УДК 681.3:519.1

ИННОВАЦИОННЫЕ КОМПЬЮТЕРНЫЕ СИСТЕМЫ: ПОКАЗАТЕЛИ И МОДЕЛИ КАЧЕСТВА ТЕХНОЛОГИЧЕСКОГО УПРАВЛЕНИЯ КОМПЛЕКСОМ ПРОГРАММНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В КОМПЬЮТЕРНЫХ СИСТЕМАХ

С.В. Скрыль, М.А. Багаев, Д.В. Малышев, С.А. Малышев

Обосновывается система показателей качества технологического управления комплексом программных средств защиты информации от несанкционированного доступа в инновационных компьютерных системах. Рассматриваются особенности моделирования процессов защиты информации с целью определения значений отдельных показателей обеспечения конфиденциальности информации инновационного характера

Ключевые слова: компьютерная система, комплекс программных средств защиты информации от несанкционированного доступа, показатели качества технологического управления комплексом программных средств защиты информации от несанкционированного доступа

Исходя из сформулированных в /1/ методологических оснований для систематизации показателей качества защиты информации в компьютерных системах (КС) предполагается упорядочение такого рода показателей. По аналогии с /2/ сформируем классификационные основания структуры системы показателей качества технологического управления комплексом программных средств защиты информации (КПСрЗИ) от несанкционированного доступа (НСД) в КС (в терминах выражения /1/ – упорядочивающее множество). Такими основаниями являются следующие /3/:

интегративность;
нормативность;
конфликтность;
физическая измеримость.

Интегративность системы показателей качества управления защитой информации от НСД в КС, как свойство системы /3/, определяется целостностью такого рода системы, ее сохранения в условиях неоднородности и противоречивости элементов системы. Исходя из данного свойства системы определим его как классификационное основание, которому будет соответствовать показатель третьего (верхнего) уровня в иерархической структуре системы показателей. Таким показателем является защищенность информации в КС.

Нормативность охватывает показатели, которые определены нормативными документами ФСТЭК (Гостехкомиссии) /4/. Нормативность как значимость показателя, по определению, имеет высокий уровень, но уступает общесистемной значимости. Исходя из этого обстоятельства, определим нормативность как классификационное основание, которому будут соответствовать показатели второго уровня в иерархической структуре системы показателей. К таким показателям относятся конфиденциальность, целостность и доступность информации в КС.

Конфликтность отражает конфликтный характер взаимодействия КПСрЗИ с источниками угроз несанкционированного доступа к информации в КС. Конфиденциальность, как значимость показателя, должна обеспечивать представление в КПСрЗИ характеристик, связанных с характеристиками угроз НСД, и наоборот. Такие показатели, в отличие от нормативных, не определены документами ФСТЭК (Гостехкомиссии), что делает уровень их значимости ниже уровня значимости нормативных показателей. К таким показателям относятся информативная и временная критичность КПСрЗИ и угроз НСД, а также функциональность и адекватность КПСрЗИ и угроз НСД.

В таблице представлены характеристики угроз и КПСрЗИ, отражающиеся в этих показателях.

Скрыль Сергей Васильевич – ТКОС, ВИ ФСИН России, д-р техн. наук, профессор, e-mail: bsvlabs@mail.ru
Багаев Максим Александрович - МГТУ им. Н.Э. Баумана, соискатель, канд. техн. наук, тел. (495) 632-22-47
Малышев Дмитрий Валерьевич - ВГТУ, соискатель, тел. (473) 243-77-18
Малышев Сергей Анатольевич - ВГТУ, соискатель, e-mail: acs@vorstu.ru

Характеристики угроз и КПСрЗИ, отражающиеся в системе показателей качества защиты информационных источников

№ п/п	Наименование показателя	Характеристика
1	Информативная критичность КПСрЗИ	Объем защищаемой информации
2	Временная критичность КПСрЗИ	Время реакции на угрозу
3	Функциональность КПСрЗИ	Набор функций защиты от НСД
4	Адекватность КПСрЗИ	Снижение интенсивности потока проявления угроз НСД
5	Информативная критичность источников угроз компьютерным системам	Минимальный объем информации, подверженный воздействию угрозы
6	Временная критичность источников угроз компьютерным системам	Время существования угрозы
7	Функциональность источников угроз компьютерным системам	Требуемый набор функций
8	Адекватность источников угроз компьютерным системам	Потенциальная интенсивность потока проявления угроз НСД

Физическая измеримость охватывает те показатели, которые измеряются конкретными физическими величинами: временем и объемом. Такие показатели являются базовыми и относятся к показателям нулевого уровня.

