ЮРИСТ & ЗАКОН
АНАЛИТИЧЕСКОЕ ИЗДАНИЕ

08.06.2018 – 14.06.2018, № 21

КОМПЕТЕНТНОЕ МНЕНИЕ

Новый Закон "Об основных принципах обеспечения кибербезопасности в Украине". Теория и практика защиты информации

9 мая вступил в силу Закон Украины "Об основных принципах обеспечения кибербезопасности в Украине". Его принятие было крайне необходимым и довольно прогрессивным шагом для Украины. Ранее вопрос киберзащиты не был закреплен в законодательстве. Понятия по кибербезопасности были разбросаны среди разных норм, которые были скорее общими, чем конкретными.

При детальном анализе данного Закона нужно, во-первых, обратить внимание на сферу его действия. Законодатель не приводит исчерпывающий перечень сфер, на которые распространяется Закон. А вот в статье 2 закреплено, что данный ***Закон не распространяет свое действие*** на социальные сети, частные электронные информационные ресурсы в сети Интернет (включая блог-платформы, видеохостинги, другие веб-ресурсы), если такие информационные платформы не содержат информацию, необходимость защиты которой установлена законом, отношения и услуги, связанные с функционированием таких сетей и ресурсов. В соответствии с положениями данной статьи можно сделать вывод, что сфера действия Закона не распространяется на частные сети субъектов хозяйствования.

В то же время объектами киберзащиты являются ***объекты критической информационной инфраструктуры***, к которым относятся, в частности, предприятия, учреждения и организации независимо от формы собственности, деятельность которых непосредственно связана с технологическими процессами и/или предоставлением услуг, имеющих большое значение для экономики и промышленности.

То есть можно сделать вывод, что частные сети субъектов хозяйствования подпадают под действие Закона в том случае, если их можно отнести к объектам критической инфраструктуры.

Основной целью принятия нового Закона было собрать все нормы воедино, упорядочить их, привести к общему знаменателю терминологию, касающуюся данного вопроса, а также перевести в правовую плоскость определения и термины, касающиеся киберзащиты и кибербезопасности. Кроме этого, Закон о кибербезопасности призван определить и закрепить полномочия субъектов национальной системы кибербезопасности и средства их взаимодействия.

В частности, к таким ***субъектам*** относятся: Государственная служба специальной связи и защиты информации Украины, Нацполиция, СБУ, Минобороны и Генштаб Вооруженных Сил, разведывательные органы, Нацбанк.

Кроме этого, будет функционировать ***правительственная команда реагирования на компьютерные чрезвычайные события Украины (CERT-UA)***. Основными задачами этой команды будет:

– накопление и проведение анализа данных о киберинцидентах, ведение государственного реестра киберинцидентов;

– предоставление владельцам объектов киберзащиты практической помощи по вопросам предупреждения, выявления и устранения последствий киберинцидентов по данным объектам;

– подготовка и размещение на своем официальном веб-сайте рекомендаций по противодействию современным видам кибератак и киберугроз;

– взаимодействие с правоохранительными органами, обеспечение их своевременного информирования о кибератаках;

– обработка полученной от граждан информации о киберинцидентах относительно объектов киберзащиты и т. д.

Однако неизвестно, будет ли действовать команда CERT-UA на всей территории Украины, или ограничит сферу своей деятельности только Киевом. В случае если эта команда будет действовать только в Киеве, без создания территориальных филиалов, не все граждане смогут воспользоваться своим правом на их помощь.

К сожалению, несмотря на большое количество субъектов, ответственных за киберзащиту, новый Закон не прописывает систему их взаимодействия, ограничиваясь только общими нормами и положениями. Это может привести к тому, что в случае возникновения инцидента все перечисленные субъекты могут просто перенаправлять "потерпевших" друг к другу, в то время как убытки от вторжения уже будут причинены.

Что касается ***ответственности*** за нарушение норм законодательства о кибербезопасности, новый Закон также отмалчивается, ограничиваясь только стандартной и размытой формулировкой, что ответственность наступает в соответствии с действующим законодательством Украины. Однако о том, каким образом виновников атак будут привлекать к ответственности, Закон не говорит.

Кроме этого, законодатель предусмотрел такую превентивную меру от кибератак, как обязательное прохождение ***аудита*** государственными и частными учреждениями. Этот аудит будет проводиться по

требованиям Кабинета Министров. И тут также возникает ряд вопросов. Во-первых, с какой периодичностью будет проводиться этот аудит. Если предприятия будут проводить такой аудит раз в год – в нем абсолютно не будет смысла, поскольку киберпространство растет и развивается в геометрической прогрессии и система защиты, которой пользовались вчера, сегодня будет уже полностью устаревшей. С другой стороны, следует понимать, какую сферу кибербезопасности будет затрагивать данный аудит, будут ли проверяться сами системы защиты или же просто их наличие и соблюдение минимальных предупредительных мер от атак.

Во-вторых, будут иметь ли результаты данного аудита императивный характер с обязательным исправлением нарушений или же проведение аудита будет носить только рекомендательный характер. К тому же как будут действовать проверяющие в случае выявления нарушений норм киберзащиты? Будут ли это штрафные санкции или обязательство исправить нарушение в определенный срок?

ВЫВОД:

То есть в теории новый Закон довольно оптимистичный и прогрессивный, однако при переносе его норм в практическую, повседневную плоскость возникает много вопросов, на которые законодателю еще надо будет ответить. Возможно, в будущем Закон еще будет дополнен нормативными актами, которые в совокупности создадут целый правовой каркас для защиты от киберпреступности.

Анна Шарапова,
юрист
Корпорации "Глобал Консалтинг"