УДК 349:004

Н.М. Курбатов

ИЗМЕНЕНИЯ В НОРМАТИВНОМ ПРАВОВОМ РЕГУЛИРОВАНИИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационная безопасность всегда была важной составляющей национальной безопасности России. В 2018 году вступил в силу Федеральный закон Российской Федерации от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», определяющий основные понятия в данной сфере и устанавливающий правовые механизмы обеспечения безопасности критической информационной инфраструктуры. Впервые была признана важность критической информационной инфраструктуры для государственной безопасности, определен институциональный механизм ее обеспечения, установлена уголовная ответственность за посягательства на критическую информационную инфраструктуру в форме неправомерного воздействия; неправомерного доступа и нарушении правил эксплуатации информационной инфраструктуры. В настоящее время обеспечение информационной безопасности требует согласованности действий всех заинтересованных ведомств и организаций, четкого правового регулирования данной сферы жизнедеятельности в интересах своевременного выявления и локализации угроз информационной безопасности России. Относительная «новизна» проблем защиты критической информационной инфраструктуры России требует тщательного анализа полномочий компетентных структур в данной области, выработки надежных механизмов регулирования отношений в сфере кибербезопасности, а также подготовки предложений по совершенствованию имеющихся нормативно-правовых актов.

В статье проведен анализ последних нормативно-правовых актов, принятых в Российской Федерации, и проектов нормативно-правовых актов в сфере обеспечения безопасности объектов критической информационной инфраструктуры. В заключение предложены мероприятия, способствующие устранению выявленных недостатков, а также повышению эффективности мер обеспечения безопасности объектов критической инфраструктуры.

Ключевые слова: критическая информационная инфраструктура, компьютерная безопасность, информационная безопасность, обеспечение безопасности критической информационной инфраструктуры, международная информационная безопасность, угрозы информационной безопасности, компьютерные атаки, государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак, национальный координационный центр по компьютерным инцидентам.

В настоящее время развитие Российской Федерации можно охарактеризовать как планомерный переход на более инновационный путь развития, который включает в себя изменение всех сфер, в том числе модернизацию экономики, науки, культуры, сферы финансов, образования, транспорта, оборонного комплекса и многих других, затрагивающих жизнедеятельность как государства, так и общества. Анализируя процесс модернизации указанных сфер, можно выделить ряд характерных особенностей данных изменений, среди которых особую важность представляют, во-первых, повышенные требования к качеству и эффективности проводимых изменений, а также последующему управлению указанными сферами; во-вторых, процесс развития отраслей характеризуется интенсивным и повсеместным внедрением передовых информационных технологий.

Однако процесс компьютеризации производств обладает не только положительными аспектами. Так, эффективная компьютерная атака, направленная на важное инфраструктурное предприятие, может привести не только к полному прекращению или нарушению функционирования данного объекта, но и оказать более комплексное воздействие на экономику страны в целом, а также привести к существенному изменению уровня безопасности граждан, связанных с функционированием данного инфраструктурного объекта.

Для урегулирования описанной выше ситуации государством предпринимается комплекс мер в сфере обеспечения информационной безопасности. Так, с целью противодействия компьютерным атакам был принят ряд нормативно-правовых актов. Из них к основным и наиболее важным относятся следующие:

1) «Доктрина информационной безопасности Российской Федерации», утвержденная указом Президента Российской Федерации от 5 декабря 2016 г. № 646;

2) «Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы», утвержденная указом Президента Российской Федерации от 9 мая 2017 г. № 203;

3) Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;

4) Указ Президента Российской Федерации от 22 декабря 2017 г. № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

Указанные нормативные правовые акты регламентируют деятельность государственных органов власти по вопросам обнаружения, ликвидации и устранения последствий компьютерных атак, вводят в законодательство новые определения, такие как компьютерная атака, объекты критической информационной инфраструктуры, компьютерные инциденты, а также выделяют в отдельную группу инфраструктурные объекты Российской Федерации, представляющие особую важность (объекты критической информационной инфраструктуры).

Однако несмотря на то, что вопросам обеспечения информационной безопасности объектов критической инфраструктуры в последнее время уделяют пристальное внимание, остается ряд пробелов и нерешенных проблем в действующем законодательстве. Именно поэтому особую актуальность приобретает анализ проектов нормативно-правовых актов, нацеленных на решение возникающих проблем и устранение неурегулированных областей в законодательстве Российской Федерации.