Иерархичность структуры системы показателей качества управления защитой информации от НСД в КС предполагает следующую иерархию их представления:

1. Интегральный показатель нулевого уровня, определяющий состояние защищенности информации в КС в условиях воздействия множества угроз НСД, рассчитывается по вероятностной шкале и оценивает качество КПСрЗИ как системы, функционирующей по своему прямому назначению.

2. Частные показатели первого уровня рассчитываются по относительно-вероятностной шкале и определяют количественные значения качественного состояния информации.

3. Частные показатели второго уровня рассчитываются по абсолютной шкале определяют количественные значения негативных факторов при воздействии КПСрЗИ на КС и факторов, характеризующих качество функционирования КПСрЗИ.

Существует 13 типов взаимосвязи между показателями первого и второго уровня, представленные следующими параметрами (рисунок):

для информативной критичности:

1 - по объему перехватываемой информации;

2 - по объему информации, защищаемой от перехвата;

3 - по объему искажаемой информации;

4 - по объему информации, защищаемой от искажения;

для временной критичности:

5 - по времени старения информации;

6 - по времени доступа к информации;

для функциональности КПСрЗИ:

7 - по наличию функций защиты информации от копирования;

8 - по наличию функций контроля и восстановления корректности обрабатываемой информации;

9 - по наличию функций защиты информации от блокирования доступа к ней;

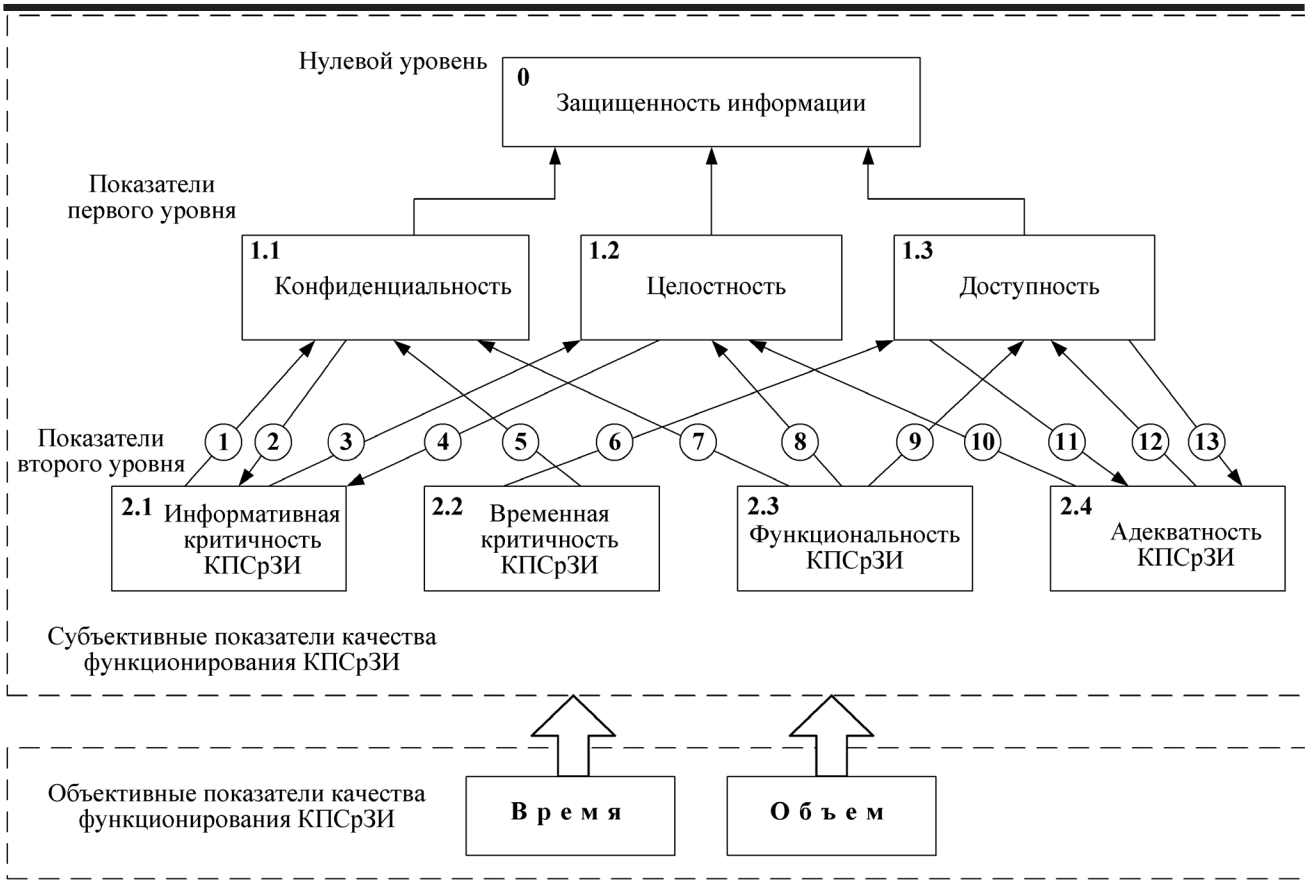
для адекватности КПСрЗИ:

