ЗАЩИЩЕННОСТЬ СЛОЖНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ СИТУАЦИОННЫХ ЦЕНТРОВ МЧС РОССИИ

С.П. Еременко, кандидат технических наук, доцент;
С.Б. Хитов;
В.А. Онов, кандидат технических наук, доцент.
Санкт-Петербургский университет ГПС МЧС России

Рассмотрена актуальность проблемы разработки методов, позволяющих обеспечить требуемые уровни показателей защищенности информационных систем ситуационных центров МЧС России с учетом роста их сложности. Приведены формулы, определяющие данные показатели.

Ключевые слова: система распределенных ситуационных центров, ситуационный центр, информационная безопасность, защищенность, сложная система, показатели защищенности

SECURITY OF COPLEX OF INFORMATION SYSTEMS OF THE SITUATIONAL CENTERS OF EMERCOM OF RUSSIA

S.P. Eremenko; S.B. Khitov; V.A. Onov.
Saint-Petersburg university of State fire service of EMERCOM of Russia

Relevance of a problem of development of the methods allowing to provide the required levels of indicators of security of information systems of the situational centers of EMERCOM of Russia taking into account growth of their complexity is considered by authors. The formulas defining these indicators are given.

Keywords: system of the distributed situational centers, situational center, information security, security, complex system, information security indicators

Одним из ключевых направлений создания и развития системы распределенных ситуационных центров (СРСЦ) МЧС России, представляющей собой трехуровневую систему ситуационных центров (СЦ): Национальный центр управления в кризисных ситуациях (НЦУКС) – ЦУКС региональных центров – ЦУКС главных управлений [1, 2], является обеспечение информационной безопасности (ИБ).

Сегодня в СЦ МЧС России функционирует значительное количество информационных систем (ИС) различного назначения, материальной (технической) основой которых являются распределенные вычислительные сети, объединяющие большое количество средств вычислительной и оргтехники, коммуникационного и сетевого оборудования. Данные системы характеризуются тем, что могут иметь как простую, так и сложную структуру. При этом в последнее время прослеживается усложнение структуры ИС СЦ МЧС России по ряду направлений. Одно их таких направлений связано с тем, что в состав систем входит все большее число образующих системы элементов. Кроме того, усложняется структура этих элементов, определяющая их объединение в системы и взаимодействие между собой в процессе функционирования. Возрастает количество задач, решаемых с помощью ИС, повышается ответственность выполняемых ими функций, растет их многообразие и сложность.

Определяя безопасность ИС СЦ МЧС России через состояние их защищенности, при котором обеспечивается способность функционирования систем без перехода в опасное состояние (под опасным состоянием будем понимать состояние, связанное с нарушением

конфиденциальности, целостности и доступности обрабатываемой в ИС информации), можно отметить, что при прочих равных условиях система, состоящая из большого числа входящих в нее элементов и имеющая более сложную структуру и алгоритм функционирования, является менее защищенной по сравнению с более простой системой. В связи с этим требуется разработка специальных методов обеспечения защищенности ИС СЦ МЧС России, учитывающих рост сложности данных систем, включая разработку математических методов расчета показателей защищенности.

В качестве одной из основных характеристик защищенности ИС примем время ее безопасной работы [3]. Обозначим это время как случайную величину – T. Будем считать, что в момент времени $t = 0$ система начинает работу, а в момент времени $t = T$ в системе происходит инцидент ИБ. Инцидент ИБ рассматриваем как результат успешной атаки на ИС (попытки реализации угрозы ИБ) – случайное событие во времени, приводящее к такому состоянию системы, при котором прекращает функционировать ее функция защищенности.

Рассматриваемая случайная величина – время безопасной работы системы T будет иметь закон распределения, характеризующийся интегральной функцией распределения:

$$F(t) = P(T_k < t),$$

где T_k представляет собой случайный момент времени, в который в системе произошёл инцидент. Тогда получим, что:

$$Q(t) = F(t)$$

будет представлять собой вероятность инцидента на интервале времени $[0, t]$.

