УДК 004.056
DOI 10.33764/2618-981X-2023-6-284-290

А. В. Цыпкина[1], А. В. Шабурова[1]*

Применение вероятностного метода оценки опасности объектов КИИ при возникновении чрезвычайных ситуаций

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

Аннотация. В современных условиях глобальной информатизации общества большинство объектов оборонной промышленности требуют комплексный подход к защите от различных угроз, включая терроризм, чрезвычайные ситуации, стихийные бедствия и преступную деятельность. В данной статье будет рассматриваться оборонное предприятие со стороны физической защиты от чрезвычайных ситуаций, возникающих от рук злоумышленников. Основной целью статьи является категорирование объектов критической информационной инфраструктуры для предотвращения возникновения чрезвычайных ситуаций с применением вероятностного метода, результатом которого будет являться вероятность безопасного состояния объекта критической информационной инфраструктуры, а также предложены меры по совершенствованию физической защиты рассматриваемой организации. Актуальность темы категорирования критической информационной инфраструктуры объясняется важностью оборонной промышленности в обеспечении национальной безопасности Российской Федерации.

Ключевые слова: категорирование, объект КИИ, чрезвычайная ситуация, физическая защита

A. V. Cypkina[1], A. V. Shaburova[1]*

Application of a Probabilistic Method for Assessing the Danger of CII Objects in the Event Of Emergencies

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

Abstract. In modern conditions of global informatization of society most objects of the defense industry require an integrated approach to protection from various threats, including terrorism, emergencies, natural disasters and criminal activity. In this article, a defense enterprise will be considered from the side of physical protection against emergencies arising at the hands of intruders. The main purpose of the article is to categorize objects of critical information infrastructure to prevent the occurrence of emergency situations using a probabilistic method, the result of which will be the probability of a safe state of the object of critical information infrastructure, and also proposed measures to improve the physical protection of the organization in question. 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, CII object, emergency situation, physical protection

Введение

В настоящее время вопросам обеспечения безопасности критической информационной инфраструктуры Российской Федерации уделяется большое внимание.

В отношении значимых объектов критической информационной инфраструктуры деструктивные воздействия нарушителей могут повлечь за собой негативные последствия для предприятия и даже возникновение чрезвычайных ситуаций (далее – ЧС). Основной целью статьи является определение вероятности безопасного состояния объекта критической информационной инфраструктуры (далее – КИИ) с помощью вероятностного метода при возникновении чрезвычайных ситуаций. Обеспечение безопасности информационных инфраструктур на оборонных предприятиях является одним из важнейших направлений деятельности организации [1].

Методы и материалы

Чрезвычайной ситуацией является обстановка на определенной территории или акватории, возникшая в результате опасного природного явления, аварии, катастрофы, стихийного бедствия или другого неблагоприятного события, которая может привести к человеческим жертвам, ущербу здоровью людей или окружающей среде, значительные материальным потерям и нарушению условий жизнедеятельности людей. Чрезвычайные ситуации различаются по характеру источника (природные, техногенные, биолого-социальные и военные) и по масштабам (трансграничные, федеральные, региональные, территориальные, местные, локальные) [2].

При оценке угроз безопасности информации необходимо определить потенциальные источники угроз безопасности информации, связанные с действиями людей или групп людей (антропогенные источники угроз), которые могут совершить несанкционированный доступ или воздействовать на информационные ресурсы и компоненты систем и сетей, – актуальные нарушители [3, 4].

Для оборонного предприятия основными нарушителями были определены:

а) внешние нарушители:
   1) специальные службы иностранных государств;
   2) отдельные физические лица (хакеры);

б) внутренние нарушители:
   1) авторизованные пользователи систем и сетей;
   2) системные администраторы и администраторы безопасности.

Используя классификацию ЧС природного и техногенного характера, принятую в постановлении Правительства Российской Федерации от 21 мая 2007 № 304 «О классификации чрезвычайных ситуаций природного и техногенного характера», определим возможный характер масштаба ЧС, возникшей от рук злоумышленников [5].

По классификации ЧС, исходя из размера зоны ЧС, для внутреннего нарушителя масштаб ЧС будет иметь локальный характер, а для внешнего нарушителя – муниципальный и межмуниципальный характер. Классифицируя объект, присваиваем возможному масштабу ЧС межмуниципальный характер.

В пределах концепции защиты будут рассматриваться угрозы, связанные с физическим доступом на объект защиты [6].

Возможными угрозами нарушения функционирования объекта при возникновении нештатных ситуаций внешнего характера могут выступать стихийные

бедствия, физические воздействия от рук злоумышленников и инциденты, связанные с технологическими процессами.

Обусловленное влияние внешних физических условий и окружающей среды при эксплуатации защищаемого объекта оборонной промышленности несёт ряд ограничений на применение технических средств охраны и допуск на охраняемый объект, что объясняется особенностью технологического процесса предприятия.

Исходя из вышеизложенного, для построения физической защиты исследуемого объекта будем осуществлять категорирование КИИ по методу Костина В.Н [7, 8].

