УДК 004.056.53 **DOI** 10.15622/sp.2019.18.6.1301-1332

О.И. Бокова, И.Г. Дровникова, А.С. Етепнев, Е.А. Рогозин, В.А. Хвостов

МЕТОДИКИ ОЦЕНИВАНИЯ НАДЕЖНОСТИ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

Бокова О.И., Дровникова И.Г., Етепнев А.С., Рогозин Е.А., Хвостов В.А. **Методики оценивания надежности систем защиты информации от несанкционированного доступа в автоматизированных системах.**

Аннотация. Современные методы защиты информации от несанкционированного доступа в обязательном порядке включаются в виде дополнительных модулей в программное обеспечение автоматизированных систем в защищенном исполнении. Применение систем защиты информации от несанкционированного доступа может снизить надежность автоматизированных систем, если они содержат ошибки, не обнаруживаемые при отладке.

Методической основой при формировании облика систем защиты информации как в процессе разработки, так и в процессе модернизации являются руководящие документы Федеральной службы по техническому и экспортному контролю (ФСТЭК) России. Руководящие документы ФСТЭК России не содержат методических подходов к оценке надежности указанных программных систем. В этой связи актуальна разработка методик оценивания надежности систем защиты информации от несанкционированного доступа, структурная сложность и значительное количество выполняемых функций которых обусловили необходимость использования трех показателей надежности, характеризующих систему при решении задач обеспечения конфиденциальности, целостности и доступности информации. Для разработки методик использованы известные методы оценивания надежности сложных систем, не допускающие их разложение на последовательное и параллельное соединение. Разработанные методики апробированы при оценивании надежности систем защиты информации от несанкционированного доступа, имеющих типовые показатели исходных характеристик. Результаты расчетов и перспективы использования разработанных методик представлены в статье.

Ключевые слова: несанкционированный доступ, система защиты информации, надежность, отказ, автоматизированная система, конфиденциальность информации, целостность информации, доступность информации.

1. Введение. Проникновение современных информационных технологий (ИТ) во все сферы человеческой деятельности обуславливает необходимость научного осмысления последствий их внедрения и практического применения, а также требует содержательного анализа проблемы информационной безопасности (ИБ).

Необходимость осмысления результатов внедрения ИТ в значительной степени связана с объектами информатизации критического применения (ОИКП) (автоматизированными

системами (АС), используемыми в военной сфере, органах государственной безопасности и охраны, органах внутренних дел и т.д.), выход из строя которых может привести к существенным финансовым, человеческим и другим потерям, что является неприемлемым для общества.

Трудности правового регулирования ИТ и недостатки организационного регулирования процесса обеспечения ИБ, отсутствие методик оценивания и обоснования требований к ИБ, проблемы с кадровым обеспечением ОИКП могут привести к тому, что конфиденциальная информация, используемая узким кругом потребителей, становится объектом неправомерного доступа для злоумышленников.

Исключительная важность задач, решаемых в АС на ОИКП с использованием средств вычислительной техники, а также существенный ущерб интересам личности и государства, который возникает в результате снижения уровня безопасности информации в АС, подчеркивают значимость задачи обеспечения надежности функционирования АС в защищенном исполнении и в особенности безопасности хранимой, обрабатываемой и передаваемой конфиденциальной информации.

Классификационная схема угроз ИБ АС представлена как в нормативных документах ФСТЭК России [1, 2], так и в общедоступной научно-технической литературе [3-6]. В указанных источниках рассматривается основное содержание угроз ИБ, точки их приложения, оценки ущербов от возникновения и реализации угроз. Формализованы угрозы ИБ в виде базы знаний угроз ФСТЭК России [4-6], включающей как описательную, так и расчетную части в виде калькулятора оценки опасности угрозы. База знаний содержит информацию об уязвимостях операционных систем (ОС) и систем управления базами данных, прикладных программ, методов защиты информации, а также о связанных с этими уязвимостями и методами защиты рисках.

Международные стандарты, регламентирующие область обеспечения БИ и созданные для развития и углубления методологии ГОСТ «Общие критерии оценки безопасности информационных технологий» ISO/IEC 15408: 2013. «Информационная технология — Методы и средства защиты информации — Критерии оценки безопасности информационных технологий» (ОК), содержат классификацию угроз ИБ АС. Подробный перечень угроз ИБ, предназначенный для обоснования и выбора мер по защите информации от несанкционированного доступа АС, приведен в стандарте Национального института стандартов США (NIST)

ISO/IEC13335:2004 «Information technology — Security techniques — Management of information and communication technology security» (информационный портал национального института стандартов США http://www.nist.org) [7, 8].

В целях обнаружения и противодействия наиболее опасным видам угроз ИБ, связанных с НСД к информации АС, традиционно применяют системы защиты информации (СЗИ) от НСД, которые в обязательном порядке включаюися в виде дополнительных программных систем в состав ОС АС критического применения. Системы защиты могут разрабатываться совместно с АС в ходе ее проектирования или устанавливаться в общесистемное программное обеспечение готовой системы.

Использование систем защиты снижает надежность АС, поскольку они, как и большинство программ, могут содержать не обнаруженные при отладке ошибки. В процессе эксплуатации ошибки СЗИ приводят к снижению интегральной надежности АС. Надежность, в свою очередь, оказывает влияние на эффективность защиты информации (обеспечение конфиденциальности, целостности и доступности информации).

Методической основой обоснования требований к системам защиты является ряд руководящих документов ФСТЭК России, в которых установление требований к защите информации определяется требуемым классом защищенности [9, 10]. Для СЗИ, разрабатываемых в соответствии с международным стандартом ISO/IEC 15408 ОК [7], установление требований состоит в выполнении профиля защиты. Замена понятия класса защищенности понятиями профиля защиты и задания по безопасности является отличительным признаком стандарта ОК.

Профиль защиты включает в себя совокупность функций защиты, применяемых в конкретном профиле, и элементы доверия для конкретного изделия ИТ.

Результаты анализа отечественной и международной нормативной документации показали, что в нормативных документах в области ИБ фактически задается совокупность функций защиты, которые требуется реализовать в СЗИ от НСД. Совокупность функций защиты является признаком, определяющим соответствие СЗИ от НСД как классу защищенности, так и профилю защиты.

Качеству программных систем в Российской федерации посвящены ГОСТ 28195 — 89 и ГОСТ28806 — 90 [11, 12]. Анализ их содержания позволяет сделать вывод об ограниченной применимости методик, содержащихся в стандартах для оценивания надежности СЗИ

от НСД. В представленных стандартах СЗИ не рассматривается как объект оценки качества программных систем. Данное обстоятельство требует творческой доработки методического обеспечения указанных стандартов как в части показателей надежности СЗИ от НСД, так и в части методик их оценивания.

Аналогичные утверждения применимы и в отношении известной научно-технической литературы, посвященной вопросам качества программных систем [13-18].

Оценивание показателей надежности технических систем в России регламентировано рядом ГОСТ, составляющих целую группу стандартов. В частности, стандарты группы 27.XXX посвящены общим проблемам надежности в технике. Несмотря на методическую полноту системы стандартов указанной серии, вопросы оценивания надежности СЗИ от НСД в них напрямую не проработаны. Существует лишь возможность применения отдельных теоретических положений и подходов к оцениванию надежности при разработке математических зависимостей, используемых в методиках.

Известная научно-техническая литература, посвященная проблеме надежности, в частности [19-28], также не рассматривает вопросы оценивания надежности СЗИ от НСД.

При создании АС в защищенном исполнении согласно нормативной документации [29], в которой определены имеющиеся недостатки существующих систем обеспечения ИБ на ОИКП и направления совершенствования АС в части обеспечения защиты информации, оценивание надежности СЗИ от НСД является неотъемлемой составляющей процессов проектирования и эксплуатации указанных АС. При этом вопросам оценивания надежности посвящена конструкторская документация («Техническое задание...», «Эскизный проект...», «Технический проект...», «Пояснительная записка...» и др.) и разрабатываемая на ее основе эксплуатационная документация («Руководство пользователя», «Руководство администратора безопасности», «План мероприятий по обеспечению защиты информации», «Руководство по резервному копированию и восстановлению» и др.).

Таким образом, разработка методического обеспечения, включающего конкретные методики оценивания надежности функционирования СЗИ от НСД при решении задач обеспечения конфиденциальности, целостности и доступности информации, является актуальной проблемой для обеспечения ИБ АС в защищенном исполнении на ОИКП.

Поставлена научная задача разработать и апробировать методики оценивания надежности СЗИ от НСД, включающих показатели вероятности безотказной работы СЗИ от НСД на этапах проектирования и эксплуатации АС в защищенном исполнении.

2. Методика оценивания вероятности безотказной работы систем защиты информации от несанкционированного доступа при обеспечении конфиденциальности информации. Анализ научно-технической литературы [26-28, 30-32] показал, что наиболее целесообразным методом расчета вероятности безотказной работы СЗИ от НСД в АС является метод эквивалентных схем. В основе указанного метода используется следующая формула для расчета полной вероятности [26]:

$$P_c = f(p_1, p_2, ...p_n) = p_1 P(t \mid p_1 = 1) + q_1 P(t \mid p_1 = 0), \quad (1)$$

где: p_i — вероятность безотказной работы i-го элемента; $q_i = 1 - p_i$ — вероятность отказа i-го элемента; $P(t \mid p_1 = 1)$, $P(t \mid p_1 = 0)$ — условные вероятности работоспособного состояния системы при работоспособном состоянии (отказе) первого элемента.

Математические выражения $P(t \mid p_1 = 1)$, $P(t \mid p_1 = 0)$ предназначены для расчета вероятностей безотказной работы структурных схем, эквивалентных исходной схеме, при условии, что первый элемент первой схемы является абсолютно надежным, а первый элемент второй схемы отказал. Отражаемая выражением (1) операция называется операцией разрезания по элементу 1 [31]. В источниках [26, 27, 31-36] показано, что операция разрезания может проводиться по любому элементу структурной схемы надежности системы. При этом выполняется следующая последовательность действий.

1. Определяются простые точки соединения исходной структурной схемы и в соответствии с этим правилом выбирается элемент, по которому будет реализовываться операция разрезания.

2. Исходная структура преобразуется в две эквивалентные схемы. В первой из них элемент разрезания заменяется абсолютно надежной перемычкой. Во второй схеме элемент полностью удаляется.

3. Проводится расчет надежности по каждой эквивалентной схеме и используется математическое выражение (1) для получения результирующего выражения расчета показателя надежности.

Исходная структурная схема по надежности СЗИ от НСД, разработанная в [37], представлена на рисунке 1.

