DOI: 10.22184/1992-4178.2019.187.6.12.16

Цифровая эра требует нового правового сознания

Рассказывает первый заместитель председателя Комитета Совета Федерации по обороне и безопасности В. И. Кожин

Роль кибербезопасности в условиях цифровизации экономики и общества в целом трудно переоценить. Как и любой вопрос, впрямую касающийся жизни общества, кибербезопасность требует нормативной базы. В декабре прошлого года в Совете Федерации РФ была создана Временная комиссия Совета Федерации по законодательному регулированию вопросов кибербезопасности, развития и использования цифровых технологий. О текущей деятельности комиссии, планируемых законодательных инициативах в отношении кибербезопасности, а также о том, как меняется нормативная база в области создания образцов ВВСТ, и о востребованности российской продукции в мире нам рассказал председатель Временной комиссии, первый заместитель председателя Комитета Совета Федерации по обороне и безопасности Владимир Игоревич Кожин.

Владимир Игоревич, вы возглавляете созданную в декабре 2018 года Временную комиссию Совета Федерации по законодательному регулированию вопросов кибербезопасности, развития и использования цифровых технологий. Что стало причиной создания этой комиссии и какие задачи перед ней поставлены?

Мотивы, которые послужили созданию Временной комиссии, можно перечислять долго, и, я думаю, они сейчас для всех очевидны. Мы говорим о вступлении в эру цифровой экономики, цифрового общества, но на самом деле мы уже живем в обществе, в котором нас повсюду окружает цифровизация. С одной стороны, это, безусловно, очередная технологическая революция, которая открывает для нас огромные возможности. Но с другой – цифровизация несет новые угрозы, количество которых растет в геометрической прогрессии. Сегодня, открыв свежую газету, почти наверняка увидишь в ней новость – и не одну, предметом которой является то или иное киберпреступление: похищение персональных данных, кибермошенничество, кража денег со счетов, атака на информационные ресурсы... И самое главное, что при таком масштабном характере этих угроз, правовая преграда для них практически отсутствует.

Задача комиссии, которую мы создали, – обобщить всё то, что происходит на этом поле, понять основы и направления этих угроз – на основе не газетных статей, а мнений экспертов, с тем чтобы начать формировать правовое пространство, которое ляжет в основу защиты от этих опасностей. Защиты – как людей,

граждан нашего государства, так и юридических лиц, общества и экономики в целом.

Собственно, с этого мы и начали: с общения со специалистами по относящимся к этой сфере вопросам, с узкопрофильными экспертами, с представителями профильных министерств, ведомств, которые делились с членами комиссии своими взглядами и соображениями, и с анализа полученной информации.

Позволяют ли результаты этого анализа уже сделать некоторые выводы о текущем состоянии правовой базы в области кибербезопасности и наметить первоочередные шаги для ее приведения в соответствие требованиям времени?

Нужно сказать, что картина вырисовывается весьма тревожная. Если с технологической точки зрения Россия движется в сторону цифровизации достаточно быстро и эффективно, даже с опережением других стран в определенных аспектах, то с точки зрения нормативного регулирования это движение очень медленное, а порой вообще отсутствует.

Сегодня эту работу необходимо начинать с самых базовых вещей, таких как понятийный аппарат. Терминология в этой области совершенно не устоявшаяся, одни и те же вещи разные люди, разные ведомства называют по-разному. А без четко очерченных понятий говорить о каком-либо правовом поле не приходится.

Сейчас мы плотно заняты решением этой проблемы и надеемся ближе к концу года подойти к этапу, когда результаты консультаций со специалистами, сбора и анализа информации позволят создать проекты определенных документов.

Безусловно, у нас нет иллюзий, что в самом ближайшем будущем удастся создать универсальный закон, снимающий все вопросы нормативного регулирования в области кибербезопасности. Ожидать этого было бы абсурдно. Но то, что просто необходимо как можно скорее выпустить некий базовый документ, который систематизирует проблемы в этой области и определит пути их решения, сомнений не вызывает.

