Новый подход к построению моделей безопасности систем электронного документооборота

М.И. Поддубный

Краснодарское высшее военное орденов Жукова и Октябрьской Революции Краснознаменное училище имени генерала армии С.М. Штеменко

Аннотация: В статье подтверждена необходимость системного подхода к научному обоснованию безопасности систем электронного документооборота (СЭД) и актуальность исследования, приведены результаты анализа руководящих документов в части разработки математических моделей и имеющегося опыта, обобщен порядок научного обоснования безопасности СЭД, выделены основные тенденции в моделировании на сегодняшний день, предложен новый подход к построению моделей безопасности СЭД, определена его роль и место в существующей теории и практике.
Ключевые слова: модели безопасности компьютерных систем, политика безопасности, система электронного документооборота, системный подход.

Предметом исследования являются процессы обработки и хранения электронных документов в системе электронного документооборота (СЭД), объектом – методы и модели безопасной обработки и хранения электронных документов в СЭД.

Целями указанного исследования являются: экспликация порядка моделирования безопасности СЭД, разработка предложения по совершенствованию существующих подходов к построению моделей безопасности.

Требование об обязательной разработке модели безопасности, согласно приказу ФСТЭК России № 76 от 02.06.20 г, предъявляется системам от 4-го уровня доверия и выше.

Требования являются обязательными в области технического регулирования и предъявляются к продукции (работам, услугам), используемой в целях защиты сведений ограниченного доступа, охраняемых, в соответствии с законодательством Российской Федерации, применяются к программным и программно-техническим средствам технической защиты информации, средствам обеспечения безопасности информационных

технологий, включая защищенные средства обработки информации, к которым должна относиться и моделируемая СЭД.

Рассматривая подобные системы с точки зрения потребности Вооруженных Сил Российской Федерации (ВС РФ), можно отметить актуальность подобных исследований.

Такой пример является наиболее показательным в смысле многообразия обрабатываемой информации, постоянного возрастания угроз, высокой квалификации нарушителей и очевидного ограничения применения заимствованных технологий.

С точки зрения научного обоснования безопасности функционирования в заданном пространстве угроз, СЭД ВС РФ объединяет в себе несколько основных систем: систему управления базами данных, сервер приложений и программное обеспечение автоматизированных рабочих мест должностных лиц. Кроме того, необходимым является доказательство безопасного взаимодействия с существующими моделями безопасности операционных систем и сетевых сервисов, применяемых в ВС РФ, так как без этих элементов применение СЭД невозможно.

На сегодняшний день исследования в указанном направлении ведутся разрозненно в интересах развития безопасности отдельных элементов. Отсутствие системного подхода на этапе научного обоснования может привести к необходимости доработок на завершающей стадии объемом, сопоставимым с разработкой нового продукта, либо принципиальной невозможностью безопасного применения СЭД в заданных условиях эксплуатации.

Основные руководящие документы, регламентирующие указанную деятельность, представлены на рис. 1.

