направить мотивированные возражения в срок не более 10 (десяти) рабочих дней с момента получения претензии.

## В случае, если претензия одной Стороны не удовлетворена и мотивированные возражения не получены, либо полученные мотивированные возражения не считаются Стороной, право которой нарушено, обоснованными, споры подлежат разрешению в Арбитражном суде г. Москвы, применимое право – право Российской Федерации.

## Внесение изменений (новые условия) в Соглашение осуществляется в письменной форме по взаимному согласию Сторон путем оформления документа, подписываемого уполномоченными представителями Сторон, который является неотъемлемой частью Соглашения.

## Соглашение составлено в двух экземплярах, имеющих одинаковую юридическую силу по одному экземпляру для каждой из Сторон.

# ПОДПИСИ ПРЕДСТАВИТЕЛЕЙ СТОРОН

|  |  |
| --- | --- |
| * **От**
 | * **От Контрагента**
 |
| * <Должность>
 | * <Должность>
 |
| * \_\_\_\_\_\_\_\_\_\_\_\_\_\_ / \_\_\_\_\_(указать ФИО) /
 | * \_\_\_\_\_\_\_\_\_\_\_\_\_\_ / \_\_\_\_\_(указать ФИО) /
 |
| * м.п.
 | * м.п.
 |

Приложение № 1

К Соглашению о кибербезопасности

**Состав технических требований по защите информации**

| **№ п/п** | **Описание технического требования** |
| --- | --- |
|  | Осуществление логического доступа пользователями и эксплуатационным персоналом под уникальными и персонифицированными учетными записями |
|  | Хранение эталонной информации о предоставленных правах логического доступа и обеспечение целостности указанной информации |
|  | Контроль соответствия фактических прав логического доступа эталонной информации о предоставленных правах логического доступа |
|  | Исключение возможного бесконтрольного самостоятельного расширения пользователями предоставленных им прав логического доступа |
|  | Исключение возможного бесконтрольного изменения пользователями параметров настроек средств и систем защиты информации, параметров настроек АС, связанных с защитой информации |
|  | Контроль прекращения предоставления логического доступа и блокирование учетных записей при истечении периода (срока) предоставления логического доступа |
|  | Установление фактов неиспользования субъектами логического доступа, предоставленных им прав на осуществление логического доступа на протяжении периода времени, превышающего 90 дней |
|  | Реализация возможности определения состава предоставленных прав логического доступа для конкретного ресурса доступа |
|  | Реализация возможности определения состава предоставленных прав логического доступа для конкретного субъекта логического доступа |
|  | Определение состава ролей, связанных с выполнением операции (транзакции) в АС, имеющих финансовые последствия для Компании, клиентов и контрагентов, и ролей, связанных с контролем выполнения указанных операций (транзакций), запрет выполнения указанных ролей одним субъектом логического доступа |
|  | Реализация правил управления правами логического доступа, обеспечивающих запрет совмещения одним субъектом логического доступа ролей, предусмотренных мерой 10 настоящей таблицы |
|  | Регистрация событий защиты информации, связанных с действиями, и контроль действий эксплуатационного персонала, обладающего привилегированными правами логического доступа, позволяющими осуществить деструктивное воздействие, приводящие к нарушению выполнения бизнес-процессов или технологических процессов Компании |
|  | Регистрация событий защиты информации, связанных с действиями, и контроль действий эксплуатационного персонала и пользователей, обладающих правами логического доступа, в том числе в АС, позволяющими осуществить операции (транзакции), приводящие к финансовым последствиям для Компании, клиентов и контрагентов |
|  | Регистрация событий защиты информации, связанных с действиями, и контроль действий эксплуатационного персонала, обладающего правами по управлению логическим доступом |
|  | Регистрация событий защиты информации, связанных с действиями по управлению учетными записями и правами субъектов логического доступа |
|  | Регистрация событий защиты информации, связанных с действиями, и контроль действий эксплуатационного персонала, обладающего правами по управлению техническими мерами, реализующими многофакторную аутентификацию |
|  | Регистрация событий защиты информации, связанных с действиями, и контроль действий эксплуатационного персонала, обладающего правами по изменению параметров настроек средств и систем защиты информации, параметров настроек информационных систем, связанных с защитой информации |
|  | Регистрация событий защиты информации, связанных с действиями, и контроль действий эксплуатационного персонала, обладающего правами по управлению криптографическими ключами |
|  | Идентификация и однофакторная аутентификация пользователей |
|  | Идентификация и многофакторная аутентификация эксплуатационного персонала |
|  | Аутентификация программных сервисов, осуществляющих логический доступ с использованием технических учетных записей |
|  | Аутентификация СВТ эксплуатационного персонала, используемых для осуществления логического доступа |
|  | Сокрытие (неотображение) паролей при их вводе субъектами доступа |
|  | Временная блокировка учетной записи пользователей после выполнения ряда неуспешных последовательных попыток аутентификации на период времени не менее 30 мин |
|  | Запрет множественной аутентификации субъектов логического доступа с использованием одной учетной записи путем открытия параллельных сессий логического доступа с использованием разных СВТ, в том числе виртуальных |
|  | Обеспечение возможности выполнения субъектом логического доступа - работниками Компании процедуры принудительного прерывания сессии логического доступа и (или) приостановки осуществления логического доступа (с прекращением отображения на мониторе СВТ информации, доступ к которой получен в рамках сессии осуществления логического доступа) |
|  | Автоматическое прерывание сессии логического доступа (приостановка осуществления логического доступа) по истечении установленного времени бездействия (неактивности) субъекта логического доступа, не превышающего 15 мин, с прекращением отображения на мониторе СВТ информации, доступ к которой получен в рамках сессии осуществления логического доступа |
|  | Выполнение процедуры повторной аутентификации для продолжения осуществления логического доступа после его принудительного или автоматического прерывания (приостановки осуществления логического доступа), предусмотренного мерами 26 и 27 настоящей таблицы  |
|  | Использование на СВТ субъектов логического доступа встроенных механизмов контроля изменения базовой конфигурации оборудования (пароль на изменение параметров конфигурации системы, хранящихся в энергонезависимой памяти) |
|  | Запрет на использование технологии аутентификации с сохранением аутентификационных данных в открытом виде в СВТ |
|  | Запрет на передачу аутентификационных данных в открытом виде по каналам и линиям связи и их передачу куда- либо, кроме средств или систем аутентификации |
|  | Смена паролей пользователей не реже одного раза в год |
|  | Смена паролей эксплуатационного персонала не реже одного раза в квартал |
|  | Использование пользователями паролей длиной не менее восьми символов |
|  | Использование эксплуатационным персоналом паролей длиной не менее шестнадцати символов |
|  | Использование при формировании паролей субъектов логического доступа символов, включающих буквы (в верхнем и нижнем регистрах) и цифры |
|  | Обеспечение возможности самостоятельной смены субъектами логического доступа своих паролей |
|  | Авторизация логического доступа к ресурсам доступа, в том числе информационных систем |
|  | Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод) при разграничении логического доступа к ресурсам доступа |
