УДК 621.3 **DOI** 10.15622/sp.57.8

О.С. Авсентьев, И.Г. Дровникова, И.И. Застрожнов, А.Д. Попов, Е.А. Рогозин

МЕТОДИКА УПРАВЛЕНИЯ ЗАЩИТОЙ ИНФОРМАЦИОННОГО РЕСУРСА СИСТЕМЫ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

Авсентьев О.С., Дровникова И.Г., Застрожнов И.И., Попов А.Д., Рогозин Е.А. **Методика управления защитой информационного ресурса системы электронного документооборота.**

Аннотация. В статье рассматриваются методологические основы организационно-технологического управления (ОТУ) защитой информационного ресурса (ЗИР) систем электронного документооборота (СЭД) на базе программных средств (ПСр) защиты информации. Разработана концептуальная модель управления ЗИР СЭД на основе концептуальной проработки аспектов формирования методологии ОТУ ЗИР СЭД на базе ПСр ЗИР, обладающая широкими возможностями по ее использованию для разработки способов решения управленческих задач. Представлена методика управления эффективностью функционирования подсистемы защиты информационного ресурса (ПЗИР) в СЭД, предполагающая оптимизацию управляемых параметров подсистемы, обеспечивающих максимизацию интегрального показателя эффективности функционирования ПЗИР, и соответственно, выполнение требований, предъявляемых к подсистеме. Приведен алгоритм определения оптимальных значений управляемых параметров ПЗИР и оптимального значения интегрального показателя эффективности функционирования подсистемы, обеспечивающий возможность создания конкретных подсистем автоматизированного управления эффективностью функционирования ПЗИР в СЭД. Анализируются результаты расчетов по исследованию показателя временной неконфликтности функционирования ПЗИР.

Ключевые слова: организационно-технологическое управление, система электронного документооборота, защита информации, информационный ресурс, эффективность функционирования системы, управление эффективностью.

1. Введение. Значительное увеличение потока информации в жизнедеятельности общества и повсеместная компьютеризация различных сфер деятельности человека способствовало широкому внедрению систем электронного документооборота (СЭД) в структуру различных организаций. Особенностью функционирования СЭД является работа в многопользовательском режиме с информацией разного уровня конфиденциальности. При этом пользователи СЭД имеют различные полномочия по доступу к информации, циркулирующей в ней. Поэтому проблема защиты информационного ресурса (ЗИР) в СЭД от угроз несанкционированного доступа (НСД) с целью обеспечения информационной безопасности (ИБ) СЭД является актуальной. Для решения задач ЗИР СЭД от НСД создается специализированная подсистема ЗИР.

Одно из основных требований стандарта по ИБ [1] — организация управления процессом ЗИР автоматизированных систем (АС). Поэтому при организации ЗИР СЭД на основе ПЗИР необходимо обеспе-

чить непрерывное управление ЗИР. Важный элемент процесса управления сложными системами, включая и управление ЗИР СЭД — процесс принятия решений (ПР) [2-4]. При этом управляющие решения целесообразно принимать с учетом оценки эффективности функционирования АС, рассматриваемой как объект управления (ОУ). Поэтому перспективным направлением организации управления ПЗИР является реализация ОТУ защитой информации в СЭД на базе оценки эффективности функционирования подсистемы. Исходя из этого, актуальна проблема формирования методологии ОТУ ЗИР от НСД в СЭД на основе комплексной оценки эффективности ПЗИР.

Разработанная методика ОТУ ЗИР от НСД в СЭД позволяет автоматизировать процесс принятия управленческих решений по ЗИР СЭД.

2. Концептуальная модель ОТУ ЗИР в СЭД. Под ОТУ ЗИР в СЭД с использованием ПСр ЗИР понимают меры и мероприятия, установленные инструкциями организации, эксплуатирующей СЭД, а также способы управления на базе ПСр управления ЗИР СЭД, которые позволяют автоматизировать процедуру ПР или обеспечить компьютерную поддержку для ПР [4]. Вопросам управления ЗИР уделяется значительное внимание в стандартах по информационной безопасности (ИБ) [1, 5-9]. В основных стандартах по ИБ [1, 9] функциональные требования содержат классы требований управления безопасностью, регламентирующие аспекты управления средствами защиты, параметрами средств защиты, атрибутами безопасности и конфигурацией механизмов защиты. Во всех разделах функциональных требований стандартов [1, 9] существует пункт «Управляемые параметры», обеспечивающий управление параметрами ПСр ЗИР. В этом пункте приводятся параметры, которые позволяют осуществлять управление ПСр ЗИР для реализации требований соответствующего раздела.

Анализ литературы по ИБ и управлению АС [1-4, 12-14, 16, 17] позволяет определить структуру задач ОТУ ЗИР СЭД на базе ПСр ЗИР. Защита информации в СЭД реализуется комплексом программных средств защиты (КПСЗ) (входящим в состав ПЗИР), включающим систему разграничения доступа (СРД) и следующие основные подсистемы: обеспечения целостности; управления доступом; криптографическая; регистрации и учета. Подсистема управления доступом осуществляет идентификацию и аутентификацию пользователей при их доступе в СЭД. Подсистема обеспечения целостности осуществляет контроль целостности модулей ПЗИР, а также файлов и каталогов пользователя. Подсистема регистрации и учета выполняет регистрацию событий, связанных с работой ПЗИР, регистрацию запуска и завершения программ, а также сигнализацию попыток нарушения ЗИР. Криптографическая подсистема осуществляет шифрование защищаемой информации при ее

хранении или передаче по открытым каналам. СРД реализует полномочия пользователей СЭД по доступу к файлам, дискам, ПСр и так далее. Исходя из этого, управление КПСЗ должно включать в себя управление СРД и управление вышеназванными подсистемами.

Процесс управления АС в общем случае включает следующие этапы [3, 4, 12, 17]:

– сбор информации о параметрах функционирования ОУ (получение данных об информационном процессе, передача этих данных для обработки);

– обработка информации и ПР (анализ накопленной, справочной и поступающей информации; ПР по результатам анализа);

– исполнение принятого решения (создание управляющего сигнала и выполнение воздействия на ОУ).

ОТУ ЗИР обеспечивается подсистемой управления ЗИР (ПУЗР). ПУЗР — это функциональная подсистема СЭД, включающая программные средства и организационные мероприятия, предусмотренные для осуществления ОТУ ЗИР СЭД. Данная подсистема управления ЗИР реализует два взаимосвязанных вида управления: управление КПСЗ (осуществляет управление отдельными ПСр ПЗИР) и управление ПЗИР (осуществляет управление организацией ЗИР СЭД на базе ПСр ЗИР). В каждом из этих видов управления существуют два взаимодействующих блока — ОУ и управляющая система. Данные о функционировании ОУ поступают в управляющую систему, где производится их обработка и анализ, по результатам которых формируется управляющее воздействие на ОУ. Для управления КПСЗ ОУ является КПСЗ, а управляющей системой является подсистема управления эффективностью функционирования ПЗИР, функционально относящаяся и к ПЗИР, и к ПУЗР. При управлении ПЗИР ОУ — ПЗИР, а в качестве управляющей системы используется подсистема управления ПЗИР, функционально относящаяся к ПУЗР.

При управлении КПСЗ его ПСр, с одной стороны, играют роль исполнительных органов, получающих управляющие сигналы от подсистемы управления ПЗИР (набор целесообразных для использования ПСр ЗИР и конфигурация ПЗИР), с другой стороны — управляющих органов, осуществляющих управление параметрами КПСЗ. Управление КПСЗ представляет собой управление некоторыми ПСр ЗИР и соответствующими организационными мероприятиями. Организация управления КПСЗ основана на возможности изменения значений некоторых параметров ПСр ЗИР. Поэтому процесс управления КПСЗ включает в себя процедуры анализа состояния ПЗИР, принятие управляющего решения и на его основе осуществление соответствующего воздействия на ПСр ЗИР путем изменения значений их управляемых параметров.

