НОВОЕ РОССИЙСКОЕ ЗАКОНОДАТЕЛЬСТВО В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ И РЕГУЛИРОВАНИЯ ИНТЕРНЕТА

Этим летом в России было принято три закона в сфере кибербезопасности и регулирования Интернета:

(1) Федеральный закон № 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" ("**Закон о КИИ**"), которым были введены требования о безопасности инфраструктуры;

(2) Федеральный закон № 276-ФЗ "О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации", регулирующий использование сервисов для получения доступа к запрещенным в России вебсайтам ("**Закон о VPN**"); и

(3) Федеральный закон № 241-ФЗ "О внесении изменений в статьи 10.1 и 15.4 Федерального закона "Об информации, информационных технологиях и о защите информации", который вводит определенные требования к операторам сервисов мгновенных сообщений ("**Закон о мессенджерах**").

В настоящем обзоре приводится краткий обзор вышеперечисленных законов.

Основные моменты

Закон о КИИ

- Закон о КИИ вводит требования к безопасности Объектов КИИ, которые используются в важных секторах российской экономики;
- Владельцы обязаны оценивать значимость своих Объектов КИИ и, при необходимости, регистрировать их в государственном реестре;
- Владельцы Значимых объектов КИИ должны соблюдать дополнительные требования по безопасности и сотрудничать с государственными органами по вопросам предотвращения и расследования компьютерных инцидентов.

Закон о VPN

- Провайдеры сервисов VPN обязаны сотрудничать с государством и блокировать пользователям доступ к сайтам, запрещенным на территории РФ.

Закон о мессенджерах

- Анонимное использование мессенджеров запрещено;
- Операторы мессенджеров обязаны проводить идентификацию пользователей по номеру мобильного телефона.

ЗАКОН О КИИ

Основная цель Закона о КИИ – обеспечение безопасности критической

информационной инфраструктуры[1] в России, а также ее устойчивое функционирование при проведении в отношении нее компьютерных атак[2]. Закон о КИИ вступит в силу с 1 января 2018 г., а необходимые для его применения подзаконные акты еще не разработаны органами исполнительной власти РФ. Тем не менее, когда необходимое регулирование будет полностью сформировано, оно повлияет на большинство участников рынка.

Закон о КИИ вводит определенные обязанности для российских юридических лиц и индивидуальных предпринимателей ("**Операторы КИИ**"), которым на праве собственности, аренды или на ином законном основании принадлежат объекты критической информационной инфраструктуры[3] в одной из следующих сфер: (i) здравоохранение, (ii) наука, (iii) транспорт, (iv) связь, (v) энергетика, (vi) банковская сфера и иные сферы финансового рынка, (vii) топливно-энергетический комплекс, (viii) атомная энергетика, (ix) оборонная промышленность, (x) ракетно-космическая промышленность, (xi) горнодобывающая промышленность, (xii) металлургия и (xiii) химическая промышленность ("**Объекты КИИ**").

Каждый Оператор КИИ обязан, помимо прочего:

- незамедлительно информировать о "компьютерных инцидентах"[4] федеральный орган исполнительной власти ("**Орган**")[5], а также Центральный банк Российской Федерации (в случае, если Оператор КИИ осуществляет деятельность в банковской сфере и в иных сферах финансового рынка);
- оказывать содействие Органу (1) в обнаружении, предупреждении и ликвидации последствий компьютерных атак и (2) в установлении причин и условий возникновения компьютерных инцидентов.

Также Закон о КИИ устанавливает, что каждый Оператор КИИ обязан оценивать "значимость" Объектов КИИ, принадлежащих ему на праве собственности, аренды или на ином законном основании. Такая оценка необходима для того, чтобы определить, является ли соответствующий Объект КИИ "значимым объектом критической информационной инфраструктуры" ("**Значимый объект КИИ**") и, если да, то какую категорию значимости ему необходимо присвоить. Оценка должна будет проводиться в

---

1 Закон о КИИ определяет "**критическую информационную инфраструктуру**" как "*объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов*".

2 Закон о КИИ определяет "**компьютерную атаку**" как "*целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации*".

3 К объектам критической информационной инфраструктуры относятся: (1) информационные системы, (2) информационно-телекоммуникационные сети, (3) автоматизированные системы управления Операторов КИИ.