Так как в соответствии с Указом Президента Российской Федерации от 22 декабря 2017 г. № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» на Федеральную службу безопасности Российской Федерации возлагаются задачи по обеспечению функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (далее – ГосСОПКА) особый интерес представляют проекты нормативно-правовых актов, разработанных данной структурой. В настоящее время именно на ГосСОПКА возлагают надежды по повышению уровня информационной безопасности объектов критической информационной инфраструктуры, поэтому развитию данной системы уделяют особое внимание.

В открытом доступе на данный момент размещено 6 проектов подзаконных нормативных актов ФСБ России, 3 из которых были утверждены и зарегистрированы в Управлении Министерства юстиции Российской Федерации в июле-сентябре 2018 г.:

Приказ ФСБ России от 24 июля 2018 г. № 366 «О Национальном координационном центре по компьютерным инцидентам» (далее – Приказ ФСБ России от 24 июля 2018 г. № 366) [1];

Приказ ФСБ России от 24 июля 2018 г. № 367 «Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» (далее – Приказ ФСБ России от 24 июля 2018 г. № 367) [2];

Приказ ФСБ России от 24 июля 2018 г. № 368 «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами критической информационной инфраструктуры Российской Федерации информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения» (далее – Приказ ФСБ России от 24 июля 2018 г. № 368) [3];

Проект Приказа ФСБ России «Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты» (далее – проект Приказа «Об утверждении Требований к средствам…») [4];

Проект Приказа ФСБ России «Об утверждении порядка, технических условий установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, за исключением средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации» (далее – проект Приказа «Об утверждении порядка, технических условий установки…») [5];

Проект Приказа ФСБ России «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации» (далее – проект Приказа ФСБ России «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах…) [6].

Рассмотрим указанные документы более подробно.

Приказ ФСБ России от 24 июля 2018 г. № 366 определил создание Национального координационного центра по компьютерным инцидентам (далее – НКЦКИ) с целью повышения взаимодействия и координации между субъектами критической информационной инфраструктуры Российской Федерации, а данный центр является одной из составных частей ГосСОПКА.

Кроме того, на НКЦКИ возложены следующие функции:

– участие в процессе обнаружения, ликвидации и предупреждении компьютерных инцидентов;

– координация мероприятий по реагированию на компьютерные атаки;

– сбор, анализ и хранение информации о компьютерных атаках;

– анализ эффективности мероприятий по ликвидации компьютерных инцидентов;

– разработка форматов представления информации о компьютерных инцидентах.

Структура НКЦКИ в разрезе выполняемых функций представлена на рисунке.