Результаты

С использованием информационно-вероятностного метода был оценен потенциальный масштаб чрезвычайных ситуаций. Для каждого из шести уровней масштаба потерь была определена доля энтропии. В табл. 1 представлены результаты, где нелинейно были распределены потенциалы опасности чрезвычайных ситуаций.

Таблица 1

Соотношение потенциалов опасности ЧС по шестибалльной и энтропийной шкале

Оценочные шкалы	Уровень масштаба потерь при ЧС различного характера					
	локальный	муниципальный	межмуниципальный	региональный	межрегиональный	федеральный
Шестибалльная	1	2	3	4	5	6
Энтропийная	0,0066	0,116	0,173	0,555	0,621	0,878

Проанализировав таблицу, можно сделать вывод, что объекту исследования по шестибальной шкале присваивается 2 и 3 баллы по муниципальному и межмуниципальному характерам.

Категорирование проводится с учетом наихудших сценариев действий нарушителя наиболее опасного типа. Определяются шесть категорий потерь, которые применяются для оценки опасности защищаемых объектов:

– политические (снижение уровней авторитета властей и политическая нестабильность);

– людские (утрата жизней людей, их здоровья);

– финансовые (потеря материальных ценностей);

– экономические (затраты на переселение людей из зоны ЧС и выплаты компенсаций);

– экологические (потери природных ресурсов, ухудшение экологии);

– культурно-информационные (утрата художественных ценностей и передовых технологий).

Был проведен анализ потенциальных рисков объекта в случае возникновения чрезвычайных ситуаций с использованием метода главных компонент, в рамках которого было изучено взаимодействие между параметрами частных видов потерь. С использованием информационно-вероятностного подхода была проведена оценка уровня риска для различных категорий объектов, и на основе полученных результатов был предложен соответствующий уровень вероятности нахождения объекта в состоянии, которое можно считать безопасным [10].

Табл. 2 содержит информацию об оценках опасности при авариях каждой категории объектов, оцененных по шестибалльной шкале в шести масштабах потерь.

Таблица 2

Параметры последствий ЧС объектов по шестибалльной шкале

Частные виды потерь	Масштаб потерь объектов						
	1 кат.	2 кат.	3 кат.	4 кат.	*5 кат.*	6 кат.	7 кат.
Политические	5	4	3	3	*2*	2	1
Людские	5	4	4	3	*2*	2	1
Финансовые	5	5	4	3	*2*	2	1
Экономические	6	5	4	3	*3*	2	1
Экологические	6	5	4	3	*3*	2	2
Информационные	6	5	4	3	*3*	2	2

Проанализировав табл. 2 и сравнив полученные оценки частных видов потерь, получаем 5 категорию для оборонного предприятия.

Исследования были проведены в отношении каждой категории масштаба потерь, в результате чего были определены соответствующие энтропийные величины ущерба. Табл. 2 была преобразована в табл. 3, где шестибальная шкала опасности представлена энтропийной величиной масштаба потерь.

Таблица 3

Характеристики категорий объектов по энтропийной шкале

Частные виды потерь	Масштаб потерь объектов						
	1 кат.	2 кат.	3 кат.	4 кат.	*5 кат.*	6 кат.	7 кат.
Политические	0,621	0,555	0,173	0,173	*0,116*	0,116	0,0066
Людские	0,621	0,555	0,555	0,173	*0,116*	0,116	0,0066
Финансовые	0,621	0,621	0,555	0,173	*0,116*	0,116	0,0066
Экономические	0,878	0,621	0,555	0,173	*0,173*	0,116	0,0066
Экологические	0,878	0,621	0,555	0,173	*0,173*	0,116	0,116
Информационные	0,878	0,621	0,555	0,173	*0,173*	0,116	0,116

С помощью входных данных из табл. 3 была проведена оценка энтропийного потенциала опасности для каждой категории объекта, и результаты данной оценки представлены в табл. 4.

Таблица 4

Потенциалы категорируемых объектов по энтропийной шкале

Частные виды потерь	Масштаб потерь объектов						
	1 кат.	2 кат.	3 кат.	4 кат.	*5 кат.*	6 кат.	7 кат.
Политические	0,621	0,555	0.173	0,173	*0,116*	0,116	0,0066
Людские	0,621	0,555	0,555	0,173	*0,116*	0,116	0,0066
Финансовые	0,621	0,621	0,555	0,173	*0,116*	0,116	0,0066
Экономические	0,878	0,621	0,555	0,173	*0,173*	0,116	0,0066
Экологические	0,878	0,621	0,555	0,173	*0,173*	0,116	0,116
Информационные	0,878	0,621	0,555	0,173	*0,173*	0,116	0,116
Энтропийный потенциал опасности	1,371	1,182	1,011	0,522	*0,289*	0,206	0,102
P безопасного состояния объекта	0,999	0,95	0,90	0,77	*0,69*	0,65	0,60

Вероятность безопасного состояния объекта исследования является значение показателя защищенности объекта, значение которого может быть определено исходя из потенциалов опасности категорируемых объектов. Вероятность безопасного состояния нашего объекта равна 69 %.