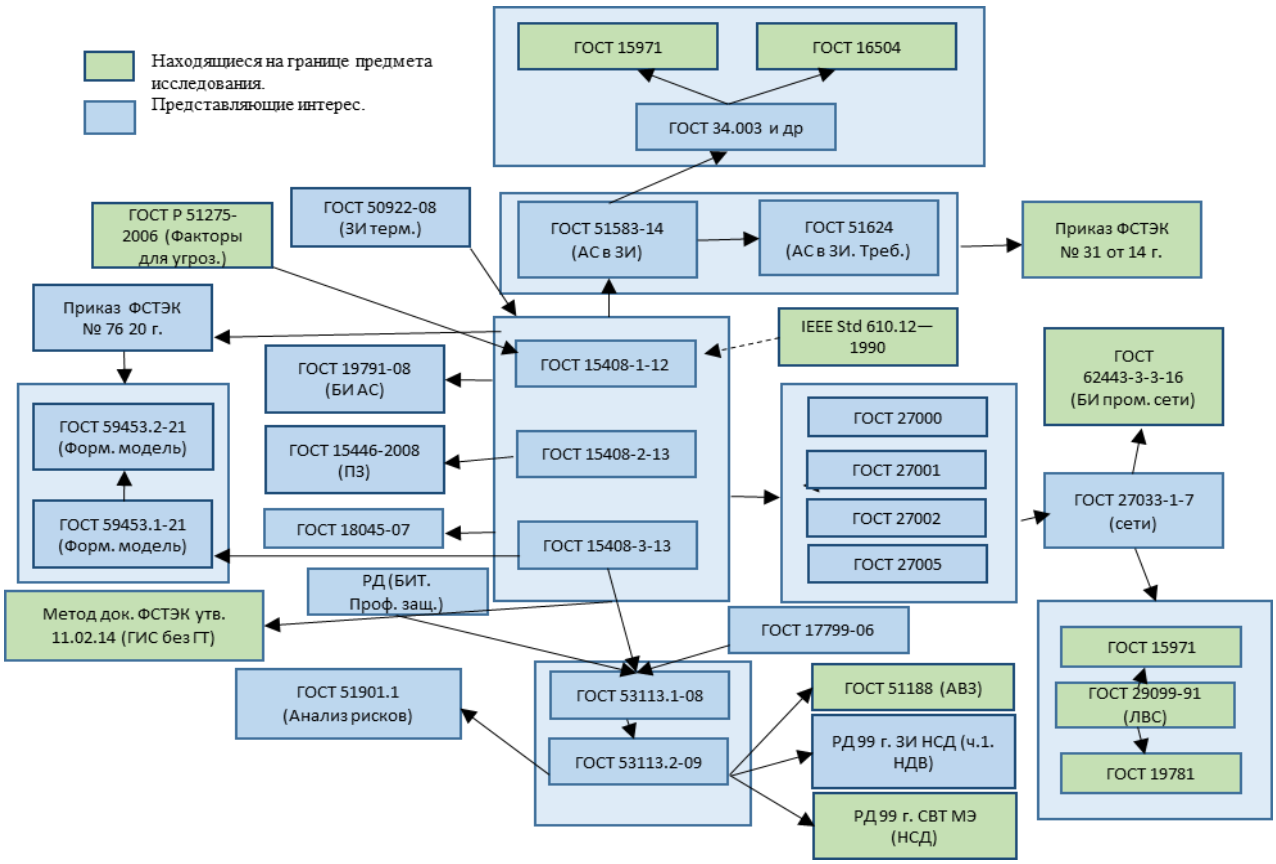

Рис. 1. – Руководящие документы по части моделирования безопасности автоматизированных систем

Анализ представленных документов позволил обобщить порядок разработки математической модели безопасности СЭД (рис.2):

