DOI 10.37882/2223–2966.2022.01.32

АНАЛИЗ ПРОБЛЕМ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ КРИТИЧЕСКИХ ИНФОРМАЦИОННЫХ СИСТЕМ

ANALYSIS OF PROBLEMS OF COMPLEX SECURITY OF CRITICAL INFORMATION SYSTEMS

V. Simankov
A. Drilenko

Summary. Modern critical information systems are vulnerable to numerous internal and external influences, the article deals with the problem of such influences, the emphasis is placed on the study of the use of intelligent situational center in the analysis of security of critical information systems.

Keywords: intelligent situation center, critical information systems, analysis of security problems, security damage, structure of intelligent situation center.

Симанков Владимир Сергеевич
Д.т.н., профессор, Кубанский государственный технологический университет
vs@simankov.ru
Дриленко Александра Александровна
Аспирант, Кубанский государственный технологический университет
a.drilenko@russia.ms

Аннотация. Современные критические информационные системы являются уязвимыми для многочисленных внутренних и внешних воздействий, в статье рассматривается проблема таких воздействий, сделан акцент на изучение вопросов использования интеллектуального ситуационного центра при анализе безопасности критических информационных систем.

Ключевые слова: интеллектуальный ситуационный центр, критические информационные системы, анализ проблем безопасности, ущерб безопасности, структура интеллектуального ситуационного центра.

Критичные информационные системы являются классом информационных систем, обеспечивающих функционирование критичных систем управления. Критичность исследуемого класса информационных систем заключается в необходимости обеспечения стабильности их функционирования, которая является одним из основных показателей эффективности, поскольку полный или частичный отказ системы может привести к значительному экономическому, политическому, военному, экологическому, моральному или другому ущербу [1].

В соответствии с п. 8 статьи 2 Федерального закона № 187 к субъектам критической информационной инфраструктуры Российской Федерации относятся [3]:

Государственные органы, государственные учреждения, российские юридические лица, индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в 12 сферах деятельности.

Российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.

В стандартной терминологии нежелательное поведение информационных систем (включая компьютерные системы) называется отказом [2], который определяется как прекращение нормальной работы, а в международных стандартах — как прекращение способности выполнять требуемую функцию. Поэтому следует подчеркнуть, что изучение отказов начинается с определения уровня перехода от нормального функционирования системы к чрезвычайному.

Наука, которая в целом имеет дело с отказами (и, естественно, со средствами и методами, которые должны быть реализованы для их контроля), называется эксплуатационной безопасностью. Она включает в себя четыре дисциплины[6]: надежность (измеряется вероятностью безотказной работы системы в течение заданного периода времени), доступность (измеряется мгновенной вероятностью того, что система не выйдет из строя), ремонтопригодность (измеряется вероятностью возможности ремонта отказавшей системы в течение заданного периода времени) и безопасность.

Безопасность может быть определена неформализованным образом как способность системы не вызывать так называемых катастрофических событий (с точки зрения ущерба людям или имуществу) [4]. Она включает в себя два различных понятия, которые фор-

мируют понятие устойчивости (в отношении возможных катастрофических последствий):

- события внутри или вне системы, которые не являются действиями человека со злым умыслом;
- события внутри или вне системы, которые являются следствием действий человека с намерением причинить вред.

Термин «препятствия для эксплуатационной безопасности» используется для разграничения трех уровней: неисправности, ошибки и сбои.

Таким образом, в основе отказа может лежать ошибка (ошибочное состояние системы), которая сама является следствием неисправности. Поэтому теория надежности информационных систем развивается вокруг этих причинно-следственных цепочек: неисправности => ошибки => отказы (иногда сильно разветвленных из-за явления, известного как распространение ошибок). Важность различия между неисправностями и ошибками связана с тем, что неисправность может оставаться скрытой или «спящей» и не приводить к ошибке.

Типология причин отказов информационных систем может быть получена достаточно четко на основе классификации неисправностей, являющихся основной причиной отказа, по пяти критериям:

- причина: физическая или человеческая;
- характер: случайный, умышленный с намерением причинить вред, умышленный без намерения причинить вред;
- фаза создания неисправности: в разработке, в эксплуатации;
- ситуация по отношению к системе: внутренняя или внешняя;
- временная устойчивость: постоянная или временная.

