О.М. Булгаков,
доктор технических наук, профессор

В.П. Удалов,
кандидат физико-математических наук, доцент

Е.А. Кучмасов,
ФКУ «Главный центр связи и защиты информации МВД России»

ПРИНЦИПЫ ПОСТРОЕНИЯ МОДЕЛИ НАДЕЖНОСТИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

THE PRINCIPLES OF THE INFORMATION PROTECTION SYSTEM RELIABILITY MODEL CONSTRUCTING

Показана возможность применения методов теории надежности технических систем к построению моделей надежности систем защиты информации. В общем виде получены выражения для вероятности безотказной работы систем защиты информации и ее основных компонентов. Рассмотрена возможность оптимизации систем защиты информации по различным параметрам в рамках предложенной модели.

The structure of the information protection system of the informatization object is considered. The probability of the system reliable operation taking into account the cause of the physics of failures of the individual components is obtained. The existence of the optimal period of the information protection system components replacement and the direction of subsequently reliability improving is indicated.

Оценка надежности систем защиты информации (СЗИ) какого-либо объекта информатизации должна основываться на адекватных моделях надежности, с одной стороны, согласующихся с общими подходами к построению такого рода моделей, а с другой — учитывающих специфику реальных объектов. Существующие в настоящее время модели надежности по ряду причин неприменимы к СЗИ, т.е. нельзя задать систему уравнений, позволяющую найти количественные закономерности между входными и выходными параметрами системы с учетом особенностей ее функционирования. Таким образом, вопрос о разработке модели надежности СЗИ является важной и актуальной задачей [1, 2].

Схемы надежности, представляемые последовательно-параллельными соединениями элементов с известными количественными характеристиками надежности, широко применяются при построении моделей надежности сложных технических систем [3]. Однако такие схемы достаточно редко применяются для анализа систем защиты информации ввиду проблем детализации структуры объектов (декомпозиции) и четкого выделения элементов схемы.

Рассмотрим типовую структурную схему средств защиты информации объекта информатизации (рис.1).

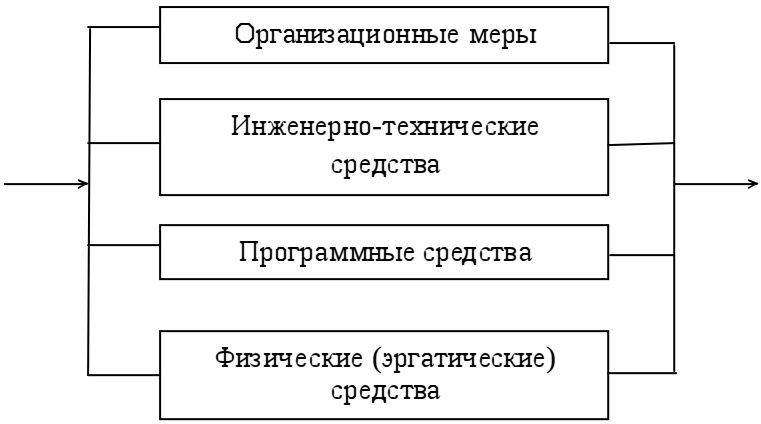

Рис. 1. Схема надежности системы защиты информации объекта

Под организационными методами защиты информации объекта информатизации понимается регламентация деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающей или существенно затрудняющей неправомерное овладение конфиденциальной информацией и проявление внутренних и внешних угроз. Организационные меры включают в себя регламентацию [2]:

- формирования и организации деятельности службы безопасности, обеспечения деятельности этих служб нормативно-методическими документами по организации защиты информации;
- составления и регулярного обновления состава защищаемой информации, составления и ведения перечня защищаемых бумажных и электронных документов;
- разрешительной системы разграничения доступа персонала к защищаемой информации и др.

Под инженерно-техническими средствами защиты понимается совокупность специальных органов, технических средств и мероприятий по их использованию в целях защиты информации.