Функцию $Q(t)$ рассмотрим как вероятность инцидента до момента времени t. Плотность распределения вероятности инцидента будет равна:

$$f(t) = \frac{dF}{dt} = F'(t).$$

Понятие «безопасная работа» рассмотрим как событие, являющееся противоположным по отношению к событию инцидента и, исходя из этого, вероятность безопасной работы в течение времени t рассчитаем как:

$$P(t) = 1 - Q(t).$$

При этом, если $F(t)$ – дифференцируемая функция (на практике данное условие выполняется практически во всех случаях), то в таком случае дифференциальная плотность инцидента будет равна:

$$f(t) = \frac{dQ(t)}{dt} = -\frac{dP(t)}{dt}.$$

Такие показатели, как вероятность инцидента и вероятность безопасной работы системы в течение времени t в заданных условиях будет определяться через плотность вероятности инцидента:

$$Q(t) = \int_0^t f(t)dt; \quad P(t) = \int_t^\infty f(t)dt$$

.

В практических расчетах наиболее часто применяется такая характеристика защищенности, как интенсивность инцидентов ИБ – $\lambda(t)$. Интенсивность инцидентов рассмотрим как относительную скорость уменьшения значений функции защищенности с увеличением интервала времени $(0, t)$:

$$\lambda(t) - \frac{f(t)}{P(t)} - -\frac{\frac{dP(t)}{dt}}{P(t)} \quad . \tag{1}$$

Решение уравнения (1) при начальном условии $P(0) = 1$ дает для функции защищенности системы формулу:

$$P(t) = exp\left\{-\int_0^t \lambda(t)dt\right\} \quad . \tag{2}$$

При постоянной интенсивности инцидентов $(\lambda(t) = const)$ указанная выше формула (2) приобретает более упрощенный вид:

$$P(t) = exp\{-\lambda t\} \quad .$$

Интенсивность инцидентов $\lambda(t)$ – будет представлять собой условную плотность их вероятности в предположении, что до момента t система функционировала безопасно. Таким образом, случайная величина T будет иметь следующие характеристики: $P(t)$, $f(t)$, $\lambda(t)$.

В качестве показателей защищенности применяют также числовые характеристики случайной наработки до инцидента ИБ [4]. Данные характеристики по экспериментальным данным, как правило, определяются значительно проще, чем определенные выше зависимости: $P(t)$, $\lambda(t)$, $f(t)$. Из наиболее широко используемых характеристик выделим среднюю наработку системы до инцидента (математическое ожидание наработки до инцидента или первый начальный момент):

$$m_t = M[T] = \int_0^\infty t f(t)dt = \int_0^\infty t\frac{dF(t)}{dt}dt = -\int_0^\infty t\frac{dp(t)}{dt}dt, \tag{3}$$

где $F(t)$ – функция распределения случайной величины T.

Проинтегрировав выражение (3) по частям, получим:

$$m_t = \int_0^\infty p(t)dt \quad .$$

При постоянной интенсивности инцидентов $(\lambda(t) = const)$ будем иметь:

$$m_t = \int_0^\infty exp\{-\lambda t\}\, dt = \frac{1}{\lambda}$$

.

Второй центральный момент (среднее квадратичное отклонение) тогда будет равен:

$$\sigma^2 = \int_0^\infty (t - a_1)^2 f(t)\, dt$$

.

Очень часто этих двух моментов бывает достаточно для полной характеристики функций распределения наработки до инцидента ИБ. Например, в довольно часто встречающихся случаях на практике, когда $f(t) - \lambda\, exp\{-\lambda t\}$ (экспоненциальное распределение), такие показатели как:

$$P(t) = exp\{-\lambda t\} \quad \text{и} \quad m_t = \bar{\tau} = \frac{1}{\lambda}$$

– несут исчерпывающую информацию о защищенности системы [4].