При управлении ПЗИР управляющими воздействиями являются набор целесообразных для использования ПСр ЗИР, конфигурация ПЗИР и связанные с этим управлением организационные мероприятия. Управление структурой ПЗИР осуществляется на основе принципа блочной архитектуры, учитывая специфику задач ЗИР СЭД [1-4, 10, 15, 16]. Учет этого принципа при разработке ПЗИР позволяет использовать унифицированные стандартные ПСр ЗИР, что дает возможность упростить разработку, отладку, контроль и верификацию алгоритмов и программ, модернизацию ПЗИР, обеспечить простоту и удобство эксплуатации. Используя данный принцип, можно сформировать ядро защиты ПЗИР, обеспечивающее минимально допустимый уровень защищенности СЭД, а при необходимости повысить уровень защиты путем инсталляции дополнительных ПСр ЗИР.

Обоснованные предложения, принципы организации управления сложными системами позволили разработать структурную схему концептуальной модели ОТУ ПЗИР, представленную на рисунке 1.

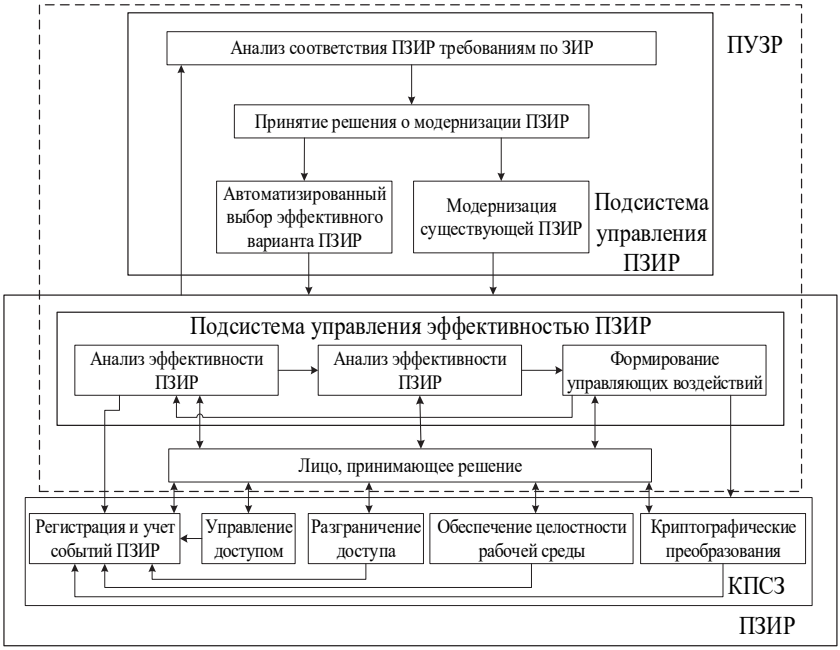


Рис. 1. Структурная схема концептуальной модели ОТУ ПЗИР

3. Оптимальное управление ЗИР СЭД. Задача управления ЗИР СЭД с помощью ПСр ЗИР при управлении КПСЗ представляет собой задачу оптимального управления, решение которой обеспечивает

поддержание экстремального значения целевой функции. Данная функция зависит, во-первых, от группы регулируемых параметров, значения которых могут изменяться с помощью управляющего сигнала подсистемы управления эффективностью функционирования ПЗИР; во-вторых, от группы внешних параметров, нерегулируемых данной подсистемой.

При управлении процессами ЗИР в СЭД необходимо учесть противоречивость требований ИБ СЭД требованиям к СЭД по ее назначению (производительности, удобству эксплуатации и т.д.) [2, 4]. Учет этого противоречия позволяет определить принцип методологии оценивания эффективности функционирования ПЗИР, заключающийся в том, что эффективность функционирования СЭД по прямому назначению неразрывно связана с эффективностью функционирования ПЗИР СЭД.

Эффективное функционирование ПЗИР обеспечивает возможность эффективного функционирования защищаемой СЭД. Управление ЗИР СЭД заключается в решении задачи оптимизации эффективности функционирования ПЗИР в СЭД, позволяющей, с одной стороны, обеспечить ЗИР СЭД, с другой — оказать минимальное негативное влияние реализации функций ЗИР на функционирование СЭД по назначению. Оптимальное управление ЗИР целесообразно осуществлять по интегральному показателю эффективности функционирования ПЗИР, поэтому для реализации данного управления необходимо решать многокритериальную задачу. Данная задача управления является трудной, так как необходимо решать достаточно сложные задачи формализации процессов ЗИР и ПР. Задачу ПР при оптимальном управлении функционированием ПЗИР СЭД при управлении КПСЗ можно формализовано представить как задачу оптимизации: необходимо выбрать альтернативу $\vec{a}$ (комплект значений управляемых параметров ПЗИР) из множества A ($\vec{a} \in A$) (всех возможных комплектов), при которой интегральный показатель эффективности функционирования ПЗИР $\vec{E}_u$ имел бы максимальное значение:

$$\vec{E}_u(a) \rightarrow max. \qquad (1)$$

Под максимизацией векторного показателя $\vec{E}_u$ (1) понимается увеличение наименьшего значения элементов вектора данного показателя.

4. Система показателей эффективности функционирования ПЗИР. Оценку эффективности реализации функций ЗИР в АС проводят с помощью показателей, которые достаточно полно характеризуют эффективность ЗИР в АС [4, 18-23]. Для оценки эффективности функционирования ПЗИР и осуществления на ее базе ОТУ ЗИР в СЭД целесообразно использовать систему показателей, содержащую интегральный показатель $\vec{E}_u$, который агрегирует 6 элементарных показателей: $E_ф$ —

показатель функциональности ПЗИР; $\vec{E}_{аф}$ — показатель адекватности функционирования ПЗИР; $E_{вн}$ — показатель временной неконфликтности функционирования ПЗИР; $E_{рн}$ — показатель ресурсной неконфликтности функционирования ПЗИР; $E_{фн}$ — показатель функциональной неконфликтности функционирования ПЗИР; $E_{уи}$ — показатель удобства использования ПЗИР.

Показатель адекватности функционирования ПЗИР отражает соответствие подсистемы требованиям по ЗИР, характеризующим эффективность реализации защитных функций ПЗИР. Оценку показателя $\vec{E}_{аф}$ осуществляют путем анализа параметров управляемых программных средств (УПСр) ЗИР подсистемы, которые характеризуют эффективность выполнения этими средствами своих функций. Показатель адекватности функционирования ПЗИР представляется в виде вектора частных показателей адекватности УПСр ЗИР ($E_{аф\,i}$) и оценивается по таблицам соответствия значений управляемых параметров ПЗИР значениям частных показателей адекватности функционирования УПСр ЗИР [4]. Измерение частных показателей осуществляется при помощи качественной шкалы, предполагающей балльную оценку.

Показатели $E_{ф}, E_{фн}, E_{рн}$ и $E_{уи}$, отражают соответствие ПЗИР требованиям по полноте реализуемого набора защитных функций ЗИР, функциональной и ресурсной неконфликтности функционирования ПЗИР в СЭД (неконфликтность взаимодействия ПЗИР с другими подсистемами и ПСр СЭД) и удобству использования ПЗИР в процессе эксплуатации СЭД соответственно. Оценку данных показателей проводят путем определения соответствия ПЗИР предъявляемым к ней требованиям на основе анализа ее программной документации [4, 23, 24]. Измерение этих показателей осуществляют по качественной шкале, имеющей значения «допустимо» и «недопустимо», что позволяет использовать булеву переменную. Таким образом, элементарные показатели $E_{ф}$, $\overrightarrow{E_{аф}}$, $E_{фн}, E_{рн}$ и $E_{уи}$ являются качественными показателями эффективности функционирования ПЗИР.

Количественный показатель временной неконфликтности функционирования ПЗИР отражает вероятностно-временные свойства динамики функционирования ПЗИР, влияющие на эффективность функционирования СЭД. Реализация функций ПЗИР приводит к увеличению продолжительности решения функциональных задач по назначению СЭД, так как часть процессорного времени СЭД тратится на решение задач ЗИР. При этом ИБ СЭД может быть обеспечена только при своевременной реализации защитных функций ПЗИР. Поэтому временная

неконфликтность функционирования ПЗИР определяется как вероятность своевременной реализации функций ЗИР:

$$E_{вн} = P(\tau \le \tau_{max}), \qquad (2)$$

где τ — время выполнения подсистемой функций ЗИР, τ_{max} — максимально допустимое время выполнения подсистемой функций ЗИР. Оценка данного показателя осуществляется с помощью полумарковской модели на основе представления динамики функционирования ПЗИР в виде конечного полумарковского процесса [4, 10, 11].