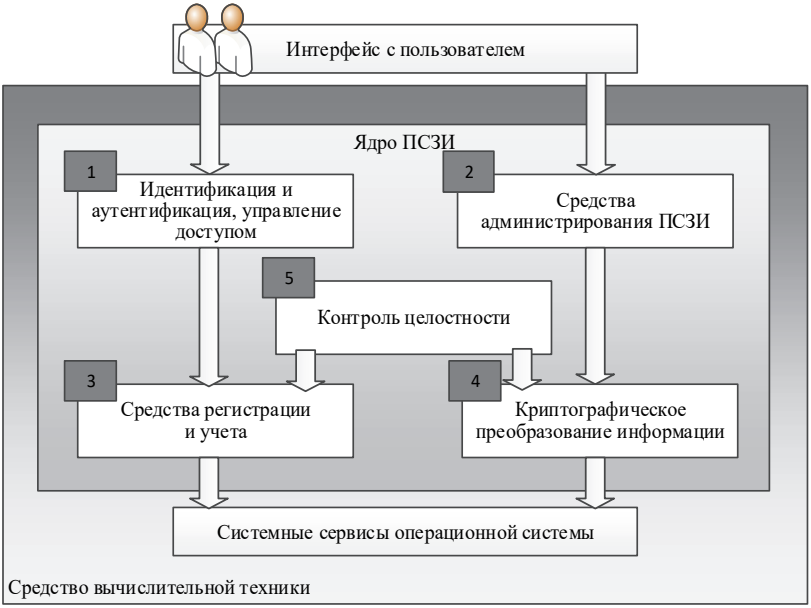

Рис. 1. Исходная структурная схема по надежности СЗИ от НСД

При оценивании вероятности безотказной работы данную структурную схему СЗИ от НСД можно представить в виде двух эквивалентных схем.

Разрезание структурной схемы СЗИ целесообразно провести по элементу «Контроль целостности».

При этом в результате операции разрезания получим две эквивалентные схемы СЗИ от НСД, представленные на рисунках 2 и 3.

Используя формулу (1), с учетом разрезания по элементу «Контроль целостности» (элемент идеально работоспособен или полностью отказал) результирующий показатель надежности СЗИ можно получить в виде:

$$P_c = p_5(1-q_1q_2)(1-q_3q_4)+q_5(1-(1-p_1p_3)(1-p_2p_4)), \qquad (2)$$

где $p_i = 1-q_i$ — вероятность безотказной работы i-го элемента [26].

Математическое выражение (2) позволит оценивать вероятность безотказной работы СЗИ от НСД в АС.

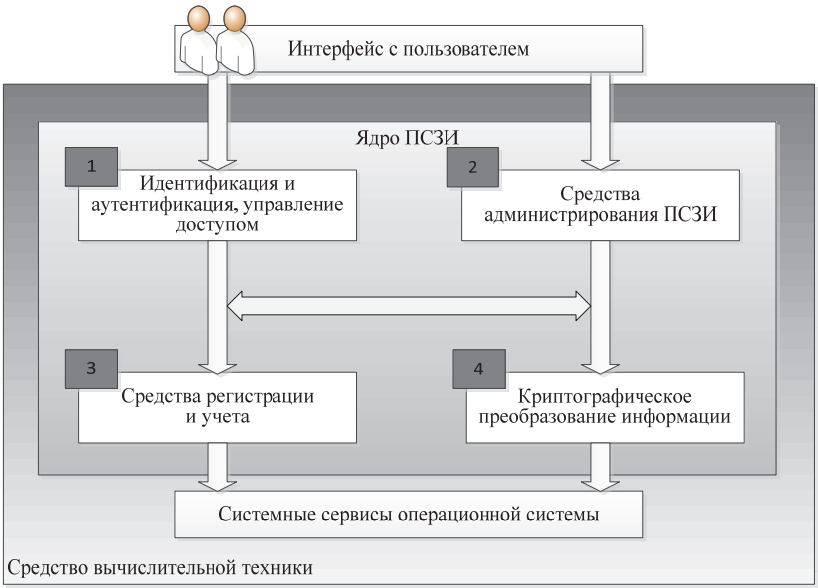

Рис. 2. Эквивалентная схема структуры СЗИ от НСД с заменой элемента «Контроль целостности» абсолютно надежной перемычкой

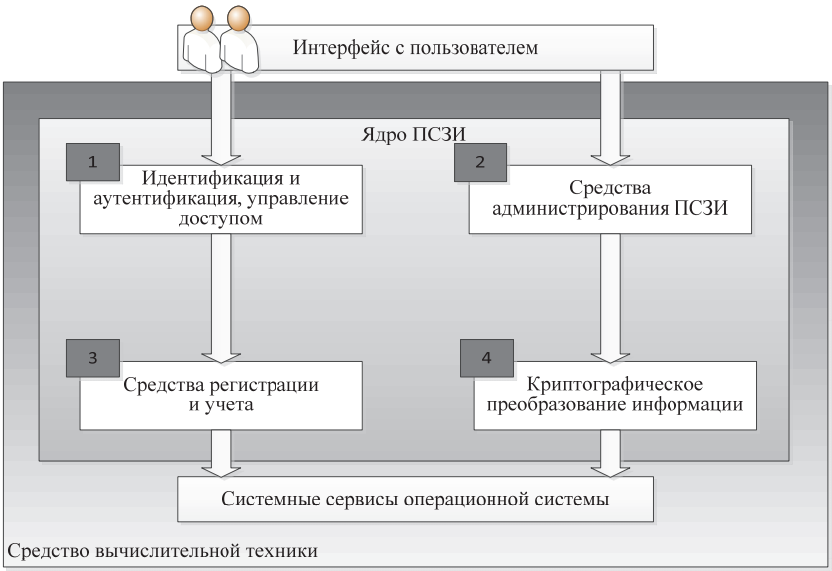

Рис. 3. Эквивалентная схема структуры СЗИ от НСД с заменой элемента «Контроль целостности» разрывом

3. Методика оценивания коэффициента готовности систем защиты информации от несанкционированного доступа при обеспечении доступности информации. При расчетах показателя надежности СЗИ от НСД «Коэффициент готовности» целесообразно использовать метод построения логико-вероятностной функции надежности СЗИ. Основой методики является математический аппарат булевой алгебры. На начальной стадии оценивания надежности структурно-сложных систем при построении расчетной зависимости необходимо последовательно реализовать ряд этапов [37-41].

Элементам сопоставляются логические переменные x_i, принимающие значения единицы при работоспособности элемента и нуля — при его неработоспособности. По результатам логического анализа работоспособности системы конструируется логическая функция работоспособности (ЛФР), имеющая следующий вид: $f(X)$, где многомерный аргумент ЛФР $X = (x_1, x_2, ...x_n)$ является вектором логических переменных.

Наличие хотя бы единственного пути от исходного структурного элемента схемы надежности до ее конечного элемента позволяет считать данную схему частично работоспособной $(f(X) = 1)$. Такой путь может считаться работоспособным при условии работоспособности всех входящих в него элементов СЗИ. Формализация всех возможных путей в ЛФР осуществляется элементарными конъюнкциями булевых переменных, которые соответствуют входящим в данные пути элементам. Функция $f(X)$ выражается в виде дизъюнкции элементарных конъюнкций, соответствующих всем работоспособным путям ЛФР. Форма ЛФР, полученная в ходе составления дизъюнкций элементарных конъюнкций, будет являться исходной для последующего построения математического выражения расчета коэффициента готовности СЗИ от НСД.

Исходная форма ЛФР может быть преобразована к любой форме полного замещения (ФПЗ). ЛФР СЗИ от НСД в виде ФПЗ используется для построения аналитической зависимости для оценивания надежности. При этом проводится замена логических переменных вероятностями, а логических операций — арифметическими.

В соответствии с выше изложенным осуществим ряд замещений: переменная x_i замещается вероятностью $p_i = P(x_i = 1)$, операция инверсии логической переменной $\overline{x_i}$ — вероятностью $q_i = P(x_i = 0)$,

операция дизъюнкции $\vee$ — сложением $+$, операция конъюнкции $\wedge$ — умножением $\times$. Операция логического отрицания $\neg y$ замещается вычитанием вероятности из единицы: $1 - P(y = 1)$.

Для проведения оценки коэффициента готовности СЗИ от НСД целесообразно использовать ФПЗ в базисе «конъюнкция-отрицание» [38, 41].

ЛФР СЗИ от НСД, представленной на рисунках 1 и 2, имеет следующий вид:

$$f = x_1(x_3 \vee x_4 x_5) \vee x_2(x_4 \vee x_3 x_5). \quad (3)$$

Число вхождений математического выражения (3) определяется как двойное. Дважды входят переменные x_3, x_4, x_5. Выбрав x_5 для операции разрезания, получим из исходной формы следующее математическое выражение:

$$f = x_5(x_1(x_3 \vee x_4)) \vee x_2(x_3 \vee x_4) \vee x_5'(x_1 x_3 \vee x_4 x_2). \quad (4)$$

Преобразуя математическое выражение (4) к ФПЗ, получим следующее математическое выражение:

$$f = x_5((x_1'x_2')'(x_3'x_4')')' \vee x_5'((x_1'x_3')'(x_2'x_4')')'. \quad (5)$$

Заменив логические переменные арифметическими в математическом выражении (5), получим:

$$P(f = 1) = p_5(1 - q_1 q_2)(1 - q_3 q_4) + q_5(1 - (1 - p_1 p_3)(1 - p_2 p_4)). \quad (6)$$

Коэффициент готовности СЗИ от НСД ($K_{ГСЗИ}$) получим путем замены вероятности безотказной работы программных модулей СЗИ коэффициентами готовности этих модулей ($K_{Гi}$) [38]. Вероятности отказа заменим коэффициентами простоя ($K_{ПРi}$):

$$K_{ГСЗИ} = p_5(1 - q_1 q_2)(1 - q_3 q_4) + q_5(1 - (1 - p_1 p_3)(1 - p_2 p_4)), \quad (7)$$

где: $p_i = K_{Гi}$, $q_i = 1 - K_{Гi}$.

Для марковской модели надежности имеем:

$$K_{Гi} = \frac{\mu_i}{\mu_i + \lambda_i},$$

$$K_{ПРi} = \frac{\lambda_i}{\mu_i + \lambda_i}.$$

При одинаковых значениях характеристик надежности программных модулей СЗИ от НСД $\lambda_i = \lambda$, $\mu_i = \mu$, приняв $\rho = \frac{\lambda}{\mu}$, математическое выражение (7) можно преобразовать к следующему виду:

$$K_{ГСЗИ} = \frac{(1 + 5\rho + 8\rho^2 + 2\rho^3)}{(1+\rho)^5}. \quad (8)$$

Математическое выражение (8) позволит рассчитать коэффициент готовности СЗИ от НСД в АС [42, 43].