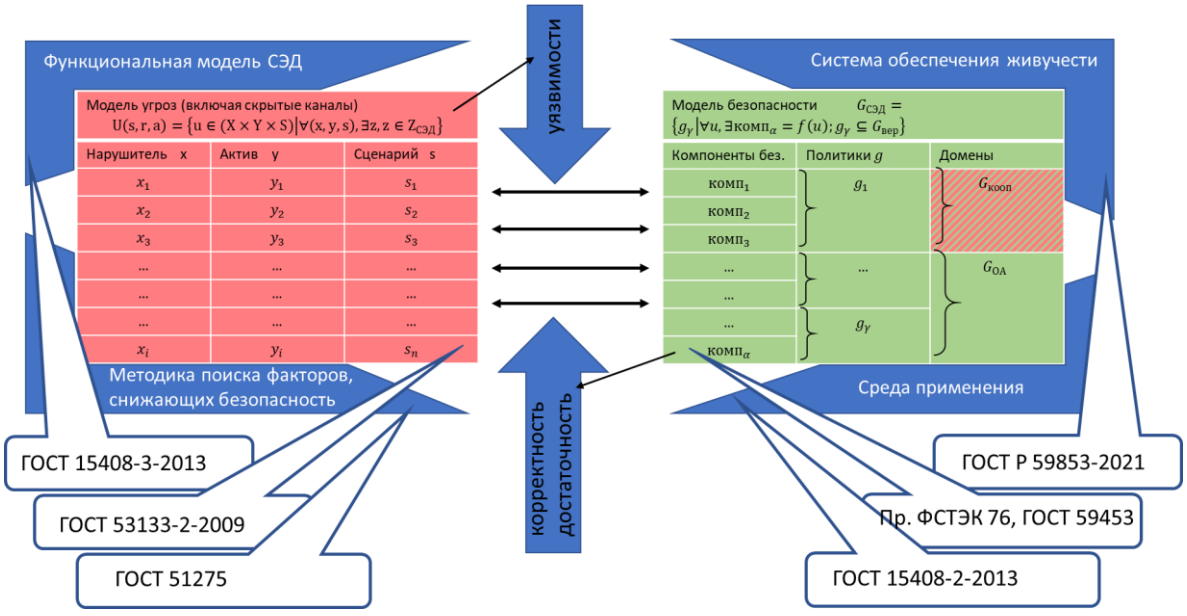

Рис. 2. – Порядок разработки модели безопасности АС

1. Разработка модели угроз $U(\mathrm{x},\mathrm{y},s)=\{u\in(X\times Y\times S)|\forall(x,y,s),\exists z,z\in Z_{\text{СЭД}}\}$,

где $X=\{x\}$ – конечное множество нарушителей одного из установленных типов;

$Y=\{y\}$ – конечное множество активов системы;

$S=\{s\}$ – конечное множество сценариев воздействия на актив;

$U=\{u\}$ – конечное множество угроз безопасности;

$Z_{\text{СЭД}}=\{z\}$ – множество уязвимостей СЭД.

Как видно, каждая угроза представляет собой тройку элементов: нарушителя x, атакуемый актив y и возможный сценарий проведения атаки s. Для описания угроз, определения защищаемых активов требуется понимание процессов обработки в разрабатываемой системе. С этой целью разумно разработать функциональную модель СЭД. Если при этом имеется уязвимость z, то мы говорим уже о риске [1, 2].

2. Для устранения указанного риска или приведения его к приемлемому уровню для каждой угрозы подбирается минимум один компонент безопасности, которые образуют политики безопасности. Сегменты системы, реализующие одинаковые политики безопасности, формируют домены безопасности (например, $G_{\text{кооп}}$ и $G_{\text{ОА}}$)

С целью доказательства корректности и достаточности подобранных компонентов безопасности, с учетом требований среды применения, разрабатывается математическая модель безопасности $G_{\text{СЭД}}$, которую в общем виде можно выразить формулой:

$$G_{\text{СЭД}}=\{g_\gamma|\forall u,\ \exists\text{комп}_\alpha=f(u);g_\gamma\subseteq G_{\text{вер}}\},$$

где g_γ – политики безопасности, состоящие из некоторых компонентов безопасности комп_α;

$f(u) = \{\text{комп}_\mu | \text{комп}_\mu \in g_\gamma\}$ – функция отображения множества угроз на множество компонентов безопасности;

$G_{\text{вер}}$ – множество политик безопасности, потенциально верифицируемых существующими инструментами [3].

3. Полнота и непротиворечивость разработанной модели доказывается с использованием существующих средств автоматизации работы со спецификациями и соответствующих сред разработки [4].

4. На основе модели безопасности и модели угроз целесообразно (в случае, если речь идет об конкретном изделии, или есть четкое понимание исполнения будущего изделия) сформировать методики поиска факторов, снижающих информационную безопасность и их устранения. Подобные методики, как правило, сохраняются в тайне.

5. Применительно к ВС РФ, следует также обратить внимание на учет живучести системы. При разработке модели серия ГОСТ 15408 требует максимально снизить сложность системы, что, по сути, является противоречивой задачей по отношению к обеспечению живучести. Судьба системы зачастую зависит от эффективности и оперативности работы средств обеспечения живучести.

На сегодняшний день представлены 4 политики безопасности, описываемые соответствующими математическими моделями: дискреционная; мандатная; ролевая; безопасности информационных потоков, а также различные их комбинации.