Из рассмотренных существующих неисправностей [5], к которым относится текущая классификация, выделим основные и разделим их на три категории:

1. Случайные физические неисправности.
- внутренние при разработке (производственные дефекты);
- внутренние в процессе эксплуатации (отказы компонентов аппаратной поддержки);
- внешние факторы в процессе эксплуатации (нарушения в окружающей среде, например, радиация).
2. Случайная или преднамеренная ошибка человека без намерения причинить вред.
- разработка стажеров (например, «жучки»);
- внешние факторы в работе (ошибки оператора, часто называемые «человеческими ошибками»).
3. Противоправные действия человека с намерением причинить вред.
- внутренние при разработке (внутренние неисправности, намеренно внесенные разработчиком, как правило для того, чтобы создать слабое место, используемое позже в процессе эксплуатации, например, черный ход или логическая бомба);
- внутренние по действию (вирусы и черви, которые должны находиться внутри, хотя происхождение заражения обязательно внешнее);
- внешние в эксплуатации (вторжения всех других типов, использующих открытость системы для внешнего доступа).

Таким образом, комплексная безопасность — это способность системы избежать катастрофических событий после неисправностей первых двух категорий (включая случайные человеческие ошибки, разработка “безопасной” системы подразумевает методы контроля “ошибок” и анализ рисков человеческой ошибки при эксплуатации). Безопасность конфиденциальности — это способность избежать катастрофических событий в результате третьей категории неисправностей.

Неисправности, не связанные со злым умыслом человека

В этом разделе рассматривается классификация ошибок, приведенная выше, и описываются основные методы, используемые для того, чтобы неисправности, не связанные со злым умыслом человека, не приводили к катастрофическим отказам. Далее следует обзор основных методов обеспечения безопасности, которые также охватывают или могут быть расширены для охвата попыток злоумышленника.

Внутренние случайные физические неисправности при разработке

Внутренние случайные физические дефекты при разработке (производственные дефекты) в основном обеспечиваются контролем качества производства. Следует отметить, однако, что такая неисправность, преодолевшая этот барьер, может оставаться в спящем состоянии до тех пор, пока она не активируется в процессе эксплуатации (когда она вызывает ошибку).

Внутренние или внешние случайные физические неисправности в работе

Защита от внутренних или внешних случайных физических неисправностей в процессе эксплуатации является одной из основных тем безопасности, т.е. средств, которые должны быть реализованы для предотвращения любого поведения, которое может вызвать повреждения значительной тяжести в системе, которая

правильно спроектирована и изготовлена, но которая страдает в процессе эксплуатации от внутренних отказов ее электронных компонентов или от нарушений функционирования ее компонентов со стороны окружающей среды. Все методы обработки этих недостатков основаны на понятии избыточности.

Внутренняя случайная человеческая ошибка при разработке.

Внутренние случайные человеческие ошибки при разработке или баги определяются методологиями разработки, адаптированными к уровню критичности предполагаемого приложения. Именно для обработки такого рода неисправностей планируются мероприятия по верификации и валидации, которые могут быть самыми разнообразными (тесты, исчерпывающее моделирование, доказательства и т.д.). Для критических систем крайне важно, чтобы эта деятельность осуществлялась командой, полностью независимой от команды разработчиков (что не мешает последней проводить собственные тесты).

Внешняя случайная человеческая ошибка при эксплуатации.

Внешние случайные ошибки человека при эксплуатации являются привилегированной областью исследований интерфейса человек/технологическая система и затрагивает аспекты эргономики и когнитивной психологии. Эти аспекты, имеющие первостепенное значение для критических систем, где большинство инцидентов или крупных аварий связано с тем, что обычно называют "человеческой ошибкой", не являются объектом данной статьи, в которой предлагается показать, что некоторые методы обеспечения устойчивости к случайным неисправностям фактически охватывают или могут быть расширены для охвата человеческого злого умысла.

Неисправности, связанные со злым умыслом человека (киберпреступность, терроризм)

Описав основные методы покрытия случайных неисправностей, независимо от их происхождения (физического или человеческого), теперь опишем, как эти методы или их расширение могут покрыть определенные человеческие воздействия, например, злого умысла, что является проблемой киберпреступности или кибертерроризма.

Внутреннее вредоносное ПО в разработке

Проблема внутренних вредоносных программ в процессе разработки является чрезвычайно важной и, вероятно, недооцененной на сегодняшний день. Фрагмент вредоносного кода, внедренный в критически важное приложение одним из его злонамеренных разработчиков, независимо от его мотивации, представляет собой значительную уязвимость для критически важных систем, охват которых вряд ли очевиден. Более того, после тайного внедрения злоумышленниками, проникающими в команды разработчиков, "Логические бомбы", как их называют, могут лежать в спящем состоянии, ожидая секретного сигнала, который может быть послан позже (для любой системы, которая каким-то образом общается с внешним миром, для которой логическая бомба — это секретный черный ход).

Из всех описанных методов обеспечения отказоустойчивости очень немногие способны охватить этот тип внутреннего кибервредоносного ПО в командах разработчиков [6]. Резервирование разработки частично позволяет это сделать (при условии, что команды достаточно независимы и набираются таким образом, чтобы можно было с достаточной уверенностью исключить злонамеренное проникновение скоординированных элементов).