|  | Реализация необходимых типов (чтение, запись, выполнение или иной тип) и правил разграничения логического доступа к ресурсам доступа, в том числе информационных систем |
|  | Запрет реализации пользователями бизнес-процессов и технологических процессов Компании с использованием учетных записей эксплуатационного персонала, в том числе в информационных систем |
|  | Запрет выполнения пользователями бизнес-процессов с использованием привилегированных прав логического доступа, в том числе работы пользователей с правами локального администратора СВТ |
|  | Контроль состава разрешенных действий в информационных системах до выполнения идентификации и аутентификации |
|  | Регистрация выполнения субъектами логического доступа ряда неуспешных последовательных попыток аутентификации |
|  | Регистрация осуществления субъектами логического доступа идентификации и аутентификации |
|  | Регистрация авторизации, завершения и (или) прерывания (приостановки) осуществления эксплуатационным персоналом и пользователями логического доступа, в том числе в информационных системах |
|  | Регистрация запуска программных сервисов, осуществляющих логический доступ |
|  | Регистрация изменений аутентификационных данных, используемых для осуществления логического доступа |
|  | Оборудование помещений средствами видеонаблюдения |
|  | Хранение архивов информации средств видеонаблюдения не менее 14 дней |
|  | Учет созданных, используемых и (или) эксплуатируемых ресурсов доступа |
|  | Контроль фактического состава созданных, используемых и (или) эксплуатируемых ресурсов доступа (баз данных, сетевых файловых ресурсов, виртуальных машин) и их корректного размещения в сегментах вычислительных сетей Компании |
|  | Контроль выполнения операций по созданию, удалению и резервному копированию ресурсов доступа (баз данных, сетевых файловых ресурсов, виртуальных машин) |
|  | Регистрация событий защиты информации, связанных с созданием, копированием, в том числе резервным, и (или) удалением ресурсов доступа (баз данных, сетевых файловых ресурсов, виртуальных машин) |
|  | Выделение в вычислительных сетях Компании отдельных сегментов (групп сегментов), предназначенных для размещения информационной инфраструктуры каждого из контуров безопасности (далее - сегменты контуров безопасности) |
|  | Реализация сетевого взаимодействия и сетевой изоляции на уровне не выше третьего (сетевой) по семиуровневой стандартной модели взаимодействия открытых систем, определенной в ГОСТ Р ИСО/МЭК 7498-1, сегментов контуров безопасности и внутренних вычислительных сетей Компании, не предназначенных для размещения информационной инфраструктуры, входящей в контуры безопасности (далее - иные внутренние вычислительные сети Компании) |
|  | Межсетевое экранирование вычислительных сетей сегментов контуров безопасности, включая фильтрацию данных на сетевом и прикладном уровнях семиуровневой стандартной модели взаимодействия открытых систем, определенной в ГОСТ Р ИСО/МЭК 7498-1 |
|  | Реализация и контроль информационного взаимодействия между сегментами контуров безопасности и иными внутренними вычислительными сетями Компании в соответствии с установленными правилами и протоколами сетевого взаимодействия |
|  | Выделение в вычислительных сетях Компании отдельных сегментов (групп сегментов), предназначенных для размещения информационной инфраструктуры, используемой только на этапе создания и (или) модернизации информационных систем, в том числе тестирования программного обеспечения и СВТ (далее - сегмент разработки и тестирования) |
|  | Реализация запрета сетевого взаимодействия сегмента разработки и тестирования и иных внутренних вычислительных сетей Компании по инициативе сегмента разработки и тестирования |
|  | Выделение отдельных сегментов для размещения общедоступных объектов доступа (в том числе банкоматов, платежных терминалов) |
|  | Реализация сетевого взаимодействия и сетевой изоляции на уровне не выше второго (канальный) по семиуровневой стандартной модели взаимодействия открытых систем, определенной в ГОСТ Р ИСО/МЭК 7498-1, внутренних вычислительных сетей Компании и сети Интернет |
|  | Межсетевое экранирование внутренних вычислительных сетей Компании, включая фильтрацию данных на сетевом и прикладном уровнях семиуровневой стандартной модели взаимодействия открытых систем, определенной в ГОСТ Р ИСО/МЭК 7498-1 |
|  | Реализация и контроль информационного взаимодействия внутренних вычислительных сетей Компании и сети Интернет в соответствии с установленными правилами и протоколами сетевого взаимодействия |
|  | Сокрытие топологии внутренних вычислительных сетей Компании |
|  | Реализация сетевого взаимодействия внутренних вычислительных сетей Компании и сети Интернет через ограниченное количество контролируемых точек доступа |
|  | Реализация почтового обмена с сетью Интернет через ограниченное количество контролируемых точек информационного взаимодействия, состоящих из внешнего (подключенного к сети Интернет) и внутреннего (размещенного во внутренних сетях Компании) почтовых серверов с безопасной репликацией почтовых сообщений между ними |
|  | Регистрация изменений параметров настроек средств и систем защиты информации, обеспечивающих реализацию сегментации, межсетевого экранирования и защиты вычислительных сетей Компании |
|  | Контроль отсутствия (выявление) аномальной сетевой активности, связанной с возможным несанкционированным информационным взаимодействием между вычислительными сетями Компании и сетью Интернет |
|  | Контроль отсутствия (выявление) аномальной сетевой активности, связанной с возможным несанкционированным логическим доступом к ресурсам доступа, размещенным в вычислительных сетях Компании, подключенных к сети Интернет |
|  | Контроль отсутствия (выявление) аномальной сетевой активности, связанной с возможным несанкционированным удаленным доступом |
|  | Контроль отсутствия (выявление) аномальной сетевой активности, связанной с возможным осуществлением атак типа "отказ в обслуживании", предпринимаемых в отношении ресурсов доступа, размещенных в вычислительных сетях Компании, подключенных к сети Интернет |
|  | Блокирование атак типа "отказ в обслуживании" в масштабе времени, близком к реальному |
|  | Контроль и обеспечение возможности блокировки нежелательных сообщений электронной почты (SPAM) |
|  | Реализация контроля, предусмотренного мерами 69 — 72 настоящей таблицы, путем сканирования и анализа сетевого трафика между группами сегментов вычислительных сетей Компании, входящих в разные контуры безопасности |
|  | Реализация контроля, предусмотренного мерами 69 — 72 настоящей таблицы, путем сканирования и анализа сетевого трафика в пределах сегмента контура безопасности |
|  | Реализация контроля, предусмотренного мерами 69 — 72 настоящей таблицы, путем сканирования и анализа сетевого трафика между вычислительными сетями Компании и сетью Интернет |
|  | Регистрация фактов выявления аномальной сетевой активности в рамках контроля, предусмотренного мерами 69 — 72 настоящей таблицы |
|  | Применение сетевых протоколов, обеспечивающих защиту подлинности сетевого соединения, контроль целостности сетевого взаимодействия и реализацию технологии двухсторонней аутентификации при осуществлении логического доступа с использованием телекоммуникационных каналов и (или) линий связи, не контролируемых финансовой организацией |
|  | Реализация защиты информации от раскрытия и модификации, применение двухсторонней аутентификации при ее передаче с использованием сети Интернет, телекоммуникационных каналов и (или) линий связи, не контролируемых финансовой организацией |
|  | Контроль отсутствия и обеспечение оперативного устранения известных (описанных) уязвимостей защиты информации, использование которых может позволить осуществить несанкционированное (неконтролируемое) информационное взаимодействие между сегментами контуров безопасности и иными внутренними сетями Компании |