10 - по интенсивности искажения информации;

11 - по возможности снижения интенсивности искажения информации;

12 - по интенсивности блокирования информации;

13 - по возможности снижения интенсивности блокирования информации.



Типы взаимосвязи между показателями первого и второго уровня

Исходя из того, что субъективные показатели первого уровня описаны в соответствующих документах ФСТЭК (Гостехкомиссии), рассмотрим подробно показатели второго уровня.

Показатель функциональности КПСрЗИ отражает степень его способности при заданных параметрах функционирования обеспечивать в заданной ситуации информационную безопасность КС. Это достигается полнотой набора защитных функций КПСрЗИ. Подобно другим стандартам информационной безопасности, Руководящие документы Гостехкомиссии предлагают свой набор функциональных требований к КПСрЗИ /5/, на основе которого можно оценивать показатель функциональности КПСрЗИ.

В отличие от других стандартов информационной безопасности, в частности «Единых критериев», Руководящие документы Гостехкомиссии не содержат требований адекватности средств защиты. Однако п. 3.6 основного Руководящего документа Гостехкомиссии - «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации» /6/, содержащего систему взглядов ФСТЭК на проблему информационной безопасности и основные принципы защиты компьютерных систем, гласит: «Неотъемлемой частью работ по защите является оценка эффективности средств защиты, осуществляемая по методике, учитывающей всю совокупность технических характеристик оцениваемого объекта, включая технические решения и практическую реализацию средств защиты». Поэтому актуальной проблемой является дополнение существующих экспертных подходов к обоснованию требований к средствам защиты информации, отраженных в существующих нормативно-методических документах Гостехкомиссии (ФСТЭК) формальными количественными требованиями, также требованиями по организации управления защитой информации в КС.

При решении этой проблемы можно опираться на мировой опыт стандартизации в области информационной безопасности.

Так, требования адекватности «Единых критериев» жестко структурированы и регламентируют все этапы проектирования, создания и, что представляет особый интерес, эксплуатации продукта информационных технологий с точки зрения обеспечения надежности работы средств защиты и их соответствия функциональным требованиям, задачам защиты и угрозам информационной безопасности, действующим в среде эксплуатации данного продукта, что, в итоге, отражает степень корректности реализации средств защиты.

Подобное соответствие характеризует эффективность КПСрЗИ для данной ситуации реализации в данной КС набора защитных функций при заданных параметрах функционирования КПСрЗИ. Этот показатель весьма существенно зависит от специфики конкретной задачи технологического управления КПСрЗИ в КС.