На практике наиболее эффективное покрытие связано с мероприятиями по верификации и валидации, которые, при условии исчерпывающего покрытия всех ветвей кода (критерий, часто используемый для так называемых тестов "белого ящика"), пройдут через фрагменты кода логической бомбы и обнаружат вредоносные функциональные возможности. Это ясно показывает абсолютную необходимость того, чтобы мероприятия по проверке и валидации проводились командой, независимой от команды разработчиков, независимой в плане набора персонала, чтобы исключить любые скоординированные действия одной команды, внедряющей логическую бомбу, и другой (соучастие через умышленное необнаружение), а также независимой в процессе составления спецификаций тестов.

Внутренняя недобросовестность в работе

Внутренние злонамеренные человеческие ошибки в работе (вирусы, черви, троянские кони и т.д.) в настоящее время не сильно влияют на критически важные системы, поскольку они менее открыты для внешнего мира, чем персональные компьютеры (практически все из которых в настоящее время подключены к Интернету), и поскольку операции по обслуживанию (такие как обновление программного обеспечения, установка и т.д.) регулируются строгими процедурами, выполняемыми квалифицированным персоналом. Распростра-

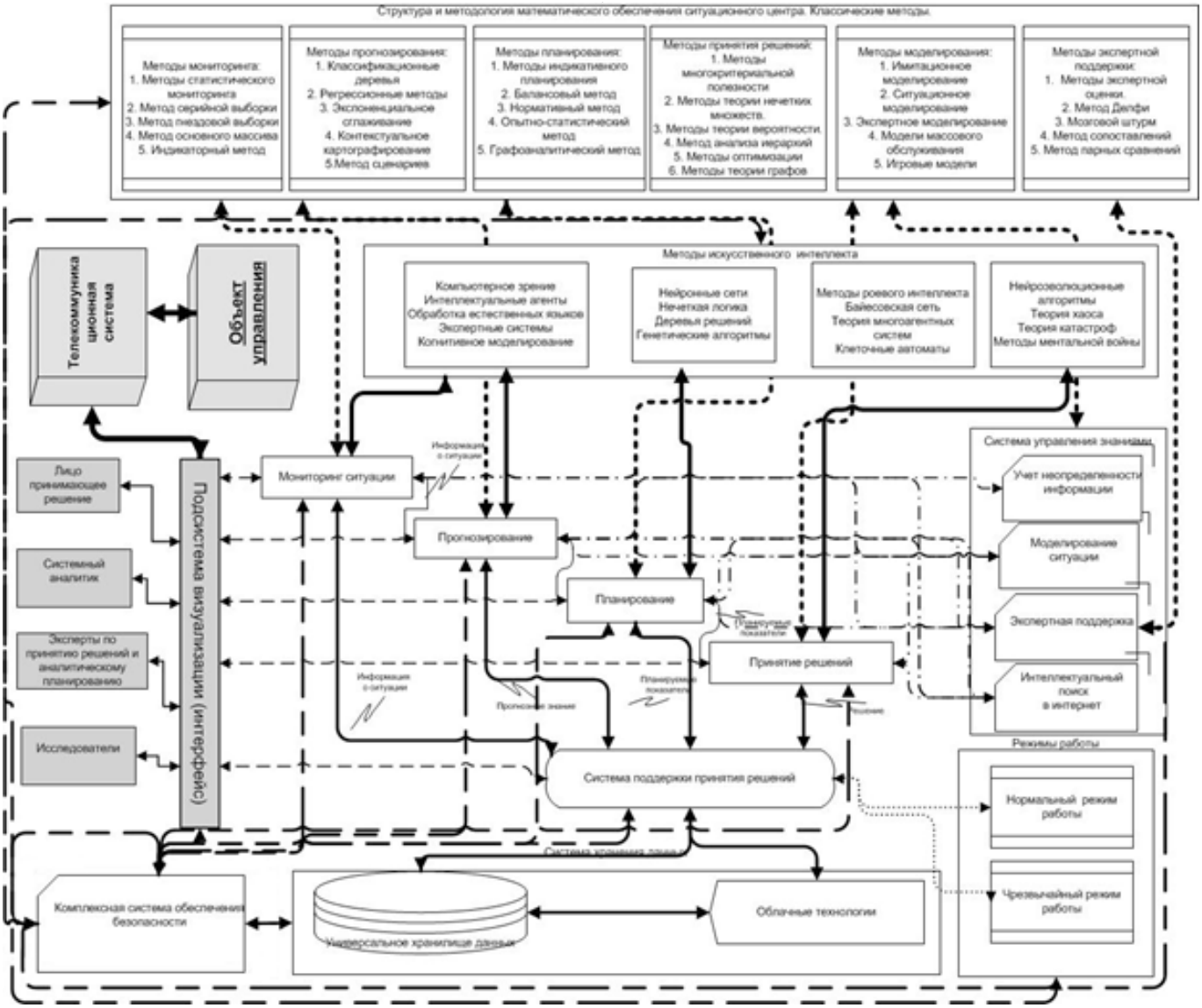

Рис. 1. Структура СЦ КИИ

нение вируса или червя в сетях персональных машин чаще всего является результатом приложений сомнительного происхождения (скачанных или полученных по электронной почте), которые пользователь выполняет или даже устанавливает. Такая уязвимость, которая приводит к процветанию антивирусной индустрии на персональных машинах, к счастью, не существует для критически важных систем, которые должны запускать только те приложения, для которых они были разработаны, и обслуживание которых тщательно организовано. Последний пункт представляется крайне важным в этом свете, поскольку киберпреступность, проникающая через обслуживающий персонал, является, после развивающейся киберпреступности, упомянутой выше, второй точкой входа для злоумышленных действий в отношении критически важных систем.

Внешние неисправности в процессе эксплуатации

Внешние злонамеренные действия при эксплуатации (вторжения всех типов, использующие коммуникации системы с внешним миром) составляют ядро проблемы киберпреступности и терроризма.

Критические системы, которые менее открыты для внешнего мира, в настоящее время в меньшей степени подвержены влиянию этих явлений, но ситуация быстро меняется.

Оценка комплексной безопасности критических информационных систем может эффективно осуществляться на базе интеллектуального ситуационного центра (Рисунок 1).

Это позволяет осуществлять использование такого центра для мониторинга, прогнозирования, планирования и принятия решений при управлении критическими информационными системами.

Заключение