4. Методика оценивания средней наработки систем защиты информации от несанкционированного доступа на отказ при обеспечении целостности и доступности информации. В основе методики проведения оценки средней наработки СЗИ от НСД на отказ использована система алгебраических уравнений полумарковской модели оценки надежности [40, 41, 43]. Для конструирования расчетной формулы оценки средней наработки на отказ применим следующий алгоритм.

В соответствии с исходной структурой СЗИ от НСД S_0 определим минимальный d и максимальный m запасы живучести. При этом согласно [38] под минимальным запасом живучести будем понимать число элементов СЗИ от НСД в минимальном замыкающем множестве s (s — минимальное количество модулей, при которых СЗИ от НСД остается частично работоспособной), уменьшенное на единицу.

Для максимального запаса живучести необходимо определить максимальное количество отказавших элементов, при котором остается хотя бы один работоспособный путь от входного элемента структуры по надежности СЗИ до ее выходного элемента.

Выделим m уровней деградации СЗИ от НСД и зададим состояния S_{ij}, при которых структурная схема по надежности СЗИ считается частично работоспособной. В качестве номера уровня деградации СЗИ выберем количество отказавших элементов.

Каждому типу структуры СЗИ от НСД сопоставим состояние S_{ij}. Назначим для каждого состояния номер соответствующей структуры, используя сквозную нумерацию состояний, а также зададим обобщенное неработоспособное состояние СЗИ от НСД.

Зададим возможные переходы между различными работоспособными состояниями, а также возможные переходы из работоспособных состояний в обобщенное неработоспособное состояние.

Установив интенсивности переходов между состояниями работоспособности и обобщенным состоянием неработоспособности, получим взвешенный граф состояний. Далее необходимо составить систему алгебраических уравнений для полумарковской модели расчета надежности системы со сложной структурой [39] и решить ее относительно состояния СЗИ $S_0(\overline{T_0})$.

Анализ технической документации основных типов СЗИ от НСД в АС [41] показал, что интенсивности отказов отдельных программных модулей можно принять равными, то есть $\lambda_i = \lambda$, интенсивности восстановления работоспособности отдельных программных модулей — также равными друг другу, то есть $\mu_i = \mu$, а число операций по восстановлению работоспособности — равным 3.

Анализ структурной схемы по надежности СЗИ от НСД в АС [40], представленной на рисунке 1, позволяет выбрать следующие параметры: $d = 1$, $m = 3$. В соответствии с принятыми значениями минимального и максимального запасов живучести СЗИ выделим три уровня их деградации.

Для первого уровня деградации можно выделить две различные структуры СЗИ от НСД — S_{11} и S_{12}, остающиеся частично работоспособными. Структурные схемы СЗИ от НСД при первом уровне деградации представлены на рисунках 4 и 5 соответственно.

Для второго уровня деградации можно выделить три различные структуры СЗИ от НСД — S_{21}, S_{22}, S_{23}, остающиеся частично работоспособными. Структурные схемы СЗИ от НСД при втором уровне деградации представлены на рисунках 6-8 соответственно.

Для третьего уровня деградации можно выделить структуру СЗИ от НСД S_{31}, остающуюся частично работоспособной. Структурная схема СЗИ от НСД при третьем уровне деградации представлена на рисунке 9.