Введение показателей информативной и временной критичности КПСрЗИ обусловлено недостатками применения этих комплексов в КС. К таким недостаткам следует отнести:

необходимость использования времени работы процессора, что ведет к увеличению времени отклика КС на запросы и, как следствие, к уменьшению эффективности ее работы;

уменьшение объемов оперативной памяти и памяти на внешних запоминающих устройствах, доступной для использования функциональными задачами.

С другой стороны, доступные для КПСрЗИ вычислительные ресурсы являются одними из важнейших факторов, определяющих достижимую защищенность КС. Поэтому для размещения ПСрЗИ в КС еще на этапе проектирования должна быть предусмотрена информационная избыточность в виде ресурсов внешней и внутренней памяти СВТ /7/. Кроме того, для функционирования ПСрЗИ необходима временная избыточность - дополнительная производительность СВТ. Эти виды избыточности вычислительных ресурсов при обеспечении безопасности используются для /7/:

- контроля и корректировки искажений информации, поступающей от источников данных;

- оперативного контроля и обнаружения дефектов исполнения программ и обработки данных при использовании КС по прямому назначению;

- размещения и обеспечения функционирования применяемых ПСрЗИ для защиты от всех видов угроз безопасности КС;

- генерации тестовых наборов или хранения тестов для контроля работоспособности, сохранности и целостности программных средств при функционировании КС;

- накопления и хранения данных о выявленных инцидентах, попытках несанкционированного доступа к информации, о дефектах, сбоях и отказах в процессе исполнения программ и обработки данных, влияющих на безопасность;

- реализации процедур анализа и мониторинга выявленных дефектов и оперативного восстановления вычислительного процесса, программ и данных (рестарта) после обнаружения дефектов и отказов функционирования КС.

При управлении процессами защиты информации в КС на основе ПСрЗИ нужно разделять вычислительные ресурсы, необходимые для программных модулей, непосредственно обеспечивающих решение основных функциональных задач КС, и ресурсы, требующиеся для ПСрЗИ. Соотношение между этими видами ресурсов в реальных КС зависит от сложности и состава решаемых функциональных задач, степени их критичности и требований к безопасности всей КС. По материалам аналитических обзоров, периодически публикуемых на официальном сайте ФСТЭК России /8/, в компьютерных системах различного назначения ресурсы на обеспечение информационной безопасности могут составлять от 5 - 20 % до 100 - 300 % ресурсов, используемых на решение функциональных задач. При этом в военных системах превышение составляет 2 - 4 раза, в административных и организационных системах - 10 - 20% вычислительных ресурсов.

Эти обстоятельства оцениваются двумя приведенными выше показателями: временной и информационной критичностью, ха-

рактеризующие временную и информационную избыточность соответственно. Это позволяет при создании КС, реализовать интеграцию процесса защиты информации в процесс ее обработки, что в свою очередь обусловливает требования к КПСрЗИ как элементу КС, в соответствии с которыми ПСрЗИ не должны вступать в конфликт с существующими приложениями и сложившимися технологиями обработки информации, а, напротив, должны стать неотъемлемой частью этих средств и технологий.

Следует отметить, что подобным образом можно характеризовать любое программное средство (не обязательно защиты информации). При этом критичность понимается как способность программного средства к выполнению предусмотренных спецификацией функций в условиях огрничений на использование ресурсов.

Структурная схема системы показателей качества функционирования КПСрЗИ как объекта технологического управления представлена на рисунке.

Из рисунка видно, что система показателей качества функционирования ПСрЗИ содержит четыре элементарных показателя (2.1, 2.2, 2.3, 2.4), не сводящихся к другим, более частным, и три составных показателя (1.1, 1.2, 1.3), образующихся путем агрегирования более частных показателей.

Представленные показатели можно разделить на статические и динамические в соответствии с возможностью и необходимостью учета временного фактора. Данное деление достаточно условно, так как управление само по себе предполагает учет временного фактора, однако степень этого учета может быть различной. В этом плане выделяются показатели временной и информационной критичности КПСрЗИ, а также показатель ее адекватности, предполагающие учет динамики конфликтного взаимодействия с источником угроз НСД. Поэтому данные показатели можно считать динамическими, а показатель функциональности - статическим.