Комплексная оценка эффективности функционирования ПЗИР проводится с использованием интегрального показателя эффективности функционирования ПЗИР, агрегирующего рассмотренные выше элементарные показатели. Показатели $E_ф, E_{фн}, E_{рн}$ и $E_{уи}$ можно использовать только в ограничениях, так как они являются булевыми функциями. Учитывая, что показатель временной неконфликтности функционирования ПЗИР отражает временные ограничения функционирования ПЗИР в СЭД (2), этот показатель также необходимо использовать в ограничениях. Напротив, показатель адекватности ПЗИР характеризует эффективность реализации этой подсистемой своих функций, поэтому данный показатель необходимо рассматривать как интегральный показатель эффективности функционирования ПЗИР, учитывая выполнение вышеназванных ограничений.

С учетом выше изложенного, оценивание интегрального показателя эффективности функционирования ПЗИР предлагается выполнять с помощью выражения:

$$\overrightarrow{E_и} = \begin{cases} \overrightarrow{E_{аф}}, & \textit{если} \quad \left(E_{вн} \ge E_{\min\ вн}\right),\ E_ф \wedge E_{фн} \wedge E_{рн} \wedge E_{уи} = 1, \\ 0, & \textit{иначе} \end{cases} \qquad (3)$$

где $E_{\min вн}$ — минимально допустимое значение временной неконфликтности функционирования ПЗИР, заданное документацией на СЭД [4, 11].

5. Организационно-технологическое управление эффективностью функционирования ПЗИР. Управление эффективностью функционирования ПЗИР реализуется с помощью управляемых параметров, позволяющих регулировать эффективность функционирования ПЗИР путем изменения их значений при воздействии сигналов управления. В качестве управляемых параметров ПЗИР взяты параметры УПСр ЗИР подсистемы, которые оказывают влияние на динамику функционирования ПЗИР. К управляемым параметрам функционирования ПЗИР, выявленным на основе анализа динамики ее функционирования [4], можно отнести: $l_{аут}$ — количество символов пароля, вводимого пользователем вручную для его аутентификации; $l_{доп\ аут}$ — количество символов пароля, вводимого пользовате-

лем вручную для его дополнительной аутентификации в процессе обращения к наиболее важному ресурсу; $p_{сп}$ — вероятность применения специальных преобразований для файлов; $p_{кц}$ — вероятность старта теста проверки целостности рабочей среды СЭД. Значения этих управляемых параметров определяют значения частных показателей адекватности УПСр ЗИР $E_{аф\ аут}, E_{аф\ доп.\ аут}, E_{аф\ сп}, E_{аф\ кц}$ отражающих эффективность выполнения ПЗИР возложенных на нее защитных функций по основной и дополнительной аутентификации пользователей СЭД, специальным преобразованиям информации и контролю целостности рабочей среды СЭД соответственно.

Оптимальное управление АС в случае, когда нерегулируемые параметры в системе в рассматриваемом периоде времени неизменны, сводится к установлению таких значений регулируемых параметров, при которых обеспечивается максимизация (или минимизация) критерия оптимального управления [3, 4, 12, 25, 26]. Для управления эффективностью функционирования ПЗИР необходимо определить такой вектор значений управляемых параметров ПЗИР, который обеспечивает максимизацию интегрального показателя эффективности функционирования ПЗИР (3). В данном случае задачу ПР при управлении эффективностью функционирования ПЗИР можно формализовано представить как задачу математического программирования [4, 12] — необходимо выбрать такую альтернативу из множества альтернатив, чтобы выполнялись условия:

$$\overrightarrow{E_{аф}} \to \max, \tag{4}$$

$$E_{вн} \geq E_{\min вн}, \tag{5}$$

$$E_{ф} \wedge E_{фн} \wedge E_{рн} \wedge E_{уи} = 1. \tag{6}$$

Исходя из предположения о равнозначности УПСр подсистемы с точки зрения ЗИР, максимизация векторного показателя $\overrightarrow{E_{аф}}$ (4) заключается в последовательном увеличении значения частных показателей УПСр ЗИР, имеющих наименьшее значение. Выражения (5) и (6) в данной системе являются ограничениями, отражающими требования к ПЗИР в СЭД. Выполнение данных ограничений обеспечивает достаточную полноту набора функций ПЗИР, своевременность выполнения данных функций подсистемой, функциональную и ресурсную неконфликтность ПЗИР в СЭД и удобное использование ПЗИР СЭД пользователями и обслуживание персоналом.

Анализ функционирования ПЗИР [2, 22, 25, 26] показал, что увеличение времени, отводимого на выполнение функций ЗИР, дает возможность увеличения эффективности функционирования УПСр ЗИР, измеряемой набором частных показателей адекватности данных средств ЗИР, которые определяют показатель адекватности ПЗИР. Исходя из этого задача оптимального управления эффективностью функционирования ПЗИР сво-

дится к задаче выбора оптимальных значений управляемых параметров, обеспечивающих выполнение ограничений (5), (6) и выражения:

$$E_{вн} - E_{min\ вн} \rightarrow min. \quad (7)$$

При этом, учитывая критичность СЭД к обеспечению ИБ, в качестве критерия оптимальности при выборе значений управляемых параметров предлагается использовать критерий максимизации наименьшего из значений частных показателей адекватности УПСр ЗИР.

При условии $E_{вн} < E_{min\ вн}$ управление эффективностью функционирования ПЗИР целесообразно осуществлять более чувствительным параметром из вышеназванной совокупности управляемых параметров, который обеспечивает выполнение ограничения (5) за счет минимального снижения эффективности функционирования УПСр ЗИР в данной ситуации. В этом случае в управлении эффективностью функционирования ПЗИР не используются управляемые параметры:

– имеющие значения, соответствующие минимальным значениям, заданным эксплуатационной документацией на СЭД;

– УПСр ЗИР которых имеют наименьшее значение частных показателей адекватности (исключая случай, когда все УПСр подсистемы имеют одинаковые значения частных показателей).

В случае, если при управлении ПЗИР все управляемые параметры достигли минимальных значений, заданных эксплуатационной документацией на СЭД, а ограничение (5) не выполнено, то данную ПЗИР заменяют другой.

Если $E_{вн} < E_{min\ вн} + \delta$, где δ — заданная величина, то управление эффективностью функционирования ПЗИР целесообразно осуществлять управляемым параметром средств ЗИР, имеющим наименьшее значение оценки частного показателя адекватности. При наличии нескольких УПСр ЗИР, имеющих наименьшее значение частного показателя, управление осуществляют менее чувствительным управляемым параметром, который обеспечивает выполнение выражений (5) и (7) при максимальном увеличении эффективности функционирования ПЗИР.

Структурно-функциональная модель управления эффективностью функционирования ПЗИР СЭД представлена на рисунке 2. ОТУ эффективностью функционирования ПЗИР предлагается осуществлять с помощью подсистемы автоматизированного управления эффективностью функционирования ПЗИР в СЭД. Данная подсистема реализует приведенную выше модель оптимального управления эффективностью функционирования ПЗИР через управляемые параметры подсистемы.