Под программными средствами защиты информации будем понимать средства защиты данных, функционирующие в составе программного обеспечения системы защиты. Среди них можно выделить [1, 2]:

- средства архивации данных;
- антивирусные программы;
- криптографические средства;
- средства аутентификации пользователей;
- средства управления доступом;
- протоколирование и аудит.

Под физическими (эргатическими) средствами защиты понимается:

- физическая охрана объекта информатизации;
- наличие администраторов и пользователей системы защиты;
- обслуживающий персонал и другие.

В теории надежности широко используются понятия последовательного и параллельного соединения элементов в системе. При параллельном соединении отказ системы наступает лишь при одновременном отказе всех элементов системы, а при последовательном — при выходе из рабочего состояния хотя бы одного из них. В нашем случае выход из строя одного компонента защиты увеличивает вероятность несанкционированного доступа к информации, но не приводит к отказу всей системы в целом. Каждый компонент может функционировать вне зависимости от работоспособности трех других, обеспечивая некоторый уровень защиты. Отсюда можно сделать вывод,

что все четыре компонента СЗИ на схеме ее надежности должны быть соединены параллельно (рис.1).

Тогда вероятность безотказной работы СЗИ:

$$P_{\text{ðàá}} = 1 - P_{\text{îòê}} = 1 - P_{\text{Î}} \cdot P_{\text{Ò}} \cdot P_{\text{Ï}} \cdot P_{\text{Ô}}, \quad (1)$$

где $P_{отк}$ — вероятность отказа СЗИ; $P_О$, $P_Т$, $P_П$, $P_Ф$ — вероятности отказа соответственно организационных, инженерно-технических, программных и физических компонентов СЗИ.

Под отказом в теории надежности понимается случайное событие, приводящее к невозможности выполнения системой в течение некоторого промежутка времени возложенных на нее функций [3]. Применительно к системе защиты информации функциональный отказ следует трактовать как возникновение уязвимости, возможности преодоления СЗИ злоумышленником.

Рассмотрим причины и механизмы отказов отдельных компонентов СЗИ.

Применительно к организационным мерам и средствам защиты информации причиной отказа может стать устаревание нормативных правовых актов, по которым работает организация, должностных инструкций сотрудников, системы руководящих документов и документов, регламентирующих ее работу, схем помещений и т.д. С другой стороны, вероятность отказа данного компонента СЗИ существенно возрастает именно в моменты существенного обновления действующих или введения новых инструкций, регламентов и т.п., так как требуется определенное время на их изучение, адаптацию к конкретным условиям с учетом практики применения и др.

Действие первого из рассмотренных механизмов («старения») приводит к монотонному возрастанию вероятности отказа с течением времени:

$$P_{\text{ÎÑ}}(t) = \exp\left(\frac{\alpha t}{\tau_0} - 1\right). \quad (2)$$

Здесь α — интенсивность внешних и внутренних изменений, снижающих актуальность организационных средств защиты; τ_0 — характерное время обновления организационных средств защиты, определяемых нормативными документами и реалиями практической деятельности.

Математическая модель второго механизма («приработки»):

$$P_{\text{ÎÏ}}(t) = P_0^* \exp\left(-\frac{t}{\tau_0^*}\right). \quad (3)$$

В выражении (3): P_0^* — некоторый начальный уровень, определяемый степенью отличия новых организационных средств защиты от ранее действовавших; τ_0^* — время внедрения (освоения) новых организационных средств защиты, которое характеризует профессиональные качества персонала объекта информатизации.

Вероятность отказа организационного компонента СЗИ в текущий момент времени:

$$P_{\text{О}}(t) = P_{\text{ОС}}(t) + P_{\text{ОП}}(t). \quad (4)$$

Применительно к инженерно-техническим средствам и методам защиты информации отказ системы может возникнуть при моральном и физическом устаревании устройств защиты, несоответствии задач системы защиты её возможностям в настоящее время и др.

