Экспертное заключение
по анализу законодательства на предмет необходимости получения саморегулируемыми организациями – операторами реестра НРС аттестата соответствия автоматизированных рабочих мест, с которых осуществляется доступ в АИС «НРС»

Федорченко Максим Владиславович

Руководитель рабочей группы Экспертного совета

координатор НОСТРОЙ по Сибирскому федеральному округу,
руководитель Совета Ассоциации строительных организаций Новосибирской области (АСОНО),
президент Союза строителей Новосибирской области

При проведении правовой экспертизы проанализированы:

- Приказ ФСТЭК РФ от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»
- Приказ Минстроя России от 06.04.2017 № 688/пр «О порядке ведения национального реестра специалистов в области инженерных изысканий и архитектурно-строительного проектирования, национального реестра специалистов в области строительства, включения в такие реестры сведений о физических лицах и исключения таких сведений, внесения изменений в сведения о физических лицах, включенные в такие реестры, а также о перечне направлений подготовки, специальностей в области строительства, получение высшего образования по которым необходимо для специалистов по организации инженерных изысканий, специалистов по организации архитектурно-строительного проектирования, специалистов по организации строительства»
- Положение по аттестации объектов информатизации по требованиям безопасности информации (утв. председателем Государственной технической комиссии при Президенте РФ от 25.11.1994 г.)
- Информационное сообщение ФСТЭК России от 15 июля 2013 №240/22/2637, иные письма Роскомнадзора, ФСТЭК России
- Устав Ассоциации «Национальное объединение строителей»
- Регламент о порядке ведения национального реестра специалистов в области строительства, включения в него сведений о физических лицах, их изменения или исключения
- судебная практика по вопросам, рассмотренным в рамках подготовки экспертного заключения.

При проведении правовой экспертизы проанализированы:

- Гражданский кодекс РФ
- Градостроительный кодекс РФ

Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»
- Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
- Постановление Правительства Российской Федерации от 06.07.2015 № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации»
- 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»
- Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»

Состав рабочей группы:

Федорченко М.В. (руководитель рабочей группы), Денискин Н.Н., Дубинина Н.А., Кузьма И.Е., Макаров П.В., Максимов А.В., Малахов П.В., Разумова Н.М., Ребрищев И.Н., Худзинская А.И., Шериева А.М.

К работе над заключением привлекались эксперты:

Каширин А.П.	Директор Департамента решений в сфере жилищно-коммунального хозяйства Департамента информационных технологий города Москвы
Мокринский Д.А.	Ведущий администратор информационной безопасности Отдела информационной безопасности Департамента решений в сфере жилищно-коммунального хозяйства Департамента информационных технологий города Москвы
Елисеев С.Е.	Директор департамент национального реестра специалистов и развития профессиональных квалификаций НОСТРОЙ
Карпов В.А.	Заместитель исполнительного директора НОСТРОЙ, директор департамент информационных технологий и анализа данных
Панарина В.В.	Директор правового департамента НОСТРОЙ

Анализ правового статуса АИС «НРС» и необходимости проведении аттестации АИС «НРС»

Информационные системы, подлежащие обязательной аттестации:

государственные информационные системы
(пункт 17 Приказа ФСТЭК РФ от 11.02.2013 № 17)

с информацией о гос. тайне, об управлении экологически опасными объектами, для ведения секретных переговоров (п.1.5 Положения по аттестации объектов информатизации по требованиям безопасности информации (утв. Государственной технической комиссией при Президенте РФ от 25.11.1994).

В остальных случаях аттестация информационной системы носит добровольный характер

Признаки государственной информационной системы:

- созданы в целях реализации полномочий гос. органов и обеспечения обмена ими информацией (ч.1 ст.14 ФЗ № 149-ФЗ);
- создаются с учетом требований законодательства о контрактной системе для обеспечения государственных и муниципальных нужд (ч.2 ст.14 ФЗ № 149-ФЗ);
- основанием созданием является обязанность органа исполнительной власти по созданию системы, для реализации полномочий органа исполнительной власти, для реализации проекта ГЧП и др.

АИС «НРС» не отвечает признакам государственной информационной системы => не является государственной информационной системой

Требования к негосударственным информационным системам

При работе с персональными данными оператор должен:

- соблюдать организационные и технические меры защиты персональных данных;

- проводить оценку эффективности и контроль выполнения требований по защите персональных данных 1 раз в 3 года;

- оценка эффективности и контроль проводится оператором самостоятельно и (или) с привлечением по договору организации, имеющей лицензию;

- законодательных требований к форме оценки эффективности и контроля не установлено

Информационное сообщение ФСТЭК России от 15.07.2013 №240/22/2637:

- в отношении негосударственных информационных систем собственник системы сам принимает решение о форме оценки эффективности защиты персональных данных

- в случае добровольной аттестации негосударственной информационной системы оценка эффективности может быть проведена в рамках работ по аттестации

Оценка эффективности принимаемых мер по обеспечению безопасности персональных данных в виде аттестационных испытаний АИС «НРС» осуществлена НОСТРОЙ на добровольной основе

Анализ взаимоотношений НОСТРОЙ и СРО - Операторов НРС

Регламент НОСТРОЙ о порядке ведения национального реестра специалистов

СРО – Оператор НРС выполняет функции:

- прием заявлений и документов от физических лиц о включении в НРС;
- первичная проверка предоставленных документов;
- внесение сведений из документов в АИС «НРС» и их передача на рассмотрение в НОСТРОЙ;
- выдача физическому лицу расписки в получении документов Оператором НРС.

Полномочия Оператора НРС предоставляются СРО на основании поданных ими заявлений

Таким образом, Регламент НРС основывает передачу полномочий Оператора НРС наличием корпоративных (членских) отношений между НОСТРОЙ и СРО.