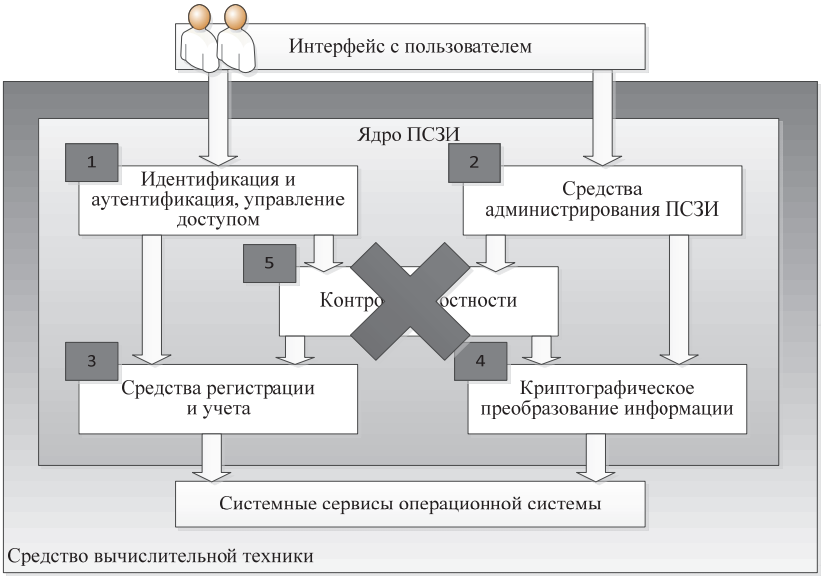

Рис. 4. Структурная схема S_{11} СЗИ от НСД для первого уровня деградации

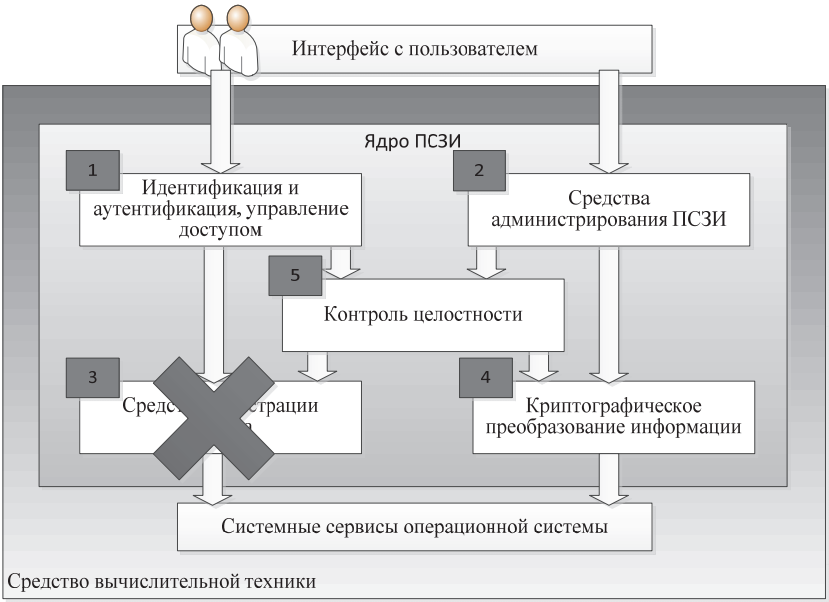

Рис. 5. Структурная схема S_{12} СЗИ от НСД для первого уровня деградации

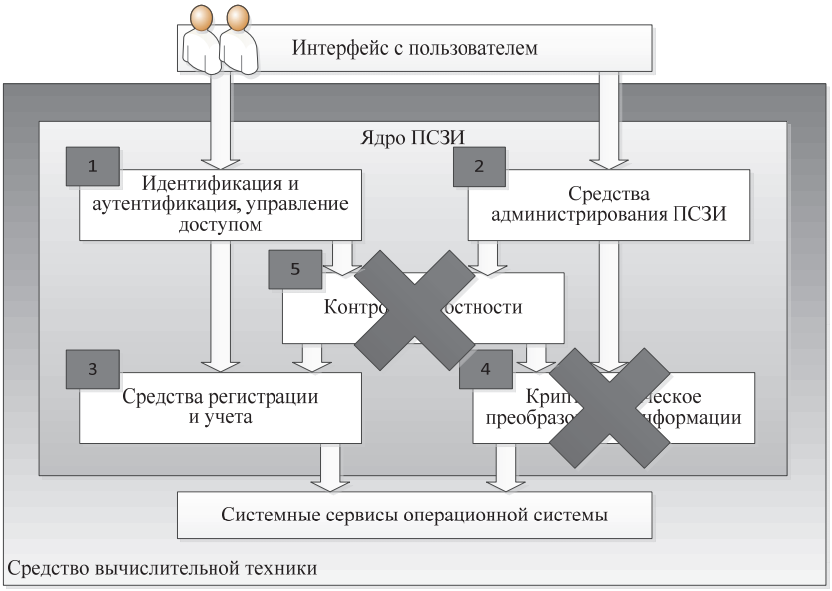

Рис. 6. Структурная схема S_{21} СЗИ от НСД для второго уровня деградации

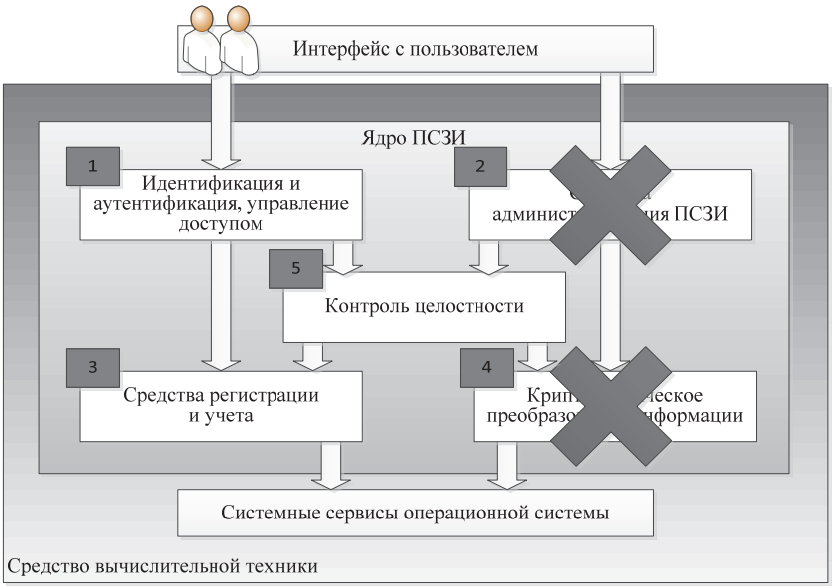

Рис. 7. Структурная схема S_{22} СЗИ от НСД для второго уровня деградации

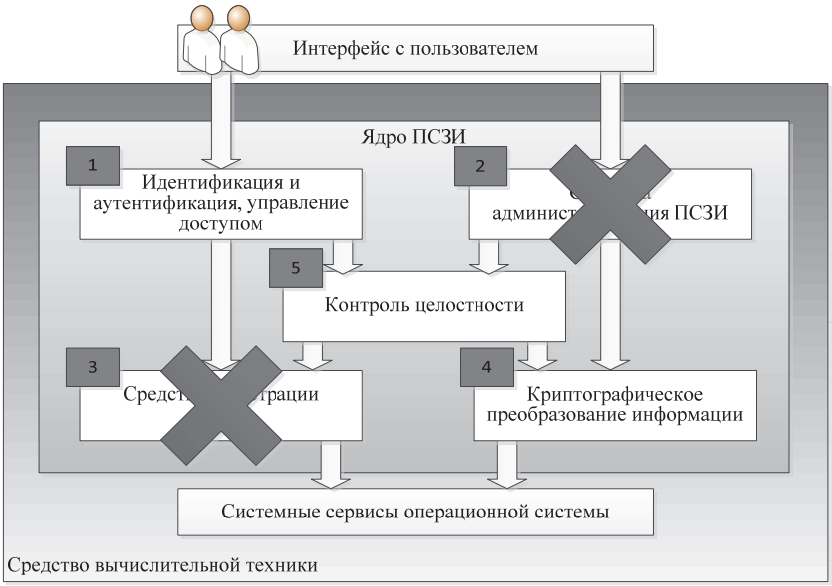

Рис. 8. Структурная схема S_{23} СЗИ от НСД для второго уровня деградации

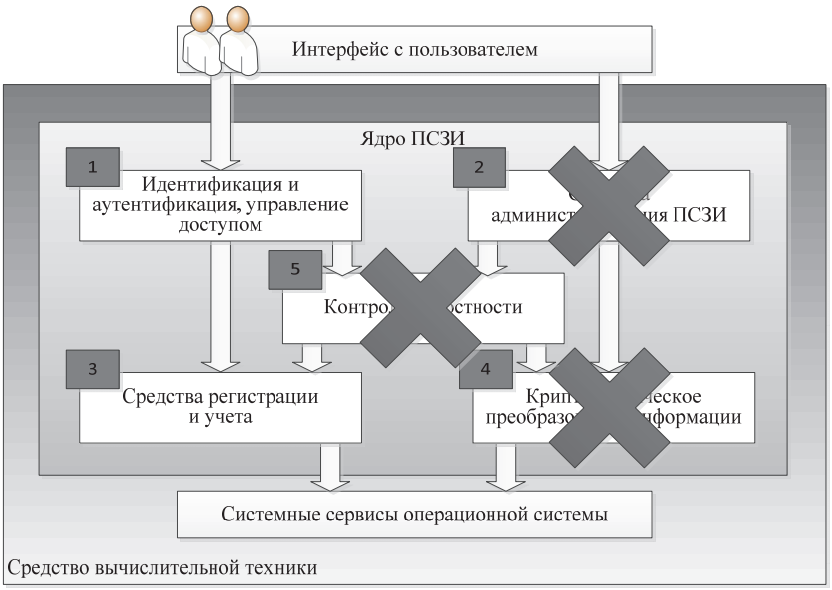

Рис. 9. Структурная схема S_{31} СЗИ от НСД для третьего уровня деградации

Составим граф смены состояний структурной схемы по надежности СЗИ от НСД. При этом можно выделить 6 состояний с частичной работоспособностью, одно состояние определить как полностью работоспособное, а другое — как обобщенное неработоспособное состояние.

Граф смены состояний работоспособности программных модулей СЗИ представлен на рисунке 10.

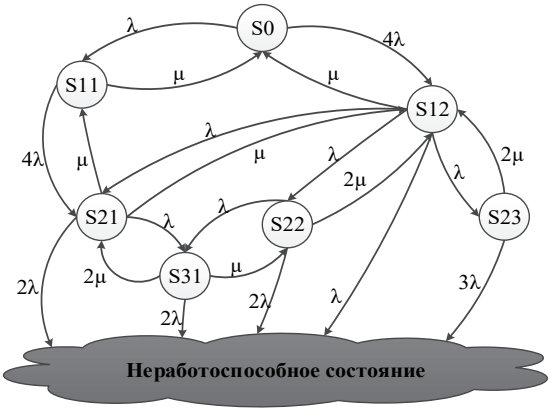

Рис. 10. Граф смены состояний работоспособности СЗИ от НСД

Система алгебраических уравнений имеет следующий вид:

$$\begin{cases} \overline{T}_0 = \dfrac{1}{5\lambda} + \dfrac{1}{5}\overline{T}_1 + \dfrac{4}{5}\overline{T}_2, \\ \overline{T}_1 = \dfrac{1+\mu\overline{T}_0 + 4\lambda\overline{T}_3}{\mu+4\lambda}, \\ \overline{T}_2 = \dfrac{1+\mu\overline{T}_0 + \lambda\overline{T}_3 + \lambda\overline{T}_4 + \lambda\overline{T}_5}{\mu+4\lambda}, \\ \overline{T}_3 = \dfrac{1+\mu\overline{T}_1 + \mu\overline{T}_2 + \lambda\overline{T}_6}{2\mu+3\lambda}, \\ \overline{T}_4 = \dfrac{1+2\mu\overline{T}_2 + \lambda\overline{T}_6}{2\mu+3\lambda}, \\ \overline{T}_5 = \dfrac{1+2\mu\overline{T}_2}{2\mu+3\lambda}, \\ \overline{T}_6 = \dfrac{1+2\mu\overline{T}_1 + \mu\overline{T}_4}{3\mu+2\lambda}, \end{cases} \quad (9)$$

где $\overline{T_i}$ — среднее время нахождения процесса, формализуемого графом (рисунок 10), в *i*-ом состоянии.

Для решения представленной системы алгебраических уравнений перейдем к безразмерным переменным $a_i = \lambda \overline{T_i}$ и $\rho = \frac{\lambda}{\mu}$. Тогда систему уравнений (9) можно преобразовать к виду:

$$\begin{cases} a_o = \dfrac{(1 + a_1 + 4a_2)}{5}, \\ a_1 = \dfrac{(\rho + a_0 + 4\rho a_3)}{1 + 4\rho}, \\ a_2 = \dfrac{(\rho + a_0 + \rho(a_3 + a_4 + a_5)}{1 + 4\rho}, \\ a_3 = \dfrac{(\rho + a_1 + a_2 + \rho a_6)}{(2 + 3\rho)}, \\ a_4 = \dfrac{(\rho + 2a_2 + \rho a_6)}{(2 + 3\rho)}, \\ a_5 = \dfrac{(\rho + 2a_2)}{(2 + 3\rho)}, \\ a_6 = \dfrac{(\rho + 2a_2 + a_4)}{(3 + 2\rho)}. \end{cases} \tag{10}$$

Совершив эквивалентные преобразования, упростим систему алгебраических уравнений (10) и приведем ее к виду:

$$\begin{cases} a_o = \dfrac{(1 + a_1 + 4a_2)}{5}, \\ a_1 = \dfrac{(\rho + a_0 + 4\rho a_3)}{1 + 4\rho}, \\ a_2 = \dfrac{(2\rho(1 + 2\rho) + (2 + 3\rho)(a_0 + \rho a_3 + \rho a_4)}{(2 + 9\rho + 12\rho^2)}, \\ a_3 = \dfrac{(3\rho(1 + \rho) + (3 + 2\rho)(a_1 + a_2) + \rho a_4)}{(6 + 11\rho + 6\rho^2)}, \\ a_4 = \dfrac{(3\rho(1 + \rho) + 2(3 + 2\rho)a_2 + 2\rho a_3)}{(6 + 10\rho + 6\rho^2)}. \end{cases} \tag{11}$$

Для решения полученной системы алгебраических уравнений (11) относительно состояния S_0 целесообразно использовать метод определителей:

$$P_0 = a_0 = \lambda \overline{T}_0 = \Delta_0 / \Delta, \tag{12}$$

где:

$$\Delta = \begin{vmatrix} 1 & -0.2 & -0.8 & 0 & 0 \\ \frac{-1}{1+4\rho} & 1 & 0 & -\frac{4\rho}{1+4\rho} & 0 \\ \frac{-2-2\rho}{2+9\rho+12\rho^2} & 0 & 1 & \frac{-\rho(2+3\rho)}{2+9\rho+12\rho^2} & \frac{-\rho(2+3\rho)}{2+9\rho+12\rho^2} \\ 0 & \frac{-3-2\rho}{6+11\rho+6\rho^2} & \frac{-3-2\rho}{6+11\rho+6\rho^2} & 1 & \frac{-\rho}{6+11\rho+6\rho^2} \\ 0 & 0 & \frac{-2(3+2\rho)}{6+10\rho+6\rho^2} & \frac{-2\rho}{6+10\rho+6\rho^2} & 1 \end{vmatrix},$$

$$\Delta_0 = \begin{vmatrix} 0.2 & -0.2 & -0.8 & 0 & 0 \\ \frac{\rho}{1+4\rho} & 1 & 0 & -\frac{4\rho}{1+4\rho} & 0 \\ \frac{2\rho(1+2\rho)}{2+9\rho+12\rho^2} & 0 & 1 & \frac{-\rho(2+3\rho)}{2+9\rho+12\rho^2} & \frac{-\rho(2+3\rho)}{2+9\rho+12\rho^2} \\ \frac{3\rho(1+\rho)}{6+11\rho+6\rho^2} & \frac{-3-2\rho}{6+11\rho+6\rho^2} & \frac{-3-2\rho}{6+11\rho+6\rho^2} & 1 & \frac{-\rho}{6+11\rho+6\rho^2} \\ \frac{3\rho(1+\rho)}{6+10\rho+6\rho^2} & 0 & \frac{-2(3+2\rho)}{6+10\rho+6\rho^2} & \frac{-2\rho}{6+10\rho+6\rho^2} & 1 \end{vmatrix}.$$

Выражение (12) является результирующим аналитическим выражением оценивания среднего времени наработки на отказ СЗИ от НСД в АС.

5. Результаты оценивания надежности систем защиты информации от несанкционированного доступа. При использовании разработанных методик и автоматизированных средств оценивания показателей надежности СЗИ от НСД в АС выбрана распространенная технологическая схема обработки конфиденциальной информации, рекомендованная технической документацией [38, 41]. При этом приняты следующие допущения: АС представляет собой отдельное автоматизированное рабочее

место; объектом защиты является конфиденциальная информация; защита информации реализуется СЗИ от НСД в соответствии с 3 классом защищенности [9, 10]; ЭВМ работает под управлением ОС Windows на ПЭВМ класса Pentium.

Расчеты по оцениванию надежности СЗИ проведены в среде Mathcad 15.