|  | Контроль отсутствия и обеспечение оперативного устранения известных (описанных) уязвимостей защиты информации, использование которых может позволить осуществить несанкционированное (неконтролируемое) информационное взаимодействие между внутренними вычислительными сетями Компании и сетью Интернет |
|  | Контроль отсутствия и обеспечение оперативного устранения известных (описанных) уязвимостей защиты информации, использование которых может позволить осуществить несанкционированное (неконтролируемое) информационное взаимодействие между сегментами, предназначенными для размещения общедоступных объектов доступа (в том числе банкоматов, платежных терминалов), и сетью Интернет |
|  | Контроль отсутствия и обеспечение оперативного устранения известных (описанных) уязвимостей защиты информации, использование которых может позволить осуществить несанкционированный логический доступ к ресурсам доступа, размещенным в вычислительных сетях Компании, подключенных к сети Интернет |
|  | Контроль отсутствия и обеспечение оперативного устранения известных (описанных) уязвимостей защиты информации, использование которых может позволить осуществить несанкционированный удаленный доступ |
|  | Контроль отсутствия и обеспечение оперативного устранения известных (описанных) уязвимостей защиты информации, использование которых может позволить осуществить несанкционированный логический доступ к ресурсам доступа, размещенным во внутренних вычислительных сетях Компании |
|  | Контроль отсутствия и обеспечение оперативного устранения известных (описанных) уязвимостей, предусмотренных мерами 81 — 86 настоящей таблицы, путем сканирования и анализа параметров настроек серверного и сетевого оборудования |
|  | Контроль отсутствия и обеспечение оперативного устранения известных (описанных) уязвимостей, указанных в пунктах 81 — 86 настоящей таблицы, путем сканирования и анализа состава, версий и параметров настроек прикладного программного обеспечения, программного обеспечения информационных систем и системного программного обеспечения, реализующего функции обеспечения защиты информации и (или) влияющего на обеспечение защиты информации (далее в настоящем разделе —системное программное обеспечение, в том числе программное обеспечение операционных систем, программное обеспечение СУБД, программное обеспечение серверов приложений, программное обеспечение систем виртуализации), установленного на серверном и сетевом оборудовании |
|  | Контроль отсутствия и обеспечение оперативного устранения известных (описанных) уязвимостей, предусмотренных мерами 81 — 86 настоящей таблицы, путем сканирования и анализа состава, версий и параметров настроек прикладного программного обеспечения, программного обеспечения информационных систем и (или) системного программного обеспечения, установленного на СВТ пользователей и эксплуатационного персонала |
|  | Контроль отсутствия и обеспечение оперативного устранения известных (описанных) уязвимостей, предусмотренных мерами 81 — 86 настоящей таблицы, путем сканирования и анализа состава, версий и параметров настроек средств и систем защиты информации |
|  | Контроль отсутствия и обеспечение оперативного устранения известных (описанных) уязвимостей защиты информации после выполнения обновлений программного обеспечения, в рамках осуществления контроль размещения и своевременного обновления на серверном и сетевом оборудовании программного обеспечения средств и систем защиты информации, прикладного программного обеспечения, программного обеспечения информационных систем, системного программного обеспечения и сигнатурных баз средств защиты информации, в том числе с целью устранения выявленных уязвимостей защиты информации |
|  | Контроль состава разрешенного для использования программного обеспечения СВТ пользователей и эксплуатационного персонала |
|  | Исключение возможности установки и (или) запуска неразрешенного для использования программного обеспечения СВТ пользователей и эксплуатационного персонала |
|  | Контроль состава программного обеспечения СВТ пользователей и эксплуатационного персонала, запускаемого при загрузке операционной системы |
|  | Контроль (выявление) использования технологии мобильного кода |
|  | Регистрация фактов выявления уязвимостей защиты информации |
|  | Регистрация установки, обновления и (или) удаления программного обеспечения информационных систем, программного обеспечения средств и систем защиты информации, системного программного обеспечения на серверном и сетевом оборудовании |
|  | Регистрация установки, обновления и (или) удаления прикладного программного обеспечения, программного обеспечения информационных систем, программного обеспечения средств и систем защиты информации, системного программного обеспечения на СВТ пользователей и эксплуатационного персонала |
|  | Регистрация результатов выполнения операций по контролю состава программного обеспечения СВТ пользователей и эксплуатационного персонала |
|  | Регистрация результатов выполнения операций по контролю состава программного обеспечения, запускаемого при загрузке операционной системы СВТ пользователей и эксплуатационного персонала |
|  | Регистрация выявления использования технологии мобильного кода |
|  | Реализация защиты от вредоносного кода на уровне физических СВТ пользователей и эксплуатационного персонала |
|  | Реализация защиты от вредоносного кода на уровне виртуальной информационной инфраструктуры |
|  | Реализация защиты от вредоносного кода на уровне серверного оборудования |
|  | Реализация защиты от вредоносного кода на уровне контроля межсетевого трафика |
|  | Реализация защиты от вредоносного кода на уровне контроля почтового трафика |
|  | Реализация защиты от вредоносного кода на уровне входного контроля устройств и переносных (отчуждаемых) носителей информации |
|  | Реализация защиты от вредоносного кода на уровне контроля общедоступных объектов доступа (в том числе банкоматов, платежных терминалов) |
|  | Функционирование средств защиты от вредоносного кода в постоянном, автоматическом режиме, в том числе в части установки их обновлений и сигнатурных баз данных |
|  | Функционирование средств защиты от вредоносного кода на СВТ пользователей и эксплуатационного персонала в резидентном режиме (в режиме service - для операционной системы Windows, в режиме daemon - для операционной системы Unix), их автоматический запуск при загрузке операционной системы |
|  | Применение средств защиты от вредоносного кода, реализующих функцию контроля целостности их программных компонентов |
|  | Контроль отключения и своевременного обновления средств защиты от вредоносного кода |
|  | Выполнение еженедельных операций по проведению проверок на отсутствие вредоносного кода |
|  | Использование средств защиты от вредоносного кода различных производителей, как минимум для уровней:* физические СВТ пользователей и эксплуатационного персонала;
* серверное оборудование;
* контроль межсетевого трафика
 |
|  | Выполнение проверок на отсутствие вредоносного кода путем анализа информационных потоков между сегментами контуров безопасности и иными внутренними вычислительными сетями Компании |
|  | Выполнение проверок на отсутствие вредоносного кода путем анализа информационных потоков между внутренними вычислительными сетями Компании и сетью Интернет |
|  | Выполнение проверок на отсутствие вредоносного кода путем анализа информационных потоков между сегментами, предназначенными для размещения общедоступных объектов доступа (в том числе банкоматов, платежных терминалов), и сетью Интернет |
|  | Входной контроль всех устройств и переносных (отчуждаемых) носителей информации (включая мобильные компьютеры и флеш-накопители) перед их использованием в вычислительных сетях Компании |