Процессы временной деградации технических средств характеризуются вероятностью отказа:

$$P_{\text{ТС}}(t) = P_{\text{ТВ}}(t)\exp\left(\frac{\beta_C t}{\tau_T} - 1\right), \quad (5)$$

где $P_{ТВ}(t)$ определяется соответствием технических возможностей СЗИ задачам по обеспечению информационной безопасности; β_C характеризует действие естественного (условия эксплуатации аппаратуры) и человеческого (квалификация персонала) факторов, влияющих на долговечность аппаратуры; τ_T — характерное время износа технических средств, определяемое гарантийными обязательствами производителя, технической политикой в отношении ремонта и сервисного обслуживания, замены находящегося в эксплуатации оборудования на более современное.

В свою очередь,

$$P_{ТВ}(t) = P_{ТВ0} + P_{ТВ*}(t), \tag{6}$$

где $P_{ТВ0}$ характеризует уровень изначального соответствия технических возможностей СЗИ решаемым задачам, $P_{ТВ*}(t)$ отражает совершенствование с течением времени возможностей злоумышленников по преодолению инженерно-технических средств защиты объекта.

Начальному периоду эксплуатации технических средств поставим в соответствие вероятность отказа:

$$P_{ТП}(t) = P_T^* \exp\left(-\frac{\beta_П t}{\tau_T^*}\right). \tag{7}$$

Параметр P_T^* определяется интенсивностью отказов технических средств защиты информации в начальный период τ_T^* или их общим количеством до некоторого момента $t_Н$; $\beta_П$ характеризует эффективность работы по замене и ремонту неисправных устройств.

Очевидно,

$$P_Т(t) = P_{ТС}(t) + P_{ТП}(t). \tag{8}$$

Причиной возникновения отказа в программных средствах могут стать: моральное устаревание используемых программ, физическое разрушение (возникновение ошибок в программном коде продукта), несовместимость программных средств защиты с современными операционными системами, несвоевременное обновление программных продуктов.

По аналогии с выражениями (5)—(8):

$$P_П(t) = P_{ПС}(t) + P_{ПП}(t), \tag{9}$$

где

$$P_{ПС}(t) = P_{ПВ}(t)\exp\left(\frac{\gamma_C t}{\tau_П} - 1\right), \tag{10}$$

$$P_{ПВ}(t) = P_{ПВ0} + P_{ПВ*}(t), \tag{11}$$

$$P_{ПП}(t) = P_П^* \exp\left(-\frac{t}{\tau_П^*}\right). \tag{12}$$

Здесь $P_{ПС}(t)$ и $P_{ПП}(t)$ — вероятности отказов, обусловленные временной деградацией и отладкой программных средств (с устранением программных ошибок и проблем совместимости с другими программными продуктами) соответственно; $P_{ПВ}(t)$ характеризует степень соответствия возможностей программных средств СЗИ возложенным на них задачам по обеспечению информационной безопасности; $P_{ПВ0}$ отвечает начальному уровню защищенности информации программными средствами, $P_{ПВ*}(t)$ отражает возможности злоумышленников по преодолению программных средств СЗИ; γ_C — параметр, отражающий деградацию программных средств вследствие целенаправленного деструктивного воздействия, например путем внедрения в систему вредоносных программ; $\tau_П$ и $\tau_П^*$ — характерные времена использования и освоения (внедрения) кон-

кретной версии программного продукта; параметр $P_{П}^{*}$ определяется интенсивностью отказов программного обеспечения в начальный период эксплуатации или их общим количеством за наблюдаемый период $t_{Н}$.