5.1. Результаты оценивания вероятности безотказной работы систем защиты информации от несанкционированного доступа в течение рабочей смены. На рисунках 11-19 представлены значения вероятностей работоспособного состояния СЗИ от НСД с исходным уровнем первичных ошибок $\lambda_i = 10^{-7}, 10^{-6}, 10^{-5}$ и временем работы СЗИ, равным 5, 10 и 20 часов соответственно, рассчитанные с использованием формулы (1) расчета вероятности безотказной работы СЗИ от НСД для следующих возможных размеров исходного кода программы, реализующей СЗИ от НСД [11]:

——— — размер исходного кода программы — 100 Мб;

– – – – – — размер исходного кода программы — 150 Мб;

..... — размер исходного кода программы — 200 Мб;

— · — · — размер исходного кода программы — 250 Мб.

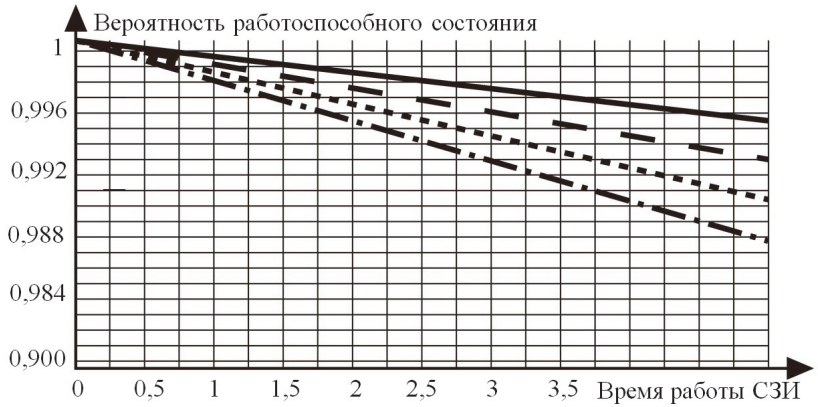

Рис. 11. Зависимость вероятности работоспособного состояния СЗИ от НСД от времени с исходным уровнем первичных ошибок $\lambda_i = 10^{-7}$, время работы СЗИ — 5 часов

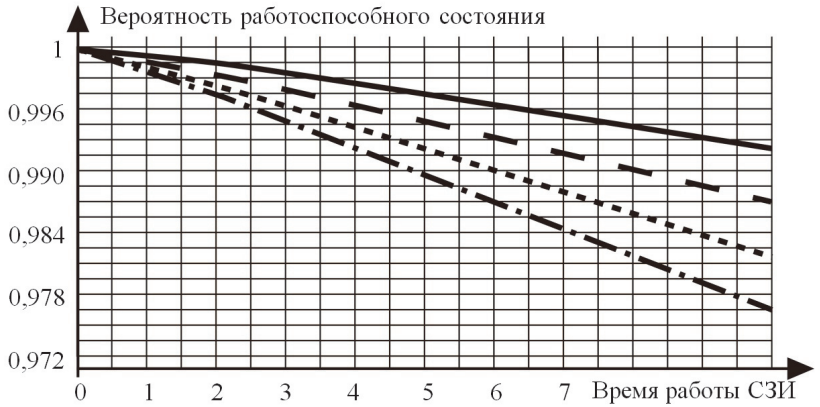

Рис. 12. Зависимость вероятности работоспособного состояния СЗИ от НСД от времени с исходным уровнем первичных ошибок $\lambda_i = 10^{-7}$, время работы СЗИ — 10 часов

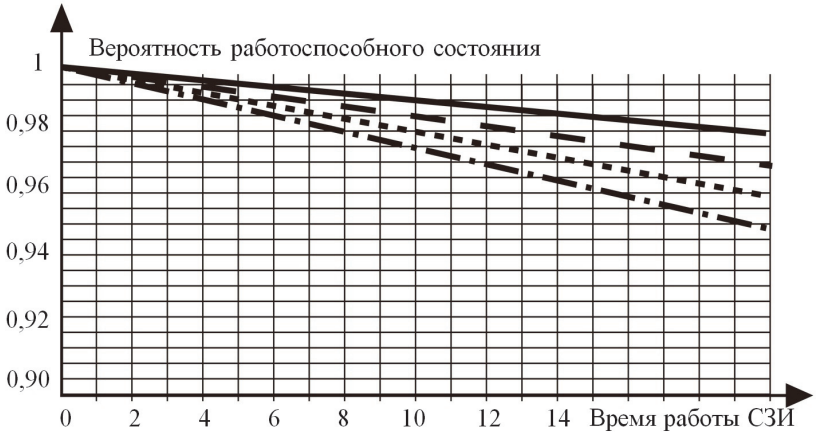

Рис. 13. Зависимость вероятности работоспособного состояния СЗИ от НСД от времени с исходным уровнем первичных ошибок $\lambda_i = 10^{-7}$, время работы СЗИ — 20 часов

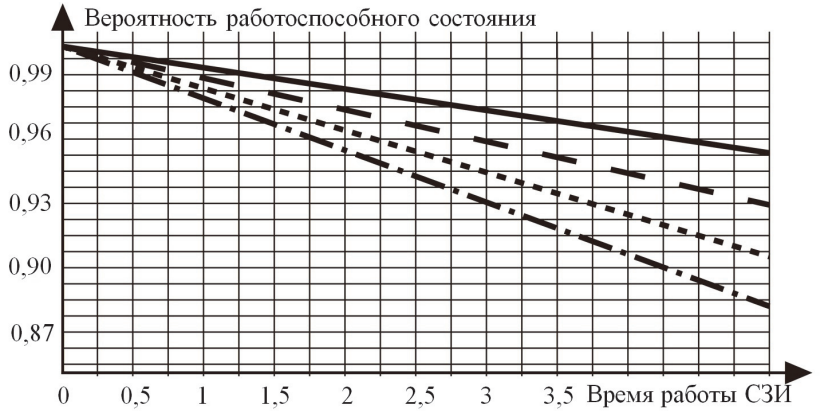

Рис. 14. Зависимость вероятности работоспособного состояния СЗИ от НСД от времени с исходным уровнем первичных ошибок $\lambda_i = 10^{-6}$, время работы СЗИ — 5 часов

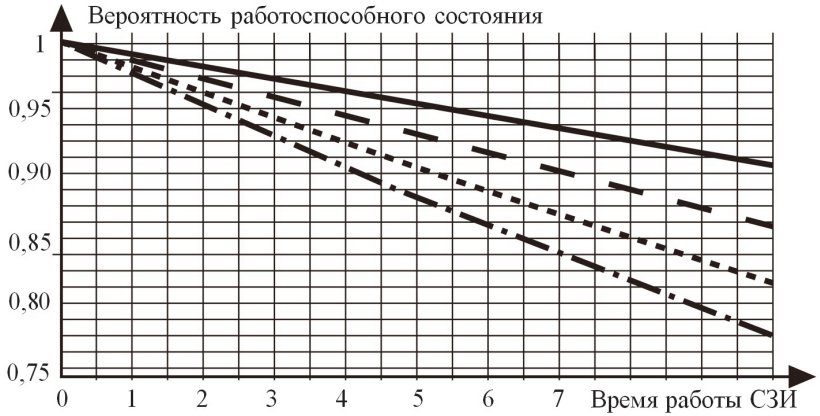

Рис. 15. Зависимость вероятности работоспособного состояния СЗИ от НСД от времени с исходным уровнем первичных ошибок $\lambda_i = 10^{-6}$, время работы СЗИ — 10 часов

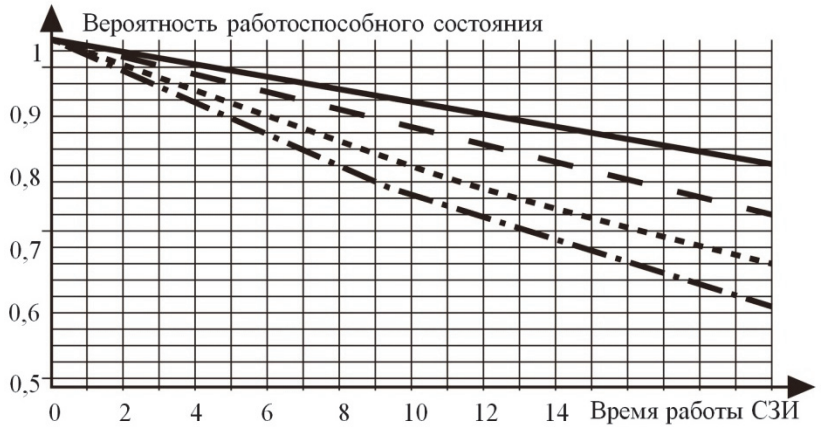

Рис. 16. Зависимость вероятности работоспособного состояния СЗИ от НСД от времени с исходным уровнем первичных ошибок $\lambda_i = 10^{-6}$, время работы СЗИ — 20 часов

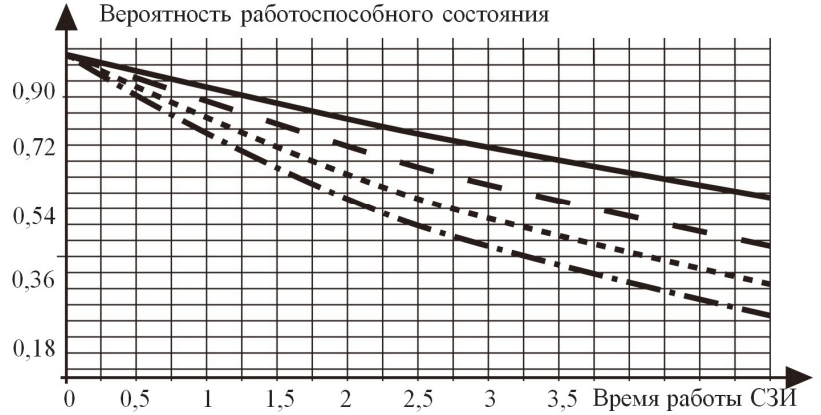

Рис. 17. Зависимость вероятности работоспособного состояния СЗИ от НСД от времени с исходным уровнем первичных ошибок $\lambda_i = 10^{-5}$, время работы СЗИ — 5 часов

