Закон о безопасности критической информационной инфраструктуры: новый вызов для игроков на рынках здравоохранения, телекоммуникаций, финансов, банковских услуг, транспорта и в других сферах

26 июля 2017 года

Уважаемые Дамы и Господа,

Информируем вас о предстоящих изменениях российского законодательства в области информационной безопасности. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» был принят Государственной Думой в трех чтениях и затем одобрен Советом Федерации. Ожидается, что в ближайшее время он будет подписан Президентом. Закон среди прочего вводит определение критической информационной инфраструктуры («**КИИ**»), обозначает ключевые индустрии, в которых задействована КИИ, устанавливает обязанности владельцев объектов КИИ, а также полномочия компетентных государственных органов в данной сфере.

В случае подписания Президентом закон вступит в силу 1 января 2018 года.

Каким компаниям следует обратить внимание на закон?

Закон регулирует деятельность государственных органов, российских юридических лиц и индивидуальных предпринимателей, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления («**Объекты КИИ**»), функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, а также в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности («**Субъекты КИИ**»). Закон также применим к российским юридическим лицам и индивидуальным предпринимателям, обеспечивающим взаимодействие указанных систем или сетей.

Государственный реестр значимых объектов КИИ

Законом предусмотрено присвоение категорий (одной из трех) Объектам КИИ в зависимости от их социальной, экономической, политической, экологической значимости, а также их важности для обеспечения обороны страны, безопасности государства и правопорядка.

Решение о присвоении категории или об отсутствии необходимости ее присвоения должно быть принято Субъектом КИИ самостоятельно. Далее принятое решение необходимо сообщить уполномоченному государственному органу, который вправе либо одобрить, либо оспорить такое решение.

В случае одобрения присвоенной Объекту КИИ категории, объект рассматривается в качестве значимого Объекта КИИ, и информация о нем вносится в реестр значимых объектов КИИ.

Обязанности Субъектов КИИ

На Субъектов КИИ возложены следующие ключевые обязанности:

- Незамедлительно информировать уполномоченные государственные органы о компьютерных инцидентах;
- Содействовать уполномоченным государственным органам в обнаружении, предупреждении и ликвидации последствий компьютерных атак, установлении причин и условий возникновения компьютерных инцидентов;

- Обеспечивать выполнение порядка, технических условий установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.

На Субъектов КИИ, которым принадлежат значимые объекты КИИ, возложены дополнительные обязанности, в частности:

- Соблюдать специфические требования по обеспечению безопасности значимого объекта КИИ; Выполнять предписания должностных лиц уполномоченных государственных органов в части требований по обеспечению безопасности значимого объекта КИИ;
- Реагировать на компьютерные инциденты в установленном порядке, принимать меры по ликвидации последствий компьютерных атак;
- Обеспечивать беспрепятственный доступ должностных лиц уполномоченных государственных органов к значимым объектам КИИ при осуществлении этим лицами их полномочий.

Применимость законодательства о государственной тайне к Субъектам КИИ

В соответствии с законом информация о мерах по обеспечению безопасности КИИ составляет государственную тайну. Обращаем ваше внимание, что в отношении информационных систем, содержащих государственную тайну, действует специальное законодательное регулирование (например, могут быть использованы только сертифицированные средства защиты информации могут использоваться для защиты таких систем, подрядчики, оказывающие услуги по защите такой информации, должны иметь специальную лицензию, и т.д.).

Вопросы ответственности

Уголовный кодекс был также дополнен рядом новых видов преступлений в сфере информационной безопасности. В частности, предусматривается уголовная ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в КИИ (вплоть до лишения свободы).

Юристы АЛРУД имеют обширный опыт комплексной поддержки клиентов по всем отраслям права, в том числе в области защиты данных и кибербезопасности.

Юристы АЛРУД готовы оказать необходимую правовую помощь по всем вопросам, связанным с описанным нововведением.

Надеемся, предоставленная информация окажется для Вас полезной. Если кто-то из Ваших коллег также хотел бы получать наши информационные письма, пожалуйста, направьте нам его электронный адрес в ответ на это сообщение. Если Вы хотите больше узнать о нашей **Практики Защиты данных и кибербезопасности**, пожалуйста, сообщите об этом в ответном письме – мы будем рады направить Вам наши материалы.

В случае возникновения вопросов, пожалуйста, свяжитесь с Партнером АЛРУД **Марией Осташенко** – MOstashenko@alrud.com.

С уважением,

Юридическая фирма АЛРУД

Примечание: Обращаем Ваше внимание на то, что вся информация была взята из открытых источников. Автор данного письма не несет ответственность за последствия, возникшие в результате принятия решений на основе данной информации.