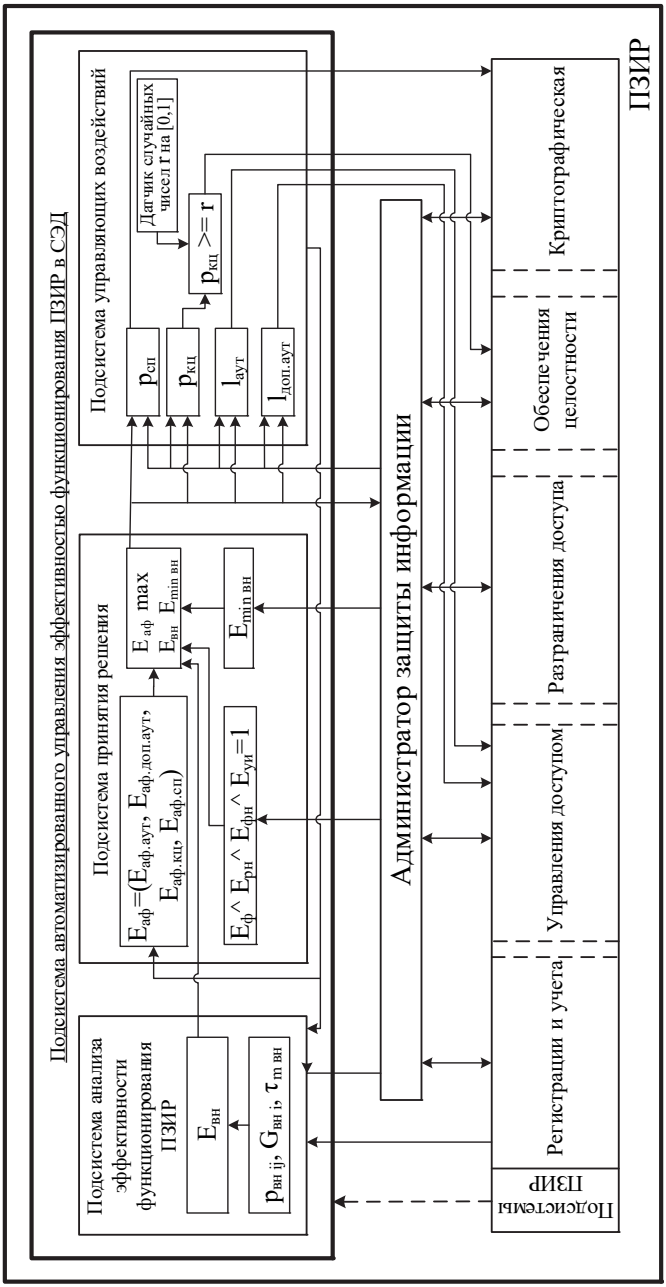


Рис. 2. Структурно-функциональная модель управления эффективностью функционирования ПЗИР СЭД

Подсистема автоматизированного управления эффективностью функционирования ПЗИР включает в свой состав подсистемы: анализа эффективности функционирования ПЗИР, ПР и управляющих воздействий.

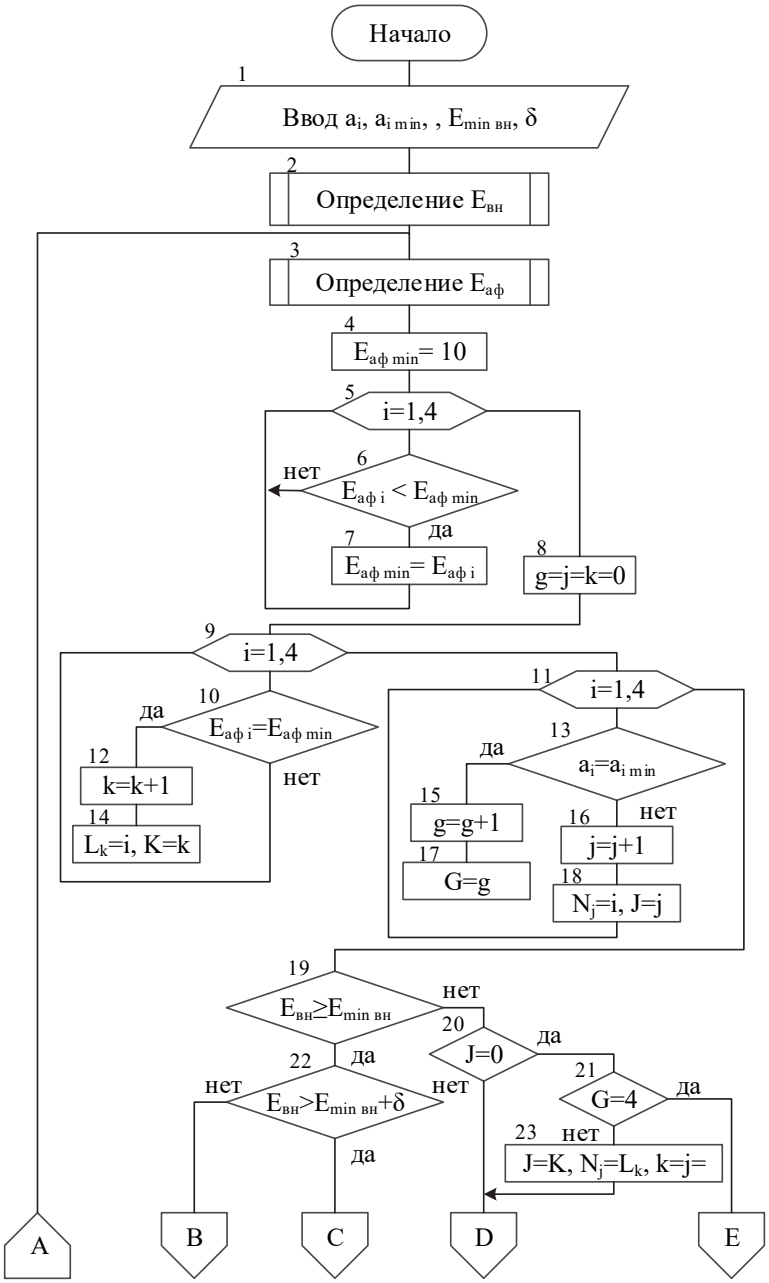
Подсистема анализа эффективности функционирования ПЗИР осуществляет оценку показателя $E_{вн}$ на основе данных о выполнении ПЗИР своих функций в СЭД. Эти данные поступают от подсистемы регистрации и учета. Эффективность функционирования ПЗИР оценивается в этом случае для обеспечения обратной связи в процессе управления эффективностью функционирования ПЗИР.

Подсистема ПР реализует функцию ПР по оптимальному управлению ЗИР в СЭД [18-21, 23]. Принятие решения осуществляется на основе комплексной оценки эффективности функционирования ПЗИР для обеспечения и поддержания разумного компромисса между уровнем защищенности информации в СЭД и эффективностью функционирования СЭД по прямому назначению. В результате принятия управленческого решения выбирается такой набор значений управляемых параметров функционирования ПЗИР, который обеспечивает максимальное значение интегрального показателя.

Подсистема управляющих воздействий формирует управляющее воздействие на ПЗИР в соответствии с ПР (набором значений управляемых параметров), которое обеспечивает выполнение условий (5), (7).

6. Алгоритмизация управления ЗИР СЭД. Алгоритмизация процесса управления на основе комплексной оценки эффективности функционирования ПЗИР заключается в разработке алгоритма оптимизации управляемых параметров при ОТУ эффективностью функционирования ПЗИР АС. Алгоритм определения оптимальных значений управляемых параметров ПЗИР и оптимального значения интегрального показателя эффективности функционирования ПЗИР при управлении ЗИР представлен на рисунке 3.

В рассматриваемом алгоритме вначале выполняются процедуры определения показателей $E_{вн}$ (блок 2) и $\overrightarrow{E_{аф}}$ (блок 3), алгоритмы которых приведены в [4]. Далее проводится начальная установка значения $E_{аф\,\min}$, соответствующее максимально возможному значению частных показателей $E_{аф\,i}$ (блок 4), и реализуется цикл определения минимального значения частных показателей адекватности функционирования УПСр ЗИР (блоки 5-7). Затем последовательно выполняются циклы определения частных показателей адекватности функционирования УПСр ЗИР (блоки 9, 10, 12, 14) и текущих управляемых параметров, имеющих минимальные значения (блоки 11, 13, 15-18).