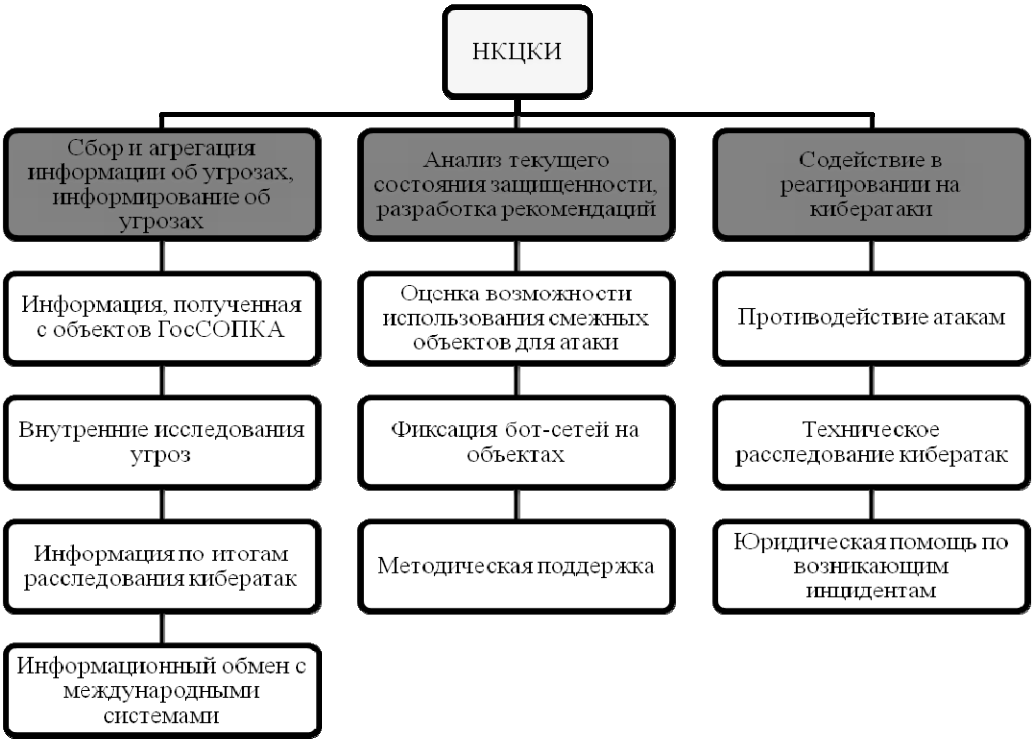

Рис. Структура НКЦКИ в разрезе выполняемых функций

Информационно-аналитическое, организационное и материально-техническое обеспечение НКЦКИ осуществляется Центром защиты информации и специальной связи ФСБ России.

Для выполнения поставленных задач и функций НКЦКИ имеет следующие полномочия:

– привлекать экспертов и организации, компетентных в вопросах реагирования на компьютерные инциденты;

– заниматься информированием по вопросам обнаружения, ликвидации и предупреждения компьютерных атак, а именно распространение справочно-информационных материалов, участие в научно-технических конференциях, выставках и т.д.;

– направлять уведомления и запросы в субъекты, отнесенные к объектам критической информационной инфраструктуры, а также иным организациям по вопросам обнаружения, ликвидации и предупреждения компьютерных инцидентов;

– отвечать (отказывать) на запросы международных организаций по вопросам обнаружения, ликвидации и предупреждения компьютерных инцидентов.

Таким образом, НКЦКИ является главным CERT (компьютерная группа реагирования на чрезвычайные ситуации) России. Проведенный анализ нормативно-правовой базы, регламентирующей деятельность данной структуры, позволяет сформулировать основные операции, выполнение которых будет возложено на НКЦКИ. К ним относятся:

– блокирование и разделегирование доменов;

– удаление ссылок, осуществляющих вредоносные действия.

Кроме того, с учетом информации поступающей от субъектов критической инфраструктуры, НКЦКИ сможет проводить комплексный анализ и выявлять более детальную информацию о злоумышленниках, в том числе способ оплаты доменов и их владельцев, каналы, по которым осуществлялось подключение к инфраструктуре, с которой производилась компьютерная атака.

Создание подобной структуры является стратегическим решением, направленным на всесторонний анализ компьютерных атак с целью агрегации наиболее полной информации о злоумышленнике, составлению полного сценария атаки и выработке мер по противодействию.

Важным аспектом деятельности НКЦКИ как национального CERT является возможность его деятельности не только на уровне нашего государства, но и международное взаимодействие. Участие всех сторон, задействованных в компьютерном инциденте, а также обмен опытом с иностранными структурами позволит эффективнее противодействовать будущим атакам, а также ускорит процесс поиска злоумышленников, использующих иностранные хостинги и IP-адреса.

Подводя итог, отметим, что принятие Приказа ФСБ России от 24 июля 2018 г. № 366 направлено на развитие взаимодействия между субъектами критической информационной инфраструктуры, а также создание центра, ответственного за сбор, анализ и хранение информации о компьютерных атаках. Согласно проведенному анализу нормативной правовой базы, НКЦКИ представляет огромную информационную базу данных об актуальных угрозах безопасности инфраструктуре, которая позволит повысить уровень защищённости инфраструктурных объектов, что в долгосрочной перспективе должно способствовать укреплению информационной безопасности и предотвращению типовых компьютерных атак.

Приказ ФСБ России от 24 июля 2018 г. № 367 регламентирует перечень информации, подлежащий передаче в ГосСОПКА. В данный перечень включена следующая информация:

– информация о зоне ответственности сегмента (центра) ГосСОПКА;

– данные о компьютерных атаках;

– данные о компьютерных инцидентах;

– данные об информационных ресурсах;

– общая информация о защищенности субъекта;

– данные об актуальных угрозах для сегмента ГосСОПКА;

– детальная информация о защищенности ресурсов, доступных из сети Интернет;

– сведения о самостоятельно обнаруженных фактах компрометации информационных ресурсов.