|  | Входной контроль устройств и переносных (отчуждаемых) носителей информации перед их использованием в вычислительных сетях Компании, в выделенном сегменте вычислительной сети, с исключением возможности информационного взаимодействия указанного сегмента и иных сегментов вычислительных сетей Компании (кроме управляющего информационного взаимодействия по установленным правилам и протоколам) |
|  | Запрет неконтролируемого открытия самораспаковывающихся архивов и исполняемых файлов, полученных из сети Интернет |
|  | Регистрация операций по проведению проверок на отсутствие вредоносного кода |
|  | Регистрация фактов выявления вредоносного кода |
|  | Регистрация неконтролируемого использования технологии мобильного кода, в том числе Java, JavaScript, ActiveX, VBScript и иные аналогичные технологии |
|  | Регистрация сбоев в функционировании средств защиты от вредоносного кода |
|  | Регистрация сбоев в выполнении контроля (проверок) на отсутствие вредоносного кода |
|  | Регистрация отключения средств защиты от вредоносного кода |
|  | Регистрация нарушений целостности программных компонентов средств защиты от вредоносного кода |
|  | Блокирование неразрешенной и контроль (анализ) разрешенной передачи информации конфиденциального характера на внешние адреса электронной почты |
|  | Блокирование неразрешенной и контроль (анализ) разрешенной передачи информации конфиденциального характера в сеть Интернет с использованием информационной инфраструктуры Компании |
|  | Блокирование неразрешенной и контроль (анализ) разрешенной печати информации конфиденциального характера |
|  | Блокирование неразрешенного и контроль (анализ) разрешенного копирования информации конфиденциального характера на переносные (отчуждаемые) носители информации |
|  | Контентный анализ передаваемой информации по протоколам исходящего почтового обмена |
|  | Ведение единого архива электронных сообщений с архивным доступом на срок не менее 6 (Шести) месяцев и оперативным доступом на срок не менее 1 (Одного) месяца |
|  | Ограничение на перечень протоколов сетевого взаимодействия, используемых для осуществления передачи сообщений электронной почты |
|  | Ограничение на перечень форматов файлов данных, разрешенных к передаче в качестве вложений в сообщения электронной почты |
|  | Ограничение на размеры файлов данных, передаваемых в качестве вложений в сообщения электронной почты |
|  | Контентный анализ информации, передаваемой в сеть Интернет с использованием информационной инфраструктуры Компании |
|  | Классификация ресурсов сети Интернет с целью блокировки доступа к сайтам или типам сайтов, запрещенных к использованию в соответствии с установленными правилами |
|  | Ограничение на перечень протоколов сетевого взаимодействия и сетевых портов, используемых при осуществлении взаимодействия с сетью Интернет |
|  | Запрет хранения и обработки информации конфиденциального характера на объектах доступа, размещенных в вычислительных сетях Компании, подключенных к сети Интернет |
|  | Контентный анализ информации, выводимой на печать |
|  | Контентный анализ информации, копируемой на переносные (отчуждаемые) носители информации |
|  | Блокирование неразрешенных к использованию портов ввода-вывода информации СВТ |
|  | Блокирование возможности использования незарегистрированных (неразрешенных к использованию) переносных (отчуждаемых) носителей информации в информационной инфраструктуре Компании |
|  | Стирание информации конфиденциального характера с материальных носителей информации (далее – МНИ) средствами гарантированного стирания или способом (средством), обеспечивающим невозможность их восстановления, при осуществлении вывода МНИ из эксплуатации или вывода из эксплуатации СВТ, в состав которых входят указанные МНИ, а также при необходимости их передачи в сторонние организации |
|  | Стирание информации конфиденциального характера с МНИ средствами гарантированного стирания или способом (средством), обеспечивающим невозможность их восстановления, при передаче (перезакреплении) МНИ между работниками и (или) структурными подразделениями Компании |
|  | Регистрация использования разблокированных портов ввода-вывода информации СВТ |
|  | Регистрация операций, связанных с осуществлением доступа работниками Компании к ресурсам сети Интернет |
|  | Регистрация фактов вывода информации на печать |
|  | Регистрация результатов выполнения контентного анализа информации, предусмотренного мерами 132, 137, 141, 142 настоящей таблицы |
|  | Организация мониторинга данных регистрации о событиях защиты информации, формируемых техническими мерами, входящими в состав системы защиты информации |
|  | Организация мониторинга данных регистрации о событиях защиты информации, формируемых сетевым оборудованием, в том числе активным сетевым оборудованием, маршрутизаторами, коммутаторами |
|  | Организация мониторинга данных регистрации о событиях защиты информации, формируемых сетевыми приложениями и сервисами |
|  | Организация мониторинга данных регистрации о событиях защиты информации, формируемых системным программным обеспечением, операционными системами, СУБД |
|  | Организация мониторинга данных регистрации о событиях защиты информации, формируемых АС и приложениями |
|  | Организация мониторинга данных регистрации о событиях защиты информации, формируемых контроллерами доменов |
|  | Централизованный сбор данных регистрации о событиях защиты информации, формируемых объектами информатизации, определенных мерами 155 и 156 настоящей таблицы |
|  | Генерация временных меток для данных регистрации о событиях защиты информации и синхронизации системного времени объектов информатизации, используемых для формирования, сбора и анализа данных регистрации |
|  | Контроль формирования данных регистрации о событиях защиты информации объектов информатизации, определенных мерами 155 и 156 настоящей таблицы |
|  | Реализация защиты данных регистрации о событиях защиты информации от раскрытия и модификации, двухсторонней аутентификации при передаче данных регистрации с использованием сети Интернет |
|  | Обеспечение гарантированной доставки данных регистрации о событиях защиты информации при их централизованном сборе |
|  | Резервирование необходимого объема памяти для хранения данных регистрации о событиях защиты информации |
|  | Реализация защиты данных регистрации о событиях защиты информации от НСД при их хранении, обеспечение целостности и доступности хранимых данных регистрации |
|  | Обеспечение возможности доступа к данным регистрации о событиях защиты информации в течение трех лет |
|  | Обеспечение возможности выполнения операции нормализации (приведения к единому формату), фильтрации, агрегации и классификации данных регистрации о событиях защиты информации |
|  | Обеспечение возможности выявления и анализа событий защиты информации, потенциально связанных с инцидентами защиты информации, в том числе несанкционированного доступа к информации (далее – НСД) |
|  | Обеспечение возможности определения состава действий и (или) операций конкретного субъекта доступа |
|  | Обеспечение возможности определения состава действий и (или) операций субъектов доступа при осуществлении логического доступа к конкретному ресурсу доступа |
|  | Регистрация нарушений и сбоев в формировании и сборе данных о событиях защиты информации |
|  | Регистрация доступа к хранимым данным о событиях защиты информации |
|  | Регистрация операций, связанных с изменением правил нормализации (приведения к единому формату), фильтрации, агрегации и классификации данных регистрации о событиях защиты информации |
|  | Регистрация информации о событиях защиты информации, потенциально связанных с инцидентами защиты информации, в том числе НСД, выявленными в рамках мониторинга и анализа событий защиты информации |
|  | Регистрация информации, потенциально связанной с инцидентами защиты информации, в том числе НСД, полученной от работников, клиентов и (или) контрагентов Компании |
