group, по некоторым оценкам, обошлась компании в 2 млн. долларов [1]. И это лишь один пример подобной системы [2].

Сегодня практически любая компания, которая сопровождает какой-либо программный продукт, нуждается в подобного рода системе. Конечно, не все компании могут позволить себе такое количество ресурсов на разработку подобной системы, поэтому существуют гораздо более простые, быстрые и дешёвые решения этой задачи [3].

В докладе также представлены некоторые существующие подходы к решению задачи поддержки пользователей информационных систем, оценены их преимущества и недостатки.

Существует задача организовать подсистему технической поддержки пользователей расчётно-платёжного комплекса «Абонент+» [4]. На сегодняшний день компоненты программного комплекса «Абонент+» используются в подавляющем большинстве ресурсоснабжающих и управляющих компаний ЖКХ Рязанской области, а некоторые компоненты используются и в других регионах Российской Федерации. Исходя из этого измерять потенциальную аудиторию пользователей разрабатываемой подсистемы можно тысячами человек.

В докладе представлен обзор существующих решений поддержки пользователей и на его основе поставлена задача на разработку подсистемы поддержки пользователей компонентов расчётно-платёжного комплекса «Абонент+».

Библиографический список

1. Голосовой помощник «Маруся» | Mail.ru group [Электронный ресурс]. URL: https://marusia.mail.ru/ (дата обращения 13.10.2022).

2. Создание голосовых помощников крупными IT-компаниями | Forbes [Электронный ресурс]. URL: https://www.forbes.ru/tehnologii/378035-bitva-za-9-mlrd-zachem-kompanii-odna-za-drugoy-vklyuchayutsya-v-voynu-boltalok (дата обращения 13.10.2022).

3. Какому бизнесу полезен голосовой бот | RUcenter [Электронный ресурс]. URL: https://www.nic.ru/info/blog/voice-bot/?ipartner=4444&adv_id=191121blog_usl_fz_but&utm_source=sbscr&utm_medium=but&utm_campaign=191121blog_usl_fz (дата обращения 13.10.2022).

4. Программный комплекс «Абонент+» | ООО «Абонент+» [Электронный ресурс]. URL: https://www.abonent.plus/ (дата обращения 13.10.2022).

ОЦЕНКА НАДЁЖНОСТИ ЭЛЕКТРОННЫХ СИСТЕМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: СОСТОЯНИЕ И ПРОБЛЕМЫ

А.А. Батура

Научный руководитель – Боровиков С.М., канд. техн. наук, доцент

Белорусский государственный университет информатики и радиоэлектроники

В настоящее время обеспечение информационной безопасности является весьма важной задачей для всех организаций, использующих

информационные технологии в своей деятельности (производственной, научной, управленческой, рекламной и т.д.). Для решения задач по обеспечению информационной безопасности организации применяют как специализированное программное обеспечение, так и технические средства. Используемые технические средства представляют собой системы обеспечения физической безопасности, обеспечивая контроль и доступ к информационным ресурсам уполномоченных специалистов и предотвращая несанкционированный доступ посторонних лиц. К надёжности таких технических систем предъявляются повышенные требования, поэтому в большинстве случаев системы обеспечения безопасности включают резервирование (избыточность) для увеличения вероятности выполнения важнейших функций, возлагаемых на системы.

На этапе проектирования систем для подтверждения обеспечения проектных требований к надёжности выполняют инженерный расчёт надёжности, пользуясь классическими методами [1–4], принимая обычно во внимание устойчивые отказы составных функциональных частей системы обеспечения безопасности. Известно [1], что для некоторых функциональных частей технических систем иногда могут возникать врѐменные отказы. Эти отказы согласно новому ГОСТ, устанавливающему термины и определения в области надёжности технических изделий, называют сбоями [5]. Сбой (en interruption) – это самоустраняющийся отказ или однократный отказ, устраняемый незначительным вмешательством оператора. Для электронных систем обеспечения безопасности, в отличии от других технических систем, сбои (временные отказы) являются принципиальными с точки зрения выполнения системой своих функций по защите объекта.