Как динамические, так и статический показатели целесообразно выражать действительными числами, вычисляемыми на основе моделирования динамики функционирования КПСрЗИ.

Временная критичность функционирования КПСрЗИ проявляется через снижение эффективности КС как системы массового обслуживания. В частности, при увеличении времени сеанса работы пользователей, необходимого для решения заданного набора функциональных задач, соответственно уменьшается пропускная способность КС. Причиной этого является тот факт, что только часть исходной пропускной способности КС используется для решения функциональных задач, то есть по прямому назначению, оставшаяся же часть используется для обеспечения информационной безопасности КС, то есть для решения КПСрЗИ своих задач. Необходимость использования части пропускной способности КС для обеспечения функционирования КПСрЗИ обусловлена невозможностью полного распараллеливания во времени решения функциональных задач и задач обеспечения информационной безопасности. В силу этого, время сеанса работы пользователей складывается из функциональной составляющей и защитной составляющей, что и приводит к увеличению общего времени сеанса работы и соответствующему дополнительному использованию пропускной способности КС. Защитная составляющая времени сеанса работы представляет собой то совокупное время сеанса работы, которое характеризуется простоем выполнения функциональных задач. Функциональная составляющая времени сеанса работы есть оставшееся совокупное время сеанса работы, оно не связано с простоем выполнения функциональных задач, хотя в общем случае, не исключает и одновременное выполнение каких-либо частных задач защиты информации.

Будем называть защитную составляющую времени сеанса работы временем реализации КПСрЗИ защитных функций. Наличие этого времени лежит в основе временной критичности КПСрЗИ. В общем случае это время является случайной величиной. Так как КС должна проектироваться с учетом временной избыточности для обеспечения функционирования КПСрЗИ, то особое значение имеет не само по себе наличие време-

ни $\tau_{(d)}$ реализации КПСрЗИ защитных функций, а возможность превышения этим временем некоторого максимально допустимого времени реализации КПСрЗИ защитных функций $\tau_{(m)}$, определяемого временной избыточностью КС.

Практическое вычисление величины показателя Э временной критичности производится на основе моделирования динамики функционирования КС как системы массового обслуживания, причем при таком моделировании функциональная составляющая времени сеанса работы полагается равной нулю. Тогда время реализации КПСрЗИ защитных функций $\tau_{(d)}$ представляет собой просто длительность сеанса работы, то есть промежуток времени с момента начала очередного сеанса работы пользователем до момента времени окончания данным пользователем этого же сеанса работы. Фактически при рассмотренном подходе моделирование динамики функционирования КС вырождается в моделирование динамики функционирования КПСрЗИ.

Одним из основных этапов при моделировании систем, существенным образом определяющим качество модели, является формализация моделируемых процессов /9/. Для формализации именно динамики функционирования сложных систем в рамках графового подхода разработаны различные математические объекты в развитие идеи о формализации сложных систем ориентированным графом. Проведенный анализ таких математических объектов дает основание считать, что наиболее приемлемым формальным аппаратом для представления динамики функционирования КПСрЗИ являются Е-сети (оценочные сети), которые возникли на основе известных сетей Петри и существенно расширяют их возможности для представления и моделирования систем.

Таким образом, способ оценки показателя Э базируется на математическом моделировании динамики функционирования КПСрЗИ на основе ее Е-сетевой формализации с целью исследования времени жизни объектов Е-сети.

В общем случае стохастическую модель динамики функционирования КПСрЗИ в соответствии с ее Е-сетевой формализацией можно описать матрицей $|H_{ij}(\tau)|$, произвольный элемент которой $H_{ij}(\tau)$ есть вероятность того, что КПСрЗИ, оказавшись в состоянии i, перейдет из него в состояние j в результате срабатывания соответствующего перехода Е-сети, причем за время, меньшее τ. Адекватным математическим аппаратом анализа такой стохастической модели является теория конечных полумарковских процессов (КПП) /10/. При этом динамика функционирования КПСрЗИ представляется КПП, характеризующимся полумарковской матрицей $|H_{ij}(\tau)|$, что позволяет учитывать произвольность закона распределения пребывания КПСрЗИ в любом из своих состояний. Конечное состояние - поглощающее, так что и сам КПП является поглощающим.