В последние месяцы в новостях периодически проходила информация о готовящемся в Совете Федерации законопроекте по кибербезопасности. Это тот документ, о котором вы говорите?

Да, но с той поправкой, что некоторые журналисты, называя его законопроектом по кибербезопасности, как говорится, бегут впереди паровоза. Как такового «закона по кибербезопасности» не будет, потому что невозможно сделать так, чтобы один документ закрывал весь спектр проблем: от преступлений против личности до крупных финансовых махинаций, от утечки персональных данных до угроз в сфере хранения и обработки больших данных, от кражи паролей от соцсетей до вторжения в управление беспилотным транспортом. Сегодня цифровизация охватывает такое количество сфер применения, что объединить их все в одном законе просто не представляется возможным.

Сейчас речь идет именно о базовом документе, отправной точке. На данный момент я даже не могу предположить, как он будет называться. Когда мы коллективно подойдем к этапу, позволяющему на основе анализа массива собранной информации определить статус этого документа и его название, тогда уже можно будет об этом говорить.

Но в любом случае, это будет некий обобщающий документ, который позволит всем говорить на одном юридическом языке и определит дальнейшие шаги, в том числе даст понимание того, какие поправки и в какие законы потребуется вносить. А это, вероятно, затронет практически все ключевые законы: и Уголовно-процессуальный, и Гражданский кодекс, и многие другие.

Представьте простую и достаточно распространенную ситуацию: вам пришло письмо о блокировке вашей банковской карты, вы перешли по ссылке на поддельный сайт, ввели все данные карты, тем самым передав их злоумышленникам, и в результате у вас со счета списали деньги. Что это: кража, мошенничество? Сейчас даже в этом вопросе не существует однозначности: ведь, с одной стороны, вы свои данные отдали сами в результате обмана или злоупотребления доверием, а с другой – деньги с карты украли.

Сегодня работу по нормативному регулированию в области кибербезопасности необходимо начинать с самых базовых вещей, таких как понятийный аппарат

Вы приходите в полицию, и вам говорят: «По-человечески мы вас понимаем, но сделать ничего не можем: у нас нет ни базы, ни свидетельств, ни доказательств». Допустим, вы предоставите распечатку всех движений средств, данные о маршруте сообщения электронной почты, даже код мошеннического сайта. Тогда встает вопрос специализированных судов, потому что если вы это принесете

в обычный суд, судья не будет знать, что с этим делать. Для него код сайта – не орудие преступления, а данные сервера электронной почты – не отпечатки пальцев.

Поэтому данный вопрос – комплексный, затрагивающий очень много аспектов. И этот закон, скорее всего, должен иметь форму дорожной карты, благодаря которой появится возможность сразу перейти к конкретным законодательным инициативам, к конкретным законопроектам, которые будут сконцентрированы на определенных направлениях, видах угроз и т. п.

Сам базовый закон, вероятнее всего, тоже будет подвергаться изменениям по мере появления правоприменительной практики и ее анализа, а также изменения ситуации, что, конечно же, будет происходить, учитывая ту скорость, с которой развиваются технологии в информационной сфере и появляются новые вызовы и угрозы. Только представьте себе, какие изменения произойдут с широким распространением квантовых вычислений, искусственного интеллекта.

Базовый закон, скорее всего, должен иметь форму дорожной карты, благодаря которой появится возможность сразу перейти к конкретным законопроектам

Эволюция законов – обычная практика, в особенности когда речь идет о такой широкой области, как кибербезопасность. Можно вспомнить Федеральный закон «Об использовании атомной энергии», который был принят в 1995 году. Если вы сравните его первоначальную редакцию с действующей на сегодняшний момент, то, кроме общих фраз, не найдете ничего общего. За почти четверть века в данный закон было внесено множество изменений, которые позволяли ему идти в ногу со временем. То же следует ожидать и здесь: должен появиться базовый документ, который опишет ситуацию сегодняшнего дня, а затем – буквально на следующий день – уже потребуется начинать работу над новыми нововведениями и поправками.