При необходимости в параметр $\gamma_{С}$ может быть введен аддитивный компонент:

$$\gamma_{О} = \gamma_{ОН} - \gamma_{ОУ},$$

отражающий возникновение и накопление ошибок в программном продукте в процессе его эксплуатации, обусловленных действием случайных факторов, не связанных с внешними атаками ($\gamma_{ОН}$), а также эффективность мер по устранению такого рода ошибок ($\gamma_{ОУ}$). В первом приближении $\gamma_{ОН}$ и $\gamma_{ОУ}$ можно считать не зависящими от времени, хотя можно предположить существование некоторого критического уровня $\gamma_{О}$, при превышении которого функция $\gamma_{ОН}$ ($\gamma_{О}$,t) монотонно возрастает, а функцию $\gamma_{ОУ}$ можно априори считать асимптотически возрастающей до некоторого уровня насыщения, что отражает возрастание накопленных навыков специалистов по обслуживанию программных средств в выявлении и устранении ошибок в программном продукте.

Надежность физического персонала и физических (эргатических) средств защиты в целом также может быть представлена двумя различными по характеру монотонности временными функциями:

$$P_{эф}(t) = P_{ФС}(t) + P_{ФП}(t). \qquad (13)$$

Вероятность отказа $P_{ФС}$(t) отражает физическое старение персонала, т.е. постепенное уменьшение возможностей выполнять свои обязанности по обеспечению защиты информации на необходимом уровне из-за возраста сотрудниками службы безопасности, инженерно-техническим персоналом и другими сотрудниками организации в применяемых в ней эргатических системах защиты информации.

Представим данный временной процесс выражением:

$$P_{эфС}(t) = P_{ПФ0} \cdot \exp\left(\frac{(\delta_{С} - \delta_{В})t}{\tau_{эф}} - 1\right). \qquad (14)$$

Здесь $P_{ПФ0}$ — начальный уровень физического состояния персонала; $\delta_{С}$ и $\delta_{В}$ отражают соответственно негативное действие на физическое состояние персонала условий труда (ночных дежурств, переработок, работы с компьютерными и телевизионными мониторами и др.) и меры по восстановлению здоровья и профилактике профессиональных заболеваний; $\tau_{Ф}$ — некоторый характерный период обновления персонала, например среднее время работы сотрудников физических или эргатических компонентов СЗИ в рассматриваемой организации.

Функция $P_{ФП}$(t) характеризует рост квалификации персонала:

$$P_{эфП}(t) = P_{эф}^{*} \cdot \exp\left(-\frac{\delta_{О} t}{\tau_{КФ}}\right), \qquad (15)$$

где $P_{эф}^{*}$ определяется начальным уровнем квалификации персонала; $\delta_{О}$ характеризует приобретение опыта решения типичных и нестандартных профессиональных задач; $\tau_{КФ}$ — характерное время приобретения профессиональных знаний, умений и навыков, в качестве которого могут выступать время стажировки в новой должности или периодичность повышения квалификации.

Каждая из функций (4), (8), (9) и (13) представляет собой классическую «корытообразную» кривую интенсивности или вероятности отказов [4, 5]. В нашем случае показано, что каждая из этих кривых образуется в результате суммирования убывающей и возрастающей экспонент (рис. 2): (2) и (3), (5) и (7), (10) и (12), (14) и (15) соответственно.

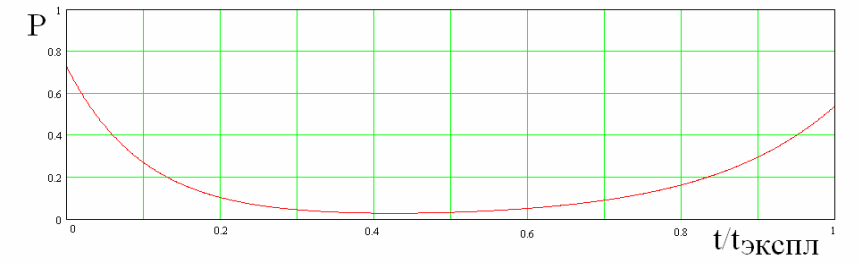

Рис. 2. Вероятность отказов системы

Продление оси абсцисс за рассматриваемый временной интервал приведет к тому, что графики, по крайней мере, для программных и инженерно-технических компонентов СЗИ будут выглядеть как несколько «склеенных» в моменты τ_i замены оборудования или программных средств «корытообразных» кривых (рис. 3, кривые 1 и 2). В меньшей степени такой характер замен выражен для организационного и физического компонентов СЗИ (рис. 3, кривые 3 и 4).