|  | Установление и применение единых правил регистрации и классификации инцидентов защиты информации в части состава и содержания атрибутов, описывающих инцидент защиты информации, и их возможных значений |
|  | Своевременное (оперативное) оповещение уполномоченных лиц Компании о выявленных инцидентах защиты информации |
|  | Реализация защиты информации об инцидентах защиты информации от НСД, обеспечение целостности и доступности указанной информации |
|  | Разграничение доступа уполномоченных лиц Компании к информации об инцидентах защиты информации в соответствии с определенным распределением ролей, связанных с реагированием на инциденты защиты информации |
|  | Обеспечение возможности доступа к информации об инцидентах защиты информации в течение трех лет |
|  | Регистрация доступа к информации об инцидентах защиты информации |
|  | Разграничение и контроль осуществления одновременного доступа к виртуальным машинам с СВТ пользователей и эксплуатационного персонала только в пределах одного контура безопасности |
|  | Разграничение и контроль осуществления одновременного доступа виртуальных машин к системе хранения данных в пределах контура безопасности |
|  | Идентификация и аутентификация пользователей серверными компонентами виртуализации и (или) средствами централизованных сервисов аутентификации при предоставлении доступа к виртуальным машинам |
|  | Реализация необходимых методов предоставления доступа к виртуальным машинам, обеспечивающих возможность доступа с использованием одних аутентификационных данных только к одной виртуальной машине |
|  | Обеспечение возможности принудительной блокировки (выключения) установленной сессии работы пользователя с виртуальной машиной |
|  | Контроль и протоколирование доступа эксплуатационного персонала к серверным компонентам виртуализации и системе хранения данных с реализацией двухфакторной аутентификации |
|  | Размещение средств защиты информации, используемых для организации контроля и протоколирования доступа эксплуатационного персонала к серверным компонентам виртуализации и системе хранения данных на физических СВТ |
|  | Выделение в вычислительных сетях Компании отдельных сегментов (групп сегментов), в том числе виртуальных, используемых для размещения совокупности виртуальных машин, предназначенных для размещения серверных компонент АС, включенных в разные контуры безопасности |
|  | Межсетевое экранирование сегментов (групп сегментов) вычислительных сетей, определенных мерой 187 настоящей таблицы, включая фильтрацию данных на сетевом и прикладном уровнях семиуровневой стандартной модели взаимодействия открытых систем, определенной в ГОСТ Р ИСО/МЭК 7498-1. |
|  | Реализация и контроль информационного взаимодействия между сегментами (группами сегментов) вычислительных сетей мерами, указанными в пункте 187 настоящей таблицы, в соответствии с установленными правилами и протоколами сетевого взаимодействия |
|  | Исключение возможности информационного взаимодействия и переноса информации между сегментами вычислительных сетей, входящими в разные контуры безопасности, с использованием СВТ пользователей и эксплуатационного персонала, эксплуатируемых для осуществления доступа к виртуальным машинам разных контуров безопасности |
|  | Выделение отдельных логических разделов системы хранения данных для каждого из контуров безопасности |
|  | Регистрация операций, связанных с запуском (остановкой) виртуальных машин |
|  | Регистрация операций, связанных с изменением параметров настроек виртуальных сетевых сегментов, реализованных средствами гипервизора |
|  | Регистрация операций, связанных с созданием и удалением виртуальных машин |
|  | Регистрация операций, связанных с изменением прав логического доступа к серверным компонентам виртуализации |
|  | Регистрация операций, связанных с изменением параметров настроек серверных компонентов виртуализации |
|  | Регистрация операций, связанных с аутентификацией и авторизацией эксплуатационного персонала при осуществлении доступа к серверным компонентам виртуализации |
|  | Регистрация операций, связанных с аутентификацией и авторизацией пользователей при осуществлении доступа к виртуальным машинам |
|  | Регистрация операций, связанных с изменением параметров настроек технических мер защиты информации, используемых для реализации контроля доступа к серверным компонентам виртуализации |
|  | Регистрация операций, связанных с изменением настроек технических мер защиты информации, используемых для обеспечения защиты виртуальных машин |
|  | Аутентификация мобильных (переносных) устройств удаленного доступа |
|  | Предоставление удаленного доступа только с использованием мобильных (переносных) устройств доступа, находящихся под контролем системы централизованного управления и мониторинга (системы Mobile Device Management, MDM) |
|  | Реализация защиты информации от раскрытия и модификации, применение двухсторонней взаимной аутентификации участников информационного обмена при ее передаче при осуществлении удаленного логического доступа |
|  | Идентификация, двухфакторная аутентификация и авторизация субъектов доступа после установления защищенного сетевого взаимодействия, выполнения аутентификации, предусмотренной мерами 201 и 203 настоящей таблицы |
|  | Запрет прямого сетевого взаимодействия мобильных (переносных) устройств доступа и внутренних сетей Компании на уровне выше второго (канальный) по семиуровневой стандартной модели взаимодействия открытых систем, определенной в ГОСТ Р ИСО/МЭК 7498-1 |
|  | Реализация доступа к ресурсам сети Интернет только через информационную инфраструктуру Компании после установления защищенного сетевого взаимодействия, выполнения аутентификации, предусмотренной мерами 201 и 203 настоящей таблицы |
|  | Контентный анализ информации, передаваемой мобильными (переносными) устройствами в сеть Интернет с использованием информационной инфраструктуры Компании |
|  | Реализация и контроль информационного взаимодействия внутренних вычислительных сетей Компании и мобильных (переносных) устройств в соответствии с установленными правилами и протоколами сетевого взаимодействия |
|  | Применение системы централизованного управления и мониторинга (MDM-системы), реализующей:* шифрование и возможность удаленного удаления информации, полученной в результате взаимодействия с информационными ресурсами Компании;
* аутентификацию пользователей на устройстве доступа;
* блокировку устройства по истечении определенного промежутка времени неактивности пользователя, требующую выполнения повторной аутентификации пользователя на устройстве доступа;
* управление обновлениями системного программного обеспечения устройств доступа;
* управление параметрами настроек безопасности системного программного обеспечения устройств доступа;
* управление составом и обновлениями прикладного программного обеспечения;
* невозможность использования мобильного (переносного) устройства в режиме USB-накопителя, а также в режиме отладки;
* управление ключевой информацией, используемой для организации защищенного сетевого взаимодействия;
* возможность определения местонахождения устройства доступа;
* регистрацию смены SIM-карты;
* запрет переноса информации в облачные хранилища данных, расположенные в общедоступных сетях (например, iCloud);
* обеспечение возможности централизованного управления и мониторинга при смене SIM-карты
 |
|  | Обеспечение защиты мобильных (переносных) устройств от воздействий вредоносного кода |
|  | Стирание информации конфиденциального характера с мобильных (переносных) устройств средствами, обеспечивающими полную перезапись данных, при осуществлении вывода мобильных (переносных) устройств из эксплуатации, а также при необходимости их передачи в сторонние организации, между работниками и (или) структурными подразделениями Компании |