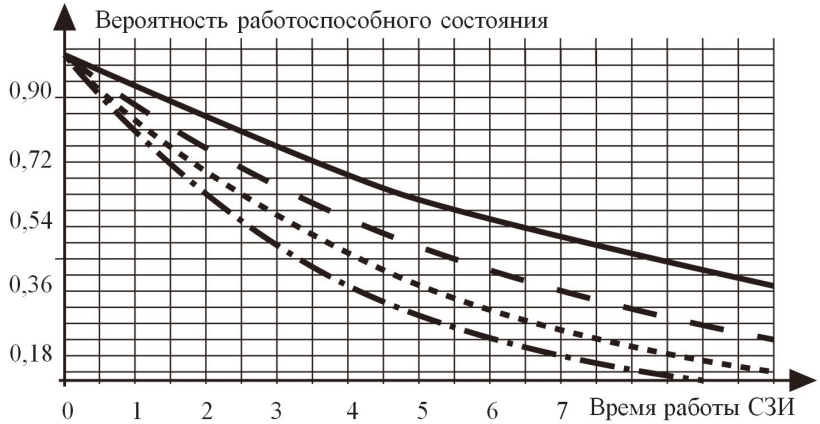

Рис. 18. Зависимость вероятности работоспособного состояния СЗИ от НСД от времени с исходным уровнем первичных ошибок $\lambda_i = 10^{-5}$, время работы СЗИ — 10 часов

Рис. 19. Зависимость вероятности работоспособного состояния СЗИ от НСД от времени с исходным уровнем первичных ошибок $\lambda_i = 10^{-5}$, время работы СЗИ — 20 часов

5.2. Результаты оценивания коэффициента готовности систем защиты информации от несанкционированного доступа. На рисунке 20 представлены значения коэффициента готовности СЗИ от НСД, рассчитанные с использованием методики расчета коэффициента готовности для следующих возможных размеров исходного кода программы (из всего диапазона возможных значений), реализующей СЗИ от НСД, с исходным уровнем первичных ошибок $\lambda_i = 10^{-7}$ [11]:

— размер исходного кода программы — 100 Мб:

— размер исходного кода программы — 200 Мб;

— размер исходного кода программы — 300 Мб:

— размер исходного кода программы — 1000 Мб.

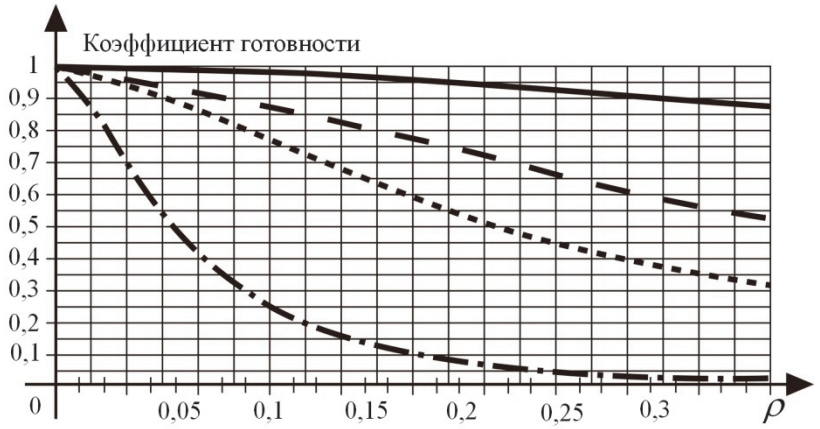

Рис. 20. Зависимость коэффициента готовности СЗИ от обобщенного параметра потоков отказов восстановлений ρ

5.3. Результаты оценивания показателя средней наработки систем защиты информации от несанкционированного доступа на отказ. В таблице 1 представлены результаты расчетов средней наработки СЗИ от НСД на отказ. Расчеты проведены в соответствии с методикой оценивания показателя средней наработки СЗИ от НСД на отказ, разработанной в статье. В таблице приведены средние значения наступления событий, связанных с деградацией структуры СЗИ от НСД, в соответствии с рисунком 10 (шесть состояний СЗИ от НСД с частичной работоспособностью).

Таблица 1. Результаты расчётов средней наработки СЗИ от НСД на отказ

ρ	$\lambda_0 \overline{T}_0$	$\lambda_0 \overline{T}_{11}$	$\lambda_0 \overline{T}_{21}$	$\lambda_0 \overline{T}_{22}$	$\lambda_0 \overline{T}_{23}$	$\lambda_0 \overline{T}_{31}$
0,01	25,47	35,46	25,22	25,21	25,10	25,06
0,05	5,52	5,50	5,47	5,27	5,15	5,12
0,10	3,07	3,03	3,03	2,82	2,69	2,68
0,20	1,87	1,83	1,83	1,64	1,51	1,51
0,30	1,49	1,44	1,44	1,26	1,14	1,14

6. Заключение. В статье впервые предложены методики оценивания надежности СЗИ от НСД АС в защищенном исполнении, учитывающие особенности архитектурного построения СЗИ от НСД и принципы их функционирования при решении задач защиты информации. При решении триединой задачи обеспечения конфиденциальности, целостности и доступности информации применены разные критерии надежности. Разработанные методики апробированы путем проведения расчетов показателей надежности СЗИ от НСД с типовыми структурными схемами построения и типовыми значениями характеристик остаточных первичных ошибок в программном коде и объеме программы.

Применение предложенных методик позволит разработать разделы конструкторской документации («Пояснительная записка к техническому проекту») при создании СЗИ от НСД, содержащие расчеты надежности. Полученные оценки показателей надежности для усредненных характеристик СЗИ могут служить основой для обоснования требований к системе эксплуатации СЗИ от НСД АС подразделениями по обеспечению ИБ, а также использоваться как требования по надежности, содержащиеся в нормативной документации регуляторов совместно с техническими требованиями по защите информации.

Литература

1. ФСТЭК РФ. Руководящий документ. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). URL: https://azanpa.ru/fstek-rossii-vypiska-ot15022008-h1468056/6/6.3/ (дата обращения: 10.07.2019).
2. ФСТЭК РФ. Руководящий документ. Методика определения угроз безопасности информации в информационных системах. URL: https://fstec.ru/component/attachments/download/ 812 (дата обращения: 10.07.2019).
3. *Герасименко В.А., Малюк А.А.* Основы защиты информации // М.: МИФИ. 1997. 537 с.
4. *Zhu R., Zeng Y., Xu L., Yi X.* Lightweight Privacy Preservation for Securing Large-Scale Database-Driven Cognitive Radio Networks with Location Verification // Security and Communication Networks. 2019. vol. 10. pp. 1–12.

5. *Nia M.A., Bahrak B., Kargahi M., Fabian B.* Detecting New Generations of Threats Using Attribute-Based Attack Graphs // IET Information Security. 2019. vol. 13. no. 4. pp. 293–303.
6. *Яковина В.С., Федасюк Д.В., Мамроха Н.М.* Аналіз використання аспектно-орієнтованого програмування як засобу підвищення надійності програмного забезпечення // Інженерія програмного забезпечення. 2010. Т. 2. №. 2. С. 24–29.
7. ГОСТ Р ИСО/МЭК 15408-1-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Часть 2. Функциональные компоненты безопасности. Часть 3. Компоненты доверия к безопасности // М.: Стандартинформ. 2014.
8. National vulnerability database. URL: https://nvd.nist.gov (дата обращения: 22.06.2019).
9. ФСТЭК РФ. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации. URL:https://dokipedia.ru/document/5326599 (дата обращения: 10.07.2019).
10. ФСТЭК РФ. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. URL:https://dokipedia.ru/document/ 5182727 (дата обращения: 10.05.2019).
11. ГОСТ 28195. Оценка качества программных средств. Общие положения. URL:http://www.a-podkidyshev.ru/GOST/28195-89.pdf (дата обращения: 23.04.2019).
12. ГОСТ 28806-89. Качество программных средств. Термины и определения. URL: http://www.kimmeria.nw.ru/standart/glosys/gost_ 28806_90.pdf (дата обращения: 23.04.2019).
13. *Dordevic N.* Software quality standards // Military Technical Courier. 2017. vol. 65. no. 1. pp. 102–124.
14. *Аббасов А.Э., Аббасов Т.Э.* Оценка качества программного обеспечения для современных систем обработки информации // Информационно-технологический вестник. 2015. № 5(3). С. 15–28.
15. *Pandian P.S.* Adopting security checks in business transactions using formal-oriented analysis processes for entrepreneurial students // International Journal of Electrical Engineering & Education. 2019. pp. 101–112.
16. *Arsanjani A.* Empowering the business analyst for on demand computing // IBM Systems Journal. 2005. vol. 44. no. 1. pp. 67–80.
17. *Пак В.О., Абраров Р.Д., Курязов Д.А.* Software testing as integral part of software quality // Молодой учёный. 2016. № 9-5. С. 29–32.
18. *Щенников А.Н.* Качество информационных систем // ИТНОУ. 2018. № 1(5). С. 53–62.
19. *Ayyub B.M., McCuen R.H.* Probability, Statistics and Reliability for Engineers and Scientists // CRC Press. 2016. 656 p.
20. *Тимашев С.А., Похабов Ю.П.* Проблемы комплексного анализа и оценки индивидуальной конструкционной надёжности космических аппаратов (на примере поворотных конструкций) // Екатеринбург: АМБ. 2018. 38 с.
21. *Shubinsky I.B., Rozenberg I.N., Papic L.* Adaptive fault tolerance in real time information systems // Reliability: Theory & Applications. 2017. vol. 12. no. 1(44). pp. 18–25.
22. *Levitin G., Finkelstein M., Huang H.Z.* Scheduling of imperfect inspections for reliability critical systems with shock-driven delayed defects and failures // Reliability Engineering & System Safety. 2019. vol. 189. . pp. 89–98.