Корпоративные права и обязанности члена ассоциации определены положениями ст. 123.11, ст. 65.2 ГК РФ и не содержат положений, которые позволяют возложить на члена ассоциации выполнение обязанностей Оператора НРС.

Ранее в 2017 году использовались агентские договоры, которые сейчас не исполняются.

Положения законодательства:

- обязанность по ведению НРС в области строительства осуществляется НОСТРОЙ *(ч.10 ст.55.5-1 ГрК РФ)*
- приказ Минстроя России от *06.04.2017 г. № 688/пр* не предусматривает первичный прием документов для включения в НРС саморегулируемыми организациями
- полномочия на совершении сделки основываются на доверенности, указании закона либо акте государственного органа или органа МСУ *(п.1 ст.182 ГК РФ).*
- в качестве оснований возникновения гражданских прав и обязанностей предусмотрены договоры и иные сделки *(пп.1 п.1 статьи 8 ГК РФ)*
- оператор персональных данных вправе поручить обработку персональных данных другому лицу на основании договора *(ч.3 ст.6 ФЗ «О персональных данных»)*
- обработка персональных данных о судимости может осуществляться только на основании указания закона *(ч.3 ст.10 Федерального закона «О персональных данных»)*, без соответствующего полномочия от НОСТРОЙ Операторы НРС не имеют права обработки данных о судимости
- Оператор НРС выдает заявителю от СРО расписку в получении документов, при этом данная расписка не влечет для НОСТРОЙ обязательств перед заявителями, т.к у Оператора НРС нет полномочий.

При анализе были выявлены следующие проблемы взаимодействия Операторов НРС с НОСТРОЙ:

1) Приказ № 688/пр и Регламент НРС устанавливают, что документы могут быть поданы заявителем в электронном виде.

Существует неопределенность является ли процедура подачи документов через Оператора НРС подачей заявителем документов в электронном виде, поскольку иного порядка подачи документов в электронном виде не предусмотрено.

2) Приказом № 688/пр и Регламентом НРС установлено, что при нарушении требований к форме заявления или форме, составу приложенных документов НОСТРОЙ возвращает документы в течение 5 рабочих дней со дня их поступления. Однако, установленная Регламентом НРС процедура не позволяет уложиться в пятидневный срок:

- Оператор НРС отправляет в НОСТРОЙ заявление и документы на бумажном носителе в течение 7 рабочих дней;
- формальная экспертиза (5 рабочих дней), по результатам которой готовится заключение;
- не сформирована практика принятия решений о возврате документов заявителю.
- в Регламенте НРС **отсутствует** возможность возврата заявителю документов непосредственно Оператором НРС, если документы были поданы через Оператора.

3) Существуют несоответствия формулировок пунктов 11.1 и 11.4 Регламента НРС, что при формальном толковании допускает проведение углубленной проверки заявлений и приложенных документов до включения сведений о заявителе в НРС.

Углубленная проверка осуществляется, в частности, в отношении поступивших в НОСТРОЙ оригиналов документов на предмет наличия внешних признаков поддельности (п.11.3 Регламента НРС). При этом Регламент НРС не содержит определения понятия «внешние признаки поддельности», не определяет алгоритм действий при наличии признаков поддельности и последствия их обнаружения

Требование к аттестации автоматизированных рабочих мест Операторов НРС:

- Оператор НРС реализует свои полномочия с использованием АИС «НРС», имеет доступ в АИС «НРС»
- Законодательство не содержит требований к аттестации автоматизированных рабочих мест для работы с АИС «НРС»
- НОСТРОЙ является собственником и оператором АИС «НРС», поэтому НОСТРОЙ несет обязанность по защите информации и принимает необходимые меры к защите информации в АИС «НРС»
- НОСТРОЙ как собственник АИС «НРС», вправе самостоятельно предъявить требования об аттестации автоматизированных рабочих мест, с которых осуществляется доступ в АИС «НРС»

Экспертный совет обратился в НКК для определение правовой основы деятельности СРО – Операторов НРС по получению от заявителей документов и передаче их в НОСТРОЙ для включения в НРС в форме договора (доверенности), установления требований к обработке Операторами НРС персональных данных в рамках договора или доверенности, формирования предложений для внесения изменений в Регламент НРС.

Возможность передачи персональных данных Операторами НРС за контуром АИС «НРС»

Если передача персональных данных в НОСТРОЙ будет осуществляется Операторами НРС **без доступа в АИС «НРС»**, то НОСТРОЙ как собственник АИС «НРС» не сможет предъявлять требования к аттестации, при этом устраняются риски информационной угрозы безопасности персональных данных для АИС «НРС».

В этом случае Оператор НРС тоже обрабатывает персональные данные (ПД) обратившихся к нему заявителей и должен принимать установленные законом меры:

правовые меры:	формирование политики обработки ПД, размещение ее на сайте, назначение ответственного лица и др.;
организационные меры:	организация режима обеспечения безопасности помещений, сохранности носителей ПД и др.;
технические меры:	установка антивирусной защиты и др.
меры контроля:	самостоятельная оценка эффективности и контроль принимаемых мер.

Административная ответственность за нарушение требований к защите персональных данных Оператором НРС в случае работы без доступа в АИС «НРС» будет возлагаться на Оператора НРС.

В целях обеспечения защищенности АИС «НРС» и сохранения СРО статуса Оператора НРС оптимально рассмотреть техническую возможность передачи персональных данных в электронном виде без доступа в АИС «НРС».

Экспертный совет обратился в НКК с поручением анализа правового механизма работы за контуром АИС «НРС», мер по защите персональных данных, ответственности НОСТРОЙ, необходимости использования криптографических средств защиты персональных данных.