Начало
1
Ввод a_i, $a_{i\,min}$, , $E_{min\ вн}$, δ
2
Определение $E_{вн}$
3
Определение $E_{аф}$
4
$E_{аф\,min}$= 10
5
i=1,4
6
нет
$E_{аф\,i} < E_{аф\,min}$
да
7
$E_{аф\,min}$= $E_{аф\,i}$
8
g=j=k=0
9
i=1,4
10
да
$E_{аф\,i}$=$E_{аф\,min}$
нет
12
k=k+1
14
L_k=i, K=k
11
i=1,4
13
да
a_i=$a_{i\,min}$
15
g=g+1
16
нет
j=j+1
17
G=g
18
N_j=i, J=j
19
$E_{вн}$≥$E_{min\ вн}$
нет
20
J=0
да
21
G=4
да
22
да
нет
$E_{вн}$>$E_{min\ вн}$+δ
нет
23
нет
J=K, N_j=L_k, k=j=
да
A
B
C
D
E

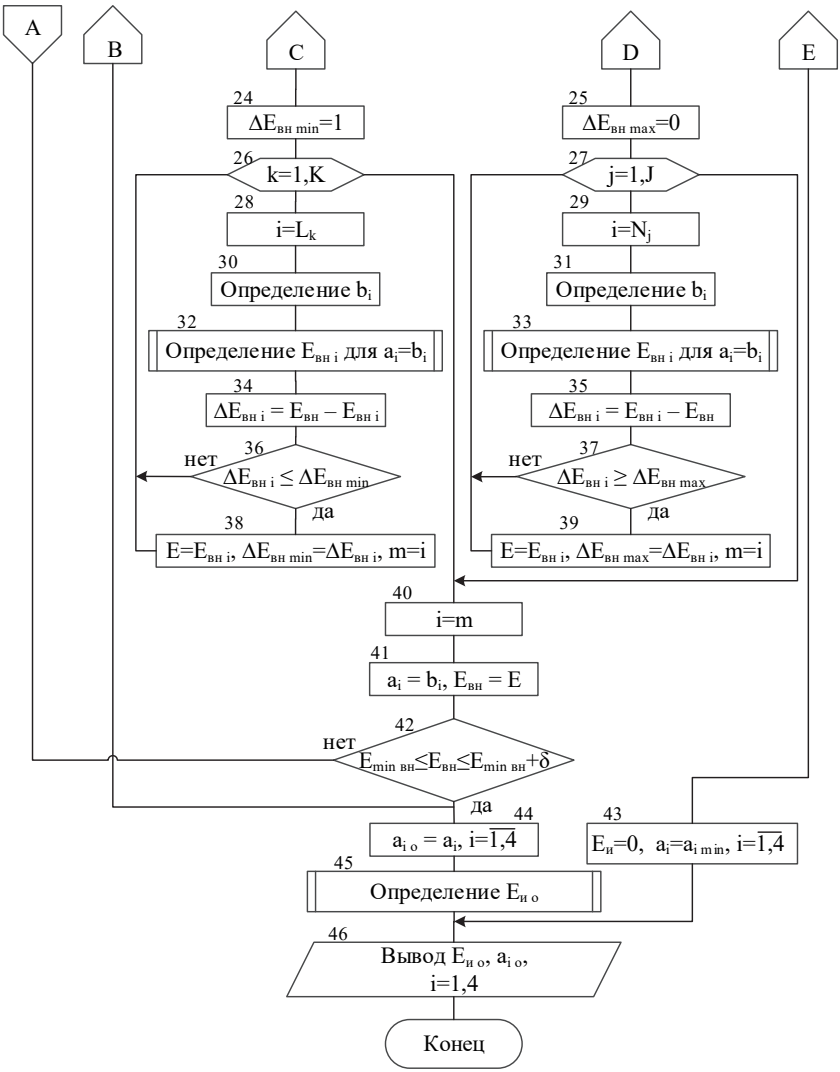


Рис. 3. Алгоритм определения оптимальных значений управляемых параметров и интегрального показателя эффективности функционирования ПЗИР при управлении ЗИР

Исходя из результата выполнения условий блоков 19 и 22 реализуются циклы выбора и увеличения (блоки 26, 28, 30, 32, 34, 36, 38) или уменьшения значения (блоки 27, 29, 31, 33, 35, 37, 39) управляемого параметра ПЗИР для выполнения выражения (7) или (5) соответ-

ственно. При выполнении условий блока 42 текущие значения управляемых параметров фиксируются как оптимальные (блок 44) и для них определяется значение интегрального показателя эффективности функционирования ПЗИР (блок 45). Иначе процедура регулирования управляемых параметров продолжается.

7. Исследование показателей эффективности функционирования ПЗИР. Построение и исследование графических зависимостей показателей эффективности функционирования ПЗИР от управляемых параметров для разных значений внешних параметров подсистемы являются важными при выявлении и изучении закономерностей ОТУ эффективностью функционирования ПЗИР в процессе эксплуатации. Оценка качественных показателей не требует проведения вычислений, и исследования зависимостей этих показателей от варьируемых параметров не представляют интереса. Значительный интерес вызывают зависимости показателя временной неконфликтности функционирования ПЗИР от варьируемых параметров.

Оценка показателя временной неконфликтности функционирования ПЗИР, активно используемая при управлении эффективностью функционирования ПЗИР, производится с использованием математической модели, созданной на базе графовой формализации динамики функционирования ПЗИР [4, 10]. Математическая модель оценки показателя временной неконфликтности функционирования ПЗИР как ОУ приведена в [4].

Комплекс программ (КП), реализующий математическую модель комплексной оценки эффективности функционирования ПЗИР, разработан на базе алгоритмов оценки показателей эффективности функционирования ПЗИР. Структурная схема КП для комплексной оценки эффективности функционирования ПЗИР в СЭД приведена на рисунке 4.

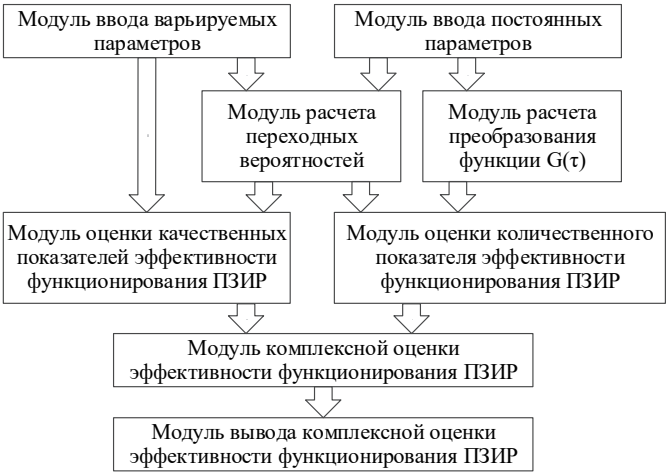


Рис. 4. Структурная схема КП для комплексной оценки эффективности функционирования ПЗИР в СЭД

Кроме управляемых параметров в качестве варьируемых параметров использовались следующие внешние параметры: $p_{да}$ — вероятность применения дополнительной аутентификации пользователя при его обращении к наиболее важному ресурсу; $p_{сб}$ — вероятность применения системной дискеты; $p_{б}$ — вероятность блокировки монитора и клавиатуры в случае не допустимых действий пользователя; $p_{пи}$ — вероятность применения преобразования информации; $p_{рв}$ — вероятность ручного восстановления вычислительной среды; $\tau_{т\,вн}$ — среднее значение максимально допустимого времени выполнения ПЗИР защитных функций [25, 26]. Для более полного анализа зависимостей $E_{вн}(a_i)$ исследования графических зависимостей осуществлялись при предельных значениях внешних параметров. На рисунке 5 приведены некоторые зависимости показателя временной неконфликтности функционирования ПЗИР от управляемых параметров.