Кроме того, данный Приказ регламентирует порядок передачи информации, определяет список лиц, ответственных за данный процесс. Особое внимание уделяется информации о совершенных компьютерных атаках. Такую информацию необходимо передать в НЦКИ в течение 24 часов с момента обнаружения компьютерного инцидента.

Стоит отметить, что данный Приказ претерпел изменения в отличии от предыдущих проектов Приказа. Так, при предоставлении информации о выявленном компьютерном инциденте, необходимо сообщать не только о дате и времени совершения атаки, но и о фактическом адресе или географическом местоположении объекта, на который была совершена компьютерная атака. Указанная информация в дальнейшем поможет подойти к исследованию причин инцидента более комплексно, позволит выявлять закономерности компьютерных атак, группировать компьютерные атаки по географическому фактору.

Кроме того, в принятом Приказе на НКЦКИ возлагается обязанность по незамедлительному уведомлению субъекта критической инфраструктуры о получении сообщения при поступлении от него информации о выявленном компьютерном инциденте.

В ходе анализа данного Приказа были выявлены следующие важные аспекты: во-первых, отсутствие четкой формы для представления информации – данная форма должна быть разработана

НЦКИ с учетом типа предоставляемой информации; во-вторых, Приказ № 367 предполагает возможность передачи сведений даже в случае отсутствия подключения объекта критической информационной инфраструктуры к инфраструктуре НЦКИ. В таком случае информация направляется посредством почтовой, факсимильной или электронной связи.

Таким образом, принятие данного Приказа ФСБ России ставило цель формализовать порядок обмена информации с ГосСОПКА и установить сроки, необходимые для обмена информацией. Проведенный анализ позволил выявить тенденцию по снижению полномочий, возлагаемых на НКЦКИ, а именно:

– перечень технических параметров компьютерных инцидентов от НКЦКИ отсутствует в принятом Приказе;

– формат обмена информацией с использованием программно-технических инструментов ГосСОПКА в данном Приказе просто устанавливается НКЦКИ, а не утверждается отдельным правовым актом.

Приказ ФСБ России от 24 июля 2018 г. № 368 устанавливает, что субъекты критической информационной инфраструктуры вправе самостоятельно определять круг лиц, с которыми осуществляется обмен информацией по вопросам обнаружения, предотвращения и ликвидации последствий компьютерных атак. Данный обмен происходит в целях минимизации последствий компьютерных атак, а также для противодействия компьютерным инцидентам на других объектах критической инфраструктуры. Данный пункт Приказа отсутствовал в изначальных версиях проекта Приказа. Таким образом, ФСБ России дает относительную свободу в рамках выбора субъектов критической инфраструктуры для обмена информацией. При этом информация о выявленных компьютерных инцидентах направляется также и в адрес НКЦКИ, о чем говорилось выше. Данная особенность позволяет сделать выбор субъектов инфраструктуры для обмена безболезненным, поскольку вся информация собирается на уровне НКЦКИ.

В случае, если программный комплекс по обеспечению безопасности инфраструктурного объекта поддерживает возможность интеграции с НКЦКИ, обмен информацией должен производиться через данную структуру. Инфраструктурные объекты, не имеющие возможности подключения к НКЦКИ, должны информировать данный центр посредством почтовой, факсимильной или электронной связи.

Кроме того, Приказ ФСБ России № 368 регламентирует порядок обмена информацией о компьютерных инцидентах с иностранными организациями. Для принятия решения о предоставлении (не предоставлении) информации НКЦКИ дается 24 часа с момента получения обращения от иностранной организации.

Рассмотренный документ также описывает источники, с помощью которых субъекты критической информационной инфраструктуры могут получать информацию о компьютерных инцидентах. Список источников включает в себя:

– официальный сайт: http://cert.gov.ru;

– направление запросов в НКЦКИ;

– направление обращений в ФСБ России;

– направление запросов другим субъектам, международным организациям.