4 Закон о КИИ определяет "**компьютерный инцидент**" как "*факт нарушения и (или) прекращения функционирования объекта критической информационной инфраструктуры, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки*".

5 Федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации. Соответствующий компетентный орган еще не определен.

соответствии с правилами, которые еще не приняты Правительством РФ[6]. Категорирование будет осуществляться исходя из:

- социальной значимости, выражающейся в оценке возможного ущерба, причиняемого жизни или здоровью людей, возможности прекращения или нарушения функционирования объектов обеспечения жизнедеятельности населения, транспортной инфраструктуры, сетей связи, а также максимальном времени отсутствия доступа к государственной услуге для получателей такой услуги;
- политической значимости, выражающейся в оценке возможного причинения ущерба интересам Российской Федерации в вопросах внутренней и внешней политики;
- экономической значимости, выражающейся в оценке возможного причинения прямого и косвенного ущерба Операторам КИИ и (или) бюджетам Российской Федерации;
- экологической значимости, выражающейся в оценке уровня воздействия на окружающую среду; и
- значимости объекта критической информационной инфраструктуры для обеспечения обороны страны, безопасности государства и правопорядка.

Оператор КИИ обязан в течение 10 дней после завершения оценки направить ее результаты в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации ("**Орган безопасности**")[7]. Орган безопасности должен независимо проверить результаты такой оценки. Если Орган безопасности сочтет, что Объект КИИ является Значимым объектом КИИ, то сведения о таком Объекте КИИ вносятся в реестр значимых объектов критической информационной инфраструктуры, ведение которого осуществляет такой орган ("**Реестр**").

После регистрации Значимого объекта КИИ в Реестре на Оператора КИИ возлагаются дополнительные обязанности. К таким обязанностям относятся:

- соблюдение требований безопасности в отношении Значимых объектов КИИ ("**Требования безопасности**")[8];
- выполнение предписаний Органа безопасности об устранении нарушений Требований безопасности;
- реагирование на компьютерные инциденты в соответствии с порядком, который будет разработан Органом, и принятие мер по ликвидации последствий компьютерных атак, проведенных в отношении Значимых объектов КИИ; и
- обеспечение беспрепятственного доступа к Значимым объектам КИИ в случае проверок, проводимых Органом безопасности.

Соблюдение Операторами КИИ требований Закона о КИИ будет проверяться Органом безопасности посредством проведения плановых и внеплановых проверок. Плановые проверки будут проводиться каждые три года.

---

6 Проект постановления можно найти по ссылке http://regulation.gov.ru/projects#npa=73423.

7 Соответствующий орган еще не определен.

8 Требования безопасности будут разработаны Органом безопасности и будут дифференцироваться в зависимости от категории значимости соответствующего Значимого объекта КИИ.

Внеплановые проверки будут проводиться при наличии обстоятельств, указанных в Законе о КИИ (например, в случае компьютерного инцидента, повлекшего за собой негативные последствия на Значимом объекте КИИ).

Должностные лица Операторов КИИ могут быть привлечены к уголовной ответственности за нарушение (1) правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре, Объектах КИИ или телекоммуникационных сетях, или (2) правил доступа к такой информации, Объектам КИИ или телекоммуникационным сетям, если такое нарушение повлекло причинение вреда критической информационной инфраструктуре. Специальных мер административной ответственности за такие нарушения не установлено. Однако, Кодекс РФ об административных правонарушениях содержит общую норму об ответственности за нарушение правил защиты информации, которая предусматривает наложение штрафа на должностных лиц, а также на российские компании.

ЗАКОН О VPN

Закон о VPN вступит в силу с 1 ноября 2017 г. Федеральный закон № 149-ФЗ "Об информации, информационных технологиях и о защите информации" запрещает доступ к определенным информационным ресурсам и информационно-телекоммуникационным сетям в России ("**запрещенные вебсайты**"). В соответствии с Законом о VPN, владельцам информационно-телекоммуникационных сетей и информационных ресурсов, которые могут быть использованы для доступа к запрещенным вебсайтам ("**VPN технологии**"), запрещается предоставлять пользователям VPN технологий ("**пользователи**") возможность их использования на территории России для получения доступа к запрещенным вебсайтам. Использование VPN технологий не запрещается, однако, Закон о VPN возлагает определенные обязанности на: (1) владельцев VPN технологий ("**владельцы**"), (2) провайдеров хостинга или иных лиц, обеспечивающих размещение в сети Интернет VPN технологий ("**хостинг провайдеры**") и (3) операторов поисковых систем, распространяющих в сети "Интернет" рекламу, которая направлена на привлечение внимания потребителей, находящихся на территории Российской Федерации ("**операторы поисковых систем**").

