ВСЕРОССИЙСКИЙ СОЮЗ СТРАХОВЩИКОВ

ВНУТРЕННИЙ СТАНДАРТ

УТВЕРЖДЕН
постановлением Президиума
Всероссийского союза страховщиков
(протокол от 25.12. 2018 № 43)

Обеспечение защиты конфиденциальной информации при осуществлении страховой деятельности

Москва
2018 год

Оглавление

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Введение

1.1.1. Внутренний стандарт «Обеспечение защиты конфиденциальной информации при осуществлении страховой деятельности» (далее – Стандарт) разработан в соответствии с положениями статьи 6 Федерального закона от 13.07.2015 № 223-ФЗ «О саморегулируемых организациях в сфере финансового рынка», иными федеральными законами и определяет требования к мерам по обеспечению защиты конфиденциальной информации при осуществлении страховой деятельности.

1.1.2. Члены Всероссийского союза страховщиков (далее - Союз) при осуществлении страховой деятельности должны обеспечить обязательное выполнение требований Стандарта на всех этапах работы с информацией, подлежащей защите в соответствии с требованиями Стандарта – создание, сбор (получение информации), хранение, обработка, передача, удаление (уничтожение).

1.1.3. Стандарт не рассматривает вопросы защиты государственной тайны.

1.2. Цели Стандарта

Стандарт разработан в целях:

1.2.1. установления обязательных для членов Союза требований по сохранению конфиденциальности информации, полученной страховыми организациями (перестраховочными организациями), организациями и лицами, действующими от имени страховой организации при осуществлении страхования (перестрахования);

1.2.2. соблюдения членами Союза требований законодательства РФ, нормативно правовых актов по защите конфиденциальной информации;

1.2.3. исключения участия работников страховых организаций в разглашении и несанкционированном распространении конфиденциальной информации при осуществлении страховой деятельности;

1.2.4. минимизации угроз международных санкций и угроз применения информационных технологий в целях нанесения ущерба суверенитету, территориальной целостности, политической и социальной стабильности Российской Федерации;

1.2.5. минимизации угроз утраты контроля над конфиденциальной информацией при передаче рисков в перестрахование иностранным партнерам.

1.3. **Термины и определения**

Для целей Стандарта используются следующие термины и определения:

1.3.1. **Конфиденциальная информация** – информация ограниченного доступа, определенная пунктом 3.1 настоящего Стандарта, требующая защиты.

1.3.2. **Страховая организация** – страховые и перестраховочные организации, являющиеся членами Союза.

1.3.3. **Товары двойного назначения** − товары, используемые в общегражданских промышленных целях, но при этом имеющие свойства, которые могут быть использованы при создании вооружения.

1.3.4. **Контрагент** - физическое или юридическое лицо, являющееся стороной в гражданско-правовых отношениях при заключении договора.

1.3.5. **Клиент** – физическое или юридическое лицо, являющееся страхователем, застрахованным лицом или выгодоприобретателем

1.3.6. **Партнер** – физическое или юридическое лицо, являющееся контрагентом страховщика, участвующее в осуществлении страховой деятельности.

1.3.7. Иные термины и определения установлены законодательством Российской Федерации.

2. НОРМАТИВНЫЕ ПРАВОВЫЕ АКТЫ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

Для целей Стандарта выделяются основные нормативные правовые акты в области защиты информации и перечень конфиденциальной информации в страховой деятельности:

- Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи»
- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне»;
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;
- Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера»**;**
- Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»;

- Постановление Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
- ГОСТ Р 57580.1-2017 «Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. ЗАЩИТА ИНФОРМАЦИИ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ. Базовый состав организационных и технических мер»;
- ГОСТ Р 57580.2-2018 «Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. ЗАЩИТА ИНФОРМАЦИИ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ. Методика оценки соответствия».