Соответственно, при возникновении чрезвычайной ситуации потенциал опасности категорируемых объектов составляет 31 %, что так же является их интегральной характеристикой. Потенциал привлекательности защищаемого объекта определяется потенциалом опасности каждой категории объекта, который в свою очередь, зависит от параметров частных потерь [11, 12].

Заключение

Для минимизации потенциала опасности предприятия необходимо рассматривать комплексную защиту, включающую и обеспечение безопасности на физическом уровне, что в последствии становится первой преградой для злоумыш-

ленника. Инструментом для обеспечения безопасности выступает система физической защиты. Это совокупность действий и мер, связанных с физическим, инженерно-техническим проектированием и организационными мероприятиями для предотвращения несанкционированного доступа к объекту [13].

На рассматриваемом оборонном предприятии уже имеется действующая физическая защита, но для совершенствования защиты и повышения безопасного состояния объекта рекомендуется установить средство контроля и управлением доступа и устройства пространственного зашумления, сетевые помехоподавляющие фильтры [14].

В результате с помощью применения вероятностного метода был найден потенциал опасности объекта КИИ оборонного предприятия при возникновении ЧС и предложены рекомендации по физической защите для повышения эффективности информационной безопасности предприятия оборонно-промышленного комплекса [15].

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 05.04.2023).
2. ГОСТ Р 22.2.06-2016. Безопасность в чрезвычайных ситуациях. Менеджмент риска чрезвычайной ситуации. Оценка риска чрезвычайных ситуаций при разработке паспорта безопасности критически важного объекта и потенциально опасного объекта : нац. стандарт Рос. Федерации : изд. офиц. – Введ. 2017- 06-01. – Москва : Стандартинформ, 2016. – 8 с.
3. Методический документ. Методика оценки угроз безопасности информации. Утвержден ФСТЭК России 5 февраля 2021 г. – Текст : электронный // ФСТЭК России : сайт – 2022. – URL: https://fstec.ru/component/attachments/download/2919 (дата обращения: 05.04.2023).
4. Костин В. Н. Оценка потенциала опасности нарушителей на основе информационного метода и метода главных компонент / В. Н. Костин // Информационные технологии и вычислительные системы, 2016, № 3. – С. 74–81.
5. Постановление Правительства РФ от 21.05.2007 № 304 «О классификации чрезвычайных ситуаций природного и техногенного характера». – Текст: электронный // Справочная правовая система КонсультантПлюс. – Режим доступа: по подписке (дата обращения 05.04.2023).
6. Костин В. Н. Задачи концептуального проектирования систем физической защиты критически важных объектов / В. Н. Костин // Проблемы информационной безопасности. Компьютерные системы, 2020, № 1. – С. 58–67.
7. Костин В. Н. Информационно-вероятностный метод формирования категорий потенциально опасных объектов / В. Н. Костин, А. К. Пономарев // Вестник компьютерных и информационных технологий, 2015, № 6 (132). — С. 34–42.
8. Костин В. Н. Оценка значимости частных видов потерь критически важных объектов при возникновении чрезвычайной ситуации / В. Н. Костин, А. С. Боровский // Научно-технический вестник Поволжья, 2020, № 8. – С. 8 – 11.
9. Костин В. Н. Оценка величины значимости чрезвычайных ситуаций на основе информационно-вероятностного метода / В. Н. Костин // Проблемы информационной безопасности. Компьютерные системы, 2019, № 3. – С. 17–23.
10. Костин В. Н. Оценка потенциала опасности критически важных объектов при возникновении чрезвычайных ситуаций на основе информационно вероятностного метода и метода главных компонент / В. Н. Костин // Информационные технологии, 2020, Т. 26, № 5. – С. 297–301.

11. Костин В. Н. Обоснование требований к эффективности подсистем физической защиты объектов информатизации / В. Н. Костин, Н. А. Соловьев, Н. А. Тишина // Научно-технический вестник Поволжья, 2018, № 4. – С. 125–128.

12. Костин В. Н. Модернизация структуры физической защиты критически важных объектов информатизации на основе выбора эффективных решений // Вестник компьютерных технологий, 2019, № 12 (186). — С. 27–39.

13. Панин О. Категорирование объектов для создания эффективных систем физической защиты – Текст: непосредственный // Безопасность. Достоверность. Информация, 2007, № 70. – С. 20–24.

14. Мельников Ю.С. Актуальные вопросы физической защиты информации – Текст: непосредственный // Проблемы науки, Москва, 2020, № 7 (55). – С. 35–40.

15. Давыдов Д.М. Особенности обеспечения информационной безопасности инновационной деятельности предприятий оборонно-промышленного комплекса – Текст: непосредственный // Инновации и инвестиции, 2019, № 10. – С. 8–10.