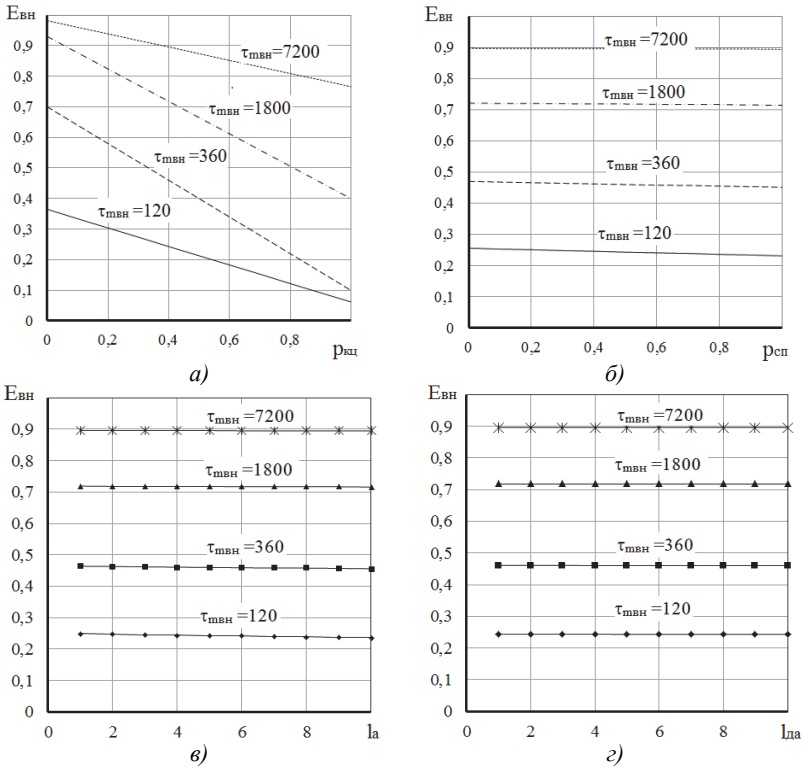


Рис. 5. Зависимости показателя временной неконфликтности функционирования ПЗИР от управляемых параметров

Зависимости даны для значений $p_{да} = 0,1$; $p_{сб} = 0,05$; =0,05; $p_{рв} = 0,01$; $p_{б} = 0,03$; $p_{пи} = 0,8$. Значения управляемых параметров, не участвующих в определении конкретной графической зависимости, были фиксированы: $p_{сп} = 0,5$; $p_{кц} = 0,4$; $l_{аут} = 5$; $l_{доп\ аут} = 5$ и приняты в качестве типовых. Если зависимости $E_{вн}(a_i)$ с ростом управляемого параметра возрастают, то это обозначает повышение эффективности функционирования ПЗИР по данному показателю, а если убывают — снижение ее эффективности.

Исследования и анализ зависимостей показателя временной неконфликтности функционирования рассматриваемой ПЗИР [4], позволяют сделать следующие выводы.

1. Зависимости $E_{вн}(a_i)$ при варьировании внешних параметров сохраняют характер своих изменений. Зависимость $E_{вн}(p_{кц})$ является линейной, убывающей при изменении $p_{кц}$ от 0 до 1. Зависимости $E_{вн}(l_{аут})$, $E_{вн}(l_{доп\ аут})$, $E_{вн}(p_{сп})$ являются линейными, значения которых при увеличении соответствующих управляемых параметров не возрастают.

2. Значения показателя временной неконфликтности функционирования исследуемой ПЗИР существенно зависят от изменений $p_{кц}$, а от изменений остальных управляемых параметров зависят слабо (диапазон изменений — единицы процентов). Это связано с тем, что временные затраты на ввод пароля в процессе стандартной и дополнительной аутентификации пользователя и использование специальных преобразований отдельных файлов незначительны для исследуемой ПЗИР.

3. При изменении $\tau_{т\,вн}$ закономерность изменения зависимостей $E_{вн}(a_i)$ сохраняется при варьировании параметров динамики функционирования ПЗИР. Значение показателя $E_{вн}$ возрастает при увеличении $\tau_{т\,вн}$. Для зависимости $E_{вн}(p_{кц})$ при увеличении $\tau_{т\,вн}$ интенсивность изменения максимального и минимального значений различна. Для малых значений $\tau_{т\,вн}$, возрастание данного параметра вызывает более интенсивное возрастание максимального значения $E_{вн}(p_{кц})$, увеличивая наклон этой зависимости. Рост $\tau_{т\,вн}$, при больших его значениях, наоборот, вызывает более интенсивное возрастание минимального значения $E_{вн}(p_{кц})$, уменьшая наклон данной зависимости.

Для других управляемых параметров зависимости $E_{вн}$ возрастают при увеличении $\tau_{т\,вн}$, уменьшая наклон этих кривых до горизонтального положения. Это связано с тем, что повышается эффективность функционирования ПЗИР при снижении требований по ЗИР СЭД.

На основе проведенного анализа можно сделать вывод, что для исследуемой ПЗИР наиболее эффективным параметром управления ее эффективностью является $p_{кц}$.

8. Заключение. Предложенная модель управления процессами ЗИР воплощает в себе результаты проработки аспектов создания методологии ОТУ ЗИР СЭД на базе ПСр ЗИР и обладает широкими возможностями по ее применению при разработке методов решения задач управления ЗИР. Концептуальная модель ОТУ ЗИР в СЭД представляет два взаимосвязанных вида управления: модель управления КПСЗ и модель управления ПЗИР. Управление КПСЗ реализуется путем оптимального управления эффективностью функционирования ПЗИР, обеспечивающее определение набора значений управляемых параметров подсистемы, позволяющего максимизировать уровень ЗИР при малом отрицательном воздействии ПЗИР на эффективность функционирования СЭД по назначению.

Разработанная методика ОТУ эффективностью функционирования ПЗИР реализуется с помощью управляемых параметров, позволяющих регулировать эффективность функционирования ПЗИР путем изменения их значений при воздействии сигналов управления. Данное управление является оптимальным, при котором определяются значения регулируемых параметров, обеспечивающие максимизация интегрального показателя эффективности функционирования ПЗИР и, соответственно, выполнение требований, предъявляемых к подсистеме. Предложенный метод организации управления позволяет осуществлять эффективное управление ПЗИР с целью повышения безопасности информационного ресурса в СЭД. Представленный алгоритм дает широкие возможности для применения при разработке ПК подсистемы автоматизированного управления эффективностью функционирования ПЗИР в СЭД.

Проведенное исследование показателя временной неконфликтности функционирования ПЗИР позволило определить некоторые закономерности, имеющие место при ОТУ эффективностью функционирования ПЗИР. Полученные результаты исследований по оценке эффективности функционирования ПЗИР как ОУ не противоречат известным данным, а также показывают широкие возможности данного метода при управлении эффективностью функционирования ПЗИР.

Разработанные модели и алгоритм ОТУ, приведенные в статье, в дальнейшем могут быть использованы для разработки предложений по совершенствованию как существующих, так и разрабатываемых СЗИ от НСД с целью повышения ИБ АС.

Литература

1. ГОСТ Р ИСО/МЭК 15408-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий // М.: Издательство стандартов. 2013. 267 с.
2. *Шаньгин В.Ф.* Защита информации в компьютерных системах и сетях // М.: ДМК Пресс. 2012. 592 с.
3. *Кузьмин А.В.* Теория систем автоматического управления // М.: ООО «ТНТ». 2012. 224 с.
4. *Застрожнов И.И.* Методологические основы безопасности использования информационных технологий в системах электронного документооборота // Воронеж: ИПЦ «Научная книга». 2011. 252 с.
5. *Qiu L. et al.* Trusted computer system evaluation criteria // National Computer Security Center. 1985. 116 p.
6. Information Technology Security Evaluation Criteria. Harmonized Criteria of France-Germany-Netherlands-United Kingdom // Department of Trade and Industry. 1991. 163 p.
7. Federal Criteria for Information Technology Security // National Institute of Standards and Technology & National Security Agency. Version 1.0. 1992.
8. The Canadian Trusted Computer Product Evaluation Criteria // Canadian System Security Center. Version 3.0e. 1993.
9. Common Criteria for Information Technology Security Evaluation // Common Criteria Project Sponsoring Organisations. Version 2.1. 1999.
10. *Львович Я.Е. и др.* Формализация функционирования перспективной программной системы защиты информации автоматизированных систем // Телекоммуникации. 2004. № 1. С. 38–43.
11. *Муратов А.В., Рогозин Е.А., Застрожнов И.И., Дубровин А.С.* Оценка качества функционирования перспективной программной системы защиты информации автоматизированных систем при проектировании радиоэлектронных средств // Проектирование и технология электронных средств. 2004. № 2. С. 2–5.
12. *Табак Д., Куо Б.* Оптимальное управление и математическое программирование // М.: Главная редакция физико-математической литературы издательства "Наука". 1975. 280 с.
13. *Yun L., Sheng-Peng L., Li L., Yuan-Yuan M.* Effectiveness Evaluation on Cyberspace Security Defense System // International Conference on Network and Information Systems for Computers. 2015. pp. 576–579.
14. *Xin Z., Shaojie M., Fang Z.* Research on effectiveness evaluation of the mission-critical system // Proceedings of 2013 2nd International Conference on Measurement, Information and Control. 2013. pp. 869–873.
15. *Ptitsyn P.S., Radko D.V., Lankin O.V.* Designing architecture of software framework for building security infrastructure of global distributed computing systems // ARPN Journal of Engineering and Applied Sciences. 2016. vol. 11. no. 19. pp. 11599–11610.
16. *Заряев А.В. и др.* Методическое обеспечение управления доступом пользователей к рабочей среде автоматизированных систем // Телекоммуникации. 2004. № 2. С. 39–44.
17. *Ощепков А.Ю.* Системы автоматического управления. Теория, применение, моделирование в MATLAB // СПб.: Лань. 2013. 208 с.

