УДК 004.056
DOI 10.33764/2618-981X-2022-6-288-293

Категорирование объектов КИИ в оборонной промышленности

А. В. Цыпкина[1]*, *А. В. Шабурова*[1]
[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: arina.arina99@mail.ru

Аннотация. В современное время всё чаще подвергаются атакам критические информационные инфраструктуры предприятий. С каждым разом эти атаки становятся более вредоносными. Поскольку деятельность организации напрямую зависит от бесперебойной работы её информационных систем, то нужно обеспечить безопасность этих объектов. В данной статье рассматриваются основные этапы категорирования объектов критической информационной инфраструктуры. Так же изучаются пункты, необходимые для выполнения организациями, относящиеся по умолчанию к сфере деятельности, которая попадает в критическую информационную инфраструктуру. Примером такой организации в данной статье выступает оборонно-промышленное предприятие, которое имеет свои основные особенности при проведении процедуры категорирования. Актуальность темы категорирования критической информационной инфраструктуры объясняется важностью оборонной промышленности в обеспечении национальной безопасности Российской Федерации.

Ключевые слова: категорирование, субъект критической информационной инфраструктуры, объект критической информационной инфраструктуры, безопасность критической информационной инфраструктуры

Categorization of CII objects in the defense industry

A. V. Cypkina[1]*, *A. V. Shaburova*[1]
[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
* e-mail: arina.arina99@mail.ru

Abstract. In modern times, critical information infrastructures of enterprises are increasingly being attacked. Each time these attacks become more malicious. Since the organization's activities directly depend on the smooth operation of its information systems, it is necessary to ensure the safety of these facilities. This article discusses the main stages of categorization of critical information infrastructure objects. We also study the items necessary for organizations to perform, which by default belong to the field of activity that falls within the critical information infrastructure. An example of such an organization in this article is a military-industrial enterprise, which has its own main features when carrying out the categorization procedure. The relevance of the topic of categorizing critical information infrastructure is explained by the importance of the defense industry in ensuring the national security of the Russian Federation.

Keywords: categorization, critical information infrastructure subject, critical information infrastructure object, security of critical information infrastructure

Введение

Обеспечение безопасности информации на оборонных предприятиях является одним из важнейших направлений деятельности организации, поэтому тема защиты критической информационной инфраструктуры (далее – КИИ) в послед-

нее время становится все более актуальной. Категорирование объектов критической информационной инфраструктуры является одним из самых важных этапов процесса обеспечения безопасности предприятия.

Методы и материалы

На текущий момент кибератакам чаще всего подвергаются промышленные технологические системы и информационные системы жизнеобеспечения городов и других объектов, входящих в критическую информационную инфраструктуру. Последствия после таких инцидентов могут быть катастрофичны, поэтому в России принят Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», направленный на защиту такой инфраструктуры [1, 3].

Данный закон позволяет отнести значительную часть организаций РФ к субъектам КИИ, что способствует реализации защиты подобных инфраструктур. Согласно закону, к субъектам КИИ относятся:

– государственные органы;

– государственные учреждения;

– российские юридические лица и индивидуальные предприниматели (при условии установления собственности объекта КИИ на законном основании).

Объекты КИИ, принадлежащие юридическим лицам и индивидуальным предпринимателям должны функционировать в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сферы и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности.

При этом к субъектам КИИ относятся те организации, которые владеют объектами, функционирующими в указанных сферах, а не организации, работающие в данных областях.

Основными мероприятиями, которые необходимо выполнить субъекту КИИ, являются:

– категорирование объектов КИИ, в рамках реализации которого выделяются значимые объекты КИИ;

– выполнение требований по обеспечению безопасности таких объектов;

– непрерывная передача сведений о компьютерных инцидентах в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ (ГосСОПКА).

Целью статьи является изучение процесса категорирования объектов КИИ в сфере оборонной промышленности, которая занимается разработкой, испытанием и производством военной продукции.

Особое место в развитии экономики и обеспечении национальной безопасности РФ занимает оборонная промышленность, определяющая направление обеспечения стратегических интересов страны. В связи с этим государству необходимо постоянно уделять внимание к проблемам развития оборонной промыш-

ленности, разработке и производству вооружений и военной техники, необходимому уровню научно-технического и военно-технического потенциала, которое обеспечивает безопасность страны.