# ПОДПИСИ ПРЕДСТАВИТЕЛЕЙ СТОРОН

|  |  |
| --- | --- |
| * **От**
 | * **От Контрагента**
 |
| * <Должность>
 | * <Должность>
 |
| * \_\_\_\_\_\_\_\_\_\_\_\_\_\_ / \_\_\_\_\_(указать ФИО) /
 | * \_\_\_\_\_\_\_\_\_\_\_\_\_\_ / \_\_\_\_\_(указать ФИО) /
 |
| * м.п.
 | * м.п.
 |

Приложение № 3

К Соглашению о конфиденциальности

СОГЛАШЕНИЕ О БЕЗОПАСНОЙ РАЗРАБОТКЕ

|  |  |  |
| --- | --- | --- |
| г. Москва |  | «\_\_\_\_\_» \_\_\_ 20\_\_ г. |

ООО «Газпромстрахование», ИНН хххххххх, далее именуемое «Общество» в лице ˂\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_˃, действующего на основании ˂\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_˃, с одной стороны,
и˂ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_˃, далее именуемое «Компания» в лице ˂\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_˃, действующего на основании ˂\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_˃,
с другой стороны, совместно именуемые «Стороны», заключили настоящее соглашение о безопасной разработке (далее – «Соглашение») о нижеследующем.