Причиной возникновения сбоев технических средств, входящих в состав электронных систем обеспечения безопасности, являются естественные и искусственные воздействия, которым подвергаются функциональные части систем. Примерами таких воздействий могут быть молнии, грозовые разряды, ураганный ветер, электромагнитные импульсы при включении мощных промышленных электрических установок, электромагнитные помехи по цепям электрического питания технических средств системы и т.д. Названные воздействия приводят к тому, что например, электронный датчик, находясь в технически исправном состоянии, кратковременно не выполнит свою функцию по обнаружению нарушителя, т.е. перейдёт в состояние неработоспособности, но после исчезновения воздействия восстановит своё работоспособное состояние без вмешательства обслуживающего персонала и выполнения ремонта. Либо второй пример. Электромагнитная помеха по цепи электрического питания микропроцессорного приёмно-контрольного устройства системы обеспечения безопасности может вызвать сбой в работе этого устройства, что приведёт к тому, что информация о несанкционированном проникновении, поступающая от датчиков, не будет воспринята, либо не будет правильно обработана. Но перезагрузка микропроцессорного устройства восстановит его работоспособное состояние.

Анализируя функционирование многих электронных систем обеспечения безопасности информационных ресурсов, и принимая во внимание

физическое окружение систем, особенно в условиях городской инфраструктуры, можно установить, что всегда имеет место соотношение

$$P_{\text{защ}} < R_{\text{ЭСБ}}, \quad (1)$$

где $P_{\text{защ}}$ – вероятность обеспечения электронной системой безопасности защиты информационных ресурсов от проникновения несанкционированных лиц; $R_{\text{ЭСБ}}$ – вероятность работоспособного состояния электронной системы безопасности в любой выбранный момент времени, найденная с учётом устойчивых отказов технических средств системы.

Поэтому актуальным является вопрос, как при оценке надёжности электронной системы безопасности, обеспечивающей защиту информационных ресурсов, учесть возможные сбои (временные отказы) функциональных частей системы и рассчитать показатель $P_{\text{защ}}$ соотношения (1), который более достоверно характеризует потенциальные возможности системы по защите информационных ресурсов в конкретных эксплуатационных условиях.

Для оценки эксплуатационной надёжности электронной системы безопасности предлагается в расчётах надёжности дополнительно использовать вероятности восприятия нарушителя датчиками системы и вероятности правильной обработки микропроцессорными устройствами (функциональными частями системы) сигналов, поступающих от датчиков или команд от приёмно-контрольных устройств. Причём эти вероятности должны учитывать факты возможного невосприятия нарушителя средствами обнаружения и факты возможной неправильной обработки микропроцессорными устройствами поступающей информации в случаях, когда функциональные устройства системы, будучи технически исправными, кратковременно теряют работоспособность из-за сбоя (временного отказа), вызываемого внешней эксплуатационной средой.

Библиографический список

1. Надёжность технических систем: справочник / Ю. К. Беляев и др.; под ред. И. А. Ушакова. – М.: Радио и связь, 1985. – 608 с.

2. Боровиков С. М., Цырельчук И.Н., Троян Ф.Д. Расчёт показателей надёжности радиоэлектронных средств: учебно-метод. пособие; под ред. С. М. Боровикова. – Минск: БГУИР, 2010. – 68 с.

3. Надёжность электрорадиоизделий, 2006: справочник / С. Ф. Прытков и др. – М.: ФГУП «22 ЦНИИИ МО РФ», 2008. – 641 с.

4. Reliability prediction of electronic equipment: Military Handbook MIL–HDBK-217F. – Washington: Department of defense DC 20301, 1995. – 205 p.

5. ГОСТ 27.002-2015. Межгосударственный стандарт. Надёжность в технике. Термины и определения. Дата введения – 01.03.2017. – М.: Стандартинформ, 2016. – 24 с.