В большинстве случаев, на оборонных предприятиях имеются информационные системы по учету заработной платы и кадров, а также автоматизированные системы управления (далее – АСУ), осуществляющие управление технологическими и (или) производственными процессами (АСУТП и АСУП). Два этих класса систем выполняют свои функции в данной сфере и, следовательно, являются объектами КИИ.

На оборонных предприятиях информационные системы представляются в виде:

– локально-вычислительной сети предприятия;

– корпоративных сервисов и информационных систем семейства 1С (Зарплата и управление персоналом, Управление производством);

– корпоративных сервисов и информационных систем семейства Microsoft.

В соответствии со ст. 7 № 187-ФЗ объекты КИИ подлежат категорированию [1]. Категорирование проводится непосредственно субъектом КИИ в соответствии с Постановлением Правительства РФ от 08.02.2018 № 127 [2]. Для этих целей субъектом создается комиссия. Категорирование объекта КИИ заключается в установлении соответствия объекта КИИ критериям значимости и показателям их значений, а также назначение ему одной из категорий значимости и проверке сведений о результатах[4].

На первом этапе определяется перечень объектов КИИ, которые подлежат категорированию. В этот перечень входят объекты, обрабатывающие информацию, которая необходима для обеспечения критических процессов. Данный перечень утверждается руководителем предприятия и далее направляется в федеральные органы исполнительной власти, уполномоченные в области обеспечения безопасности КИИ в течение пяти дней с момента утверждения [5].

На втором этапе категорирования необходимо определить уровень значимости объекта КИИ, который определяется, исходя из возможных последствий в случае нарушения ее безопасности.

Существует пять показателей критериев значимости:

– социальная;

– политическая;

– экономическая;

– экологическая;

– значимость для обеспечения обороны страны, безопасности государства и правопорядка.

Рассмотрим каждый критерий значимости по показателям в оборонной промышленности.

В социальной значимости используются следующие показатели:

– нанесение вреда жизни и здоровью людей;

– прекращение или нарушение функциональной работы объектов обеспечения жизнедеятельности населения;

– недоступность к государственной услуге.

Политическая значимость содержит:

– прекращение или дисфункциональность государственного органа в части невыполнения возложенной на него полномочий;

– нарушение условий международного договора РФ.

Экономическая значимость включает:

– нанесение вреда субъекту КИИ, который оценивается в снижении уровня дохода по всем видам деятельности;

– нанесение потерь бюджетам РФ, оцениваемых в снижении выплат в бюджеты РФ субъектом КИИ.

Экологическая значимость заключает в себе губительные воздействия на окружающую среду.

Значимость для обеспечения безопасности государства, обороны и правопорядка:

– нарушение функционирования пункта управления, оцениваемые в уровне (значимости) пункта управления или ситуационного центра;

– спад показателей гособоронного заказа, выполняемого субъектом КИИ;

– приостановка работы информационной системы в области обеспечения безопасности государства, правопорядка и обороны страны[6].

Следовательно, если объекты не соответствуют критериям значимости, принимается решение о том, что такая категория им не присваивается. Категорирование объектов КИИ проводится в срок, не превышающий одного года со дня утверждения перечня объектов. Категорирование проводится на основе масштаба возможных последствий в случае возникновения компьютерных инцидентов с учетом анализа угроз безопасности и уязвимостей объекта и анализа возможных действий нарушителя[7].

Результаты

Результатом категорирования является присвоение одной из трех категорий (I, II, III категория, где самой высокой является первая, самой низкой - третья) объекту КИИ или отсутствие необходимости присвоения, а также оформление соответствующего акта. Результаты категорирования направляются в течение десяти дней с момента подписания акта во ФСТЭК, который проверяет направленную информацию и либо возвращает акт на доработку, либо вносит сведения об объекте КИИ в реестр значимых объектов КИИ. Объекты, которым была присвоена категория, являются значимыми объектами КИИ [8].

В работе рассматривается оборонное предприятие, находящееся в г. Новосибирске, которое является одним из ведущих разработчиков и производителей интегральных схем, операционных усилителей и фото-приемных устройств. Определение уровня значимости и присвоения категории объектам КИИ, подлежащих категорированию, представлены в табл. 1.

