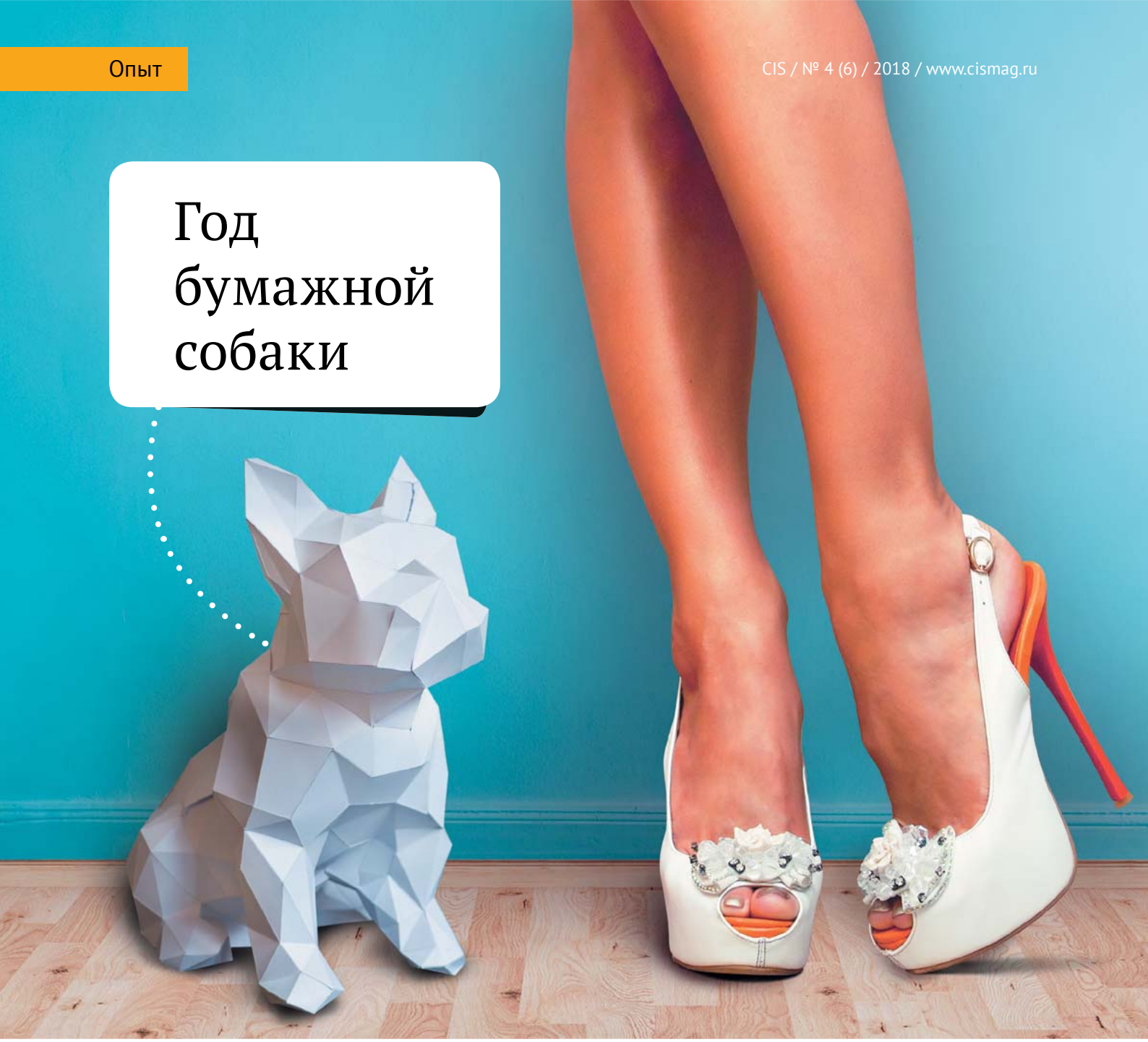
Год бумажной собаки



При подведении итогов года всегда трудно выделить главные события – неизменно накладываются эффекты недавности (самое свежее чаще представляется более важным, чем потом оказывается на самом деле) и частоты (чем чаще сталкиваешься с явлением, тем более определяющим и формирующим тенденции оно начинает казаться).

Нельзя сбрасывать со счетов и субъективность любой точки зрения – каждый из нас прожил этот год в своих личных профессиональных заботах и трудах, решая вполне конкретные прикладные задачи, с которыми было угодно свести нас провидению.

Тем не менее, если ограничиться рассмотрением узкой предметной сферы, то субъективность, недавность и частоту, упомянутые выше можно попробовать максимально нивелировать.