18. *Скрыль С.В., Окрачков А.А.* Метод количественной оценки показателей эффективности систем защиты информации от несанкционированного доступа // Вестник Воронежского института МВД России. 2013. № 3. С. 78–83.
19. *Мещерякова Т.В.* Показатели для оценки эффективности информационных процессов в условиях обеспечения их защищенности в автоматизированных информационных системах органов внутренних дел // Вестник Воронежского института МВД России. 2014. № 1. С. 141–150.
20. *Скрыль С.В. и др.* Показатели эффективности информационной деятельности в условиях комплексного технического контроля обеспечения защищенности речевой информации // Приборы и системы. Управление, контроль, диагностика. 2016. № 2. С. 28–34.
21. *Скрыль С.В., Голубков Д.А., Половинкин В.А.* Показатели эффективности информационных процессов в интегрированных системах безопасности в условиях обеспечения антивирусной защиты // Вестник Воронежского института МВД России. 2014. № 4. С. 212–220.
22. *Змеев С.А., Селютин И.Н., Скрыль Е.Б., Никитин А.А.* Рациональный выбор средств защиты при структурном синтезе программных систем защиты информации в системах электронного документооборота // Вестник Воронежского института ФСИН России. 2013. № 2. С. 55–59.
23. *Родионова Н.С., Белокуров С.В., Скрыль С.В.* Показатели эффективности управления информационными процессами в интегрированных системах безопасности // Вестник Воронежского государственного университета инженерных технологий. 2014. № 4. С. 79–84.
24. *Мещерякова Т.В., Фирюлин М.Е., Хворов Р.А.* Аналитические модели показателей состояния защищенности информации в центрах обработки данных органов внутренних дел// Вестник Воронежского института МВД России. 2015. № 3. С. 104–113.
25. *Ланкин О.В., Мещерякова Т.В., Селютин И.Н.* Обеспечение целостности информационных ресурсов подсистемы безопасности распределенных информационно-вычислительных систем // Вестник Воронежского института МВД России. 2017. № 1. С. 35–42.
26. *Скрыль С.В. и др.* Оценка характеристик компонент защиты информации от несанкционированного доступа для реализации функций обеспечения целостности и доступности информации // Приборы и системы. Управление, контроль, диагностика. 2014. № 7. С. 21–25.

Авсентьев Олег Сергеевич — д-р техн. наук, профессор, профессор кафедры информационной безопасности, Воронежский институт Министерства внутренних дел России. Область научных интересов: информационная безопасность, защита информации, моделирование систем защиты информации. Число научных публикаций — 87. osaos@mail.ru; пр. Патриотов, 53, Воронеж, 394065; р.т.: +7(473)200-52-36.

Дровникова Ирина Григорьевна — д-р техн. наук, доцент, профессор кафедры автоматизированных информационных систем органов внутренних дел, Воронежский институт Министерства внутренних дел России. Область научных интересов: системы защиты информации, эволюционное моделирование, автоматизированные информационные системы, теория вероятности, управление в социально-экономических системах. Число научных публикаций — 210. idrovnikova@mail.ru; пр. Патриотов, 53, Воронеж, 394086; р.т.: +7(472)200-51-88.

Застрожнов Игорь Иванович — к-т техн. наук, доцент кафедры эксплуатации авиационного оборудования, Военный учебно-научный центр ВВС «Военно-воздушная академия имени профессора Н.Е. Жуковского и Ю.А. Гагарина». Область научных интересов: защита информации от НСД в АИС, проектирование и управление процессами защиты

информации на основе количественной оценки СЗИ от НСД в АИС. Число научных публикаций — 112. zasigor@yandex.ru; ул. Краснознаменная, 153, Воронеж, 394052; р.т.: +7(473)200-51-88.

Попов Антон Дмитриевич — адъюнкт кафедры автоматизированных информационных систем органов внутренних дел, Воронежский институт МВД России. Область научных интересов: защита информации от НСД в АИС, проектирование и управление процессами защиты информации на основе количественной оценки СЗИ от НСД в АИС, тестирование и анализ СЗИ, разработка АИС, прикладная информатика. Число научных публикаций — 40. anton.holmes@mail.ru; пр. Патриотов, 53, Воронеж, 394086; р.т.: +7(473)200-51-80.

Рогозин Евгений Алексеевич — д-р техн. наук, профессор, профессор кафедры автоматизированных информационных систем органов внутренних дел, Воронежский институт Министерства внутренних дел России. Область научных интересов: защита информации от НСД в АИС, проектирование и управление процессами защиты информации на основе количественной оценки СЗИ от НСД в АИС, прикладная информатика. Число научных публикаций — 240. evgenirogozin@yandex.ru; пр. Патриотов, 53, Воронеж, 394086; р.т.: +7(473)200-51-88.

DOI 10.15622/sp.57.8

O.S. AVSENTEV, I.G. DROVNIKOVA, I.I. ZASTROZHNOV, A.D. POPOV, E.A. ROGOZIN

CONTROL TECHNIQUES OF INFORMATION RESOURCE PROTECTION OF ELECTRONIC DOCUMENT MANAGEMENT SYSTEM

Avsentev O.S., Drovnikova I.G., Zastrozhnov I.I., Popov A.D., Rogozin E.A. **Control Techniques of Information Resource Protection of Electronic Document Management System.**

Abstract. The article discusses methodological bases for the organizational and technological control (OTC) of the protection of an information resource (PIR) of electronic document management systems (EDMS) based on software (SW) of information security. The authors developed a conceptual model of control of PIR of EDMS on the basis of conceptual study of the aspects of the formation of OTC PIR EDMS methodology on the basis of the SW of PIR, which has ample opportunities to be used for developing methods of administrative tasks solution. The paper presents a technique for efficiency management of functioning of the information resource protection subsystem (IRPS) in EDMS, assuming optimization of the subsystem controlled parameters that maximize an integral index of efficiency of IRPS functioning and respectively execution of requirements imposed to the subsystem. The algorithm for determining best values of the IRPS controlled parameters and best value of an integral index of efficiency of the subsystem, providing a possibility of creating specific subsystems of IRPS automated management efficiency in EDMS, is given. Results of calculations for a research of an index of temporal non-conflictness of IRPS functioning are analyzed.

Keywords: organizational and technological control, protection of an information resource, electronic document management system, subsystem of protection of an information resource, efficiency of a subsystem, control of efficiency.

Avsentev Oleg Sergeevich — Ph.D., Dr. Sci., professor, professor of information security department, Voronezh Institute of the Ministry of Interior. Research interests: information security, information protection, modeling of information security systems. The number of publications — 87. osaos@mail.ru; 53, pr. Patriotov, Voronezh, 394086, Russia; office phone: +7(473)200-52-36.

Drovnikova Irina Grigorevna — Ph.D., Dr. Sci., associate professor, professor of automated information systems in interior affairs department, Voronezh Institute of the Ministry of Interior. Research interests: information systems security, evolutionary modeling, automated information systems, probability theory, social-and-economic system management. The number of publications — 210. idrovnikova@mail.ru; 53, Prospekt Patriotov, Voronezh, 394086, Russia; office phone: +7(472)200-51-88.