Несмотря на то что данный документ регламентирует порядок обмена информацией между субъектами критической инфраструктуры, большое количество вопросов вызывают ситуации по обмену информацией международных платежных систем или дочерних предприятий иностранных организаций. Для этой категории организаций оперативный обмен информацией о компьютерных атаках представляет особую важность. Однако данный Приказ позволяет производить обмен только через НКЦКИ, что создает риск блокирования передачи информации в адрес головных организаций и тем самым может привести к сбою в работе предприятий сферы экономики и бизнеса.

По итогам рассмотрения принятых Приказов ФСБ стоит отметить, что зарегистрированные документы практически не претерпели изменений в сравнении с опубликованными ранее проектами.

Проект Приказа «Об утверждении порядка, технических условий установки…» разделен на несколько разделов, каждый из которых регламентирует технические требования к следующим системам:

– к средствам ГосСОПКА;

– к средствам обнаружения;

– к средствам предупреждения;

– к средствам ликвидации последствий;

– к средствам поиска и предупреждения компьютерных атак;

– к средствам обмена и криптографическим средствам защиты информации, необходимой субъектам критической информационной инфраструктуры при обнаружении, предупреждении и (или) ликвидации последствий компьютерных атак;

– к средствам ГосСОПКА в части реализации функций собственной безопасности;

– к средствам обнаружения, средствам предупреждения и средствам ликвидации последствий.

В данном случае под средствами обнаружения компьютерных атак ФСБ России понимает системы, осуществляющие сбор, обработку и автоматический анализ событий информационной безопасности и выявленных компьютерных инцидентов. Интересной особенностью является то, что к данным системам не применяются требования по передаче информации в НКЦКИ.

Анализ требований к средствам предупреждения компьютерных атак позволил выявить следующую особенность. К данным системам применяются требования по выгрузке обобщенной информации об уязвимостях в НКЦКИ, таким образом, имеющиеся на рынке готовые решения не подходят под установленные требования, а значит на предприятия ложатся дополнительные издержки на покупку новых программных комплексов или модернизацию уже имеющихся. К средствам реагирования на компьютерные инциденты применяются аналогичные требования, предполагающие разработку решений специально под ГосСОПКА.

Несмотря на то, что регламентированные требования различны в зависимости от рассматриваемой системы, можно выделить основные черты, свойственные всем рассмотренным системам. К ним относятся:

– отсутствие возможности бесконтрольной передачи данных;

– отсутствие возможности принудительного удаления или обновления данных систем;

– возможность обслуживания данных систем российскими организациями;

– обеспечение гарантийной и технической поддержкой российскими организациями;

– реализация собственной безопасности;

– автоматический сбор, анализ, фильтрация и хранение информации;

– возможность визуализации, полученной информации;

– интеграция с НКЦКИ.

Требования, прописанные в данном нормативном правовом акте, фактически исключают возможность использования иностранных программных комплексов для защиты критических объектов инфраструктуры. Такой отказ обусловлен необходимостью контроля за инструментами на всех этапах их функционирования, а также с целью исключения возможных диверсий со стороны иностранных государств.

Таким образом, необходимость регламентирования технических требований объясняется относительной свободой в выборе программных средств по обеспечению информационной безопасности субъектами критической инфраструктуры. Данные требования устанавливают минимальные характеристики систем, обеспечивающих информационную безопасность объектов критической инфраструктуры.

По мнению автора, остается ряд «узких мест» в данных требованиях, а именно:

– в данном проекте приказа отсутствует описание процесса по оценке соответствия систем указанным требованиям, а также, в какой орган необходимо обратиться субъектам критической инфраструктуры с целью установления соответствия используемых систем;

– требование по модернизации средств силами только отечественных компаний является недостаточно проработанным, поскольку в указанном документе не определено, как субъект критической инфраструктуры может получить подобную информацию;

Также необходимо провести анализ Постановления Правительства Российской Федерации от 8 февраля 2018 г. № 127 «Об утверждении показателей критериев значимости объектов критической информационной инфраструктуы РФ и их значений, а также порядка и сроков осуществления их категорирования» (далее – Постановление Правительства) [7].

Данный нормативный правовой акт регламентирует правила категорирования объектов критической информационной инфраструктуры, который проводится субъектами данной инфраструктуры.

Категорирование производится по 5 основным группам (сферам значимости), к которым относятся:

– социальная значимость.

– политическая значимость.

– экономическая значимость.

– экологическая значимость.

– значимость для обеспечения обороны страны.