3. ВИДЫ ИНФОРМАЦИИ

3.1. При осуществлении страховой деятельности в Страховой организации выделяется следующая конфиденциальная информация, защита конфиденциальности которой обеспечивается в рамках Стандарта:

3.1.1. сведения об объектах страхования, обладателями которых являются стратегические предприятия и акционерные общества, определенные Указом Президента Российской Федерации от 04 августа 2004 года № 1009;

3.1.2. сведения об объектах страхования, относящихся к товарам двойного назначения, определенным Указом Президента Российской Федерации от 17 декабря 2011 № 1661;

3.1.3. сведения об имущественных интересах граждан и организаций Российской Федерации, находящихся под действием иностранных санкций;

3.1.4. 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;

3.1.5. сведения об ущербе и происшествиях, которые произошли в отношении имущественных интересов граждан и организаций Российской Федерации, находящихся под действием иностранных санкций.

3.1.6. 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.

3.2. Основанием для принятия информации в качестве конфиденциальной и подлежащей защите в рамках Стандарта является информация в соответствии с п.3.1.3-3.1.6, на которую страхователь в своем заявлении на страхование или по запросу страховой организации прямо указал как на подлежащую защите.

3.3. Виды информации, подлежащей защите в рамках данного Стандарта, в каждой Страховой организации могут быть дополнены.

3.4. Вся конфиденциальная информация в Страховой организации может содержаться на бумажных или электронных носителях, а также в базах данных и иных хранилищах информационных систем Страховой организации или Контрагента по ее поручению.

3.5. Защита конфиденциальности информации, полученной от Контрагентов, Клиентов и Партнеров осуществляется Страховой организацией на основе:

3.5.1. соответствующих положений в договорах и соглашениях с ними;

3.5.2. наличия ограничительных грифов на документах или на электронных носителях;

3.5.3. указаний, содержащихся в электронных сообщениях о конфиденциальном характере содержимого;

3.5.4. анализа содержания в информации сведений, определенных в п.3.1. Стандарта.

4. ВИДЫ УГРОЗ, ВЛИЯЮЩИЕ НА КОНФИДЕНЦИАЛЬНОСТЬ ИНФОРМАЦИИ

4.1. Для оценки влияния угроз безопасности должны быть осуществлены моделирование и базовая оценка угроз безопасности информации (модель угроз). Для оценки угроз рекомендуется пользоваться Банком данных угроз безопасности информации ФСТЭК России (https://bdu.fstec.ru/threat).

4.2. Должна быть определена и оценена совокупность предположений о возможностях нарушителя (модель нарушителя), которые он может использовать для разработки и проведения атак с целью нарушения конфиденциальности информации или создания условий для этого. Модель нарушителя предназначена для определения необходимого класса средств криптографической защиты информации.

5. МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

В целях обеспечения конфиденциальности информации, подлежащей защите в соответствии с требованиями Стандарта, при осуществлении страховой деятельности Страховой организацией должен быть обеспечен комплекс организационных и технических мер информационной безопасности в соответствии с положениями закона от 29 июля 2004 года № 98-ФЗ «О коммерческой тайне» с учетом ГОСТ Р 57580.1 2017 «Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций».

5.1. **Организационные меры**

В качестве организационных мер в отношении конфиденциальной информации необходимо ввести режим защиты коммерческой тайны, в том числе осуществить следующие мероприятия:

5.1.1. включить в Перечень сведений, составляющих коммерческую тайну Страховой организации (или аналогичный документ) виды информации, определенные в п.3.1 Стандарта;

5.1.2. урегулировать внутренними нормативными документами вопросы охраны конфиденциальности информации и соответствующие меры информационной безопасности при осуществлении страховой деятельности;

5.1.3. в обязательном порядке ознакомить всех работников Страховой организации с вышеуказанными документами;

5.1.4. обязать Контрагентов в договорных отношениях и соглашениях обеспечивать режим конфиденциальности в отношении информации, определенной п. 3.1.