23. *Paredes R., Dueñas-Osorio L., Meel K.S., Vardi M.Y.* Principled network reliability approximation: A counting-based approach // Reliability Engineering & System Safety. 2019. vol. 191. pp. 93–110.
24. *Jones C.* Applied software measurement: Assuring // Productivity and Quality. 1997.
25. *Kit E.* Software Testing in the Real World: Improving the Process // Addison-Wesley. 1996.
26. *Гнеденко Б.В., Беляев Ю.К., Соловьёв А.Д.* Математические методы в теории надёжности // М.: КД Либроком. 2019. 584 с.
27. *Казарин О.В., Шубинский И.Б.* Надёжность и безопасность программного обеспечения: учеб. пособие для бакалавриата и магистратуры // М.: МГУ им. М.В. Ломоносова. 2018. 342 с.
28. *Londeix B.* Cost estimation for software development // Addison-Wesley Longman Publishing Co. 1987.
29. Об утверждении Доктрины информационной безопасности Российской Федерации: указ Президента РФ от 05.12.2016 № 646. URL: http://www.consultant.ru/document/cons_doc_LAW_208191/ (дата обращения: 07.06.2019).
30. *Малафеев С.И., Копейкин А.И.* Надёжность технических систем: примеры и задачи // СПб.: Лань. 2016. 320 с.
31. *Зуб А.Т.* Принятие управленческих решений: учебник и практикум. 2-е изд. испр. и доп. // М.: Юрайт. 2018. 332 с.
32. *Гулов В.П. и др.* Методика оценки надёжности системы защиты информации от несанкционированного доступа медицинской информационной системы // Прикладные информационные аспекты медицины. № 1. 2018. С. 202–209.
33. *Скрыпников А.В. и др.* Нормирование требований к характеристикам программных систем защиты информации // Вестник Воронежского государственного университета инженерных технологий. 2018. Т. 80. № 4. С. 96–110.
34. *Филяк П.Ю., Данилова Ю.Н., Гришина Н.В., Мухаммед Н.А.* Обеспечение безопасности в сети интернет на основе сертифицированных решений для обнаружения и предотвращения вторжений/атак // Информация и безопасность. 2018. Т. 21. № 4. С. 510–515.
35. *Оленева Н.Р., Семяшкина Д.С.* Российские и зарубежные разработки в области информационной безопасности // Информация и безопасность. 2018. Т. 21 № 3. С. 380–383.
36. *Samaan N.A. et al.*. Dynamic Contingency Analysis Tool — Phase 1, PNNL-24843, Pacific Northwest National Laboratory, Richland, WA, 2015. URL: http://www.pnnl.gov/main/ publications/external/technical_reports/PNNL-24843.pdf (дата обращения: 28.05.2019).
37. *Дровникова И.Г., Етеппев А.С., Рогозин Е.А.* Основные виды уязвимостей и взаимосвязь компонентов безопасности при обосновании показателей надёжности системы защиты информации от несанкционированного доступа в автоматизированных системах // Приборы и системы. Управление, контроль, диагностика. 2019. № 3. С. 59–64.
38. *Черкесов Г.Н., Воропай Н.И., Сухарев М.Г., Чельцов М.Б.* Надёжность систем энергетики // Новосибирск: Наука. 1999. 434 с.
39. *Дровникова И.Г., Етеппев А.С., Рогозин Е.А.* Формирование критериев работоспособности и отказов системы защиты информации от несанкционированного доступа автоматизированной системы // Приборы и системы. Управление, контроль, диагностика. М.: Научтехлитиздат. 2019. № 5. С. 18–24.
40. *Рогозин Е.А. и др.* Методы и средства оценки защищённости автоматизированных систем органов внутренних дел: монография // Воронежский институт МВД России. 2017. 88 с.

41. *Conto J.* MPjobs — a tool to run PSSe scripts in parallel // ERCOT. 2015.
42. *Змеев А.А. и др.* Методы и средства эволюционного и структурного моделирования при обосновании требований к программным системам защиты информации // Воронежский институт МВД России. 2015. 91 с.

Бокова Оксана Игоревна — д-р техн. наук, профессор, заместитель начальника, институт по научной работе, Воронежский институт Министерства внутренних дел России. Область научных интересов: системы защиты информации, оптимальное управление безопасностью территориальных сегментов информационно-телекоммуникационных систем, управление в социально-экономических системах, математическое моделирование информационных процессов в условиях информационного конфликта. Число научных публикаций — 220. o.i.bokova@gmail.com; пр. Патриотов, 53, 394065, Воронеж, Российская Федерация; р.т.: +7(473) 200-50-03; факс: +7(473) 200-55-00.

Дровникова Ирина Григорьевна — д-р техн. наук, доцент, профессор, кафедра автоматизированных информационных систем органов внутренних дел, Воронежский институт Министерства внутренних дел России. Область научных интересов: проектирование систем защиты информации от несанкционированного доступа в автоматизированных системах, эволюционное моделирование, теория вероятности, прикладная информатика, управление в социально-экономических системах. Число научных публикаций — 215. idrovnikova@mail.ru; пр. Патриотов, 53, 394065, Воронеж, Российская Федерация; р.т.: +7(473) 247-67-07; факс: +7(473) 200-55-00.

Етеннев Андрей Сергеевич — адъюнкт, кафедра автоматизированных информационных систем органов внутренних дел, Воронежский институт Министерства внутренних дел России. Область научных интересов: надёжность функционирования систем защиты информации от несанкционированного доступа в автоматизированных системах, прикладная информатика. Число научных публикаций — 4. electronag@gmail.com; пр. Патриотов, 53, 394065, Воронеж, Российская Федерация; р.т.: +7(473) 247-67-07; факс: +7(473) 200-55-00.

Рогозин Евгений Алексеевич — д-р техн. наук, профессор, профессор, кафедра автоматизированных информационных систем органов внутренних дел, Воронежский институт Министерства внутренних дел России. Область научных интересов: защита информации от несанкционированного доступа в автоматизированных системах, проектирование и управление процессами защиты информации на основе количественной оценки систем защиты информации, прикладная информатика. Число научных публикаций — 250. evgenirogozin@yandex.ru; пр. Патриотов, 53, 394065, Воронеж, Российская Федерация; р.т.: +7(473) 247-67-07; факс: +7(473) 200-55-00.

Хвостов Виктор Анатольевич — канд. техн. наук, доцент, кафедра информационной безопасности, Воронежский государственный университет инженерных технологий России. Область научных интересов: надёжность систем защиты информации, применение методов системного анализа в защите информации, технология разработки программных систем защиты информации. Число научных публикаций. Число научных публикаций — 45. hvahva1@mail.ru; пр. Революции, 19, 394036, Воронеж, Российская Федерация; р.т.: +7(473) 255-42-67; факс: +7(473) 255-42-67.

DOI 10.15622/sp.2019.18.6.1301-1332

O.I. BOKOVA, I.G. DROVNIKOVA, A.S. ETEPNEV, E.A. ROGOZIN,
V.A. KHVOSTOV

METHODS OF ESTIMATING RELIABILITY OF INFORMATION SECURITY SYSTEMS WHICH PROTECT FROM UNAUTHORIZED ACCESS IN AUTOMATED SYSTEMS

Bokova O.I., Drovnikova I.G., Etepnev A.S., Rogozin E.A., Khvostov V.A. **Methods of Estimating Reliability of Information Security Systems which Protect from Unauthorized Access in Automated Systems.**

Abstract. Modern methods of protecting information from unauthorized access in automated systems are based on the use of specialized information security systems from unauthorized access. Security systems are necessarily included in the form of additional software systems in the software as in a secure execution. Information security systems from unauthorized access can be developed not only in a process of automated systems design, but also complement the system-wide software of functioning systems. The use of the information security systems from unauthorized access can reduce a overall reliability of the automated systems, if they contain errors that are not detected during debugging. The reliability of the information security systems affects effectiveness of information security (confidentiality, integrity and availability). Guidelines of the Federal Service for Technical and Export Control (FSTEC) of Russia are a methodological basis for the formation of the information security systems' image both in the process of development and in the process of modernization of the automated systems. The guidance documents of FSTEC of Russia do not contain methodological approaches to assessing the reliability of these program systems. In this regard, the actual design of techniques of estimating reliability of the information security systems from unauthorized access in automated systems in a secure execution. The structural complexity of the information security systems from unauthorized access and large number of functions performed necessitates the use of three reliability indicators that characterize the system in solving problems of confidentiality, integrity and availability of information. To develop the technique, the known methods of evaluating the reliability of complex systems are used, which do not allow their decomposition into serial and parallel connection. The developed methods were tested in assessing the reliability of the information security systems from unauthorized access with typical indicators of initial characteristics. The results of calculations and prospects of using the developed methods are presented in the paper.

Keywords: Information Security System, Unauthorized Access, Automated System, Reliability, Refusal, Information Confidentiality, Information Integrity, Information Availability.

Bokova Oksana Igorevna — Ph.D., Dr.Sci., Professor, Deputy Head, Institute of Scientific Work, Voronezh Institute of the Ministry of Interior of Russia. Research interests: information systems security, optimal security management of territorial segments of information and telecommunication systems, management in socio-economic systems, mathematical modeling of information processes in the context of information conflict. The number of publications — 220. o.i.bokova@gmail.com; 53, pr. Patriotov, 394065, Voronezh, Russian Federation; office phone: +7(473) 200-50-03; fax: +7(473) 200-55-00.

Drovnikova Irina Grigorevna — Ph.D., Dr.Sci., Associate Professor, Professor, Department of Automated Information Systems in Interior Affairs, Voronezh Institute of the Ministry of Interior of Russia. Research interests: design of information security systems against unauthorized access in automated systems, evolutionary modeling, probability theory, applied

informatics, social-and-economic system management. The number of publications — 215. idrovnikova@mail.ru; 53, pr. Patriotov, 394065, Voronezh, Russian Federation; office phone: +7(473) 247-67-07; fax: +7(473) 200-55-00.

Etepnev Andrei Sergeevich — Ph.D. student, Department of Automated Information Systems in Interior Affairs, Voronezh Institute of the Ministry of Interior of Russia. Research interests: reliability of information security systems against unauthorized access in automated systems, applied informatics. The number of publications — 4. electronag@gmail.com; 53, pr. Patriotov, 394065, Voronezh, Russian Federation; office phone: +7(473) 247-67-07; fax: +7(473) 200-55-00.

Rogozin Evgeniy Alekseevich — Ph.D., Dr.Sci., Professor, Professor, Department of Automated Information Systems in Interior Affairs, Voronezh Institute of the Ministry of Interior of Russia. Research interests: information security from unauthorized access in automated systems, design and management of information security processes based on the quantitative assessment of information security systems, applied informatics. The number of publications — 250. evgenirogozin@yandex.ru; 53, 394065, Russian Federation; office phone: +7(473) 247-67-07; fax: +7(473) 200-55-00.

Khvostov Victor Anatolevich — Ph.D., Associate Professor, Department of Information Security, Voronezh State University of Engineering Technologies. Research interests: reliability of information security systems, application of system analysis methods in information security, technology for developing software systems for information security. The number of publications — 45. hvahva1@mail.ru; 19, pr. Revolucii, 394036, Voronezh, Russian Federation; office phone: +7(473) 255-42-67; fax: +7(473) 255-42-67.