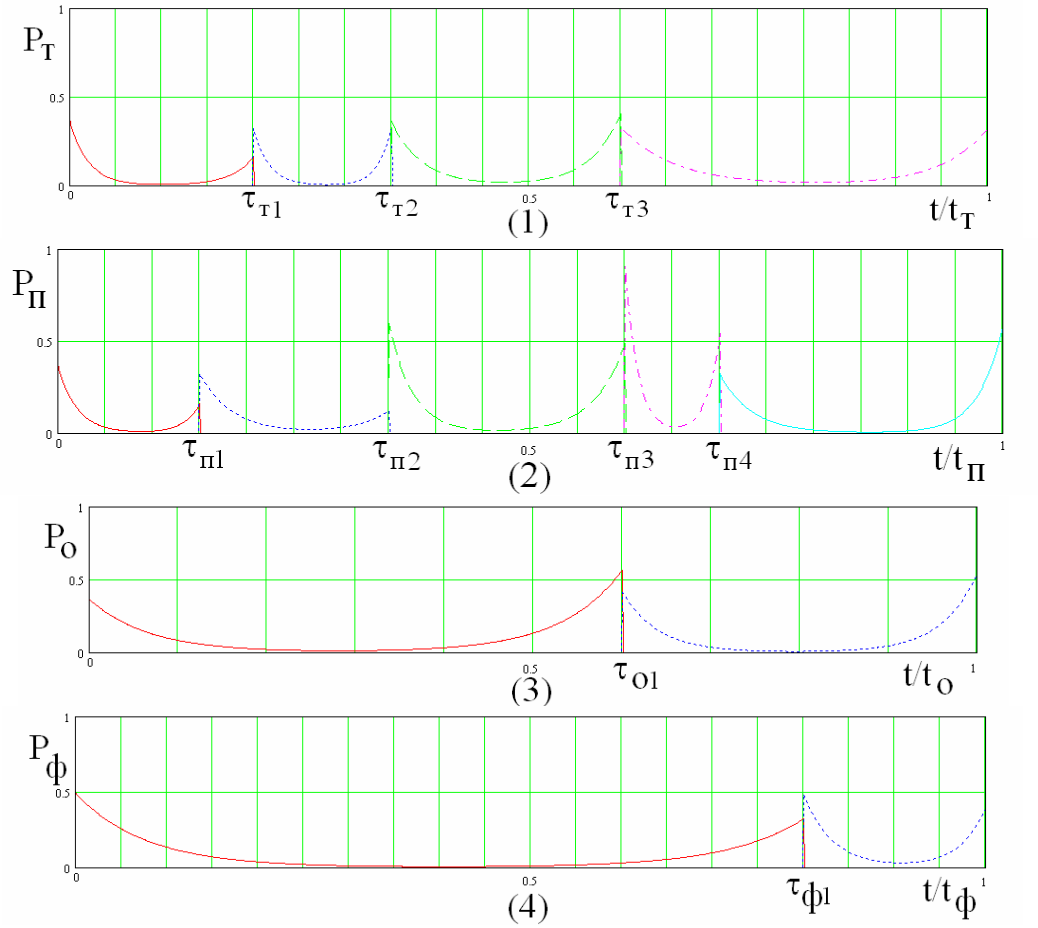

Рис. 3. Вероятности отказов инженерно-технического (1), программного (2), организационного (3) и физического (4) компонентов СЗИ

Основным различием кривых $P_О(t)$, $P_Т(t)$, $P_П(t)$ и $P_Ф(t)$ является то, что они строятся в отличных друг от друга временных масштабах, определяемых соответствующими параметрами в знаменателях показателей экспонент. График вероятности отказа СЗИ:

$$P_{отк} = P_О(t) \cdot P_Т(t) \cdot P_П(t) \cdot P_Ф(t) \qquad (16)$$

представлен на рис. 4 (кривая 1).