Выявлено порядка 30-ти основных апробированных моделей. Наиболее прогрессивный подход к моделированию особенно ярко представлен в модели разграничения доступа операционной системы Astra Linux (МРОСЛ) и может быть сформулирован в виде следующих особенностей [5]:

- уход от абстракции в сторону моделирования работы конкретного изделия (Astra Linux) [6];

- создание условий для развития модели в виде разработки новых «слоев» (например, разработка модели безопасности, штатной для Astra Linux системы управления базами данных PostgreSQL). Такой подход получил название «иерархическое представление» (иерархическое развитие) [5] модели безопасности (рис. 3).

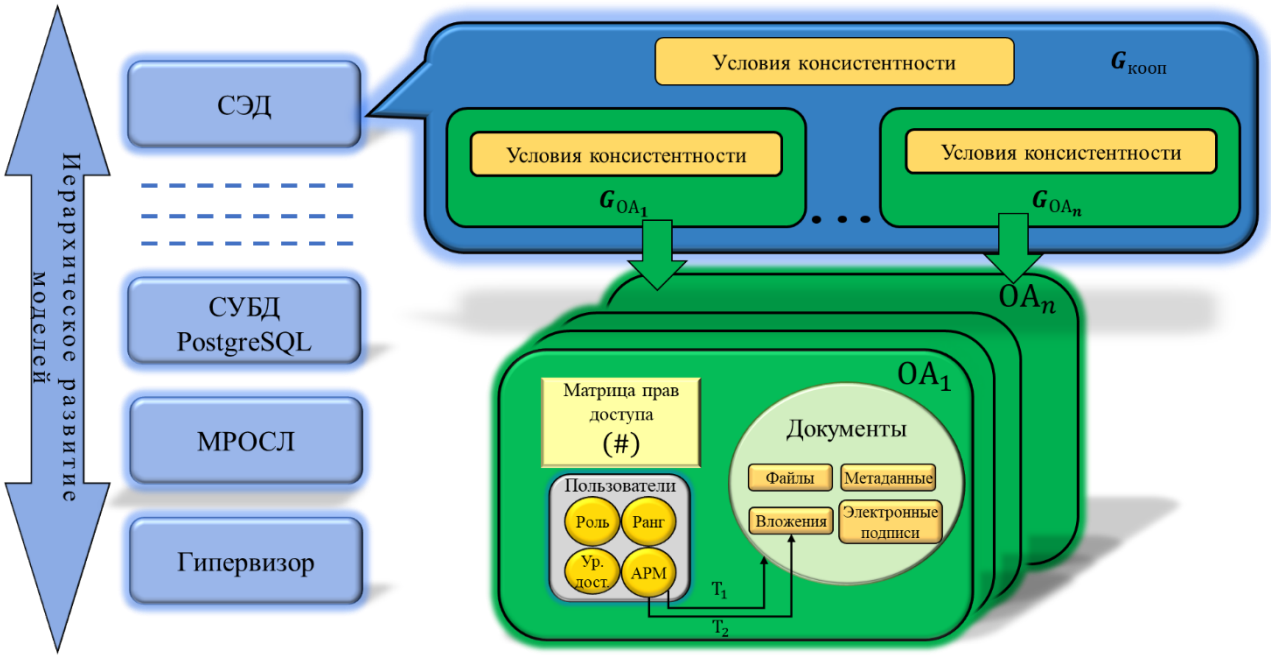

Рис. 3 – Схематическое изображение нового похода к моделированию СЭД

Одной из особенностей ВС РФ, накладывающей существенные ограничения и требующей учета при разработке модели безопасности СЭД, является необходимость в установленные сроки обеспечивать бесконфликтное взаимодействие широкого спектра объектов автоматизации (ОА), которые не только могут обрабатывать информацию различного уровня ограничения, но и реализовывать совершенно разные политики безопасности (взаимодействие с иными органами власти и ведомствами, документооборот в которых вообще регламентирован иными руководящими документами) [7].

Для повышения безопасности СЭД в ходе взаимодействия между собой ОА, а также обеспечения возможности создания перспективных моделей СЭД и их простой интеграции в общую систему предлагается представить

модель безопасности в виде двух взаимодействующих между собой доменов безопасности – объекта автоматизации и кооперации (рис.3), что ранее при разработки моделей не применялось. При этом базовая теорема безопасности может доказываться в два этапа: доказательство безопасности ОА, доказательство безопасности кооперации, где одним из условий безопасности является безопасность обслуживаемых ОА.