Анализ современных стандартов и нормативно-методических документов отечественных регуляторов в области ИБ [5] показывает, что Руководящие документы Гостехкомиссии (в настоящее время ФСТЭК) России, определяющие критерии для оценки механизмов защиты программно-технического уровня (в том числе показатели защищенности и совокупности описывающих их требований), используемые при анализе защищенности автоматизированных систем и средств вычислительной техники, не учитывают возрастающую сложность ИС, определяемые этими документами уровни защищенности не всегда отвечают современным требованиям, поэтому весьма актуальна проблема разработки методов, позволяющих обеспечить требуемые уровни показателей защищенности системы.

Литература

1. Хитов С.Б., Буйневич М.В. Система менеджмента информационной безопасности как инструмент управления рисками в системе распределенных ситуационных центров МЧС России // Сервис безопасности в России: опыт, проблемы, перспективы. Обеспечение безопасности при чрезвычайных ситуациях: материалы VII Междунар. науч.-практ. конф. СПб.: С.-Петерб. ун-т ГПС МЧС России, 2015. 200 с.

2. Еременко С.П., Хитов С.Б. Оценка результативности как важнейший аспект построения системы обеспечения информационной безопасности в системе распределенных ситуационных центров МЧС России // Науч.-аналит. журн. «Вестник С.-Петерб. ун-та ГПС МЧС России». 2016. № 2. С. 84–90.

3. Надёжность информационных систем: учеб. пособие / Ю.Ю. Громов [и др.]. Тамбов: Изд-во ГОУ ВПО ТГТУ, 2010. 160 с.

4. Рябинин И.А. Надежность и безопасность структурно-сложных систем. СПб.: Политехника, 2001.

5. Шубин А.Н. Оценка свойств информационных систем в стандартах по информационной безопасности // Известия Тульского гос. ун-та. Технические науки. 2013. № 3.

References

1. Khitov S.B., Buinevich M.V. Sistema menedzhmenta informacionnoj bezopasnosti kak instrument upravlenija riskami v sisteme raspredelennyh situacionnyh centrov MCHS Rossii // Servis bezopasnosti v Rossii: opyt, problemy, perspektivy. Obespechenie bezopasnosti pri chrezvychajnyh situacijah: materialy VII Mezhdunar. nauch.-prakt. konf. [Information security management system as the instrument of risk management in system of the distributed situational centers of Emercom of Russia. Security services in Russia: experience, problems, prospects. Ensuring the safety of emergency: materials of a VII Internat. scient.-pract. conf.]. St. Petersburg University of State Fire Service of EMERCOM of Russia, 2015. 200 p.

2. Eremenko S.P., Khitov S.B. Ocenka rezultativnosti kak vazhnejshij aspect postroeniya sistemy obespecheniya informacionnoj bezopasnosti v sisteme raspredelennyh situacionnyh centrov mchs rossii. [Productivity assessment as the most important aspect of creation of system of ensuring information security in system of the distributed situational centers of EMERCOM of Russia] // Vestnik S.-Peterb. un-ta GPS MCHS Rossii. 2016. № 2. (In Russ.).

3. Nadyozhnost informacionnyh system: uchebnoe-posobie [Reliability of information systems: manual] / Yu.Yu. Gromov, O.G. Ivanova, N.G. Mosyagina, K.A. Nabatov. Tambov: izd-vo GOU VPO TGTU, 2010. 160 p.

4. Ryabinin I.A. Nadezhnost i bezopasnost strukturno-slozhnyh system [Reliability and safety of structural and difficult systems]. SPb.: Politekhnika, 2001.

5. Shubin A.N. Ocenka svojstv informacionnyh system v standartah po-informacionnoj bezopasnosti [Evaluation of problems of information systems in standards for information security] // Izvestiya Tulskogo gos. un-ta. Tekhnicheskie nauki. 2013. № 3.