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

**Анализ кода (статический анализ, SAST) –** процесспроверки исходного кода программного обеспечения, на предмет наличия уязвимостей кибербезопасности. Производится без реального выполнения исследуемых программ.

**Динамический анализ защищённости приложения (DAST) -** процесс проверки приложения на предмет наличия уязвимостей кибербезопасности в работающем состоянии с учётом программного и аппаратного окружения.

**Кибербезопасность** – состояние защищенности киберпространства (сохранение конфиденциальности, целостности, доступности), в котором функционирует бизнес, достигающееся применением набора средств, методик и принципов, направленных на противодействие угрозам в киберпространстве и минимизацию последствий их реализации.

**Релиз –** фиксированное состояние изменений в программном продукте, связанных с исправлением выявленных ошибок функционирования программных средств (замечаний) или реализацией дополнительных требований Заказчика (предложений), не приводящих к изменению идеологии разработки программного продукта конкретной его версии.

**Релизная ветвь –** финальное для данного релиза состояние разрабатываемого приложения.

**Сервис** – совокупность взаимосогласованных компонентов программного, технического, информационного, организационного, методического, правового обеспечения, используемая пользователями для реализации заданной информационной технологии.

**Уязвимость в программном обеспечении** – недостаток в программном обеспечении, использование которого приводит к некорректной работе сервиса или серьёзным сбоям в его работе.

**RCE** – удаленное выполнение кода.

**SQLi** – SQL Injection (SQL инъекция).

**XXE** – XML Инъекция.

**LFR** – локальное чтение файлов.

**SSRF** (Server-Side Request Forgery) – возможность передавать url, по которому впоследствии перейдет уязвимый сервер.

**Account Takeover** – уязвимость, позволяющая произвести захват аккаунта.

**XSS** – Межсайтовый скриптинг. Тип атаки на веб-системы, заключающийся во внедрении в выдаваемую веб-системой страницу вредоносного кода.

**Blind XSS** – слепая XSS, обычно срабатывает в административных интерфейсах.

**JSONP Hijacking** – кража JSON объектов.

**CORS misconfiguration** – совместное использование ресурсов между разными источниками. Ошибки в предоставлении прав доступа к ресурсам другого домена.

1. ПРЕДМЕТ СОГЛАШЕНИЯ

Предметом данного Соглашения является формирование на базе требований Общества и Компании единых подходов к организации процесса безопасной разработки web-сервисов и программного обеспечения, создаваемых в интересах Общества (далее – безопасная разработка).

1. ТРЕБОВАНИЯ И ОБЯЗАННОСТИ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОЙ РАЗРАБОТКЕ

В целях обеспечения безопасной разработки должно быть обеспечено:

* 1. Документирование сервиса – состав и принцип действия подсистем сервиса должны быть описаны. Количество, состав и степень детализации уточняются на этапе разработки технического задания или отдельными соглашениями между Сторонами.
	2. Разделение информационных сред – среда разработки, тестовая и промышленная информационные среды должны быть физически разнесены друг от друга. Не допускается размещение промышленной и любой другой среды на одном и том же сервере. К тестовой среде применяются такие же требования по защищенности, как и к среде промышленной эксплуатации.
	3. Защищенность исходного кода – должны быть предприняты меры для того, чтобы исходный код сервиса не стал известен третьим лицам.
	4. Использование известных практик по кибербезопасности – при разработке необходимо ориентироваться на известные подходы и практики кибербезопасности.
	5. Управление изменениями: все изменения жизненного цикла (ввод в эксплуатацию, обновления, вывод из эксплуатации и т.д.) в разрабатываемом онлайн-сервисе (коде приложения, его бизнес-логике и т.д.), а также в составе операционной системы, система управления базами данных, web-сервера, должны быть заблаговременно перед вводом в промышленную эксплуатацию согласованы с соответствующими подразделениями Общества (подразделением-заказчиком, прочими участниками процесса разработки), проверены в тестовом сегменте и документированы. Компания должна предпринимать меры для того, чтобы процесс тестирования не приводил к сбою или остановке работы сервиса, находящегося в промышленной эксплуатации. Для этого перевод сервиса в промышленную эксплуатацию производится только после проверки работоспособности сервиса в режиме опытной эксплуатации и устранения замечаний, выявленных во время этого этапа. Для соблюдения баланса между сроками вывода релиза и сроками устранения выявленных замечаний проводится оценка выявленного риска и приоритезация работ по устранению выявленных недостатков.
	6. Удаление данных выводимого из эксплуатации сервиса – при выводе web-сервиса из эксплуатации (окончании периода использования ПО) последняя рабочая версия сервиса (ПО) передается Обществу, а все данные и настройки, связанные с сервисом (ПО), физически удаляются. Также удаляются DNS-имена сервиса с публичных DNS-серверов.
	7. Непрерывность мониторинга, а также регулярность проверок – для сервиса, работающего в режиме промышленной эксплуатации должна быть обеспечена непрерывность мониторинга, а также регулярность проверок работоспособности и соблюдения требований по кибербезопасности.
	8. Наличие резервного копирования – должно быть организовано резервное копирование компонентов сервиса, позволяющее восстановить работоспособность сервиса. Параметры резервного копирования и восстановления уточняются на этапе разработки технического задания или отдельными соглашениями между Обществом и Компанией.
	9. Запрет публикации тестовых версий сервиса и средств разработки в глобальную сеть интернет. Тестовые версии сервисов должны быть доступны исключительно через VPN или аналогичную технологию.
	10. Запрет использования одинаковых паролей для разных сред (среда разработки, тестовая среда, продуктивная среда).
	11. Запрет хранения аутентификационных данных систем и средств разработки в общедоступных базах, в том числе общедоступных в рамках Компании (база знаний, сетевые диски группового доступа и т.д.).Изоляция сред разработки и тестирования проектов Общества на сетевом уровне от любых других проектов.
	12. Зеркалирование исходного кода разрабатываемых приложений в средства хранения исходного кода Общества не реже, чем раз в сутки в автоматическом режиме.
	13. Доступ к средам и средствам разработки должен быть осуществлен исключительно из внутренней локальной сети Компании или с использованием VPN.
	14. Использование обязательной двухфакторной аутентификации в случае использования Компанией стороннего хостинг-провайдера или облачного провайдера для защиты панели управления данного провайдера.
	15. Если Компанией используется облачный провайдер, то необходимо настроить IP whitelist на доступ к его API, включая API S3 и другие, и ресурсы проекта должны быть отделены от ресурсов других проектов (чтобы другие проекты Компании не могли, используя API хостинг-провайдера, получить доступ к проекту).
	16. Компания обязуется определять критичность и устранять выявленные уязвимости в продукте и инфраструктуре согласно таблицам1 и 2.
	17. Компания обязуется брать в работу, сообщать и соблюдать назначенный срок устранения выявленных уязвимостей уровня средний и ниже. Срок устранения не должен превышать 3 месяцев.
	18. Компания обязуется предоставлять все журналы событий, внутренние базы знаний документацию по проектам Общества в течении 5 рабочих дней с даты запроса.
	19. Все обнаруженные Обществом недостатки продукта Компания устраняет за собственный счет.
	20. Компания обязуется проверять исходный код разрабатываемых для Общества продуктов статическими анализаторами кода, проводить динамический анализ кода, проводить компонентный анализ (SCA).
	21. Компания обязуется в течение всего времени поддержки проекта устранять уязвимости в приложении согласно установленным срокам и приоритетам (таблицы 1 и 2).