Таблица 1

Категория значимости, которая присвоена объекту КИИ

Показатель	Значение показателя	Категория	Относится ли показатель к объекту КИИ
I. Социальная значимость			
Причинение ущерба жизни и здоровью людей (человек)	показатель критерия значимости и его значения не применимы или не соответствует ни одному показателю критериев значимости и их значениям	-	Да
	более или равно 1, но менее или равно 50	III	Нет
	более 50, но менее или равно 500	II	Нет
	более 500	I	Нет
II. Экономическая значимость			
Возникновение ущерба субъекту критической информационной инфраструктуры, который является государственной компанией (процентов от годового объема доходов, усредненного за прошедший 5-летний период)	показатель критерия значимости и его значения не применимы или не соответствует ни одному показателю критериев значимости и их значениям	-	Да
	более или равно 1, но менее или равно 10	III	Да
	более 10, но менее или равно 20	II	Нет
	более 20	I	Нет

Исследуемым объектом являлась информационная система 1С: Зарплата и управление персоналом, которой присваивается III категория значимости.

Результаты категорирования всех объектов КИИ оборонного предприятия отображены в табл. 2.

Таблица 2

Результаты категорирования объектов КИИ для оборонного предприятия

Наименование объекта КИИ	Присвоенная категория
Локально-вычислительная сеть	II
1С: Зарплата и управление персоналом	III
1С: Управление производством	II

После категорирования объектов КИИ субъектам необходимо применить меры по защите организационного и технического характера.

При выполнении процедуры категорирования объектов КИИ предприятия решают следующие вопросы:

– выполнение требований законодательства о безопасности критической информационной инфраструктуры;

– выявление возможных угроз для организации, определение способов их устранения и предотвращения в будущем;

– оценка уровня ущерба в случае реализации киберугроз;

– избежание потенциальных штрафов и других санкций со стороны регулирующих органов.

Заключение

Изучив методику категорирования объектов КИИ на оборонном предприятии и проведя процедуру категорирования таких объектов, приходим к выводу, что решение субъектами КИИ задач по категорированию объектов на основе определения критических процессов является одним из важных направлений работы по защите значимых объектов КИИ и, соответственно, обеспечения национальной безопасности Российской Федерации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Федеральный закон от 26.07.2017 № 187 «О безопасности критической информационной инфраструктуры Российской Федерации». – Текст: электронный // Справочная правовая система КонсультантПлюс. – Режим доступа: по подписке (дата обращения 20.04.2022).
2. Постановление Правительства РФ от 08.02.2018 № 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». – Текст: электронный // Справочная правовая система КонсультантПлюс. – Режим доступа: по подписке (дата обращения 20.04.2022).
3. Ванцева И.О., Зырянова Т.Ю., Медведева О.О. Влияние федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» на владельцев критических информационных инфраструктурных системах. – Текст: непосредственный // Вестник УрФО № 1(27), 2018. – С. 71–76.
4. Трифонова Ю.В. О порядке определения оснований для отнесения субъектов и объектов к критической информационной инфраструктуре – Текст: непосредственный // Обработка, передача и защита информации в компьютерных системах. Первая Всероссийская научная конференция. Санкт-Петербург, 2020. – С. 210–212.
5. Чернов Д.В., Иванов А.П. Обзор нормативно-правовых актов в области обеспечения безопасности критической информационной инфраструктуры. – Текст: непосредственный // Инжиниринг и технологии. – 2019. – Vol. 4(1). – С. 28–30.
6. Особенности категорирования объектов критической информационной инфраструктуры оборонно-промышленного комплекса // НПП Гамма – URL: https://clck.ru/hpTer (дата обращения: 20.04.2022). – Текст : электронный.
7. Христодуло А.Д. Система защиты информации значимых объектов критической информационной инфраструктуры – Текст: непосредственный // Труды VIII Всероссийской научной конференции (с приглашением зарубежных ученых). В 2-х томах. Уфа, 2020. – С. 60–66.
8. Мазепин П.С., Гришин Н.А., Бочаров М.В. Категорирование объектов критической информационной инфраструктуры – Текст: непосредственный // Инновации. Наука. Образование, 2021. – С. 874–878.
9. Федеральная служба по техническому и экспортному контролю: Приказ ФСТЭК России от 25.12.2017 №239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» – Текст: электронный // Справочная правовая система КонсультантПлюс. – Режим доступа: по подписке (дата обращения 20.04.2022).
10. Федеральная служба по техническому и экспортному контролю: Методика оценки угроз безопасности информации ФСТЭК России от 05.02.2021 – Текст: электронный // Справочная правовая система КонсультантПлюс. – Режим доступа: по подписке (дата обращения 20.04.2022).

© А. В. Цыпкина, А. В. Шабурова, 2022