## Новое в регулировании

# Принят закон «О безопасности критической информационной инфраструктуры РФ»

С 1 января 2018 года вступает в силу Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (далее - Закон).

Закон принят в целях обеспечения компьютерной безопасности критической информационной инфраструктуры Российской Федерации. Понятие критической информационной инфраструктуры (далее - КИИ) сформулировано в Законе широко и включает как объекты КИИ (информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления производственными процессами, функционирующие в таких жизненно важных сферах, как здравоохранение, наука, транспорт, связь, энергетика, банковская сфера (и иные сферы финансового рынка), топливно-энергетический комплекс, атомная энергетика, оборонная, ракетно-космическая, горно-добывающая, металлургическая, химическая промышленность), а также сети электросвязи, используемые для организации взаимодействия объектов КИИ.

Отметим, что Закон содержит лишь рамочное регулирование, и ожидается, что его положения будут развиты в подзаконных актах, основной массив которых планируется принять в 2017-2018 году. Тем не менее содержание Закона позволяет уже сейчас определить круг обязанностей, которые будут возложены на владельцев объектов КИИ, к числу которых отнесены как государственные органы и учреждения, так и российские юридические лица, индивидуальные предприниматели, которым на праве собственности, аренды или ином законном основании принадлежат объекты КИИ.

**Владельцы объектов КИИ будут обязаны осуществлять категорирование объектов КИИ и обеспечивать безопасность таких объектов**

Категорирование предполагает присвоение объекту КИИ одной из трех категорий значимости. Обращаем внимание на то, что владельцы

Настоящее Информационное сообщение (Legal Alert) содержит сведения о принятых изменениях в законодательстве РФ, имеющих отношение к Вашей компании, предоставляющих права или закрепляющих определенные обязанности, а также влияющих на осуществление деятельности компании.

Если у вас возникли вопросы в отношении этого сообщения, пожалуйста, свяжитесь:

**Екатерина Смирнова**
Руководитель практики по интеллектуальной собственности / информационным технологиям
**моб. тел.**: +7(911) 097-74-73
**тел.**: +7(812) 602-02-25
ekaterina.smirnova@kachkin.ru

объектов КИИ обязаны самостоятельно проводить категорирование своих объектов и информировать государственный орган, уполномоченный в области обеспечения безопасности КИИ* о присвоенной категории. Этот орган будет вести реестр значимых объектов КИИ и следить за соблюдением порядка категорирования. Если владелец объекта КИИ придет к выводу о том, что находящийся в его владении объект не подпадает ни под одну из категорий значимости (не является значимым), он должен уведомить об этом орган.

От категории значимости будет зависеть объем предъявляемых к владельцу требований по обеспечению безопасности объектов КИИ. Обязательные требования к обеспечению безопасности значимых объектов КИИ установит государственный орган, уполномоченный в области обеспечения безопасности КИИ.

В этой связи Закон способен оказать влияние на требования к контрагентам в договорных отношениях. Если договоры заключаются по итогам проведения закупочных процедур** либо с использованием механизмов государственно-частного партнерства***, могут появиться дополнительные требования к участникам закупки, концессионерам, частным партнерам в части соблюдения требований к обеспечению безопасности значимых объектов КИИ. Необходимость соблюдения требований Закона может повлиять и на размер операционных расходов, которые должен будет понести владелец таких объектов.

Не будет лишним отметить, что сведения о мерах по обеспечению безопасности КИИ и о состоянии ее защищенности от компьютерных атак с 1 января 2018 года отнесены к государственной тайне****. Так что, владельцам значимых объектов КИИ будет необходимо обеспечить неразглашение таких сведений и наличие соответствующих допусков.

**Владельцы объектов КИИ будут обязаны взаимодействовать с ФСБ и государственным органом, уполномоченным в области обеспечения безопасности КИИ**

Владельцы объектов КИИ обязаны информировать о компьютерных инцидентах и оказывать содействие сотрудникам ФСБ в предупреждении, обнаружении и ликвидации последствий компьютерных атак, установлении причин и условий возникновения компьютерных инцидентов.

Владельцы значимых объектов КИИ наряду с этим будут обязаны реагировать на компьютерные инциденты в порядке, установленном ФСБ, обеспечить беспрепятственный доступ сотрудников государственного органа, уполномоченного в области обеспечения безопасности КИИ, к значимым объектам КИИ при осуществлении плановых и внеплановых проверок, принимать меры по ликвидации последствий компьютерных атак и выполнять предписания о нарушении требований к безопасности значимых объектов КИИ.

---

* Орган будет назначен Указом Президента РФ в течение полугода с даты принятия Закона.

** В том числе, в порядке, который установлен ГК РФ, Федеральным законом от 18.07.2011 № 223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц», Федеральным законом от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд», Федеральным законом от 26.07.2006 № 135-ФЗ «О защите конкуренции».

*** В том числе, в порядке, установленном Федеральным законом от 21.07.2005 № 115-ФЗ «О концессионных соглашениях», Федеральным законом от 13.07.2015 № 224-ФЗ «О государственно-частном партнерстве, муниципально-частном партнерстве в Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации».

**** Федеральный закон от 26.07.2017 № 193-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации».

Проверки соблюдения Закона и принятых в соответствии с ним подзаконных нормативных актов предусмотрены только в отношении значимых объектов КИИ. Плановые проверки будут проводиться с периодичностью один раз в три года.

Важно отметить, что проведение проверок изъято из-под действия Федерального закона № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля». Соответствующие изменения уже внесены в этот закон и вступят в силу 1 января 2018 года*.

**Нарушение Закона и принятых в его исполнение подзаконных актов может повлечь уголовную ответственность**

В связи с принятием Закона с 1 января 2018 года начнут действовать новые составы преступлений (ст. 274.1 Уголовного кодекса)**.

Повлекшее причинение вреда КИИ нарушение правил эксплуатации средств, предназначенных для работы с охраняемой и формацией, содержащейся в КИИ, информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, сетей электросвязи, относящихся к КИИ, либо правил доступа к ним может обернуться лишением свободы на срок до 6 лет.

Хотя подзаконные акты, которые конкретизируют, что именно считать объектом КИИ, определят критерии отнесения объектов КИИ к значимым и опишут конкретные мероприятия по реализации Закона, еще не приняты, государственным и частным структурам, которые с большой вероятностью будут охвачены действием Закона, уже сейчас рекомендуется провести аудит собственных систем компьютерной безопасности, убедиться в наличии достаточного количества квалифицированных специалистов в области информационной защиты, а также рассмотреть возможности по созданию и усилению системы компьютерной безопасности объектов КИИ.



---

* Федеральный закон от 26.07.2017 № 193-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации».

** Федеральный закон от 26.07.2017 № 194-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации».