УДК 004.056.3

Методика обеспечения целостности информации в программно-аппаратных комплексах связи за счет рационального резервирования

Киселев Д. В., Семенов С. С., Петров О. В.

Постановка задачи: *возрастающая роль информации в системе управления и широкий круг воздействующих на нее угроз определяют актуальность вопросов обеспечения ее целостности. Целостность информации, составляющей информационное обеспечение программно-аппаратных комплексов связи, влияет на их надежность и готовность к применению по назначению. Известные подходы к обеспечению целостности информации, основанные на ее резервировании, находят широкое применение, однако не способны предложить рациональное решение противоречия между полнотой и частотой резервирования с одной стороны и ограниченностью ресурсов с другой.* ***Целью методики*** *является получение рекомендаций по организации резервного копирования информации и определению рациональной периодичности ее резервирования. Выполнение полученных рекомендаций позволит с заданной вероятностью в кратчайшие сроки восстановить потерянные/искаженные данные.* ***Новизна:*** *разработанная методика в отличие от известных подходов к резервированию информации предлагает обоснованные параметры резервирования, рассчитанные на основе требуемой вероятности обеспечения целостности с учетом имеющихся ограничений.* ***Результат:*** *представлена постановка задачи сокращения времени восстановления информации при нарушении ее целостности с целью повышения показателей надежности техники связи. Определена последовательность действий по обеспечению целостности информации путем ее заблаговременного резервирования и последующего восстановления. Процесс резервирования информации проанализирован и рассмотрен в совокупности трех событий, происходящих в случайные моменты времени: непосредственно резервирование, санкционированное изменение информации, реализация угрозы целостности. Разработана частная методика расчета рациональных параметров резервирования информации, выходные параметры которой могут использоваться как для настройки специального программного обеспечения по организации резервного копирования данных, так и для непосредственного «ручного» резервирования.* ***Практическая значимость****: представленное решение частной методики легло в основу программы для ЭВМ «Расчет рациональны параметров резервирования информации». Применение операторами или должностными лицами, эксплуатирующими и/или обслуживающими программно-аппаратные комплексы связи и средства вычислительной техники, данной методики совместно с разработанной программой позволяет получить научно-обоснованные параметры резервирования информации, а с их помощью сократить среднее время восстановления информации. Сокращение времени восстановления приводит к приросту значений показателей готовности техники на этапе эксплуатации.*

Ключевые слова: *программно-аппаратный комплекс связи, целостность информации, надежность, рациональное резервирование информации, периодичность резервирования, угроза целостности информации, отказ информационного обеспечения.*

Введение

Объемы информации, подлежащие формированию, обработке, хранению и передаче различными средствами связи и средствами вычислительной

Библиографическая ссылка на статью:
Киселев Д. В., Семенов С. С., Петров О. В. Методика обеспечения целостности информации в программно-аппаратных комплексах связи за счет рационального резервирования // Системы управления, связи и безопасности. 2019. № 1. С. 204-220. DOI: 10.24411/2410-9916-2019-10113

Reference for citation:
Kiselev D. V., Semenov S. S., Petrov O. V. Technique of ensuring the information integrity in software-hardware communication systems by rational backup. *Systems of Control, Communication and Security*, 2019, no. 1, pp. 204-220. DOI: 10.24411/2410-9916-2019-10113 (in Russian).

техники неизменно растут. Динамичность событий и окружающей обстановки приводят к быстрому «устареванию» информации, что сокращает срок ее изменения для поддержания в актуальном состоянии. В работе [1] рассмотрен обширный круг угроз, в результате реализации которых обрабатываемые (хранимые, передаваемые) данные могут быть искажены или даже потеряны. В совокупности указанные факты определяют актуальность обеспечения целостности информации. Под целостностью информации понимается такое ее состояние, при котором любое изменение информации отсутствует либо выполняется преднамеренно уполномоченными на это субъектами.

Современные программно-аппаратные комплексы связи военного назначения (ПАКС) наряду с аппаратными средствами имеют в своем составе программное обеспечение (ПО) и информационное обеспечение (ИО) [2, 3]. Помимо семантической информации важно сохранить информацию, составляющую ИО ПАКС, так как она существенно влияет на надежность и готовность комплексов [4]. Согласно [5] наиболее приемлемым показателем надежности ПАКС является его стационарный коэффициент готовности K_{Γ}, который определяется как

$$K_{\Gamma} = \frac{T_0}{T_0 + T_{\text{В}}}, \tag{1}$$

где: T_0 – средняя наработка до отказа; $T_{\text{В}}$ – среднее время восстановления.

Из выражения (1) видно, что для повышения коэффициента готовности K_{Γ} требуется либо увеличивать среднюю наработку до отказа T_0, либо сокращать среднее время восстановления $T_{\text{В}}$. В настоящее время методы повышения средней наработки до отказа на этапе эксплуатации отсутствуют. Повышения эксплуатационной готовности техники связи (ТС) целесообразно добиваться путем сокращения среднего времени восстановления. Для ПАКС среднее время восстановления $T_{\text{В}}$ зависит от среднего времени восстановления той составной части, в которой произошел отказ:

$$T_{\text{В}} = f(T_{\text{восст АС}}, T_{\text{восст ПО}}, T_{\text{восст ИО}}), \tag{2}$$

где $T_{\text{восст АС}}$, $T_{\text{восст ПО}}$, $T_{\text{восст ИО}}$ – среднее время восстановления при отказах аппаратных средств, ПО и ИО соответственно.

Среднее время восстановления ПАКС $T_{\text{В}}$ из функциональной зависимости (2) пропорционально среднему времени восстановления информации при отказе ИО $T_{\text{восст ИО}}$. Таким образом, учитывая при расчете коэффициента готовности ПАКС отказы ИО (под которыми понимаются нарушения целостности информации, приводящие к функциональному отказу [1, 2, 6]), следует сокращать среднее время восстановления целостности информации, составляющей ИО ПАКС:

$$T_{\text{восст ИО}} \to \min_{\Theta}. \tag{3}$$

Критерий (3) дает возможность сформировать вектор параметров восстановления целостности информации, при котором показатель надежности имеет максимальное значение в соответствующей области ограничений (Θ). В работах [1, 4] показано, что основным способом обеспечения целостности информации является информационное резервирование.

Таким образом, задача обеспечения целостности информации может быть решена осуществлением информационного резервирования. При этом следует определить область имеющихся ограничений (Θ) и найти в этой области решение в виде вектора параметров: рациональной периодичности резервирования, вида резервирования, способа и места хранения резервных копий.

Постановка задачи на разработку методики обеспечения целостности информации в программно-аппаратных комплексах связи

Методика представляет выбранную совокупность способов и приёмов обеспечения целостности информации в ПАКС за счет рационального резервирования.

Постановка задачи на разработку методики включает:

1) назначение, область применения и цель решения задачи;
2) сущность задачи;
3) формализованное описание задачи, расчленение на подзадачи;
4) исходные и выходные данные;
5) принятые допущения и ограничения;
6) ожидаемые результаты от использования методики.

Методика обеспечения целостности информации в ПАКС подлежит разработке в интересах должностных лиц, эксплуатирующих ТС и автоматизированные системы управления (АСУ), и предназначена для решения следующих задач:

- определение рациональных значений параметров резервного копирования информации, таких как периодичность и вид резервирования, места хранения резервных копий;
- восстановление информации из резервных копий при нарушении ее целостности;
- сокращение среднего времени восстановления при отказах ИО и повышение показателей готовности ПАКС.

Основной целью методики является разработка рекомендаций по организации резервного копирования информации и/или определению рациональных параметров для настройки специального ПО, предназначенного для резервного копирования информации. Причем выполнение полученных рекомендаций в условиях, соответствующих исходным данным, должно обеспечить целостность информации с требуемой вероятностью.

Сущность методики концептуально представлена на рис. 1 и заключается в следующем. В процессе эксплуатации формируется и периодически обновляется информация, составляющая ИО ПАКС. К такой информации могут относиться базы данных с системами управления, файловые структуры с каталогами и системами управления, данные-результаты выполнения одних программ, являющиеся входной информацией для других, различные конфигурационные, системные файлы и прочее. Помимо изменения информации, обусловленного умышленными действиями оператора в соответствии с целями и задачами применения ПАКС по назначению, на нее оказывает воздействие множество факторов, представляющих угрозу целостности информации [1]. Для повышения

эксплуатационной надежности ПАКС применяется метод информационного резервирования. Резервирование должно выполняться таким образом, чтобы к моменту времени реализации любого из факторов, нарушающих целостность информации, с требуемой вероятностью имелась ее резервная копия, позволяющая в минимальные сроки осуществить восстановление. На основе учета условий эксплуатации, закона распределения и его характеристик, согласно которому происходят отказы ИО, имеющихся ограничений на ресурсы (вычислительные, людские, временные, материальные), требуемой вероятности обеспечения целостности информации определяются рациональные параметры информационного резервирования, которые служат выходными данными разрабатываемой методики.

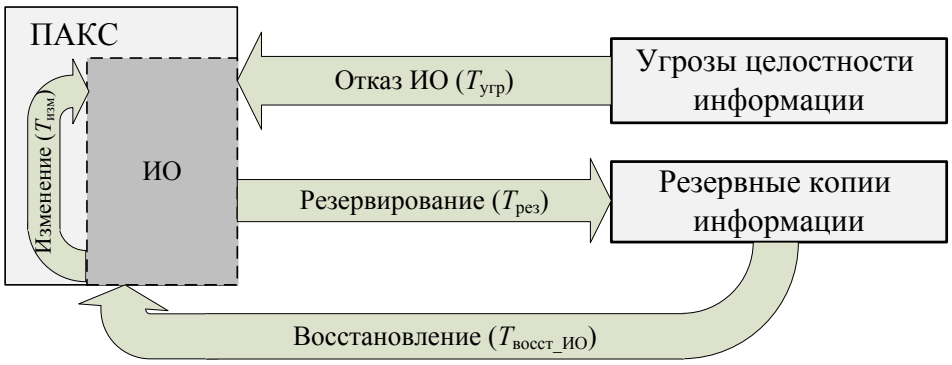

Рис. 1. Концептуальное представление методики обеспечения целостности информации

Формализованное описание задачи имеет следующий вид. Пусть имеется ПАКС с объемом информации $V_{инф}$, составляющей его ИО, и целостность которой критична для работоспособного состояния. Эта информация периодически изменяется уполномоченным должностным лицом (оператором), время изменения $T_{изм}$ является случайной величиной и фактически определяется предназначением изделия и режимом его работы. Будем считать, что значение периодичности санкционированных изменений $t_{изм}$ подчинено нормальному закону распределения с параметрами средней периодичности изменений $T_{изм.ИО}$ и средним квадратическим отклонением $\sigma_{изм.ИО}$. Плотность распределения вероятностей для нормального закона описывается выражением [7]:

$$f(t_{изм}) = \frac{1}{\sigma_{изм.ИО} \cdot \sqrt{2\pi}} e^{\frac{(t_{изм} - T_{изм.ИО})^2}{2 \cdot \sigma_{изм.ИО}^2}}. \quad (4)$$

Строго математически согласно (4) значение $t_{изм}$ может быть отрицательным (рис. 2), однако в расчетах данной методики предполагается время до очередного обновления информации, т.е. еще не наступившего события. В таком случае отрицательное значение $t_{изм}$ лишено физического смысла. Т.к. область возможных значений $t_{изм} \in (0; \infty)$, то распределение будет представлять усеченное нормальное с плотностью

$$f_{\text{у}}(t_{\text{изм}}) = \begin{cases} \dfrac{k}{\sigma_{\text{изм.ИО}} \cdot \sqrt{2\pi}} e^{\frac{(t_{\text{изм}} - T_{\text{изм.ИО}})^2}{2 \cdot \sigma_{\text{изм.ИО}}^2}}, & \text{при } t_{\text{изм}} > 0, \\ 0, \quad \text{при } t_{\text{изм}} \le 0 \end{cases} \tag{5}$$

где $k = F(\infty) - F(0) = 1 - \int_{-\infty}^{0} f(t_{\text{изм}})\, dt_{\text{изм}}$ – коэффициент усечения.

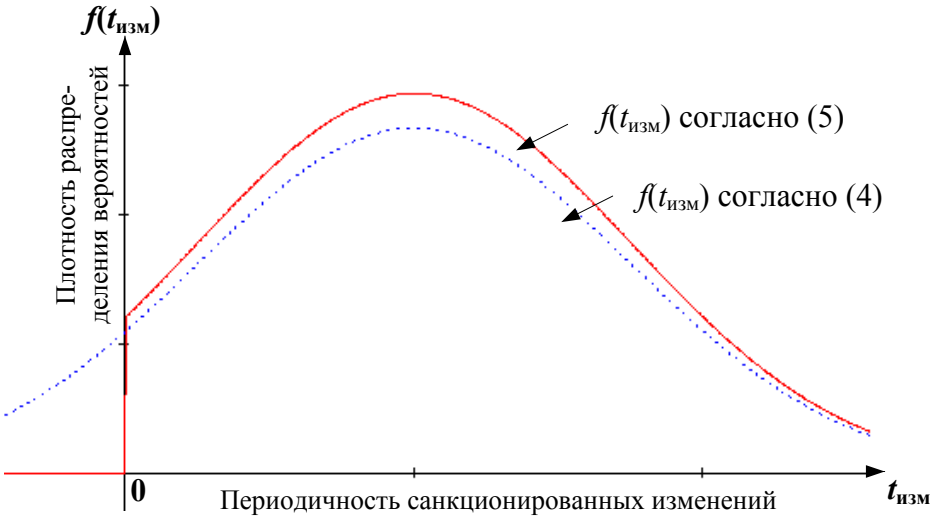

Рис. 2. Графики плотности распределения случайной величины периодичности санкционированных изменений для нормального и усеченного нормального законов

На целостность информации оказывает воздействие множество внешних и внутренних факторов, представляющих угрозу целостности информации $Y = \left\{ y_i \mid i = \overline{1, N_{\text{угр}}} \right\}$, где $N_{\text{угр}}$ – количество факторов возможных угроз. В результате реализации любой из угроз ИО будет повреждено, целостность информации и работоспособность комплекса нарушены. Т.к. проявление какого-либо фактора к моменту времени t является случайным событием, обозначим случайной величиной $T_{\text{угр}\,i}$ – время до реализации угрозы целостности информации i-ого фактора. Если потоки угроз i-ого фактора простейшие, то интенсивность угроз i-ого фактора $\lambda_{\text{угр}\,i} = 1 / T_{\text{угр}\,i}$. Суммарный поток угроз также является простейшим [7], интенсивность суммарного потока угроз $\lambda_{\text{угр}}$ и среднее время до реализации любой из угроз $T_{\text{угр}}$:

$$\lambda_{\text{угр}} = \sum_{i=1}^{N_{\text{угр}}} \lambda_{\text{угр}\,i} = \sum_{i=1}^{N_{\text{угр}}} T_{\text{угр}\,i}^{-1},$$

$$T_{\text{угр}} = \lambda_{\text{угр}}^{-1} = \frac{1}{\sum_{i=1}^{N_{\text{угр}}} T_{\text{угр}\,i}^{-1}}.$$

Допущение о простейшем потоке угроз при рассмотрении моделей надежности и безопасности является широко распространенным и применяется при решении большого количества задач [6, 8, 9]. Оно подразумевает, что поток отказов является стационарным, ординарным и без последействия.

В настоящее время в соответствии с действующими нормативными и руководящими документами в части технического обеспечения связи (ТОС) [10, 11, 12] не предусмотрен учет статистики отказов ИО ТС (в т.ч. ПАКС) и причин их возникновения, тем более отдельно по видам угроз целостности информации, в результате реализации которых эти отказы возникли. Известно [13], что использование в научно-методическом аппарате неадекватных исходных данных влечет получение неадекватных результатов. Отсутствие накопленных статистических данных и сложность получения адекватных и достоверных сведений об интенсивности угроз целостности информации *i*-го фактора делает нецелесообразным построение методики на основе исходных данных об интенсивности угроз отдельных факторов $\lambda_{угр\,i}$. На современном этапе развития системы ТОС и ее нормативно-правового регулирования целесообразно разрабатывать методический аппарат на основе эмпирических данных об интенсивности суммарного потока угроз $\lambda_{угр}$ или о среднем времени до реализации любой из угроз $T_{угр}$.

Исходные данные разрабатываемой методики обеспечения целостности информации представлены в таблице 1.

Таблица 1 – Исходные данные методики обеспечения целостности информации в ПАКС

№ п/п	Наименование исходных данных	Обозначение
1	Среднее время до реализации угрозы целостности информации	$T_{угр}$
2	Требуемая вероятность обеспечения целостности информации	$P_{треб}$
3	Объем информации	$V_{инф}$
4	Доступный объем памяти для резервирования	$V_{доп}$
5	Сведения о частоте изменения информации	
5.1	Наличие достоверной информации о факте изменения информации ИО в момент времени *t* по отношению к моменту последнего резервирования	$I_{изм}(t)$
	или	
5.2	Параметры закона распределения времени до очередного изменения информации	($T_{изм}$, $\sigma_{изм}$)

Выходными данными методики будут параметры согласно таблице 2.

Таблица 2 – Выходные данные методики обеспечения целостности информации в ПАКС

№ п/п	Наименование выходных данных	Обозначение
1	Время до очередного резервного копирования (периодичность резервирования)	$t_{рез}$
2	Вид резервного копирования	$w \in W=\{w_i \mid i=0..2\}$
3	Место хранения резервных копий	$m \in M=\{m_j \mid j=0..4\}$

Определение вида резервного копирования *w* предполагается из следующего множества $W = \{w_i \mid i=0..2\}$ доступных вариантов [14]: w_0 – полное ре-

зервное копирование; w_1 – инкрементное резервное копирование; w_2 – дифференциальное резервное копирование.

Выбор места хранения резервных копий m осуществляется из множества $M = \{m_j \mid j=0..4\}$, где m_0 – жесткий магнитный диск (HDD); m_1 – компакт-диск (CD); m_2 – цифровой многоцелевой диск (DVD); m_3 – USB-флеш-накопитель; m_4 – сетевое хранилище.

Основные допущения и ограничения методики в основном определяются допущениями и ограничениями, принятыми в модели эксплуатации ПАКС [3], т.к. предназначена для применения именно на этой стадии жизненного цикла. Кроме того, если сведения о факте изменения информации ИО $I_{изм}(t)$ в момент времени t отсутствует, то предполагается, что изменение ИО осуществляется по нормальному закону (в качестве исходных данных задан п. 5.2 вместо п. 5.1 таблицы 1).

Предполагается, что применение разрабатываемой методики обеспечит возможность скорейшего восстановления поврежденной/потерянной информации в ПАКС и повысит их эксплуатационную готовность к применению по назначению путем устранения отказов ИО.

Методика обеспечения целостности информации в программно-аппаратных комплексах связи за счет рационального резервирования

Исходя из целей, задач и сущности разрабатываемой методики для повышения эксплуатационной готовности ПАКС она должна применяться на протяжении всего этапа эксплуатации к каждому отдельному образцу техники (ПАКС, ЭВМ). Можно выделить пять основных шагов методики на этом этапе (рис. 3). Шаги следующие.

Шаг 1. Внедрение, начало использования методики. Характеризуется выполнением первого полного резервного копирования (блок 1.2), т.к. предполагается, что до начала применения методики резервирования информации не выполнялось. Если на момент внедрения методики «пользовательская» информация еще не внесена, т.е. ИО не сформировано и данные для резервирования отсутствуют (блок 1.1), то данный шаг проходит номинально.

Шаг 2. Расчет параметров резервирования (блок 2.1). Наиболее важный этап всей методики, от выполнения которого в значительной степени определяется эффективность ее применения в целом. На основе исходных данных и имеющихся ограничений рассчитываются выходные параметры, в соответствии с которыми впоследствии выполняется резервирование и, при необходимости (в случае отказа ИО), восстановление. В рамках обобщенного, концептуального описания обозначим данную процедуру как частную методику расчета рациональных параметров резервирования. Следует отметить, что в настоящее время существует немало программных продуктов, различных сервисов и фирм, которые способны выполнять резервное копирование в фоновом режиме и/или по расписанию. К ним, например, относятся: Clonezilla, Acronis, Paragon Backup&Recovery, EASEUS Todo Backup, DriveImage XML, FBackup, Veritas NET Backup Interprise Server и др. В случае использования какого-либо вспомога-

тельного ПО для резервирования (блок 2.2) осуществляется его настройка согласно полученным из частной методики параметрам (блок 2.3).

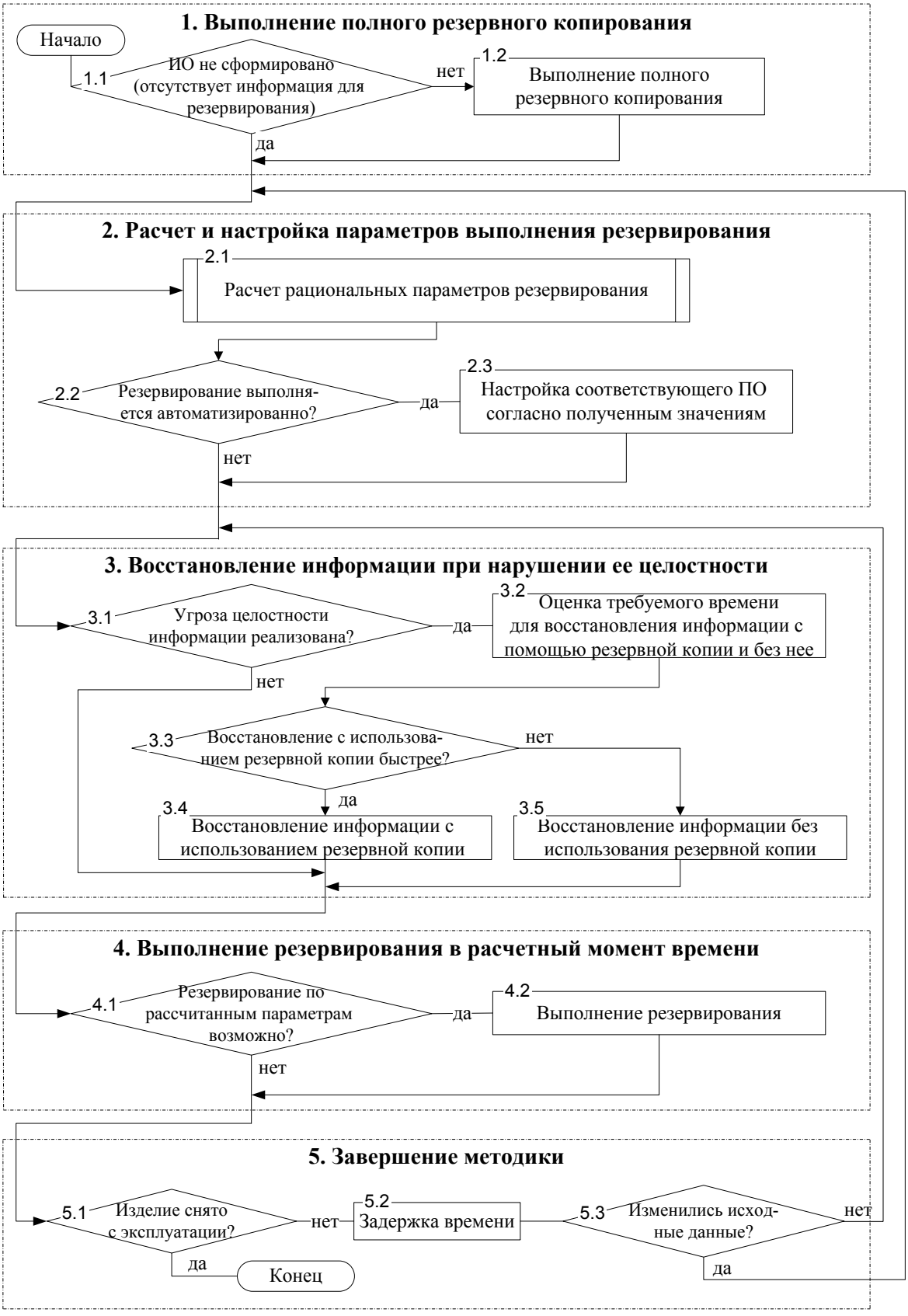

Рис. 3. Схема применения методики обеспечения целостности

Шаг 3. Восстановление информации. В случае реализации угрозы целостности информации, когда отказ ИО наступил (блок 3.1), осуществляется восстановление данных. Процессу восстановления предшествует оценка требуемых времени на восстановление информации с помощью резервной(ых) копии(й) $t_{\text{восст ИО | рез}}$ и времени на восстановление без резерва $t_{\text{восст ИО | б/р}}$ (блок 3.2).

Если условие

$$t_{\text{восст ИО | рез}} < t_{\text{восст ИО | б/р}}$$

выполняется (блок 3.3), то восстановление данных осуществляется из ранее подготовленной(ых) резервной(ых) копии(й) (блок 3.4). В противном случае восстановление выполняется «вручную» (блок 3.5). При этом текущее значение времени восстановления при отказе ИО $t_{\text{восст ИО}}$ окажется равным меньшему из двух значений:

$$t_{\text{восст ИО}} = \begin{cases} t_{\text{восст ИО | рез}}, & \text{при } t_{\text{восст ИО | рез}} < t_{\text{восст ИО | б/р}} \\ t_{\text{восст ИО | б/р}}, & \text{при } t_{\text{восст ИО | рез}} \geq t_{\text{восст ИО | б/р}} \end{cases}.$$

При прочих равных условиях выполнение на данном шаге указанной проверки позволяет минимизировать среднее время восстановления при отказе ИО $T_{\text{восст ИО}}$.

Шаг 4. Выполнение резервирования. Оно осуществляется (блок 4.2) в расчетный момент времени согласно параметрам, полученным на шаге 2. Если выполнить резервирование оказывается невозможным по различным причинам (изменение исходных данных, появление новых ограничений пр.) (блок 4.1), то осуществляется переход к шагу 2 и вызов частной методики расчета.

Шаг 5. Завершение применения методики. Применение методики относится к конкретному образцу и прекращается при снятии ПАКС с эксплуатации (утилизация, отправка в ремонт, передача в другую организацию или воинскую часть и т.д.). Если условия для прекращения не наступили (блок 5.1), то в зависимости от состояния исходных данных (блок 5.3) выполняется переход к действиям на шаге 2 или 3. Условно обозначенный элемент «задержка времени» (блок 5.2) подчеркивает динамику реализации методики и по сути определяет длительность шага по факту наступления любого из событий – изменение исходных данных, отказ ИО, наступление расчетного времени резервирования, снятие с эксплуатации и т.п.

Видно, что шаги 2, 3 и 4 выполняются циклически в течение всего срока эксплуатации комплекса. Таким образом, именно это и позволяет обеспечить возможность сокращения среднего времени восстановления при отказе ИО $T_{\text{восст ИО}}$.

Частная методика расчета рациональных параметров резервирования информации

Как видно из постановки задачи на разработку методики и обобщенной схемы ее применения (см. рис. 3), «на выходе» частной методики расчета рациональных параметров резервирования информации должны быть получены значения (варианты) периодичности, вида резервного копирования и мест хранения копий.

№1. 2019
ISSN 2410-9916

Рациональная периодичность резервирования информации, т.е. моменты времени, когда необходимо выполнять очередное копирование, зависит от двух событий: наступления какой-либо угрозы целостности и осуществления изменения информации уполномоченными операторами. Оба этих событий является случайными, а время их наступления – случайной величиной.

Рассматривая возможные варианты последовательности наступления трех событий – выполнение резервирования через время $t_{рез}$, реализация угрозы целостности через время $t_{угр}$ и изменение информации через время $t_{изм}$, получаем $3! = 6$ комбинаций (рис. 4). Рассмотрение одновременного наступления пары и тем более тройки событий лишено смысла вследствие, во-первых, пренебрежимо малой вероятности и, во-вторых, наличия гипотетической возможности посчитать одно событие произошедшим раньше другого.

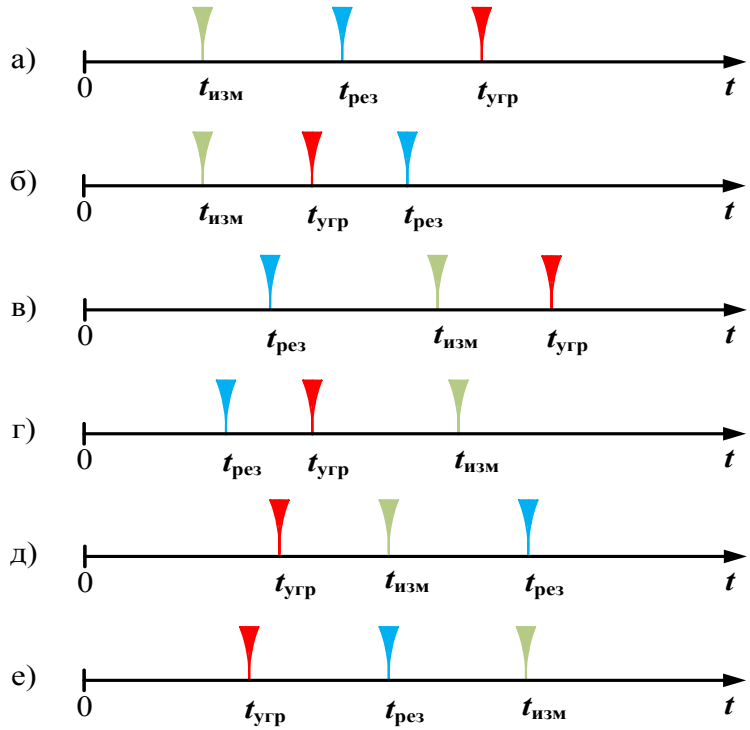

Рис. 4. Временные диаграммы, отражающие возможные варианты последовательностей наступления событий резервирования, реализации угрозы и изменения информации

Выводы из анализа представленных на рис. 4 временных диаграмм следующие. Необходимо стремиться к ситуации, чтобы резервирование выполнялось после внесения изменений, но строго до реализации угрозы, т.е. $t_{изм}<t_{рез}<t_{угр}$ (рис. 4 а). Допустимым является вариант, когда угроза реализована раньше, чем внесены изменения, а после их внесения выполнено резервирование ($t_{угр}<t_{изм}<t_{рез}$ – рис. 4 д).

Худшими случаями являются ситуации, когда нарушение целостности произошло после внесения изменений в ИО, актуальные резервные копии при этом отсутствуют (рис. 4 б, в), что влечет потерю информации (или какой-то ее доли) без возможности последующего оперативного восстановления. Случаи, когда $t_{угр}<t_{рез}<t_{изм}$ (рис. 4 е) опасны тем, что в архив могут попасть уже повре-

DOI: 10.24411/2410-9916-2019-10113
URL: https://sccs.intelgr.com/archive/2019-01/13-Kiselev.pdf

жденные данные и резервная копия будет с ошибками, что недопустимо. Вариант $t_{рез}<t_{угр}<t_{изм}$ (рис. 4 г) менее опасен, но нежелателен, т.к. требует излишних расходов ресурсов (памяти, времени, сил) на копирование «старой» информации (предполагается, что такая версия копии уже имеется).

Обобщенная блок-схема последовательности действий по расчету рациональных параметров резервирования, которые и составляют частную методику, представлена на рис. 5.

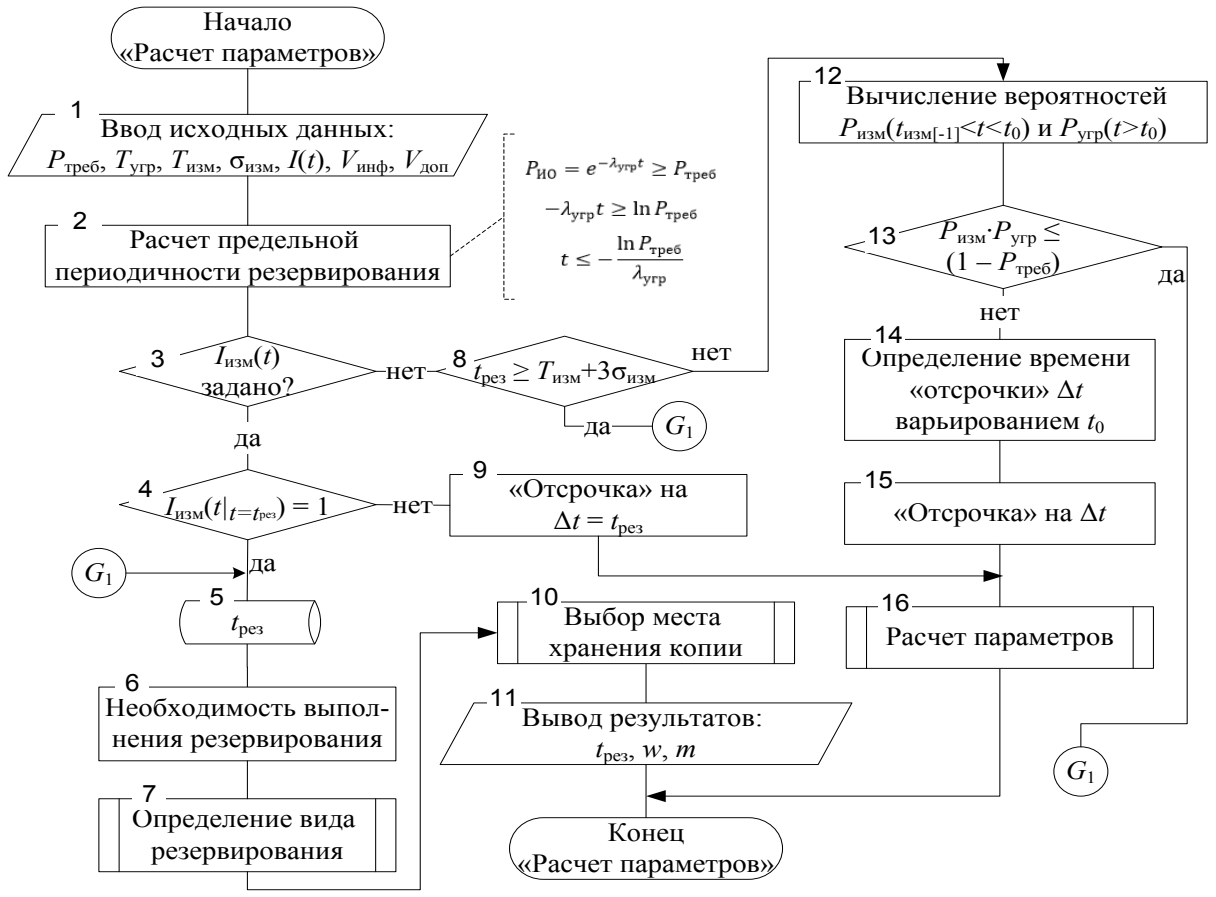

Рис. 5. Блок-схема частной методики расчета рациональных параметров резервирования информации

В блоке 1 задаются исходные данные, необходимые для расчета.

Полагая, что время до реализации угроз целостности информации $T_{ИО}$, являясь случайной величиной, описывается экспоненциальным законом распределения с параметром среднего времени $T_{угр}$, вероятность «безотказной с точки зрения отказов ИО» работы $P_{ИО}(t)$ определяется:

$$P_{ИО}(t) = P(T_{ИО} > t) = e^{-\lambda_{угр}t} = e^{\frac{-t}{T_{угр}}}.$$

Исходя из требуемого условия обеспечения целостности информации с требуемой вероятностью

$$P_{ИО}(t) = e^{\frac{-t}{T_{угр}}} \geq P_{треб}$$

находим время

$$-\frac{t}{T_{\text{угр}}} \geq \ln P_{\text{треб}},$$

$$t = t_{\text{рез}} \leq -T_{\text{угр}} \cdot \ln P_{\text{треб}}. \quad (6)$$

Значение времени $t_{\text{рез}}$ (блок 2), вычисленное согласно выражению (6), является верхним пределом, ограничивающим максимальную периодичность создания резервной копии информации для последующего ее восстановления при нарушении целостности с требуемой вероятностью. Соблюдая условие (6), с вероятностью $P_{\text{треб}}$ исключены ситуации, представленные на рис. 4 б, д, е.

Исключение ситуаций, когда к рассчитанному по (6) моменту времени измененная информация, подлежащая резервированию, отсутствует (рис. 4 в, г), зависит от характера сведений об изменении информации операторами – детерминированного или вероятностного, т.е. от способа задания исходных данных (блок 3). В первом случае (п. 5.1 исходных данных таблицы 1) подразумевается, что располагаем достоверными сведениями $I_{\text{изм}}(t)$ о наличии или отсутствии изменений в данных за период $(t_{\text{рез}[-1]}; t)$, т.е. с момента предыдущего резервирования $t_{\text{рез}[-1]}$. Формат таких сведений имеет следующий вид:

$$I_{\text{изм}}(t) = \begin{cases} 1, & \text{если } t_{\text{рез}[-1]} < t_{\text{изм}} < t \\ 0, & \text{при } (t_{\text{изм}} < t_{\text{рез}[-1]}) \,\text{OR}\, (t_{\text{изм}} > t) \end{cases}.$$

Если изменения в указанном периоде были, т.е. $I_{\text{изм}}(t) = 1$ (блок 4), то полученное значение $t_{\text{рез}}$ фиксируется (блок 5). Очередное резервирование в момент времени $t_{\text{рез}}$ необходимо выполнить (блок 6). В противном случае вернуться к резервированию через время $\Delta t = t_{\text{рез}}$ (блок 9). Такая «отсрочка» в выполнении резервирования не приведет к превышению вероятности отказа ИО за время Δt над требуемой вероятностью обеспечения целостности информации и обоснована принятым допущением об экспоненциальном законе потока угроз.

Когда сведения о фактах и времени изменения ИО отсутствуют, приходится учитывать вероятностный характер внесения уполномоченными операторами санкционированных изменений информации, предполагая, что изменение информации аппроксимируется нормальным законом распределения с параметрами $T_{\text{изм}}$ и $\sigma_{\text{изм}}$ (п. 5.2 исходных данных таблицы 1).

Воспользовавшись правилом трех сигм [7], согласно которому значение случайной величины периодичности изменения информации $t_{\text{изм}}$ практически не превышает ее отклонения от среднего значения $T_{\text{изм}}$ на величину $3\sigma_{\text{изм}}$, получим, что при выполнении условия (блок 8)

$$t_{\text{рез}} \geq t_{\text{изм}} = T_{\text{изм}} + 3\sigma_{\text{изм}} \quad (7)$$

изменения осуществляются чаще, чем расчетное по (6) значение $t_{\text{рез}}$ и выполнение копирования необходимо.

Если (7) не выполняется, то к рассчитанному согласно (4) моменту времени $t_0 = t_{\text{рез}}$ какие-либо новые изменения могут быть еще не внесены. Чтобы не допустить излишнего копирования при отсутствии изменений (и исключить варианты согласно временным диаграммам на рис. 4 в, е), вычисляется вероятность того, что к моменту времени t_0 изменения были внесены (блок 12)

$$P_{\text{изм}}(t_{\text{изм}[-1]} < t < t_0) = F(t_0) - F(t_{\text{изм}[-1]}), \quad (8)$$

а нарушений целостности информации не произошло (отказы ИО к моменту времени t_0 отсутствуют)

$$P_{\text{угр}}(t_{\text{угр}} > t_0) = 1 - P(t_{\text{угр}} < t_0) = 1 - P_{\text{ИО}}(t_0). \quad (9)$$

Вероятность наступления двух независимых событий равна произведению вероятностей каждого из них. Так, если вероятность наступления событий (8) и (9) меньше допустимой вероятности потери информации $P_{\text{пот}} = 1 - P_{\text{треб}}$, то есть условие (блок 13)

$$P_{\text{изм}} \cdot P_{\text{угр}} \le 1 - P_{\text{треб}} \quad (10)$$

не выполняется, то выполнение очередного резервирования возможно отложить на время Δt (блок 15), которое определяется варьированием момента времени резервирования t_0 до выполнения условия (10) (блок 14). По истечении времени Δt процедура расчета рациональных параметров резервирования повторяется (блок 16).