В качестве такой узкой тематики предлагаю для целей настоящей статьи выбрать вопрос так называемой «бумажной» информационной безопасности (ИБ). Тематика законодательного регулирования часто вызывает критику со стороны апологетов настоящей практической информационной безопасности, но продолжала и продолжает волновать многих по той банальной причине, что чаще всего именно соблюдение жёстко установленных норм (отраслевых, государственных, международных) и является важнейшим драйвером ИБ в организации.

Много ли вам известно CISO (chief information security officer – руководитель информационной безопасности), выбирающих межсетевой экран по причине того, что сейчас именно такие в моде? А по причине наличия у него сертификата требуемого уровня? Вопрос риторический.

Итак, ниже представлен краткий обзор двух самых значимых «бумажных» событий уходящего года собаки – по одному в мире и в России. Угадаете *финалистов*, не заглядывая дальше?

В мире

Странами Евросоюза (ЕС) ещё в далёком 1995 году была принята Директива № 95/46/ЕС о защите прав частных лиц при обработке персональных данных. И вот на смену ей 25 мая 2018 года пришёл Общий регламент по защите данных (General Data Protection Regulation – GDPR), принятый Европейским парламентом в апреле 2016 года.

Важность документа обусловливается тем, что исходя из его текста, его требования применимы не только к европейским организациям, но и к любым компаниям, работающим с персональными данными граждан ЕС или лиц, находящихся в ЕС. При этом не имеет значения месторасположение самой компании.

Опросник для самопроверки

GDPR применяется к организации, если она обрабатывает персональные данные и если ответ хотя бы на один из нижеперечисленных вопросов утвердительный.

1. Организация зарегистрирована в ЕС?
2. Организация зарегистрирована в стране, следующей законодательству ЕС на основании международного договора?
3. Организация предлагает свои услуги и товары гражданам/резидентам ЕС?
4. Организация занимается мониторингом действий лиц, находящихся на территории ЕС?
5. Организацией возможна случайная обработка персональных данных лиц, находящихся в ЕС?

Чтобы установить факт предоставления организацией услуги или товара лицам, находящимся в ЕС, будет достаточно даже её намерения к такому предложению. Согласно GDPR, намерение становится очевидным, если на сайте компании предусмотрено использование национального языка и валюты государства – члена Евросоюза, возможен заказ на этом языке. Или есть упоминания о потребителях или пользователях, которые находятся в Евросоюзе.

При этом, даже если сайт исключительно русскоязычный, нельзя быть абсолютно уверенным, что никто, находясь в Евросоюзе, не воспользуется его услугами.

Под мониторингом действий в GDPR (вопрос 4 из опросника) понимается отслеживание лиц в сети интернет с дальнейшим применением или потенциальной возможностью применения различных технологий по обработке персональных данных для анализа либо прогнозирования предпочтений, личностных характеристик, особенностей поведения.

Таким образом, если компания использует в маркетинговых целях какой-либо сервис для ведения статистики посещений – это уже и есть мониторинг, а значит – нужно применять GDPR. К сожалению, нет никакой гарантии, что лицо из ЕС не зайдёт на сайт, на котором применяются данные сервисы.

И самое главное: для усиления обязательности соблюдения норм GDPR вводит штрафы за любые нарушения. Размеры штрафов доходят до 20 миллионов евро или 4% оборота денежных средств компании (выбирается наибольшая сумма).

Но на деле – всё не так страшно. В случаях, когда нарушение незначительно, может быть объявлен просто выговор. Нематериальные санкции могут включать также запрет со стороны надзорного органа на обработку персональных данных (или их передачу контрагенту) до момента устранения нарушений.

General Data Protection Regulation – это новый большой документ с длинной преамбулой и 99 статьями, толковать который каждый может по-своему. Но если компании не хочется попасть под многомиллионный штраф, нужно выполнять требования GDPR и, конечно, не забывать о Федеральном законе «О персональных данных» и его подзаконных актах.

Роскомнадзор, к слову, на своих мероприятиях про GDPR говорит, даёт рекомендации и даже выпускает инфографику с разъяснениями.