Для анализа динамики функционирования КПСрЗИ как КПП можно воспользоваться аналитическим методом исследования вероятностно-временных характеристик (ВВХ) сложных систем, предложенным в /11/. При этом максимально допустимое время реализации защитных функций предполагается либо детерминированным, либо экспоненциально распределенным. Выбор экспоненциального распределения в данном случае связан с тем, что именно этот закон распределения широко используется для аппроксимации максимально допустимого времени выполнения сложными системами своих функциональных задач. В случае экспоненциального распределения величины $\tau_{(m)}$ показатель Э, выражается точно аналитически через ВВХ отдельных состояний функционирования ПСрЗИ /11/. В случае детерминированной величины $\tau_{(m)}$, вычисление показателя Э сводится к вычислению значения в точке $\tau_{(m)}$ функции распределения времени реализации ПСрЗИ защитных функций. Формально, эта функция распределения есть обратное преобразование Лапласа-Стилтьеса /12/ соответствующей функции из решения системы уравнений для производящих функций, описывающей данный КПП. Однако практические вычисления таким путем проблематичны. Поэтому предлагается альтернативный путь: оценка первых четырех начальных и центральных моментов случайной величины $\tau_{(di)}$ с последующей аппроксимацией по ним

искомого распределения распределением Пирсона /12/, широко использующимся в математической статистике при сглаживании распределений эмпирических данных. Если заданы первые четыре момента времени пребывания КПСрЗИ в каждом из состояний, а также вероятности переходов между состояниями, то в рамках полумарковской модели динамики функционирования КПСрЗИ первые четыре момента случайной величины $\tau_{(d)}$ можно вычислять достаточно просто точным аналитическим методом, решая четыре системы линейных алгебраических уравнений, получающиеся из системы уравнений для производящих функций ее четырехкратным дифференцированием. В любом случае в качестве исходных данных для оценки показателя Э используются ВВХ отдельных состояний функционирования КПСрЗИ. А эти характеристики либо являются управляемыми параметрами КПСрЗИ, либо определяются в ходе специальных статистических исследований на базе проведения серий натурных экспериментов.

Если КПСрЗИ не обеспечивает желаемый уровень временной критичности, то желательна корректировка параметров его функционирования. Для этого должны определяться слабые места функционирования КПСрЗИ с точки зрения временной критичности, выявляемые на основе оценки уязвимости состояний его функционирования и непосредственно указывающие на наиболее целесообразные направления корректировки. В соответствии с предложенной системой показателей качества технологического управления КПСрЗИ показателями, характеризующими уязвимость произвольного состояния его функционирования с точки зрения временной критичности, являются показатель потенциальной интенсивности потока проявления угроз НСД и показатель снижения интенсивности потока проявления угроз НСД. Потенциальная интенсивность потока проявления угроз НСД характеризует уязвимость произвольного i-го состояния функционирования КПСрЗИ, оценивается вероятностью ρ_i того, что в момент истечения максимально допустимого времени реализации КПСрЗИ защитных функций она будет находиться в состоянии i. При этом величина, равная сумме абсолютных уязвимостей всех неконечных состояний, характеризует уязвимость КПСрЗИ в целом. Снижение интенсивности потока проявления угроз НСД характеризует вклад уязвимости i-го состояния функционирования КПСрЗИ в уязвимость КПСрЗИ в целом и оценивается вероятностью c_i того, что в момент истечения максимально допустимого времени реализации КПСрЗИ защитных функций комплекс будет находиться в состоянии i при условии несвоевременной реализации КПСрЗИ защитных функций. В предположении экспоненциального закона распределения случайной величины $\tau_{(m)}$ показатели ρ_i и c_i выражаются точно аналитически через ВВХ отдельных состояний функционирования ПСрЗИ.