5.2. **Обмен конфиденциальной информацией**

5.2.1. Передача конфиденциальной информации может быть произведена на бумажном носителе, электронном носителе информации (USB-накопитель, CD/DVD-диск, SD-карта и т.п.) или в электронном виде по каналам связи (в т.ч. по сети Интернет) с применением средств защиты.

5.2.2. Передаваемые документы и носители маркируются соответствующим грифом, определенным внутренним положением организации (например: «Коммерческая тайна», «Конфиденциально»), с указанием обладателя информации.

5.2.3. Передача документов в бумажном или электронном носителе осуществляется с сопроводительным письмом, содержащим уведомление о конфиденциальном характере документов, в заклеенных и опечатанных непрозрачных конвертах, с нанесенными грифами и указанием полного наименования и адреса организации-отправителя.

5.2.4. Передача документов с конфиденциальной информацией в электронном виде по каналам связи (в т.ч. по сети Интернет) возможна с использованием информационных систем (электронного документооборота, корпоративной электронной почты, личных кабинетов и т.п.) с применением средств защиты конфиденциальной информации в системах и каналов связи. Карточка документа или электронное сообщение должны содержать уведомление о конфиденциальном характере содержимого с указанием ограничительного грифа.

5.2.5. Полученные документы учитываются и обрабатываются в соответствии с установленными в отношении конфиденциальной информации правилами.

5.2.6. Передача конфиденциальной информации в открытом виде без применения средств защиты информационных систем, каналов связи или с использованием общедоступных ресурсов сети Интернет (общедоступная электронная почта, облачные хранилища, социальные сети, файлообменные сети и т.п.) запрещена.

5.3. **Технические меры**

Технические меры включают построение системы защиты информации на основе разработанных в Страховой организации перечня сведений и моделей угроз и нарушителя. Создание, техническую поддержку и сопровождение Системы защиты информации рекомендуется осуществлять силами подрядных организаций, имеющих лицензию ФСТЭК на деятельность по технической защите конфиденциальной информации

6. КОНТРОЛЬ ЗА СОБЛЮДЕНИЕМ ТРЕБОВАНИЙ СТАНДАРТА

6.1. Контроль соблюдения требований Стандарта в Страховой организации осуществляется подразделениями (работниками) на которых возложены функции внутреннего контроля или иными подразделениями (работниками), уполномоченными работодателем осуществлять указанные функции.

6.2. Союз осуществляет контроль за соблюдением требований Стандарта:

6.2.1. В связи с поступившим в Союз сообщением о разглашении конфиденциальной информации в отношении членов Союза.

6.2.2. В соответствии с внутренним стандартом Союза «Порядок проведения проверок соблюдения членами Всероссийского союза страховщиков требований законодательства Российской Федерации, нормативных

актов Банка России, базовых стандартов, внутренних стандартов и иных внутренних документов Всероссийского союза страховщиков».

7. ОТВЕТСТВЕННОСТЬ ЗА НЕСОБЛЮДЕНИЕ ТРЕБОВАНИЙ СТАНДАРТА

Ответственность за несоблюдение требований Стандарта предусматривается в соответствии с действующим законодательством Российской Федерации и внутренним стандартом Союза «Система мер воздействия и порядком их применения за несоблюдение членами Всероссийского союза страховщиков требований базовых стандартов, внутренних стандартов и иных внутренних документов Всероссийского союза страховщиков»

8. ВСТУПЛЕНИЕ СТАНДАРТА В СИЛУ

8.1. Стандарт вступает в силу по истечении 10 календарных дней со дня его утверждения Президиумом Союза.

8.2. Страховые организации обязаны в течение 270 календарных дней со дня вступления в силу Стандарта привести свою деятельность в соответствие со Стандартом.

9. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

9.1. Изменения в Стандарт разрабатываются Союзом.

9.2. Изменения и дополнения в Стандарт вступают в силу по истечении 10 календарных дней со дня их утверждения Президиумом Союза.