Такой подход не противоречит существующему иерархическому представлению, но развивает его. Занимая свое место в иерархии, СЭД позволяет осуществлять развитие систем этого класса в рамках одного «слоя» (рис.3). Также не требуется пересмотра существующего порядка разработки моделей безопасности с точки зрения руководящих документов, т.к. новый подход ограничивается выбором и описанием соответствующих доменов: $G_{\text{кооп}}$ и $G_{\text{ОА}}$ (рис.2).

Рассматривая предложенных подход с точки зрения общей теории систем и ее развитий, прежде всего следует отметить следующее.

Структура модели носит иерархических характер. Взаимоотношения систем в иерархии наиболее полно описаны в трудах Михайло Месаровича и его последователей. Что характерно, именно двухуровневая иерархия рассмотрена наиболее подробно, подразумевая наличие координатора и систем низшего уровня [8, 9]. Вместе с тем, предлагаемый домен не ограничивается свойствами, определяемыми представленной теорией и является не сколько координатором, улучшающим работу, но и непосредственно транслирует информационные потоки между подключаемыми системами, обеспечивая их совместную работу и контроль требуемых параметров систем на этапе подключения и в процессе работы.

Такой «терминальный» характер работы системы высшей иерархии требует определения порядка корректного подключения обслуживаемых систем к терминалу, отслеживаемых свойств, ограничений, накладываемых

терминалом и обслуживаемыми системами друг на друга. В этой связи целесообразно рассмотреть параметрическую общую теорию систем Авенира Ивановича Уемова, обратив внимание на понятия системный параметр, свойства сравнимости и сопоставимости систем [10]. А также подходы к подобному взаимодействию систем, представленному в синергетическом подходе и модульной теории систем, описанных Беловым Александром Аркадьевичем [11].

Резюмируя сказанное, следует отметить, что представленный подход:

- обладает новизной и не противоречит существующей передовой практике разработки моделей – иерархическому представлению, устраняя при этом проблемы взаимодействия различных СЭД в рамках единого пространства;

- с точки зрения общей теории систем находится на стыке трех теорий [8, 10, 11], что, в свою очередь, требует отдельного исследования.

Литература

1. Шишов Н.В., Ломазов В.А. Моделирование процессов функционирования системы электронного документооборота при воздействии ARP-spoofing атак // Инженерный вестник Дона, 2022. №2 URL: ivdon.ru/ru/magazine/archive/n2y2022/7475 (дата обращения 30.01.2023).

2. Носков С.И., Бутин А.А. Применение экспертных данных при построении регрессионной модели оценки уровня защищенности носителей информации // Инженерный вестник Дона, 2022. №8 URL: ivdon.ru/ru/magazine/archive/n8y2022/7868 (дата обращения 30.01.2023).

3. Поддубный М.И., Левштанов И.В., Шавин А.А., Варов А.С. Сравнение языков написания спецификаций, используемых при верификации математических моделей // материалы III Всероссийской научно-технической конференции «Состояние и перспективы развития современной науки по

направлению «Информационная безопасность». Анапа: ВИТ «ЭРА», 2021. С. 731-737.

4. Поддубный М.И., Ртищев В.М., Лидяев Д.И., Кокорин А.О. Роль и место сертификационных испытаний в разработке подсистемы разграничения доступа // материалы I Всероссийской научно-технической конференции «Состояние и перспективы развития современной науки по направлению «IT-технологии». Анапа: ВИТ «ЭРА», 2022. С. 23-32.

5. Девянин П.Н., Ефремов Д.В., Кулямин В.В., Петренко А.К., Хорошилов А.В., Щепетков И.В. Моделирование и верификация политик безопасности управления доступом в операционных системах. М.: Горячая линия – Телеком, 2019. 214 с. ISBN 978-5-9912-0787-4.

