УТВЕРЖДЕНО
Приказом генерального директора
№ ПД-1 от 20.06.2019 года

Положение об обработке и обеспечению безопасности персональных данных в Ассоциации «Строители Омска»

I. Общие положения.

1. Безопасность персональных данных при их обработке в информационной системе обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы, определенные в соответствии с частью 5 статьи 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

2. Система защиты персональных данных включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

3. Ассоциация «Строители Омска» (далее – Ассоциация, Оператор) обеспечивает безопасность персональных данных при их обработке в информационной системе.

4. Выбор средств защиты информации для системы защиты персональных данных осуществлён в соответствии с нормативными правовыми актами, принятыми Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю во исполнение части 4 статьи 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

5. Обработка персональных данных осуществляется в порядке, определённом политикой Ассоциации «Строители Омска» в отношении обработки персональных данных, утверждённой генеральным директором Ассоциации «Строители Омска» 22.12.2017 года, а в части неурегулированной Политикой – настоящим Положением.

II. Определение типа угроз и необходимого уровня защищённости персональных данных.

Информационная система является информационной системой персональных данных субъектов персональных данных, не являющихся сотрудниками Оператора.

1. Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

2. Определение типа угроз безопасности персональных данных, актуальных для информационной системы, произведено с учетом оценки возможного вреда, проведенной во исполнение пункта 5 части 1 статьи 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», и в соответствии с нормативными правовыми актами, принятыми во исполнение части 5 статьи 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»:

- разряд персональных данных, обрабатываемых в информационной системе Ассоциации – иные;
- количество персональных данных – менее 100 000;
- для информационной системы актуальны угрозы, несвязанные с недокументированными (недекларированными) возможностями в системном и прикладном программном обеспечении;
- строение информационной системы – локальное;
- подключения информационной системы к сетям публичного применения – отсутствует;
- режим обработки персональных данных – с наличием границ доступа;
- при обработке персональных данных в информационных системах установлен 4 уровень защищенности персональных данных;
- необходимость обеспечения 4-го уровня защищенности персональных данных при их обработке в информационной системе установлена по наличию следующего условия: для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных сотрудников Оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

3. Для обеспечения 4-го уровня защищенности персональных данных при их обработке в информационных системах выполняются следующие требования:

- организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;
- обеспечение сохранности носителей персональных данных;
- утверждение руководителем Оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;
- использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

4. Контроль за выполнением настоящего Положения организуется и проводится Ассоциацией самостоятельно и

(или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанный контроль проводится не реже 1 раза в 3 года в сроки, определяемые Ассоциацией.

III. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации.

1. Организация режима обеспечения безопасности помещений, в которых размещена информационная система персональных данных препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения.

1.1 Помещения оборудованы входными дверьми с замками в количестве – 3 двери, обеспечено постоянное закрытие 1 двери помещений на замок и их открытия только для санкционированного прохода, а также оборудование помещений техническими устройствами, сигнализирующими о несанкционированном вскрытии помещений.

1.2 Утверждены правила доступа в помещения в рабочее и нерабочее время, а также в нештатных ситуациях.

2.3. Утверждён переченьлиц, имеющих право доступа в Помещения.

2. Обеспечение сохранности носителей персональных данных.

2.1. Хранение съемных машинных носителей персональных данных осуществляется в сейфах (металлических шкафах), оборудованных внутренними замками с двумя дубликатами ключей и приспособлениями для опечатывания замочных скважин. В случае если на съемном машинном носителе персональных данных хранятся только персональные данные в зашифрованном с использованием СКЗИ виде, хранение таких носителей осуществляется вне сейфов (металлических шкафов).

2.2. Осуществление поэкземплярного учет машинных носителей персональных данных, путем ведения журнала учета машинных носителей персональных данных с использованием регистрационных (заводских) номеров.

3. Утверждение руководителем Оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей и назначение должностного лица (работника), ответственного за обеспечение безопасности персональных данных в информационной системе.

3.1. Разработан и утверждён документ, определяющий перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

3.2. Поддержание в актуальном состоянии документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей, достигается контролем и внесением в него изменений по мере внесения изменений в должностные обязанности и при приёме на работу, увольнении с работы, переводах и прочих кадровых изменениях.

3.3. Назначено обладающее достаточными навыками лицо (работник), ответственное за обеспечение безопасности персональных данных в информационной системе (для третьего уровня).

4. Использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз(подлежит применению после принятия Технического регламента процедуры оценки соответствия, в порядке Федерального закона от 27.12.2002 № 184-ФЗ (ред. от 28.11.2018) «О техническом регулировании»).

4.1. Получение исходных данных для формирования совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак;

4.2. Формирование и утверждение руководителем Оператора совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак, и определение на этой основе и с учетом типа актуальных угроз требуемого класса СКЗИ;

4.3. Использование для обеспечения требуемого уровня защищенности персональных данных при их обработке в информационной системе СКЗИ класса КС1 и выше.