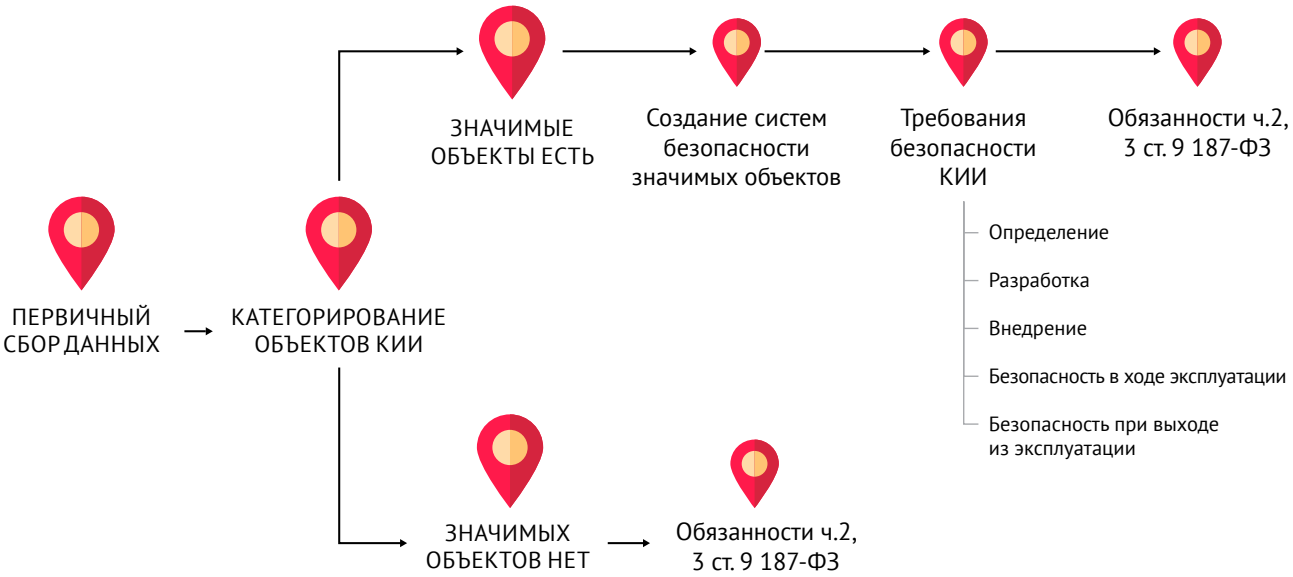
В России

Вряд ли найдётся много желающих спорить с тем, что важнейшим вступившим в силу в 2018 году законом в сфере информационной безопасности на территории России стал Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

Долгое время ожидался документ федерального уровня, который бы установил требования по информационной безопасности для промышленных предприятий и изменил бы статус с рекомендованного на обязательный для Приказа ФСТЭК России № 31 от 14.03.2014 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».

Однако принятый в прошлом году и вступивший в силу в этом году 187-ФЗ превзошёл самые смелые ожидания: под действие закона попали не только автоматизированные системы управления технологическими процессами (АСУ ТП), но и информационные системы и информационно-телекомму-

ДОРОЖНАЯ КАРТА



никационные сети предприятий из целого ряда сфер и отраслей: сферы здравоохранения, науки, транспорта, связи, энергетики, банковская и иные сферы финансового рынка, топливно-энергетический комплекс, предприятия в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности.

Более того, фактически вложенным в общую логику 187-ФЗ (связанным с ним, но всё же идущим отдельным блоком) оказался набор требований по взаимодействию с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА), за функционирование которой отвечает ФСБ России.

Новый пласт законодательства (а в дополнение к 187-ФЗ уже приняты и готовятся быть принятыми уже пара десятков различных нормативно-правовых актов) неизбежно порождает множество вопросов и недоумений. Так, в тематической группе «КИИ 187-ФЗ» в Telegram, где на момент подготовки данной статьи уже более 1500 участников, несмотря на глубокое и всестороннее обсуждение тонкостей законодательства, продолжают возникать всё новые и новые обсуждения, помогая обмениваться опытом и мнениями.

Тем не менее, несмотря на обилие вопросов, вполне реальным представляется выполнить требования законодательства и даже самостоятельно реализовать как минимум такие его шаги, как составление перечня объектов, подлежащих категорированию, а также само категорирование – своими силами без обязательного привлечения внешнего исполнителя.

Отдельно стоить отметить, что за нарушение требований непосредственно самого 187-ФЗ в настоящее время какой-либо ответственности не установлено. Ответственность может наступить в случаях, когда произойдёт инцидент с негативными последствиями.

Заключение

Вне зависимости от справедливости критикующих «бумажные» подходы к ИБ в завершение статьи хотелось бы отметить, что никакие самые современные и совершенные средства защиты не смогут обеспечить безопасность, если не будет выстроенного процесса их использования, обновления, своевременной модернизации и элементарной проверки их работоспособности, наконец.

В этом плане и GDPR, и нормативные документы, подзаконные 187-ФЗ (прежде всего, приказы ФСТЭК России № 236 и № 239), как уделяющие много внимания именно процесс-ориентированному подходу в преобладание над банальным бездумным применением какого-то шаблонного набора технических средств, дают существенную фору тем, кто решит выполнять установленные требования.

Безопасность критической информационной инфраструктуры и персональных данных должна начинаться не с распаковки свеженькой системы обнаружения вторжений или внедрения системы управления событиями информационной безопасности, а с наведения порядка в бизнес-процессах, повышения осведомлённости персонала, инвентаризации (аудита) и правильной безопасной конфигурации существующей инфраструктуры.

Тогда и требования законодательства покажутся вполне обоснованными, да и не такими уж сложными и дорогими в реализации.

Алексей Комаров, автор блога по информационной безопасности.

www.zlonov.ru