Предлагаемый способ оценки показателей ρ_i, c_i удобен для практического применения, так как он универсален (отсутствие ограничений на структуру формализующей динамику функционирования Е-сети), прост в использовании (возможность проведения расчетов даже без разработки специальной программы для СВТ) и позволяет решать задачу в принятых предположениях точно аналитически при малых объемах вычислений.

При проведении корректировки управляемых параметров функционирования КПСрЗИ представляют интерес уязвимости тех состояний функционирования КПСрЗИ, ВВХ которых зависят от тех или иных управляемых параметров (управляемые состояния функционирования КПСрЗИ). Если абсолютная уязвимость некоторого управляемого состояния велика, то соответствующая корректировка управляемых параметров может дать существенное снижение временной критичности КПСрЗИ. Относительная уязвимость управляемых состояний показывает их роль в существующем уровне временной критичности КПСрЗИ. Если достаточно мала как абсолютная, так и относительная уязвимость управляемого состояния, то соответствующую корректировку параметров можно считать нецелесообразной.

Литература

1. Джоган В.К. Теоретические и организационно-методические основы комплексной оценки защищенности информации правоохра-

нительных органов: монография / В.К. Джоган, А.П. Курило, Д.Ю. Лиходедов – Воронеж: Воронежский институт МВД России, 2011. – 88 с.

2. Скрыль С.В. Модель нарушителя как классификационное основание синтеза системы показателей защищенности информации. / С.В. Скрыль, В.К. Джоган // Охрана, безопасность и связь - 2011: материалы Международной научно-практ. конф. – Воронеж: Воронежский институт МВД России, 2012. – С. 96 – 100.

3. Основы системного анализа в защите информации: учебное пособие для студентов высших учебных заведений. / А.А. Шелупанов, С.В. Скрыль. – М.: Машиностроение, 2008. – 138 с.

4. Гостехкомиссия РФ. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. – М.: Воениздат, 1992.

5. Гостехкомиссия РФ. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. – М.: Воениздат, 1992.

6. Гостехкомиссия РФ. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. – М.: Воениздат, 1992.

7. Мамиконов А.Г. Достоверность, защита и резервирование информации в АСУ. / А.Г. Мамиконов, В.В. Кульба, А.Б. Щелков – М.: Энергоатомиздат, 1986. – 304 с.

8. www.fstec.ru

9. Оценка защищенности информационных процессов в территориальных органах внутренних дел: модели исследования: монография / А.А. Герасимов, В.К. Джоган, В.С. Зарубин, А.П. Курило [и др.]. – Воронеж: Воронежский институт МВД России, 2010. – 217 с.

10. Динамическая оптимизация системы управления и связи с помощью управляемых цепей Маркова / С.В. Скрыль [и др.]. // Современные проблемы борьбы с преступностью: материалы Всерос. науч. – практ. конф. (информационная безопасность). – Воронеж: Воронежский институт МВД России, 2005. – С. 18 - 19.

11. Основы информационной безопасности: учебник для высших учебных заведений МВД России / под ред. В.А. Минаева и С.В. Скрыля. — Воронеж: Воронежский институт МВД России, 2001. — 464 с.

12. Вентцель Е.С. Теория вероятностей: учебник. / Е.С. Вентцель – 11-е изд. – М.: КноРус, 2010. – 664 с.

Воронежский государственный технический университет
Voronezh State Technical University

FACTORS AND MODELS QUALITY TECHNOLOGICAL MANAGEMENT COMPLEX PROGRAMME MEANSES OF PROTECTION INFORMATION FROM UNAUTHORIZED ACCESS IN COMPUTER SYSTEM

S.V. Skryl', M.A. Bagaev, D.V. Malyshev, S.A. Malyshev

The system of indicators of quality of technological management of a complex of software of protection of information from unauthorized access locates in innovative computer systems. Features of modeling of processes of protection of information with the purpose of determination of values of separate indicators of ensuring confidentiality of information of innovative character are considered

Key words: computer system, a complex of software of protection of information from unauthorized access, indicators of quality of technological management of a complex of software of protection of information from unauthorized access