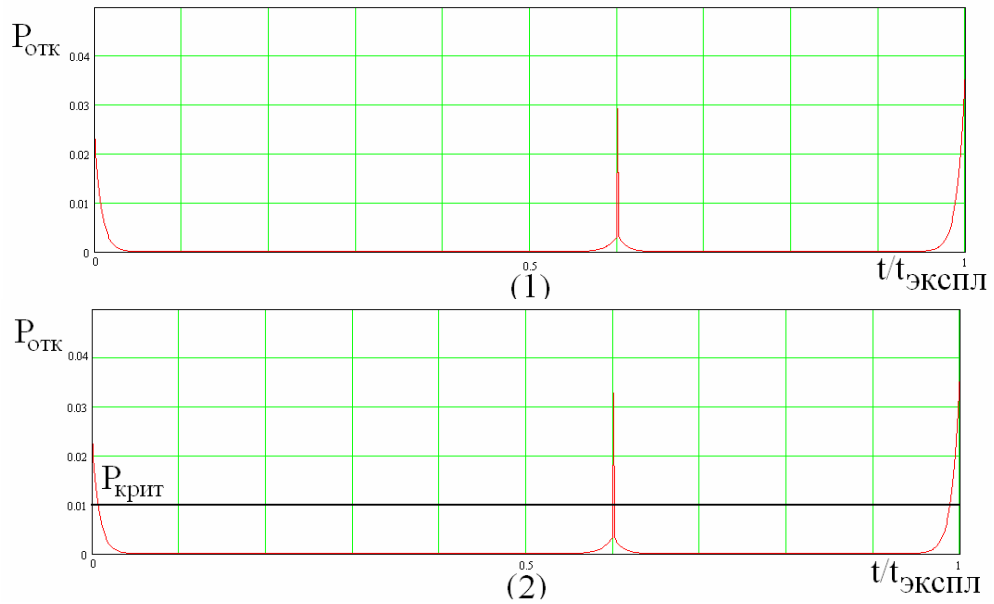

Рис. 4. Вероятность отказа системы защиты информации

Качественный анализ графиков на рис. 3 и 4 позволяет сделать следующие выводы:

1. Повышение надежности СЗИ может быть достигнуто путем минимизации некоторой целевой функции, например:

$$\frac{1}{\tau}\int_0^{\tau} P_{\text{отк}}(t)dt \to \min \qquad (17)$$

по отдельным параметрам из выражений (2), (3), (5), (6), (7), (10), (11), (12), (14) и (15) или любым их совокупностям при условии:

$$P_{\text{отк}}(t) < P_{\text{крит}}, \qquad (18)$$

где $P_{\text{крит}}$ — критическая (порог недопустимых значений) вероятность отказа СЗИ.

2. Для соблюдения условия (18) следует избегать попадания точек «склеивания» τ_i какой-либо из кривых (1)—(4) в малые окрестности точек τ_i^* других кривых. Применительно к практике это означает существенное увеличение вероятности отказа действующей СЗИ при одновременной замене двух и более компонентов, а также то, что наибольшая вероятность отказа СЗИ имеет место в начальный период ее работы (рис. 4).

3. Для различных реализаций каждого компонента СЗИ существует оптимальное время эксплуатации τ_i, не только определяемое выражением (17), но и согласованное с временами эксплуатации τ_i^* других компонентов СЗИ, т.е. следует избегать как чрезмерно больших, так и малых значений τ_i. Отсюда вытекает существование оптимального периода (квазипериода) $\Delta\tau = \tau_{i+1} - \tau_i$ замены компонентов СЗИ и оптимального временного сдвига $\Delta\tau^* = \tau_i^* - \tau_i$ для каждой реализации компонентов СЗИ. Очевидно, для определения оптимума τ_i необходимо дополнительно учитывать экономические (стоимостные) параметры рассматриваемого компонента СЗИ.