В блоках 7 и 10 определяется вид резервирования и выбирается место хранения резервных копий соответственно. На заключительном шаге частной методики расчета осуществляется вывод полученных параметры резервирования (блок 11).

Представленная частная методика расчета рациональных параметров резервирования лежит в основе второго шага методики обеспечения целостности информации в ПАКС. Для удобства практического применения она реализована в качестве программы для ЭВМ [15].

Выводы

Восстановление информации, составляющей ИО ПАКС, в результате нарушения ее целостности рассмотрено как составная часть процесса восстановления работоспособного состояния комплекса. Сокращение времени восстановления приводит к повышению показателей надежности, а минимизация среднего времени восстановления при отказах ИО при прочих равных условиях максимизирует коэффициент готовности.

Обеспечение целостности информации в целях повышения эксплуатационных показателей надежности и готовности основывается на скорейшем ее восстановлении при повреждении. Сформулирована постановка задачи на разработку методики, которая с учетом принятых ограничений и допущений в течение всего этапа эксплуатации ПАКС позволяет рационально выполнять резервирование информации и оперативно ее восстанавливать при нарушении целостности. Разработанная на основе поставленной задачи методика обеспечения целостности за счет рационального резервирования содержит частную методику расчета, которая формирует набор рациональных параметров резервирования.

Таким образом, разработанная методика в отличие от известных подходов к резервированию информации предлагает обоснованные параметры резервирования, рассчитанные на основе требуемой вероятности обеспечения целостности с учетом имеющихся ограничений.

Литература

1. Киселев Д. В., Семенов С. С., Седличенко В. Г. Проблемные вопросы обеспечения целостности информации // Проблемы технического обеспечения войск в современных условиях: Сборник трудов конференции. Том 1. – СПб.: ВАС, 2017. – С. 278-281.

2. Семенов С. С., Киселев Д. В., Федорова С. В. Анализ структуры программно-аппаратных комплексов связи и состояния их надежности // Состояние и перспективы развития технического обеспечения ВС РФ: Материалы межвузовской международной научно-теоретической конференции. – СПб.: ВА МТО, 2017. – С. 417-421.

3. Киселев Д. В., Семенов С. С., Педан А. В. Постановка задачи на моделирование процесса эксплуатации программно-аппаратных комплексов связи // T-Comm: Телекоммуникации и транспорт. 2018. Том 12. № 3. С. 46-51.

4. Киселев Д. В., Семенов С. С. Влияние целостности информации на надежность и готовность программно-аппаратных комплексов связи // Проблемы технического обеспечения войск в современных условиях: Сборник трудов конференции. Том 1. – СПб.: ВАС, 2018. – С. 287-291.

5. Киселев Д. В., Семенов С. С., Федорова С. В. Выбор и обоснование показателей надежности программно-аппаратных комплексов связи // Итоги науки и техники: Научно-технический сборник. № 100. Труды академии. – СПб.: Военная академия связи, 2017. – С. 92-95.

6. Шубинский И. Б. Функциональная надежность информационных систем. Методы анализа. – М.: «Журнал Надежность», 2012. – 296 с.

7. Гмурман В. Е. Теория вероятностей и математическая статистика : Учебник для прикладного бакалавриата. – М.: Издательство Юрайт, 2016. – 479 с.

8. Гнеденко Б. В., Беляев Ю. К., Соловьев А. Д. Математические методы в теории надежности. Основные характеристики надежности и их статистический анализ. – М.: Наука, 1965. – 524 с.

9. Черкесов Г. Н. Надежность аппаратно-программных комплексов. Учебное пособие. – СПб.: Питер, 2005. – 479 с.

10. Чихачев А. В., Третьяков С. М., Бурлаков А. А., Баринов М. А., Морозов Р. В. Техническое обеспечение связи и автоматизации: Учебник – СПб.: ВАС, 2017. – 302 с.

11. ГОСТ РВ 15.703-2005. Система разработки и постановки продукции на производство. Военная техника. Порядок предъявления и удовлетворения рекламаций. Основные положения. – М.: Стандартинформ, 2005. – 31 с.

12. Об утверждении Руководства по содержанию вооружения и военной техники общевойскового назначения, военно-технического имущества в Вооруженных Силах Российской Федерации / Приказ Министра обороны Российской Федерации от 28 декабря 2013 г. № 969.

13. Новиков А. М., Новиков Д. А. Методология. – М.: СИНТЕГ, 2007. – 668 с.

14. Борзыкин Д. В., Згерский Р. В., Семенов С. С. Технологии резервного копирования и хранения данных // Проблемы технического обеспечения войск

в современных условиях: Сборник трудов конференции. Том 1. – СПб.: ВАС, 2016. – С. 143-147.

15. Киселев Д. В. Расчет рациональных параметров резервирования информации // Свидетельство о государственной регистрации программы для ЭВМ. №2018660175. 2018.

References

1. Kiselev D. V., Semenov S. S., Sedlichenko V. G. Problemnye voprosy obespecheniia tselostnosti informatsii. *Problemy tekhnicheskogo obespecheniia voisk v sovremennykh usloviiakh. Sbornik trudov konferentsii* [Problems of technical support of troops in modern conditions. Conference proceedings]. St. Petersburg, Military Academy of Communications, 2017, vol. 1, pp. 278-281 (in Russian).

2. Semenov S. S., Kiselev D. V., Fedorova S. V. Analiz struktury programmno-apparatnykh kompleksov sviazi i sostoianiia ikh nadezhnosti. *Sostoianie i perspektivy razvitiia tekhnicheskogo obespecheniia VS RF. Materialy mezhvuzovskoi mezhdunarodnoi nauchno-teoreticheskoi konferentsii* [Status and prospects of development of technical support of the armed forces. Materials of the interuniversity international scientific and theoretical conference St. Petersburg, Military Academy of logistics, 2017, pp. 417-421 (in Russian).

3. Kiselev D. V., Semenov S. S., Pedan A. V. Postanovka zadachi na modelirovanie protsessa ekspluatatsii programmno-apparatnykh kompleksov sviazi [Statement of the problem in the simulation of the process operation of software and hardware communications]. *T-Comm - Telecommunications and Transport*, 2018, vol. 12, No. 3, pp. 46-51 (in Russian).

4. Kiselev D. V., Semenov S. S. Vliianie tselostnosti informatsii na nadezhnost' i gotovnost' programmno-apparatnykh kompleksov sviazi. *Problemy tekhnicheskogo obespecheniia voisk v sovremennykh usloviiakh. Sbornik trudov konferentsii* [Problems of technical support of troops in modern conditions. Conference proceedings]. St. Petersburg, Military Academy of Communications, 2018, vol. 1, pp. 287-291 (in Russian).

5. Kiselev D. V., Semenov S. S., Fedorova S. V. Vybor i obosnovanie pokazatelei nadezhnosti programmno-apparatnykh kompleksov sviazi. *Itogi nauki i tekhniki. Nauchno-tekhnicheskii sbornik №100. Trudy akademii* [Results of science and technology. Scientific and technical collection №100. Proceedings of the Academy]. St. Petersburg, Military Academy of Communications, 2017, no. 100, pp. 92-95 (in Russian).