Создание базового документа имеет очень важное, стратегическое значение для правовой конструкции, касающейся практически каждого из нас и всего государства в целом. Надеюсь, что мы столкнем этот камень с горы, чтобы обеспечить дальнейшее развитие нормативной базы и правового регулирования в сфере кибербезопасности.

Будет ли касаться этот закон электронной отрасли? Ведь она играет, мягко говоря, не последнюю роль в вопросах кибербезопасности.

Ровно настолько же, насколько он коснется других отраслей и видов деятельности, впрямую связанных с этой сферой. Еще раз повторю, что это – базовый документ, который опишет текущую ситуацию, определит основные понятия и направления.

Но, конечно, до уровня аппаратных решений, протоколов, компонентной базы мы в этом документе спускаться не будем, равно как и до конкретных программных решений. Это уже вопросы более специализированных документов.

Кибербезопасность – вопрос, который носит международный характер. Учитывается ли при анализе ситуации международный опыт?

Одно из направлений работы комиссии – сбор информации о том, что происходит у наших соседей и в мире в целом. Один из членов комиссии – Сергей Иванович Кисляк, профессионал высокого уровня. Одно время он был послом Российской Федерации в Соединенных Штатах. Им проделана очень большая работа, собран серьезный материал практически по всем крупным странам, европейским и не только, о том, что у них происходит, как они двигаются в этом направлении. Прежде всего это необходимо для синхронизации наших действий. Эту проблему не решить без международного сотрудничества. Ведь, если вернуться к примеру про списание денежных средств со счета банковской карты, то злоумышленник совершенно не обязательно будет находиться на территории России. Он может вести такую противозаконную деятельность из любой точки мира. Специалисты могут его вычислить, но что делать дальше, если он находится в другой стране, является гражданином другого государства?

Мы начали с анализа того, как развиваются в этом отношении европейские страны, что они берут за основу борьбы с киберпреступностью. И этот анализ показывает, что у разных стран несколько разный подход, например в отношении того, кто несет ответственность за допущение таких преступлений: оператор, провайдер, государство и т. п. На основе этого анализа мы также ищем для себя оптимальные варианты, отправные точки.

Вы упомянули про то, что развитие искусственного интеллекта принесет новые угрозы. Есть ли некое видение, как быть, если противоправное

действие, пусть и непредумышленное, совершено самой самообучающейся системой?

Вообще, искусственный интеллект – это тема отдельного разговора. Но, отвечая на данный вопрос, я, основывая свое мнение на своей прошлой профессии инженера электронной техники, исходил бы из того, что сейчас искусственному интеллекту придается слишком фантастическое, «киношное» значение. Да, системы стали саморазвивающимися, но они, к счастью, не думают за людей, не решают, кто их друг, а кто их враг. Если бы это было так, наверное, защититься от этого было бы невозможно.

Другая перспективная технология, которая уже стучится в нашу дверь, – беспилотный транспорт. Часто говорится о том, что кибербезопасность в этой сфере имеет критическое значение. Актуален ли этот вопрос с точки зрения нормативной базы?

Да, это очень важная сфера. Беспилотными летательными аппаратами уже никого не удивишь, а беспилотные автомобили уже вышли на дороги, пусть пока только в экспериментальном варианте.

Недавно мы проводили мероприятие*, специально посвященное данной теме. Здесь вопросы безопасности критически важны, потому что они касаются угроз человеческой жизни. И прежде всего это касается безопасности программного обеспечения, аппаратуры, каналов управления, потому что сбой или несанкционированное вмешательство в управление беспилотным транспортом может привести к катастрофе, независимо от того, говорим мы о беспилотных автомобилях, летательных аппаратах или водных транспортных средствах. Поэтому если не будет обеспечена практически абсолютная безопасность этих средств, ни одно правительство, ни один здравомыслящий человек не разрешит, чтобы они получили массовое распространение.

Применение различных видов транспорта регулируется разными ведомствами. Существует ли взаимопонимание между ними в этих вопросах?

Существует. Упомянутое мероприятие показало, что у всех, кто имеет к этому отношение – министерств, ведомств, специализированных организаций, институтов, – примерно один и тот же настрой. Все понимают важность темы безопасности беспилотного транспорта, ее значение для будущего, связанные с ней риски и активно ведут работы в данном направлении.