Применительно к рис. 1 и 4 может возникнуть необходимость учета значимости компонентов СЗИ, например введением весовых коэффициентов в выражения (1) или (16).

Для каждого из N сомножителей из выражений (1), (16) введем показатель степени:

$$\Theta(\omega_j) = exp(1/N - \omega_j), \qquad (19)$$

где ω_j — характеристика значимости рассматриваемого компонента СЗИ, определяемая, например, методом экспертных оценок или задаваемая на этапе проектирования СЗИ и подчиняющаяся условию нормировки:

$$\sum_{j=1}^{N} \omega_j = 1. \tag{20}$$

Таким образом,

$$\prod_{j=1}^{N} \Theta(\omega_j) = 1. \tag{21}$$

Для рассматриваемого примера СЗИ:

$$P_{\text{отк}}(t) = P_{О}(t)^{\Theta(\omega_О)} \cdot P_{Т}(t)^{\Theta(\omega_Т)} \cdot P_{\text{П}}(t)^{\Theta(\omega_П)} \cdot P_{\text{Ф}}(t)^{\Theta(\omega_Ф)}. \tag{16а}$$

Предположим, что эксперты оценили значимость компонентов СЗИ некоторого объекта информатизации по десятибалльной шкале следующим образом:

- организационный — 3;
- инженерно-технический — 6;
- программный — 8;
- физический — 7.

Кривая 2 на рис. 4 в отличие от кривой 1 построена с учетом данных оценок. В качестве приемлемой вероятности отказа рассматриваемой СЗИ принято значение $P_{\text{крит}}$= 0,01.

Для дальнейшего повышения достоверности предложенной модели надежности СЗИ требуется детализация моделей надежности ее отдельных компонентов, например на основе параллельно-последовательных схем надежности и статистики отказов или экспертных оценок показателей надежности их отдельных элементов.

Рассмотрим пример несложной структуры инженерно-технического компонента СЗИ (рис. 5), включающего в себя биометрическую систему контроля управления доступом (СКУД) на общем входе в объект, дверь с электронным кодовым замком (ЭКЗ) в каждом отдельном кабинете и систему охранной сигнализации (ОС), в каждом кабинете представленную двумя датчиками и каналом до общего блока передачи извещений (БПИ). Система видеонаблюдения отнесена к эргатическому компоненту СЗИ. Система электроснабжения представлена основным (ИЭП 1) и резервным (ИЭП 2) источниками питания и силовыми электрическими кабелями ЭК 1 и ЭК 2.