Критические информационные системы (которые могут представлять опасность для людей или окружающей среды в случае несанкционированного использования ресурсов такой системы или выведения части системы из строя) должны быть спроектированы таким образом, чтобы предотвратить возникновение таких опасностей в результате событий, которые, за неимением лучшего термина, можно назвать "случайными", учитывая, что это понятие охватывает внутренние или внешние физические явления (которые в просторечии называются "сбои" и "нарушения" соответственно), а также человеческий фактор без намерения нанести вред при проектировании или эксплуатации.

Все критические разработки систем включают в себя средства для максимального нивелирования того, что в более строгом смысле называется "техническая ошибка с намерением причинить вред" используется для описания процесса сокрытия риска. Большинство используют техники, позволяющие достичь уровня "безопасности". Но в настоящее время критически важная система должна также интегрировать проблему устойчивости к возможным негативным факторам с намерением причинить вред.

Рассмотрены различные виды возможного воздействия и степень их охвата используемыми методиками, разработанными для обеспечения безопасности. Это показало степень сходства между двумя проблемами (освещение злонамеренных действий часто приводит к внедрению методов, разработанных для обеспечения безопасности, с большей строгостью или с некоторыми корректировками). Поэтому одновременное рассмотрение двух вопросов — безопасности и конфиденциальности — в общей концепции глобальной безопасности, безусловно, является будущим для критических систем.

Для мониторинга, прогнозирования, планирования и принятия решений при управлении критическими информационными системами может быть эффективным использование интеллектуального ситуационного центра.

[Исследование выполнено при финансовой поддержке РФФИ и администрации Краснодарского края в рамках научного проекта № 20–47–235003 «Разработка теоретических основ и алгоритмов функционирования адаптивных иерархических систем управления с использованием методов искусственного интеллекта на основе ситуационных центров»]

ЛИТЕРАТУРА

1. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Российская газета от 31.07.2017 — № 167 — с. 17.
2. Симанков В.С., Сундеев П.В. Системный анализ функциональной стабильности критичных информационных систем: Монография (научное издание) Кубан. гос. технол. ун-т; ин-т совр. технол. и экон. — Краснодар, 2004. — 204 с.
3. Симанков В.С., Власенко А.В., Черкасов А.Н. Методологическое обеспечение подсистемы обеспечения комплексной безопасности в составе интеллектуального ситуационного центра // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и Технические Науки. —2021 -№ 07. -С. 107–114.
4. Dubravka, C. (2017). Doing critical information systems research — arguments for a critical research methodology. European Journal of Information Systems, 1–7. Ссылка: https://www.tandfonline.com/doi/abs/10.1057/ejis.2010.67
5. ResearchGate [Электронный ресурс]. — Режим доступа: https://www.researchgate.net/publication/286493845_Information_Systems_Critical_Perspectives. — Дата доступа: 21.11.2021.
6. SSRN: Critical Theory in Information Systems: Where Is the South? [Электронный ресурс]. — Режим доступа: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3756357. — Дата доступа: 27.11.2021.

Журнал «Современная наука: актуальные проблемы теории и практики»