Но здесь существует та же проблема, что и в вопросах кибербезопасности в целом, – отсутствие единого понятийного аппарата. Допустим, у вас три дрона. Кем вы являетесь? Оператором? Внешним пилотом? Техником? Какое разрешение должно быть у вас для эксплуатации этих дронов? Все подобные вопросы требуют выработки единых позиций, и мы активно работаем над этим.

Один из важнейших документов, оказывающих существенное влияние на отечественную электронную и радиоэлектронную отрасль – Федеральный закон от 29 декабря 2012 года № 275-ФЗ. За время его существования в него несколько раз вносились изменения. Ожидаются ли новые поправки в нормативную базу для совершенствования практики применения данного закона и в целом для повышения эффективности деятельности предприятий электронной и радиоэлектронной отрасли в области создания передовых образцов ВВСТ?

Я уже говорил о том, как сильно может измениться документ относительно его первоначальной редакции, на примере Федерального закона «Об использовании атомной энергии». То же происходит с Федеральным законом № 275-ФЗ: с момента его появления – а появился он не от хорошей жизни: тогда ситуация с регулированием в сфере гособоронзаказа была очень сложной – этот документ прошел большой путь. Совсем недавно в него был внесен новый ряд поправок, которые еще более улучшили его редакцию и упростили жизнь

Важность темы безопасности беспилотного транспорта, ее значение для будущего, связанные с ней риски понимают все, кто имеет к этому отношение

тем, кто следует ему в своей повседневной практике. Пройдет некоторое время, мы посмотрим, как работает новая редакция, затем возникнут новые предложения, и, вероятно, потребуются очередные изменения. Мы все к этому готовы. Совершенно естественно, что после того как решается одна проблема, те, кто вовлечен в выполнение работ по гособоронзаказу, обозначают новые. Это непрерывный процесс, и он происходит в большой степени благодаря обратной связи от промышленности, в том числе тем предложениям, которые

* См. статью «Правовое регулирование беспилотного транспорта» на с. 18.

вносятся Секцией ОПК Экспертного совета нашего комитета.

Но самое главное, что этот закон работает, и в целом он работает эффективно.

Насколько, по вашему мнению, хорошо доходит обратная связь от промышленности до законодательных органов?

Конечно, нет предела совершенству. Но думаю, что сегодня у нас достаточно каналов для такой взаимосвязи. И подтверждение тому – то, что в законы вносятся поправки, которые инициированы промышленностью. Иначе законы, подобные 275-ФЗ, не были бы живыми, не отвечали бы текущим вызовам, превратились бы в догму. Так что этот механизм работает.

За последние годы вы неоднократно говорили о высоком спросе на отечественную военную технику за рубежом. Какова динамика этого спроса в настоящий момент?

Спрос на российскую военную технику растет. Пожалуй, самым значимым событием, практически «тектоническим сдвигом» в этой области стал договор о поставке зенитных ракетных комплексов С-400 в Турцию. Десять лет назад представить себе такой факт было невозможно: один из самых современных российских комплексов поставляется в одну из важнейших стран – членов НАТО. И это их осознанное решение, несмотря на все претензии, угрозы, попытки санкций.

Без механизма обратной связи от промышленности законы не были бы живыми, не отвечали бы текущим вызовам, превратились бы в догму

Почему это стало возможным? Прежде всего из-за качества и характеристик этих ЗРК. На С-400 у нас очередь. Их востребованность такова, что за последнее время у нас было построено несколько заводов, которые специализируются на данной тематике в рамках Концерна ВКО «Алмаз-Антей». Вообще, спрос за рубежом на всю российскую линейку ПВО от «Панцирей» и «Буков» до С-300 и С-400 сейчас высок как никогда.

Практически во всех областях вооружения и военной техники продукция нашего ОПК очень востребована. Реализуется большой контракт по поставке в Индию наших корветов. Высок спрос на танки, самолеты. Я уже не говорю про стрелковое оружие, про знаменитые автоматы Калашникова.