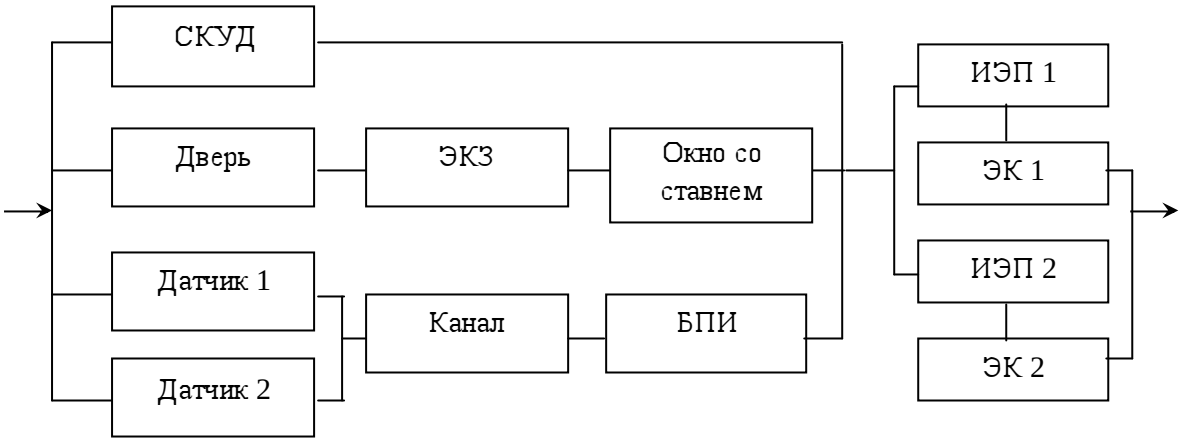

Рис. 5. Схема надежности инженерно-технического компонента СЗИ

Зачастую трудности в декомпозиции СЗИ обусловлены одновременным участием тех или иных субкомпонентов в различных подсистемах. Так, например, система видеонаблюдения может рассматриваться как компонент инженерно-технических средств защиты информации и включать в себя собственно технический (камеры, ви-

деоканалы, видеосерверы, мониторы), физический (операторы), программный (ПО видеосервера) и организационный субкомпоненты. В связи с этим возможны другие подходы к декомпозиции СЗИ и построению моделей надежности ее подсистем.

Соответственно, вероятность отказа такой системы [1, 4]:

$$P_{\text{т}}(t) = \{1 - \left[1 - \left(1 - P_{ДВ}(t)\right) \cdot \left(1 - P_{ЭКЗ}(t)\right) \cdot \left(1 - P_{ОС}(t)\right)\right] \times$$
$$\times \left[1 - \left(1 - P_{Д1}(t) \cdot P_{Д2}(t)\right) \cdot \left(1 - P_{К}(t)\right) \cdot \left(1 - P_{БПИ}(t)\right)\right] \cdot P_{СКУД}(t)\} \times$$
$$\times \{1 - \left[1 - \left(1 - P_{ИЭП1}(t) \cdot \left(1 - P_{ЭК1}(t)\right)\right)\right] \cdot [1 - \left(1 - P_{ИЭП2}(t)\right) \times$$
$$\times \left(1 - P_{ЭК2}(t)\right)]\}.$$

В правой части приведенного выражения последовательно обозначены вероятности отказов: двери ($P_{\text{дв}}$), электронного кодового замка ($P_{\text{ЭКЗ}}$), окна со ставнем ($P_{\text{ОС}}$), датчиков охранной сигнализации ($P_{\text{Д1}}$ и $P_{\text{Д2}}$), канала передачи тревожного сигнала ($P_{\text{К}}$), блока передачи извещений ($P_{\text{БПИ}}$), системы контроля управлением доступом ($P_{\text{СКУД}}$), источников электропитания ($P_{\text{ИЭП1}}$ и $P_{\text{ИЭП2}}$) и силовых электрических кабелей ($P_{\text{ЭК1}}$ и $P_{\text{ЭК2}}$).

В настоящее время теория надежности технических систем разработана достаточно хорошо. Применение основных положений, терминов и определений теории надежности в информационной безопасности открывает большие возможности для разработки моделей СЗИ, повышения достоверности оценок характеристик надежности СЗИ и их отдельных компонентов, в особенности тех, на которые не распространялись ранее классические подходы теории надежности технических систем, расширяет базу для создания алгоритмов и методик анализа надежности СЗИ, выбора эксплуатационных показателей их качества.

ЛИТЕРАТУРА

1. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. — М.: Горячая линия-Телеком, 2004. — 280 с.

2. Герасименко В.А., Малюк А.А. Основы защиты информации. — М.: МОПО, МИФИ, 1997. — 537 с.

3. Баранова А.В., Ямпурин Н.П. Основы надежности электронных средств. — М.: Академия, 2010. — 234 с.

4. Острейковский В.А. Теория надежности. — М.: Высшая школа, 2003. — 457 с.

5. Бриндли К. Измерительные преобразователи: справочное пособие: пер. с англ. — М.: Энергоатомиздат, 1991. — 144 с.