Категорирование объектов критической информационной инфраструктуры включает в себя:

– определение процессов в рамках выполнения функций (полномочий) или осуществления видов деятельности субъекта критической информационной инфраструктуры;

– выявление управленческих, технологических, производственных, финансово-экономических и (или) иных процессов в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов критической информационной инфраструктуры, нарушение и (или) прекращение которых может привести к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям для обеспечения обороны страны, безопасности государства и правопорядка (далее – критические процессы);

– определение объектов критической информационной инфраструктуры, которые обрабатывают информацию, необходимую для обеспечения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов;

– формирование перечня объектов критической информационной инфраструктуры, подлежащих категорированию (далее – перечень объектов);

– оценку в соответствии с перечнем показателей критериев значимости масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах критической информационной инфраструктуры;

– присвоение каждому из объектов критической информационной инфраструктуры одной из категорий значимости либо принятие решения об отсутствии необходимости присвоения им одной из категорий значимости.

Для проведения категорирования создается комиссия, а пересмотр результатов категорирования производится не реже одного раза в пять лет.

Категорирование производится по трем категориям: от самой высокой – первой, до самой низкой – третьей. Отнесение показателя к той или иной категории проводится в соответствии с количеством человек, пострадавших в результате компьютерного инцидента, или количества территорий, на которые повлияли компьютерные атаки.

Стоит отметить, что необходимость категорирования объектов критической инфраструктуры в первую очередь связана с требованиями, предъявляемыми к различным группам. Таким образом, к объектам, отнесенным к третьей категории, должны предъявляться более мягкие требования. Диверсификация требования в зависимости от категории в свою очередь позволит снизить издержки предприятий, отнесенных к третьей группе.

Подводя итог, отметим, что законодательные инициативы, принимаемые в Российской Федерации в последнее время, в совокупности с уже принятыми нормативными правовыми актами нацелены, в первую очередь, на обеспечение безопасности критической информационной инфраструктуры Российской Федерации.

Однако по итогам проведенного анализа нормативных правовых документов был выявлен ряд пробелов в законодательстве. Так, ни в одном из рассмотренных документов нет ни слова о форматах и протоколах обмена информацией между субъектами критической инфраструктуры, НКЦКИ, международными организациями. Кроме того, как отмечалось выше, не урегулирован вопрос по обмену информацией между дочерними компаниями иностранных представительств, отсутствует четкое понимание некоторых требований к программным комплексам, обеспечивающим безопасность объектов критической инфраструктуры.

Указанные проблемы способствуют появлению новых рисков в процессе обнаружения, предотвращения и ликвидации последствий компьютерных инцидентов.

Выявленные недостатки в законодательстве могут быть устранены за счет привлечения экспертов из крупных отечественных компаний, таких как «Лаборатория Касперского», «Позитив Технолоджис» в процесс обсуждения и доработки нормативной правовой базы. Многие отечественные компании в настоящее время заинтересованы в создании российских систем, обеспечивающих информационную безопасность. Кроме того, у данных организаций зачастую имеется опыт в создании

систем безопасности по самым высоким стандартам. Таким образом, привлечение их в процесс обсуждения законодательства позволит более четко сформулировать спорные моменты.

Кроме того, ФСБ России совместно с НКЦКИ необходимо разработать формы отчетности и протоколы передачи информации, поскольку от качества этих документов будет в дальнейшем зависеть эффективность противодействия компьютерным атакам, а также систематизация имеющихся данных об компьютерных инцидентах. В свою очередь избыточная информация в отчетности и излишняя сложность протоколов будет способствовать затягиванию сроков представления информации, а также возникновению сложностей при ее анализе.

Также наряду с развитием нормативной правовой базы необходимо не забывать об иных направлениях по обеспечению информационной безопасности, а именно:

– проведение научных исследований, основной целью которых является создание отечественных наработок в области информационных технологий;

– развитие национальных конкурентоспособных организаций в сфере информационных технологий, в том числе информационной безопасности;

– развитие криптографического суверенитета;

– работа с кадровым составом.

Наконец, для комплексного противодействия компьютерным атакам необходима разработка стандартов на международном уровне, а также обмен опытом с иностранными государствами. Сотрудничество государств на международном уровне является важной и актуальной задачей, поскольку злоумышленники при совершении компьютерных атак могут находиться далеко от атакуемого объекта, в том числе на территории иностранных государств. Договоренности о содействии позволят повысить успешность расследований таких преступлений.