Контроль за соблюдением Закона о VPN будет осуществлять Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций ("**Роскомнадзор**"). Для этого будет осуществляться ведение федеральной государственной информационной системы информационных ресурсов информационно-телекоммуникационных сетей, доступ к которым ограничен в России ("**Система**").

Владельцы будут обязаны подключится к Системе не позднее 30 дней с момента направления соответствующего требования Роскомнадзором[9]. Роскомнадзор сможет идентифицировать владельца самостоятельно или с помощью запроса хостинг провайдеру. При получении запроса от Роскомнадзора хостинг провайдер обязан (1) раскрыть данные о владельце или (2) уведомить владельца о необходимости раскрытия его данных на сайте в сети Интернет такого владельца. Операторы поисковых систем также обязаны подключиться к Системе. После подключения к Системе владельцев

[9] Проект порядка подключения и доступа к Системе можно найти по ссылке http://regulation.gov.ru/projects#npa=71495.

или операторов поисковых систем они должны блокировать доступ пользователей к запрещенным вебсайтам в течение 3 дней.

В случае неисполнения владельцем, помимо прочего, обязанностей по (1) подключению к Системе в течение установленного срока или (2) блокированию доступа к запрещенным вебсайтам Роскомнадзор ограничивает пользователям доступ к VPN технологии до устранения нарушений.

Также важно отметить, что требования Закона о VPN не распространяются на использование VPN технологии в случае, если (1) круг пользователей заранее определен владельцами и (2) VPN технологии используются в целях обеспечения деятельности пользователей.

ЗАКОН О МЕССЕНДЖЕРАХ

С 1 января 2018 г. анонимное использование сервисов мгновенных сообщений ("**мессенджеры**") будет запрещено. В связи с этим, у организаторов сервисов обмена мгновенными сообщениями ("**Сервис-провайдеры**") возникнут обязанности по Закону о мессенджерах.

Главная обязанность Сервис-провайдеров будет заключаться в идентификации пользователей мессенджеров по номеру мобильного телефона. Для этих целей Сервис-провайдерам необходимо будет заключить соответствующие соглашения об идентификации пользователей с операторами мобильной связи. Российские Сервис-провайдеры могут осуществлять идентификацию пользователей самостоятельно. Сведения об идентификации пользователей мессенджеров по номеру мобильного телефона должны храниться только на территории Российской Федерации.

Сервис-провайдеры также обязаны:

- при получении запроса от соответствующего российской государственного органа ограничить возможность осуществления пользователем передачи сообщений, которые содержат информацию: (i) распространение которой запрещено в России или (ii) которая распространяется с нарушениями российского законодательства;
- предоставить пользователям мессенджеров техническую возможность отказа от получения сообщений от других пользователей мессенджеров;
- обеспечивать конфиденциальность передаваемых сообщений;
- обеспечивать возможность передачи электронных сообщений по инициативе государственных органов в соответствии с российским законодательством;
- не допускать передачу электронных сообщений пользователям мессенджеров в случаях, установленных российским законодательством.

Если Сервис-провайдер не будет исполнять свои обязанности по Закону о мессенджерах, то их мессенджеры могут быть заблокированы Российским судом.

КОНТАКТЫ

Александр Аничкин
Партнер

T +7 495258 5089
E Alexander.Anichkin
@cliffordchance.com

Евгений Соловьёв
Советник

T +7 495 725 6420
E Evgeny.Soloviev
@cliffordchance.com

Екатерина Макарова
Старший юрист

T +7 495 725 6435
E Ekaterina.Makarova
@cliffordchance.com

www.cliffordchance.com

Клиффорд Чанс, Ул. Гашека 6, 125047 Москва, Россия