Zastrozhnov Igor Ivanovich — Ph.D., associate professor of aeronautical equipment department, Military educational scientific center of the Air Force "Air-force academy of a name of professor N.E. Zhukovsky and Yu. A. Gagarin". Research interests: information security from the unauthorized access in AIS; design and management of information security processes based on the quantitative assessment of ISS security from the unauthorized access in AIS. The number of publications — 112. zasigor@yandex.ru; 153, Krasnoznamennaya St., Voronezh, 394052, Russia; office phone: +7(473)200-51-88.

Popov Anton Dmitrievich — Ph.D. student of automated information systems in interior affairs department, Voronezh Institute of the Ministry of Interior. Research interests: infor-

mation protection against unauthorized access in AIS, design and management of information security processes based on quantitative assessment of ISS, testing and analysis of ISS, AIS development, applied computer science. The number of publications — 40. anton.holmes@mail.ru; 53, Prospekt Patriotov, Voronezh, 394086, Russia; office phone: +7(473)200-51-80.

Rogozin Evgeniy Alekseevich — Ph.D., Dr. Sci., professor, academician of RANS, professor of automated information systems in interior affairs department, Voronezh Institute of the Ministry of Interior. Research interests: information security from the unauthorized access in AIS, design and management of information security processes based on the quantitative assessment of ISS security from the unauthorized access in AIS, applied informatics. The number of publications — 240. evgenirogozin@yandex.ru; 53, Prospekt Patriotov, Voronezh, 394086, Russia; office phone: +7(473)200-51-88.

References

1. GOST P 15408-2013. [Methods and security protections. Criteria for evaluation of safety of information technologies]. M.: Izdatel'stvo standartov. 2013. 267 p. (In Russ.).
2. Shangin V.F. *Zashhita informacii v komp'juternyh sistemah i setjah* [Information security in computer systems and networks: studies. manual]. M.: DMK Press. 2012. 592 p. (In Russ.).
3. Kuzmin A.V., Skhirtladze A.G. *Teorija sistem avtomaticheskogo upravlenija* [Theory of systems of automatic control]. M.: LLC TNT. 2012. 224 p. (In Russ.).
4. Zastrozhnov I.I. Rogozin E.A., Bagayev M.A. *Metodologicheskie osnovy bezopasnosti ispol'zovanija informacionnyh tehnologij v sistemah jelektronnogo dokumentooborota* [Methodological bases of safety of use of information technologies in electronic document management systems: monograph]. Voronezh: IPTs "Scientific Book". 2011. 252 p. (In Russ.).
5. Qiu L. et al. Trusted computer system evaluation criteria. National Computer Security Center. 1985. 116 p.
6. Information Technology Security Evaluation Criteria. Harmonized Criteria of France-Germany-Netherlands-United Kingdom. Department of Trade and Industry. 1991. 163 p.
7. Federal Criteria for Information Technology Security. National Institute of Standards and Technology & National Security Agency. Version 1.0. 1992.
8. Canadian Trusted Computer Product Evaluation Criteria. Canadian System Security Center. Version 3.0e. 1993.
9. Common Criteria for Information Technology Security Evaluation. Common Criteria Project Sponsoring Organisations. Version 2.1. 1999.
10. Lvovich Ya.E. et al. [Formalization of functioning of perspective program system of information security of automated systems]. *Telekommunikacii – Telecommunications.* 2004. vol. 1. pp. 38–43. (In Russ.).
11. Muratov A.V., Rogozin E.A., Zastrozhnov I.I., Dubrovin A.S. [Otsenka of quality of functioning of perspective program system of information security of automated systems in case of design of radio-electronic means]. *Proektirovanie i tehnologija jelektronnyh sredstv – Design and technology of electronic means*. 2004. vol. 2. pp. 2–5. (In Russ.).
12. Tabak D., Kuo B.C. *Optimal Control by Mathematical Programming.* Prentice-Hall. 1971. (Russ. ed.: Tabak D., Kuo B. *Optimal'noe upravlenie i matematicheskoe programmirovanie*. M.: Glavnaja redakcija fiziko-matematicheskoj literatury izdatel'stva "Nauka". 1975. 280 p.).
13. Yun L., Sheng-Peng L., Li L., Yuan-Yuan M. Effectiveness Evaluation on Cyberspace Security Defense System. International Conference on Network and Information Systems for Computers. 2015. pp. 576–579.

14. Xin Z., Shaojie M., Fang Z. Research on effectiveness evaluation of the mission-critical system.Proceedings of 2013 2nd International Conference on Measurement, Information and Control. 2013. pp. 869–873.
15. Ptitsyn P.S., Radko D.V., Lankin O.V. Designing architecture of software framework for building security infrastructure of global distributed computing systems. *ARPN Journal of Engineering and Applied Sciences*. 2016. vol. 11. no. 19. pp. 11599–11610.
16. Zaryaev A.V. et al. [Methodical support of access control of users to a work environment of automated systems]. *Telekommunikacii – Telecommunications.* 2004. vol. 2. pp. 39–44. (In Russ.).
17. Oshchepkov A.Yu. [Systems of automatic control. The theory, application, simulation in MATLAB]. SPb.: Fallow deer. 2013. 208 p. (In Russ.).
18. Skryl' S.V., Okrachkov A.A. [The method of quantifying performance information protection from unauthorized access] *Vestnik Voronezhskogo gosudarstvennogo universiteta inzhenernyh tehnologij - Bulletin of Voronezh State University of Engineering Technology*. 2013. vol. 3. pp. 78–83. (In Russ.).
19. Mesherjakova T.V. [The method of quantifying performance information protection from unauthorized access of the Law Enforces Agencies]. *Vestnik Voronezhskogo gosudarstvennogo universiteta inzhenernyh tehnologij - Bulletin of Voronezh State University of Engineering Technology.* 2014. vol. 1. pp. 141–150. (In Russ.).
20. Skryl' S.V. et al. [Indicators of effectiveness of information activity in the conditions of complex technical control provide voice information security]. *Pribory i system. Upravlenie, kontrol', diagnostika - Instruments and systems. Management, monitoring, diagnostics*. 2016. vol. 2. pp. 28–34. (In Russ.).
21. Skryl' S.V., Golubkov D.A., Polovinkin V.A. [Performance indicators of information processes in integrated security systems in the conditions of anti-virus protection software]. *Vestnik Voronezhskogo instituta MVD Rossii - Bulletin of the Voronezh Institute of the Ministry of the Interior of Russia*. 2014. vol. 4. pp. 212–220. (In Russ.).
22. Zmeev S.A., Seljutin I.N., Skryl' E.B., Nikitin A.A. [Rational choice of means of protection in the structural synthesis of software systems for information protection in electronic document management systems]. *Vestnik Voronezhskogo instituta FSIN Rossii - Bulletin of the Voronezh Institute of the Federal Penitentiary Service of Russia*. 2013. vol. 1. pp. 82–85. (In Russ.).
23. Rodionova N.S., Belokurov S.V., Skryl' S.V. [Performance information processes management in integrated security systems]. *Vestnik Voronezhskogo gosudarstvennogo universiteta inzhenernyh tehnologij - Bulletin of Voronezh State University of Engineering Technology.* 2014. vol. 4. pp. 79–84. (In Russ.).
24. Meshherjakova T.V., Firjulin M.E., Hvorov R.A. [Analytical models of information security status indicators in the data processing centers of internal affairs bodies]. *Vestnik Voronezhskogo instituta MVD Rossii - Bulletin of the Voronezh Institute of the Ministry of the Interior of Russia*. 2015. vol. 3. pp. 104–113. (In Russ.).
25. Lankin O.V., Meshherjakova T.V., Seljutin I.N. [Ensuring the integrity of information resources of the security subsystem of distributed information and computing systems]. *Vestnik Voronezhskogo instituta MVD Rossii - Bulletin of the Voronezh Institute of the Ministry of the Interior of Russia*. 2017. vol. 1. pp. 35–42. (In Russ).
26. Skryl' S.V. et al. [Sizintsev Evaluation of information security components of the characteristics of the unauthorized access to the realization of functions to ensure the integrity and availability of information]. *Pribory i system. Upravlenie, kontrol', diagnostika - Instruments and systems. Management, monitoring, diagnostics*. 2014. vol. 7. pp. 21–25. (In Russ).