References

1. FSTEK RF. Rukovodyashchij dokument. Bazovaya model' ugroz bezopasnosti personal'nyh dannyh pri ih obrabotke v informacionnyh sistemah per-sonal'nyh dannyh (vypiska) [FSTEC RF. Guidance document. The basic model of threats to the security of personal data when they are processed in personal data information systems (extract)]. Available at: https:azanpa.ru.fstek-rossii-vypiska-ot15022008-h1468056-6-6.3 (accessed: 10.07.2019). (In Russ.).
2. FSTEK RF. Rukovodyashchij dokument. Metodika opredeleniya ugroz bez-opasnosti informacii v informacionnyh sistemah [FSTEC RF. [Guidance document. Methodology for identifying information security threats in information systems]. Available at: fstec.ru-component-attachments-download-812 (accessed: 10.07.2019). (In Russ.).
3. Gerasimenko V.A., Maljuk A.A. *Osnovy zashhity informacii* [Basis of information security]. Moscow: MIPI. 1997. 537 p. (In Russ.).
4. Zhu R., Zeng Y., Xu L., Yi X. Lightweight Privacy Preservation for Securing Large-Scale Database-Driven Cognitive Radio Networks with Location Verification. *Security and Communication Networks*. 2019. vol. 10. pp. 1–12.
5. Nia M.A., Bahrak B., Kargahi M., Fabian B. Detecting New Generations of Threats Using Attribute-Based Attack Graphs. *IET Information Security*. 2019. vol. 13. no. 4. pp. 293–303.
6. Jakovina V.S., Fedasjuk D.V., Mamroha N.M. [Analysis of the use of aspect-oriented programming as a means of improving software reliability]. *Inzhenerija programnogo zabezpechennja — Software Engineering*. 2010. Issue 2. vol. 2. pp. 24–29. (In Ukr.).
7. GOST R ISO/IEC 15408-1-2013. [Information technology. Methods and means of security. Criteria for assessing the security of information technology. Part 1. Introduction and general model. Part 2. Functional safety components. Part 3. Components of security confidence]. M.: Standardinform. 2014. (In Russ.).

8. National vulnerability database. Available at: https:nvd.nist.gov (accessed: 22.06.2019).
9. FSTEK RF. Rukovodyashchij dokument. Sredstva vychislitel'noj tekhniki. Zashchita ot nesankcionirovannogo dostupa k informacii. Pokazateli zashchishchyonnosti ot nesankcionirovannogo dostupa k informacii [FSTEC RF. Guidance document. Computing facilities. Protection against unauthorized access to information. Indicators of security against unauthorized access to information]. Available at: https:dokipedia.ru.document.5326599 (accessed: 10.07.2019). (In Russ.).
10. FSTEK RF. Rukovodyashchij dokument. Avtomatizirovannye sistemy. Zashchita ot nesankcionirovannogo dostupa k informacii. Klassifikaciya avtomatizirovannyh sistem i trebovaniya po zashchite informacii [FSTEC RF. Guidance document. Automated systems. Protection against unauthorized access to information. Classification of automated systems and information security requirements]. Available at: https:dokipedia.ru.document. 5182727. (accessed: 10.05.2019). (In Russ.).
11. GOST 28195. Ocenka kachestva programmnyh sredstv. Obshchie polozheniya [GOST 28195. Software quality assessment. General provisions]. Available at: http:www.a-podkidyshev.ru.GOST.28195-89.pdf (accessed: 23.04.2019). (In Russ.).
12. GOST 28806-89. Kachestvo programmnyh sredstv. Terminy i opredeleniya. [GOST 28806-89. Quality of software. Terms and definitions]. Available at: http:www.kimmeria.nw.ru.standart.glosys.gost_28806_90.pdf. (accessed: 23.04.2019). (In Russ.).
13. Dordevic N. Software quality standards. *Military Technical Courier*. 2017. vol. 65. no. 1. pp. 102–124.
14. Abbasov A.E., Abbasov T.E. [Quality evaluation software for modern information processing systems]. *Informacionno-tekhnologicheskij vestnik – Information Technology Bulletin.* 2015. vol. 5(3). pp. 15–28. (In Russ.).
15. Pandian P.S. Adopting security checks in business transactions using formal-oriented analysis processes for entrepreneurial students. *International Journal of Electrical Engineering & Education.* 2019. pp. 101–112.
16. Arsanjani A. Empowering the business analyst for on demand computing. *IBM Systems Journal.* 2005. vol. 44. no. 1. pp. 67–80.
17. Pak V.O., Abrarov R.D., Kuryazov D.A. [Software testing as integral part of software quality].*Young scientist*. 2016. vol. 9.5. pp. 29–32. (In Russ).
18. Shchennikov A.N. [Quality of information systems]. *ITNOU – ITNOU*. 2018. vol. 1(5). pp. 53–62. (In Russ.).
19. Ayyub B.M., McCuen R.H. Probability, Statistics and Reliability for Engineers and Scientists. CRC Press. 2016. 656 p.
20. Timashev S.A., Pohabov Ju.P. *Problemy kompleksnogo analiza i ocenki individual'noj konstrukcionnoj nadjozhnosti kosmicheskih apparatov* (*na primere povorotnyh konstrukcij*) [Problems of complex analysis and evaluation of individual structural reliability of spacecraft (on the example of rotary structures)]. Yekaterinburg: AMB. 2018. 38 p. (In Russ.).
21. Shubinsky I.B., Rozenberg I.N., Papic L. Adaptive fault tolerance in real time information systems. *Reliability: Theory & Applications.* 2017. vol. 12. no. 1(44). pp. 18–25.
22. Levitin G., Finkelstein M., Huang H.Z. Scheduling of imperfect inspections for reliability critical systems with shock-driven delayed defects and failures. *Reliability Engineering & System Safety.* 2019. vol. 189. . pp. 89–98.
23. Paredes R., Dueñas-Osorio L., Meel K.S., Vardi M.Y. Principled network reliability approximation: A counting-based approach. *Reliability Engineering & System Safety*. 2019. vol. 191. pp. 93–110.
24. Jones C. Applied software measurement: Assuring. Productivity and Quality. 1997.

25. Kit E. Software Testing in the Real World: Improving the Process. Addison-Wesley. 1996.
26. Gnedenko B.V., Belyaev Yu.K., Solov'yov A.D. *Matematicheskie metody v teorii nadyozhnosti* [Mathematical methods in the theory of reliability]. Moscow: KD Librokom. 2019. 584 p. (In Russ.).
27. Kazarin O.V., Shubinskij I.B. *Nadyozhnost' i bezopasnost' programmnogo obespecheniya: ucheb. posobie dlya bakalavriata i magistratury* [Software reliability and security: studies' manual for bachelor's and master's degrees]. M.: MGU im. M.V. Lomonosova. 2018. 342 p. (In Russ.).
28. Londeix B. Cost estimation for software development. Addison-Wesley Longman Publishing Co. 1987.
29. Ob utverzhdenii Doktriny informacionnoj bezopasnosti Rossijskoj Federacii: ukaz Prezidenta RF ot 05.12.2016 № 646. [On of the Information Security Doctrine of the Russian Federation: Decree of the President of the Russian Federation of December 5. 2016. №. 646]. Available at: http://www.consultant.ru/document/cons_doc_LAW_208191/ (accessed: 07.06.2019). (In Russ.).
30. Malafeev S.I., Kopejkin A.I. *Nadyozhnost' tekhnicheskih sistem: primery i zadachi* [Reliability of technical systems: examples and tasks]. SPb.: Lan'. 2016. 320 p. (In Russ.).
31. Zub A.T. *Prinyatie upravlencheskih reshenij*: uchebnik i praktikum. 2-e izd. ispr. i dop. [Management decision-making: textbook and workshop]. M.: Yurajt. 2018. 332 p. (In Russ.).
32. Gulov V.P. et al. [Methods of assessing the reliability of the information protection system from unauthorized access to medical information system]. *Prikladnye informacionnye aspekty mediciny —Applied information aspects of medicine*. vol. 1. 2018. pp. 202–209. (In Russ.).
33. Skrypnikov A.V. et al. [Regulation of requirements to characteristics of information security software systems]. *Vestnik Voronezhskogo gosudarstvennogo universiteta inzhenernyh tekhnologij – Proceedings of the Voronezh State University of Engineering Technologies.* 2018. Issue 80. vol. 4. pp. 96–110. (In Russ.).
34. Filyak P.Yu., Danilova Yu.N., Grishina N.V., Muhammed N.A. [Internet security based on certified intrusion/attack detection and prevention solutions]. *Informaciya i bezopasnost' – Information and security*. 2018. Issue 21. vol. 4. pp. 510–515. (In Russ.).
35. Oleneva N.R., Semyashkina D.S. [Russian and foreign developments in the field of information security]. *Informaciya i bezopasnost' – Information and security*. 2018. Issue 21. vol. 3. pp. 380–383. (In Russ.).
36. Samaan N.A. et al. Dynamic Contingency Analysis Tool — Phase 1, PNNL-24843, Pacific Northwest National Laboratory, Richland, WA, 2015. Available at: http://www.pnnl.gov/main/ publications/external/technical_reports/PNNL-24843.pdf (accessed: 28.05.2019).
37. Drovnikova I.G., Etepnev A.S., Rogozin E.A. [The main types of vulnerabilities and the relationship of security components in justifying the reliability of the information protection system from unauthorized access in automated systems]. *Pribory i sistemy. Upravlenie, kontrol', diagnostika – Instruments and systems. Monitoring, control and diagnostics.* 2019. vol. 3. pp. 59–64. (In Russ.).
38. Cherkesov G.N., Voropaj N.I., Suharev M.G., Chel'cov M.B. *Nadyozhnost' sistem energetiki* [Reliability of energy systems]. Novosibirsk:Nauka. 1999. 434 p. (In Russ.).
39. Drovnikova I.G., Etepnev A.S., Rogozin E.A. [Formation of performance criteria and failures of the system for protecting information from unauthorized access of the automated system]. *Pribory i sistemy. Upravlenie, kontrol', diagnostika – Instruments and systems. Monitoring, control and diagnostics.* Moscow: Nauchtechlitizdat. 2019. vol. 5. pp. 18–24. (In Russ.).

40. Rogozin E.A. et al. *Metody i sredstva ocenki zashchishchyonnosti avtomatizirovannyh sistem organov vnutrennih del: monografiya* [Methods and means of assessing the security of automated systems of internal Affairs bodies: monograph]. Voronezhskij institut MVD Rossii. 2017. 88 p. (In Russ.).
41. Conto J. MPjobs — a tool to run PSSe scripts in parallel. ERCOT. 2015.
42. Zmeev A.A. et al. *Metody i sredstva evolyucionnogo i strukturnogo modelirovaniya pri obosnovanii trebovanij k programmnym sistemam zashchity informacii* [Methods and means of evolutionary and structural modeling in justifying the requirements for software systems to protect information]. Voronezhskij institut MVD Rossii. 2015. 91 p. (In Russ.).