Таблица 1 – критичность

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Тип уязвимости** | **RCE, пароль по умолчанию** | **SQLi, XXE, LFR** | **SSRF** | **Account Takeover, Blind XSS в административных интерфейсах, раскрытие/изменение данных пользователей, раскрытие конфиденциальных данных сервиса/инфраструктуры** | **XSS (не Self), JSONP Hijacking или CORS misconfiguration с угоном критичных данных** | **Mobile application local account compromise or full data access, Remote DoS against mobile or desktop application** | **Прочие задачи на исправление и предотвращение уязвимостей, в том числе потенциальных** |
| Требуетсяаутентификация | нет | да | нет | да | нет | да | - | - | - | - |
| Приоритет | Critical | High | Critical | High | Critical | High | High/Medium | High/Medium | Medium/Low | Low |

Таблица 2 – сроки устранения

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Приоритет** | **Critical** | **High** | **Medium** | **Low** |
| Сроки внедрения компенсирующих мер достаточных для невозможности эксплуатации | В любое время, в том числе ночью, не более 8 часов | В рабочий день, 1 рабочий день | Frontend – в рабочий день, 1 рабочий день. Backend – не применимо | не применимо |
| Сроки устранения (считаются с окончания сроков внедрения компенсирующих мер) | В рабочий день, 1 рабочий день | В рабочий день, 2 рабочих дня | Frontend – в рабочий день, 3 рабочих дня. Backend – в ближайшем плановом хотфиксе, но не более 2 недель. | В ближайшем плановом релизе/Планово, 2 недели |

1. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ И РАЗРЕШЕНИЕ СПОРОВ
	1. Соглашение вступает в силу с момента его подписания Сторонами и действует по <\_\_\_\_\_\_\_>.
	2. Стороны несут ответственность в соответствии с законодательством Российской Федерации. В случае нарушения Стороной принятых на себя обязательств по Соглашению, такая Сторона обязуется возместить другой Стороне убытки, причиненные таким нарушением. Убытки возмещаются в соответствии с законодательством Российской Федерации.
	3. Компания обеспечивает Обществу возможность осуществлять контроль соблюдения практик безопасной разработки.
	4. Все споры, разногласия и требования, возникающие из Соглашения или в связи с ним, в том числе касающиеся его исполнения, нарушения, прекращения или недействительности, будут разрешаться сторонами претензионным путем. В случае если одна сторона посчитает, что ее право нарушено, она должна направить противной стороне обоснованную претензию.
	5. Сторона, получившая претензию, обязана удовлетворить ее, либо направить мотивированные возражения в срок не более 10 (десяти) рабочих дней с момента получения претензии.
	6. В случае, если претензия одной стороны не удовлетворена и мотивированные возражения не получены, либо они не устраивают сторону, право которой нарушено, споры подлежат разрешению в Арбитражном суде г. Москвы, применимое право – законодательство Российской Федерации.
	7. Внесение изменений в Соглашение осуществляется в письменной форме по взаимному согласию Сторон путем оформления документа, подписываемого уполномоченными представителями Сторон, который является неотъемлемой частью Соглашения.
	8. Соглашение составлено в двух экземплярах, имеющих одинаковую юридическую силу по одному экземпляру для каждой из Сторон.

# ПОДПИСИ ПРЕДСТАВИТЕЛЕЙ СТОРОН

|  |  |
| --- | --- |
| * **От**
 | * **От Контрагента**
 |
| * <Должность>
 | * <Должность>
 |
| * \_\_\_\_\_\_\_\_\_\_\_\_\_\_ / \_\_\_\_\_(указать ФИО) /
 | * \_\_\_\_\_\_\_\_\_\_\_\_\_\_ / \_\_\_\_\_(указать ФИО) /
 |
| * м.п.
 | * м.п.
 |

1. Сумма определяется подразделением владельцем бизнес-процесса, заключающим договор исходя из общей суммы Договора и экспертной оценки значимости подвергшихся риску нанесения ущерба информационных ресурсов. [↑](#footnote-ref-1)
2. В случае, если по условиям Договора разработка web-сервисов и программного обеспечения не предусмотрены, то п. 9.5. из настоящего Соглашения исключается. [↑](#footnote-ref-2)