Инструменты, используемые злоумышленниками с целью нанесения ущерба объектам критической инфраструктуры или компьютерного шпионажа, становятся более изощренными с каждым днем, однако реализация предложенных мероприятий позволит повысить эффективность ликвидации последствий уже совершенных атак, а также сделать более эффективным выявление компьютерных инцидентов на ранних этапах.

СПИСОК ЛИТЕРАТУРЫ

1. Приказ ФСБ России от 24 июля 2018 года № 366 «О Национальном координационном центре по компьютерным инцидентам (НКЦКИ)» // Российская газета. URL: https://rg.ru/2018/09/10/fsb-prikaz366-site-dok.html.
2. Приказ ФСБ России от 24 июля 2018 года № 367 «Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» // Российская газета. URL: https://rg.ru/2018/09/10/fsb-prikaz367-site-dok.html.
3. Приказ ФСБ России от 24 июля 2018 года № 368«Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами критической информационной инфраструктуры Российской Федерации информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения» // Российская газета. URL: https://rg.ru/2018/09/10/fsb-prikaz368-site-dok.html.
4. Проект приказа ФСБ России «Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты» // Федеральный портал проектов нормативно правовых актов. URL: http://regulation.gov.ru/projects#npa=78182.
5. Проект приказа ФСБ России «Об утверждении порядка, технических условий установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, за исключением средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации» // Федеральный портал проектов нормативно правовых актов. URL: http://regulation.gov.ru/projects#npa=78179.
6. Проект приказа ФСБ России «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных

в отношении значимых объектов критической информационной инфраструктуры Российской Федерации» // Федеральный портал проектов нормативно правовых актов. URL: http://regulation.gov.ru/projects#npa=78961.
7. Постановление Правительства РФ от 8 февраля 2018 года № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» // Гарант.Ру: информационно-правовой портал. URL: http://www.garant.ru/products/ipo/prime/doc/71776120.

Поступила в редакцию 14.05.2019

Курбатов Николай Михайлович, ассистент кафедры «Информационная безопасность в управлении»
ФГБОУ ВО «Удмуртский государственный университет»
426034, Россия, г. Ижевск, ул. Университетская, 1 (корп. 1)
E-mail: nikolaiudgu@mail.ru

N.M. Kurbatov

CHANGES IN THE NORMATIVE LEGAL REGULATION OF ENSURING THE SECURITY OF CRITICAL INFORMATION INFRASTRUCTURE OF THE RUSSIAN FEDERATION

Information security has always been an important component of Russia's national security. In 2018, the Federal Law of the Russian Federation of 26.07.2017 No. 187-FZ “On the Security of Critical Information Infrastructure of the Russian Federation” came into force, which defines the basic concepts in this area and establishes legal mechanisms to ensure the security of critical information infrastructure. For the first time, the importance of critical information infrastructure for state security was recognized, the institutional mechanism of its provision was determined, criminal liability for encroachments on critical information infrastructure in the form of illegal influence was established, as well as illegal access and violation of rules of information infrastructure operation. At present, ensuring information security requires coordination of actions of all interested departments and organizations, clear legal regulation of this sphere of life activity in the interests of timely identification and localization of threats to information security in Russia. The relative “novelty” of the problems of protection of the critical information infrastructure of Russia requires a careful analysis of the powers of competent structures in this area, the development of reliable mechanisms for regulating relations in the field of cyber security, as well as the preparation of proposals to improve existing regulatory legal acts.
The author analyzes the latest normative-legal acts accepted in the Russian Federation, and projects of normative-legal acts in the sphere of safety of objects of a critical information infrastructure. In conclusion, the author proposes measures to help eliminate the identified shortcomings and improve the effectiveness of measures to ensure the security of critical infrastructure facilities.

Keywords: critical information infrastructure, computer security, information security, security of critical information infrastructure, international information security, threats to information security, computer attacks, state system of detection, prevention and elimination of consequences of computer attacks, national coordination centre for computer incidents.

Received 14.05.2019

Kurbatov N.M., Assistant of the Department “Information Security in Management”
Udmurt State University
Universitetskaya st., 1/1, Izhevsk, Russia, 426034
E-mail: nikolaiudgu@mail.ru