6. Shubinskii I. B. *Funktsional'naia nadezhnost' informatsionnykh sistem. Metody analiza* [Functional reliability of information systems. Method of analysis]. Moscow, «Journal Reliability», 2012, 296 p. (in Russian).

7. Gmurman V. E. *Teoriia veroiatnostei i matematicheskaia statistika* [Probability theory and mathematical statistics]. Moscow, Publisher Yurayt, 2016, 479 p. (in Russian).

8. Gnedenko B. V. *Matematicheskie metody v teorii nadezhnosti. Osnovnye kharakteristiki nadezhnosti i ikh statisticheskii analiz* [Mathematical methods in the

theory of reliability. Basic characteristics of reliability and their statistical analysis]. Moscow, Science, 1965, 524 p. (in Russian).

9. Cherkesov G. N. *Nadezhnost apparatno-programmnykh kompleksov* [Reliability of hardware-software systems]. St. Petersburg, Piter Publ., 2005, 479 p. (in Russian).

10. Chihachev A. V., Tretyakov A. M., Burlakov A. A., Barinov M. A., Morozov R. V. *Tekhnicheskoe obespechenie sviazi i avtomatizatsii* [Technical support of communica-tion and automation]. St. Petersburg, Military Academy of Communications, 2017, 302 p. (in Russian).

11. State Standard RM 15.703–2005. System of product development and production. Military equipment. The order of presentation and satisfaction of claims. Fundamentals. Moscow, Standardinform, 2005, 31 p. (in Russian).

12. Order of the Minister of defence of the Russian Federation of December 28, 2013 No. 969. *Ob utverzhdenii Rukovodstva po soderzhaniiu vooruzheniia i voennoi tekhniki obshchevoiskovogo naznacheniia, voenno-tekhnicheskogo imushchestva v Vooruzhen-nykh Silakh Rossiiskoi Federatsii* [About the approval of the Management on the maintenance of arms and military equipment of combined arms appointment, military-technical property in Armed Forces of the Russian Federation] (in Russian).

13. Novikov A. M., Novikov D. A. *Metodologiia* [Methodology]. Moscow, SINTEG, 2007, 668 p. (in Russian).

14. Borzykin D. V., Zgerskii R. V., Semenov S. S. Tekhnologii rezervnogo kopirovaniia i khraneniia dannykh. *Problemy tekhnicheskogo obespecheniia voisk v sovremennykh usloviiakh. Sbornik trudov konferentsii* [Problems of technical support of troops in modern conditions. Conference proceedings]. St. Petersburg, Military Academy of Communications, 2016, pp. 143-147 (in Russian).

15. Kiselev D. V. *Raschet ratsional'nykh parametrov rezervirovaniia informatsii. Svidetel'stvo o gosudarstvennoi registratsii programmy dlia EVM* [Calculation of rational parameters of information reservation. The Certificate on Official Registration of the Computer Program]. No. 2018660175, 2018.

Статья поступила 01 марта 2019 г.

Информация об авторах

Киселев Денис Викторович – соискатель ученой степени кандидата технических наук. Старший преподаватель кафедры технического обеспечения связи и автоматизации. Военная академия связи. Область научных интересов: надежность техники связи. E-mail: kdspama@yandex.ru

Семенов Сергей Сергеевич – доктор технических наук, доцент. Профессор кафедры технического обеспечения связи и автоматизации. Военная академия связи. Область научных интересов: информационная безопасность; техническое обеспечение связи; надежность техники связи. E-mail: 79111171108@yandex.ru

Петров Олег Вячеславович – кандидат военных наук. Доцент военной кафедры связи. Санкт-Петербургский политехнический университет Петра Вели-

кого. Область научных интересов: информационная безопасность; техническое обеспечение связи; надежность техники связи. E-mail: allege_russia@mail.ru

Адрес: 194064, Россия, г. Санкт-Петербург, Тихорецкий пр-кт, д. 3.

Technique of ensuring the information integrity in software-hardware communication systems by rational backup

D. V. Kiselev, S. S. Semenov, O. V. Petrov

Purpose. *The role of information in the control system increases. A wide range of information threats determines the relevance of issues to ensure its integrity. The integrity of the information affects dependability and availability of software-hardware communication systems. Known approaches to ensuring the integrity of information, based on its reservation, are widely used. But they are not able to offer a rational solution to the contradiction between the completeness and frequency of backup on the one hand and the limited resources on the other. The* ***purpose*** *of the technique is to obtain recommendations on the organization of information backup and determine the rational backup frequency. The implementation of the recommendations will allow to recover lost/distorted data with a given probability in the shortest possible time.* ***Novelty.*** *The developed method, in contrast to the known approaches to the reservation of information, offers reasonable parameters of reservation, calculated on the basis of the required probability of ensuring the integrity.* ***Results.*** *The paper presents the problem of reducing the information recovery time to increase the dependability of communication equipment, if the integrity of information is broken. The sequence of actions to ensure the information integrity by its advance backup and next recovery is defined. The process of redundancy information is analyzed and considered in aggregate, the three events occurring at random points in time: the reservation, authorized changing, the implementation of the threats to the integrity. The particular calculation technique of rational parameters of information backup which output parameters can be used both for setup of the special software on the organization of backup of data, and for direct "manual" reservation is developed.* ***Practical relevance.*** *The presented solution of the particular technique formed the basis of the computer program "Calculation of rational parameters of information backup". The use of operators or officials, operating and/or servicing software-hardware communication systems and computer equipment, this technique together with the developed program allows to obtain scientifically based parameters of information backup, and with their power to reduce the average time of information recovery. Reducing the recovery time leads to an increase availability measure at the stage of operation.*

Key words: *hardware-software communication systems, information integrity, dependability, efficient backup, frequency of backup, threat the information integrity, failure of information security.*

Information about Authors

Denis Viktorovich Kiselev – Doctoral Candidate of Engineering Sciences. Senior Lecturer at the Department of technical support of communication and automation. Telecommunication Military Academy. Field of research: dependability of telecommunication equipment. E-mail: kdspama@yandex.ru

Sergej Sergeevich Semenov – Dr. habil. of Engineering Sciences, Docent. Professor at the Department of technical support of communication and automation. Telecommunication Military Academy. Field of research: information security; technical support of communication; dependability of telecommunication equipment. E-mail: 79111171108@yandex.ru

Oleg Vyacheslavovich Petrov – Ph.D. of Military Sciences. Associate Professor at the Military Department of communication. Saint-Petersburg Polytechnic University of Peter the Great. Field of research: information security; technical support of communication; dependability of telecommunication equipment. E-mail: allege_russia@mail.ru

Address: Russia, 194064, Saint-Petersburg, Tihoretskij avenue, 3.