УДК 004.056.5

Скоморохин Д.В., магистр Прикладной информатики,
Института Системного Анализа и Управления
Государственного Университета «Дубна»
Россия, г. Красноярск

К ВОПРОСУ ЗАЩИТЫ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация: *В статье рассматривается проблематика защиты объектов критической информационной инфраструктуры. Обнаружено, что с 2018 г. данная проблемная область регламентируется соответствующим нормативно-правовым актом. Защита объектов КИИ должна обеспечиваться не только частными компаниями, но и государством. Атаки на объекты КИИ могут стать угрозой национальной безопасности.*

Ключевые слова: *информационная безопасность, критическая информационная инфраструктура, информация, цифровизация, цифровая экономика, информационная инфраструктура, национальная безопасность.*

Annotation: The article deals with the problem of protecting objects of critical information infrastructure. It was found that since 2018, this problem area is regulated by the relevant regulatory legal act. The protection of CII facilities should be provided not only by private companies, but also by the goverment. Attacks on CII facilities can become a threat to the national security.

Key words: information security, critical information infrastructure, information, digitalization, digital economy, information infrastructure, national security.

В настоящее время как в России, так и в мире отмечается рост числа киберугроз, вследствие чего в Российской Федерации проводится регулярная доработка нормативно-правовых основ в области кибербезопасности в соответствии с существующими вызовами и угрозами киберсферы. Одним из наиболее развивающихся направлений кибербезопасности в России является обеспечение безопасности критических информационных инфраструктур.

1 января 2018 года вступил в силу 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017, согласно статьи 9 которого все без исключения субъекты критической информационной инфраструктуры (далее – КИИ) обязаны информировать о компьютерных инцидентах федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак.[1] Таким органом, в соответствии с приказом ФСБ №366 назначен НКЦКИ (Национальный координационном центре по компьютерным инцидентам).

Более того, те, кто владеют значимыми объектами, КИИ, в соответствии со статьей 10, обязаны обеспечивать непрерывное взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

К КИИ следует относить информацию, которая хранится в технических средствах обработки данной информации, базах данных, системах, которые предназначены для передачи данных по линиям связи, и сами сети электросвязи.

[1] Федеральный закон от 26.07.2017 N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». URL: http://www.consultant.ru/document/cons_doc_LAW_220885/

Вследствие чего, в РФ была сформирована ГосСОПКА (Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак) с целью обмена информацией о кибератаках на информационные системы, нарушение или прекращение работы которых крайне негативно скажется на экономике страны или безопасности граждан.

К ГосСОПКА должны подключиться владельцы объектов КИИ. К ним относятся организации здравоохранения, науки, транспорта, связи, энергетики, банковской сферы (системно значимые кредитные организации, операторы платёжных систем, системно значимые инфраструктурные организации финансового рынка), топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.[2]

Следовательно, если государство ставит перед собой задачу по защите КИИ от хакерских атак, то оно должно учитывать ряд следующих положений, а именно:

- организационные и технические ошибки в любой ИС могут приводить к появлению уязвимостей, которые позволяют атаковать данную ИС, так как в настоящее время отсутствуют эффективные способы избегания данного рода ошибок;
- развитие технологий приводит к возникновению более современных механизмов реализации атак на ИС, вследствие чего требуется время для совершенствования механизмов противодействия угрозам и уязвимостям;

[2] Лобач Дмитрий Владимирович, Смирнова Евгения Александровна Состояние кибербезопасности в России на современном этапе цифровой трансформации общества и становление национальной системы противодействия киберугрозам // Территория новых возможностей. 2019. №4. URL: https://cyberleninka.ru/article/n/sostoyanie-kiberbezopasnosti-v-rossii-na-sovremennom-etape-tsifrovoy-transformatsii-obschestva-i-stanovlenie-natsionalnoy-sistemy

- в некоторых организациях атаки на их ИС случаются редко, что приводит к тому, что такого рода организациям крайне нерационально держать в штате вирусных аналитиков, компьютерных криминалистов, если они востребованы только один-два раза в год.

В результате особенность данной области приводит к необходимости обеспечения безопасности предприятиям, входящим в КИИ, посредством создания центров компетенций, которые будут непосредственно подключаться к противодействию атакам. Именно этот подход и был заложен в концепцию ГосСОПКА.

Согласно указу президента №31с[3] Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА)[4] включает в себя главный, ведомственные, региональные и корпоративные центры.

Рассмотрим подробнее деятельность корпоративных центров, которые призваны решать следующие задачи:

- сбор и анализ информации о компьютерных атаках и компьютерных инцидентах;
- обеспечение оперативного реагирования на угрозы;
- реализация мероприятий по ликвидации последствий компьютерных инцидентов в информационных ресурсах с использованием специализированных программных решений и построенных процессов эксплуатации данных систем.

Формирование государственных структур контроля над обеспечением безопасности КИИ обуславливается тем, что нарушение работы объектов КИИ может создать угрозы для национальной безопасности. Тем не менее, на многих предприятиях существует дефицит кадров, а также отсутствие

[3] Указ Президента РФ от 15.01.2013 N 31с (ред. от 22.12.2017) «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации». URL: http://www.consultant.ru/document/cons_doc_LAW_140909/

[4] «Выписка из Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» (утв. Президентом РФ 12.12.2014 N К 1274). URL: https://base.garant.ru/71127868/

квалифицированных специалистов, способных формировать и поддерживать безопасность данных предприятий как объект КИИ. Вследствие чего, многие предприятия обращаются к частным компаниям, которые предоставляют услуги бизнесу по защите объектов КИИ. К таким компаниям относятся «Лаборатория Касперского», «Перспективный мониторинг», «Информзащита», «Ростелеком Солар» и др.

Таким образом, несмотря на уже предпринятые государством шаги в сфере обеспечения защиты объектов КИИ, все еще имеются актуальные проблемы, связанные с нормативным регулированием отношений в области кибербезопасности.

Использованные источники:

1. Федеральный закон от 26.07.2017 N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». URL: http://www.consultant.ru/document/cons_doc_LAW_220885/
2. Указ Президента РФ от 15.01.2013 N 31с (ред. от 22.12.2017) «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации». URL: http://www.consultant.ru/document/cons_doc_LAW_140909/
3. «Выписка из Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» (утв. Президентом РФ 12.12.2014 N К 1274). URL: https://base.garant.ru/71127868/
4. Лобач Дмитрий Владимирович, Смирнова Евгения Александровна Состояние кибербезопасности в России на современном этапе цифровой трансформации общества и становление национальной системы противодействия киберугрозам // Территория новых возможностей. 2019. №4. URL: https://cyberleninka.ru/article/n/sostoyanie-kiberbezopasnosti-v-rossii-na-

sovremennom-etape-tsifrovoy-transformatsii-obschestva-i-stanovlenie-natsionalnoy-sistemy