6. Буренин П.В., Девянин П.Н., Лебеденко Е.В., Проскурин В.Г., Цибуля А.Н. Безопасность операционной системы специального назначения Astra Linux Special Edition: учеб. пособие для вузов – 3-е издание, перераб. и доп. М.: Горячая линия – Телеком, 2019. 404 с. ISBN 978-5-9912-0807-9.

7. Носенко С.В., Королев И.Д., Поддубный М.И. О единой системе электронного документооборота // Военная мысль. Ежемесячный военно-теоретический журнал. 2019. № 3. С. 90-97.

8. Mesarovic M.D., Macko D. Takahara Y Theory of hierarchical, multilevel, systems, Academic press: New York and London, 1970. 294 p.

9. Mesarovic M.D., Takahara Y General systems theory: mathematical foundations, Academic press: New York, San Francisco, London, 1975. 292 p.

10. Параметрическая общая теория систем и ее применения: сб.науч. тр. посвященный 80-летию проф. А. И. Уёмова / Под ред. А. Ю. Цофнаса Одесса: Астропринт, 2008. 248 с.

11. Белов А.А., Гвоздев А.В. Модульное построение автоматизированной системы управления организационными процессами // Вестник ИГТУ. 2007. №3. С. 94-98.

References

1. Shishov N.V., Lomazov V.A. Inzhenernyj vestnik Dona, 2022. №2. URL: ivdon.ru/ru/magazine/archive/n2y2022/7475 (date accessed 30.01.2023).

2. Noskov S.I., Butin A.A. Inzhenernyj vestnik Dona, 2022. №8. URL: ivdon.ru/ru/magazine/archive/n8y2022/7868 (date accessed 30.01.2023).

3. Poddubnyj M.I., Levshtanov I.V., Shavin A.A., Varov A.S. Materialy III Vserossijskoj nauchno-tehnicheskoj konferencii “Sostojanie i perspektivy razvitija sovremennoj nauki po napravleniju “Informacionnaja bezopasnost'”. Anapa: VIT “JeRA”, 2021. Pp. 731-737.

4. Poddubnyj M.I., Rtishhev V.M., Lidjaev D.I., Kokorin A.O. Materialy I Vserossijskoj nauchno-tehnicheskoj konferencii “Sostojanie i perspektivy razvitija sovremennoj nauki po napravleniju “IT-tehnologii”. Anapa: VIT “JeRA”, 2022. Pp. 23-32.

5. Devjanin P.N., Efremov D.V., Kuljamin V.V., Petrenko A.K., Horoshilov A.V., Shhepetkov I.V. Modelirovanie i verifikacija politik bezopasnosti upravlenija dostupom v operacionnyh sistemah [Modeling and verification of access control security policies in operating systems]. M.: Gorjachaja linija – Telekom, 2019. 214 p. ISBN 978-5-9912-0787-4.

6. Burenin P.V., Devjanin P.N., Lebedenko E.V., Proskurin V.G., Cibulja A.N. Bezopasnost' operacionnoj sistemy special'nogo naznachenija Astra Linux Special Edition [Security of the special-purpose operating system Astra Linux Special Edition]: ucheb. posobie dlja vuzov. 3-e izdanie, pererab. i dop. M.: Gorjachaja linija. Telekom, 2019. 404 p.

7. Nosenko S.V., Korolev I.D., Poddubnyj M.I. Voennaja mysl'. Ezhemesjachnyj voenno-teoreticheskij zhurnal. 2019. № 3. Pp. 90-97.

8. Mesarovic M.D., Macko D. Takahara Y Theory of hierarchical, multilevel, systems, Academic press: New York and London, 1970. 294 p.

9. Mesarovic M.D., Takahara Y General systems theory: mathematical foundations. Academic press: New York, San Francisco, London, 1975. 292 p.

10. Parametricheskaja obshhaja teorija sistem i ee primenenija: sb.nauch. tr. posvjashhennyj 80-letiju prof. A. I. Ujomova. Pod red. A. Ju. Cofnasa Odessa: Astroprint, 2008. 248 p.

11. Belov A.A., Gvozdev A.V. Vestnik IGTU. 2007. №3. Pp. 94-98.