Конечно, это очень хорошо для нашего ОПК. Но не могу не отметить, что с общечеловеческой точки зрения ситуация в мире вызывает очень серьезные опасения. Достаточно посмотреть, что происходит с такими основополагающими для глобальной безопасности договорами, как Договор о ликвидации ракет средней и меньшей дальности и СНВ-III. Это ставит мир под угрозу еще и потому, что возрастает вероятность того, о чем говорилось в литературе и фильмах недавнего прошлого. Я говорил ранее, что искусственный интеллект пока не принимает решений за человека, но технических сбоев никто не отменял. Где гарантия, что ракета с ядерной боеголовкой не запустится помимо воли людей? Это очень серьезный вопрос.

Вы сказали про востребованность готовых изделий военной техники. Существует ли потенциал для экспорта российской ЭКБ, в том числе специального назначения?

К сожалению, компонентная база всегда была нашим слабым звеном. У нас есть программа импортозамещения, и по основным направлениям этот процесс у нас идет достаточно быстро. Хотя 100%-го импортозамещения достичь очень сложно, у нас уже есть системы вооружения, полностью состоящие из компонентов отечественного производства.

В ряде других областей имеются очень серьезные достижения, например в области корабельных двигателей. Однако в части ЭКБ еще существуют проблемы, которые необходимо решать.

А для того чтобы поставлять изделия за рубеж, нужно иметь более передовые решения, чем те, которые поставляются. Экспорт С-400 возможен, потому что у нас на подходе новый ЗРК – С-500. Это уже следующий уровень развития.

Можно ли сказать, что рекомендация компаниям – разработчикам и производителям ЭКБ звучит так: нужно делать новое, чтобы можно было продавать старое?

По сути, да. Так работает весь мир, все развитые страны. Попробуйте найти хотя бы одну страну, в которую Соединенные Штаты передали свою передовую технологию. Они продают только либо готовые изделия, либо то, что с их позиций уже давно устарело.

Так что, безусловно, нужно двигаться вперед, быть на шаг впереди. Сегодня мир устроен так, что если вы не будете идти вперед сами, вы просто отстанете.

Спасибо за интересный рассказ.

С В. И. Кожиным беседовали
П. А. Верник и Ю. С. Ковалевский

Семейство навигационной и управляющей аппаратуры отечественной разработки «Сусанин»

Устройства навигации, ориентации и управления на основе комплексированных GNSS/INS решений

- ✓ ГЛОНАСС L1/L2, GPS L1/L2/L5, Galileo E1/E5a/E5b, BeiDou B1/B2, NavIC (IRNSS) L5/S и SBAS L1
- ✓ Миллиметровая точность в режиме RTK
- ✓ Высокая точность определения углов ориентации
- ✓ Одновременная обработка сигналов, принятых от двух (трех) разнесенных антенн
- ✓ Интегрированный 9-осевой МЭМС-модуль повышенной точности
- ✓ Получение корректирующих поправок как по проводным, так и по беспроводным каналам связи (УКВ, GSM, LPWAN)

GNSS/INS+RTK

GNC

Произведено на базе отечественных модулей и микросхем!

Используется для определения точных координат и углов ориентации подвижных и стационарных объектов.
Варианты исполнения:
- ✓ NT1D - 1 антенна GNSS,
- ✓ NT2D - 2 антенны GNSS (курс, тангаж),
- ✓ NT3D - 3 антенный GNSS (крус, крен и тангаж).

Используется в составе БЛА для определения:
- ✓ пилотажно-навигационных параметров,
- ✓ автоматического управления полетом,
- ✓ управление любыми видами полезной нагрузки, в т.ч. в режиме гиростабилизации.

Точностные параметры	**В плане**	**По высоте**
автономный режим	1,5 м	2 м
DGPS режим	0,25 м	0,5 м
RTK режим	5 мм+0,5 мм/км	8 мм+1 мм/км
Углы ориентации		
курс	0.1 °	
крен	0.2 °	
тангаж	0.2 °	

www.ntlab-sk.ru
info@ntlab-sk.ru

НТЛаб