IV. Состав и содержание мер по обеспечению безопасности персональных данных.

1. В состав мер по обеспечению безопасности персональных данных, реализуемых Ассоциацией в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят:

- идентификация и аутентификация субъектов доступа и объектов доступа, которыми обеспечено присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности);
- управление доступом субъектов доступа к объектам доступа, которыми обеспечено управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа (должностных обязанностей), а также обеспечение контроля за соблюдением этих правил;
- защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных данных), которыми исключена возможность несанкционированного

доступа к машинным носителям и хранящимся на них персональным данным, а также несанкционированное использование съемных машинных носителей персональных данных;

– регистрация событий безопасности, которой обеспечены сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них;

– антивирусная защита, которой обеспечено обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации;

– контроль (анализ) защищенности персональных данных, которыми обеспечены контроль уровня защищенности персональных данных, обрабатываемых в информационной системе, путем проведения систематических мероприятий по анализу защищенности информационной системы и тестированию работоспособности системы защиты персональных данных.

– защита среды виртуализации, которой исключен несанкционированный доступ к персональным данным, обрабатываемым в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры и (или) воздействию на них, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям;

– защита технических средств, которой исключен несанкционированный доступ к стационарным техническим средствам, обрабатывающим персональные данные, средствам, обеспечивающим функционирование информационной системы (далее - средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту персональных данных, представленных в виде информативных электрических сигналов и физических полей;

– защита информационной системы, ее средств, систем связи и передачи данных, которой обеспечено защита персональных данных при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы и проектных решений, направленных на обеспечение безопасности персональных данных.

2. Выбор мер по обеспечению безопасности персональных данных, подлежащих реализации в информационной системе в рамках системы защиты персональных данных, определён базовым набором мер по обеспечению безопасности персональных данных для установленного четвёртого уровня защищенности персональных данных в соответствии Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Базовый набор мер адаптирован с учетом структурно-функциональных характеристик информационной системы, информационных технологий, особенностей функционирования информационной системы (в том числе исключение из базового набора мер, непосредственно связанных с информационными технологиями, не используемыми в информационной системе, или структурно-функциональными характеристиками, не свойственными информационной системе) Ассоциации;

3. При невозможности технической реализации отдельных выбранных мер по обеспечению безопасности персональных данных, а также с учетом экономической целесообразности на этапах адаптации базового набора мер и (или) уточнения адаптированного базового набора мер могут разрабатываться иные (компенсирующие) меры, направленные на нейтрализацию актуальных угроз безопасности персональных данных.

В этом случае в ходе разработки системы защиты персональных данных должно быть проведено обоснование применения компенсирующих мер для обеспечения безопасности персональных данных.

V. Состав и содержание мер по обеспечению безопасности персональных данных.

1. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ).

ИАФ.1 Идентификация и аутентификация пользователей, являющихся работниками Оператора.

ИАФ.3 Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов.

ИАФ.4 Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации.

ИАФ.5 Защита обратной связи при вводе аутентификационной информации.

ИАФ.6 Идентификация и аутентификация пользователей, не являющихся работниками Оператора (внешних пользователей).

2. Управление доступом субъектов доступа к объектам доступа (УПД).

УПД.1 Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей.

УПД.2 Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа.

УПД.3 Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами.

УПД.4 Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы.
УПД.5 Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы.
УПД.6 Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе).
УПД.10 Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу.
УПД.13 Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети + +
УПД.14 Регламентация и контроль использования в информационной системе технологий беспроводного доступа.
УПД.15 Регламентация и контроль использования в информационной системе мобильных технических средств.
УПД.16 Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы).

3. Защита машинных носителей персональных данных (ЗНИ).

ЗНИ.8 Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания.

4. Регистрация событий безопасности (РСБ).

РСБ.1 Определение событий безопасности, подлежащих регистрации, и сроков их хранения.
РСБ.2 Определение состава и содержания информации о событиях безопасности, подлежащих регистрации.
РСБ.3 Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения.
РСБ.7 Защита информации о событиях безопасности + +

5. Антивирусная защита (АВЗ).

АВЗ.1 Реализация антивирусной защиты.
АВЗ.2 Обновление базы данных признаков вредоносных компьютерных программ (вирусов).

6. Контроль (анализ) защищенности персональных данных (АНЗ).

АНЗ.2 Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации.
АНЗ.3 Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации.
АНЗ.4 Контроль состава технических средств, программного обеспечения и средств защиты информации.

7. Защита среды виртуализации (ЗСВ).

ЗСВ.1 Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации.
ЗСВ.2 Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин.

8. Защита технических средств (ЗТС).

ЗТС.3 Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены.
ЗТС.4 Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр.