ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

УДК 004.942

СИСТЕМА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ДОКУМЕНТООБОРОТА НА ПРЕДПРИЯТИИ

Статья поступила в редакцию 06.03.2018, в окончательном варианте – 14.06.2018.

Шевцов Вадим Юрьевич, Волгоградский государственный университет, 400062, Российская Федерация, г. Волгоград, пр. Университетский, 100
студент, e-mail: vadim94.d@mail.ru
Бабенко Алексей Александрович, Волгоградский государственный университет, 400062, Российская Федерация, г. Волгоград, пр. Университетский, 100
кандидат педагогических наук, доцент, ORCID0000-0003-0466-0877, e-mail: ba_benko@mail.ru
Козунова Светлана Сергеевна, Волгоградский государственный технический университет, 400005, Российская Федерация, г. Волгоград, пр. им. Ленина, 28
аспирант, e-mail: one1100on@gmail.com
Кравец Алла Григорьевна, Волгоградский государственный технический университет, 400005, Российская Федерация, г. Волгоград, пр. им. Ленина, 28
доктор технических наук, профессор, ORCID 0000-0003-1675-8652, e-mail: agk@gde.ru

Целью исследования является разработка системы управления информационной безопасностью документооборота. В основу данной системы положены разработанные авторами формализованная модель и процедура анализа процессов систем электронного документооборота. Представлены результаты исследования проблемы управления информационной безопасностью электронного документооборота. Проанализированы процессы систем электронного документооборота. На основе них выделены информационные потоки и типовая архитектура систем. Задача управления информационной безопасностью систем электронного документооборота слабоформализуемая. По результатам проведённого исследования данной проблемы, авторами статьи предложена формальная модель системы управления информационной безопасностью документооборота. В разработанной модели используется матрица бинарных отношений, определяющая связь между множеством средств защиты информации, множеством актуальных угроз и требованиями, предъявляемыми к системам защиты информации в системах электронного документооборота. Предложенная модель позволяет решить задачу оптимизации средств защиты информации, введённых в эксплуатацию; обеспечить их минимальную стоимость. Разработана архитектура системы управления информационной безопасностью документооборота на предприятии. Представлен интерфейс, блок-схемы алгоритмов разработанной системы документооборота. Указанная система прошла тестовые испытания на предприятии ООО «ИТЦ СКОН». Результаты испытаний показали, что применение даннойсистемы позволило повысить эффективность управления информационной безопасностью систем электронного документооборота.

Ключевые слова: организация, документооборот, система управления, информационная безопасность, средства защиты, методы оптимизации, матрица бинарных отношений, система защиты информации, схема информационных потоков, информационные технологии

INFORMATION SECURITY MANAGEMENT SYSTEM OF WORKFLOW AT THE ENTERPRISE

The article was received by editorial board on 06.03.2018, in the final version – 14.06.2018.

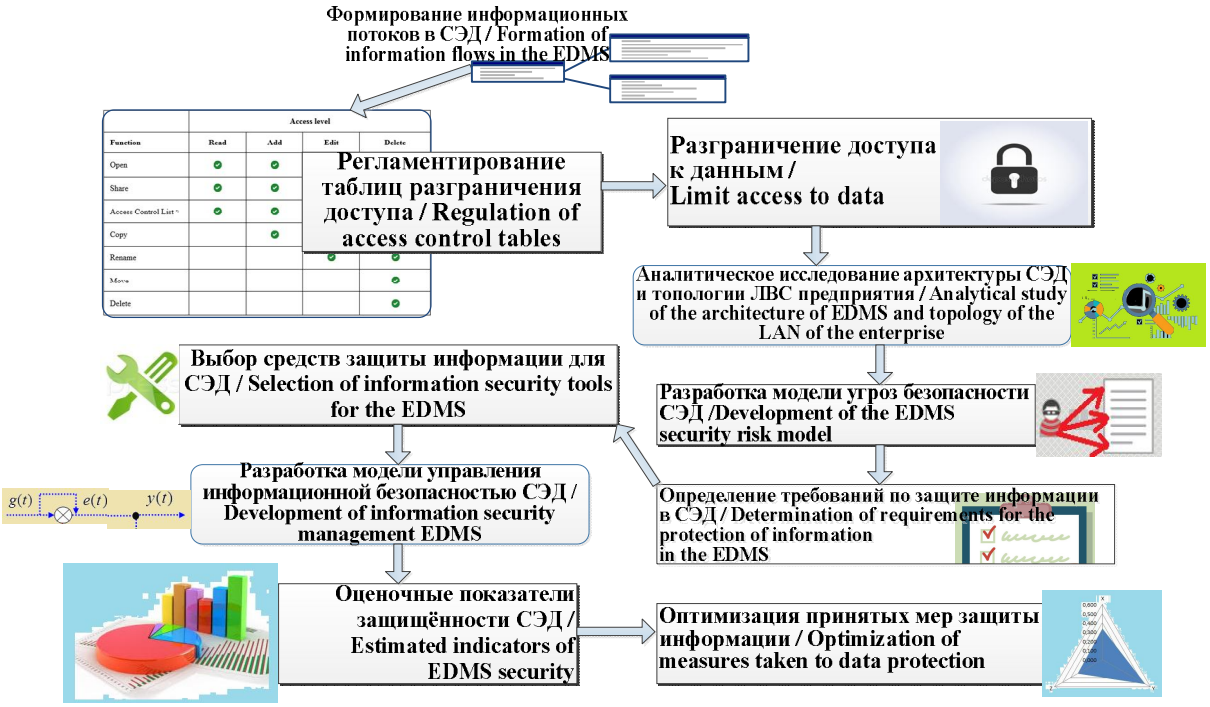
***Shevtsov Vadim Yu.*,** Volgograd State University, 100 Universitetskiy Ave., Volgograd, 400062, Russian Federation
Student, e-mail: vadim94.d@mail.ru
Babenko Aleksey A., Volgograd State University, 100 Universitetskiy Ave., Volgograd, 400062, Russian Federation
Cand. Sci. (Pedagogical), Associate Professor, ORCID 0000-0003-0466-0877, e-mail: ba_benko@mail.ru
***Kozunova Svetlana S.*,** Volgograd State Technical University, 28 Lenin Ave., Volgograd, 400005, Russian Federation
Post-graduate student, e-mail: one1100on@gmail.com
Kravets Alla G., Volgograd State Technical University, 28 Lenin Ave., Volgograd, 400005, Russian Federation
Doct. Sci. (Engineering), Professor, ORCID 0000-0003-1675-8652, e-mail: agk@gde.ru

The aim of the study is to develop of information security system of workflow. The information security system of workflow based on the formalized model developed by the authors and the procedure for analyzing the processes of workflow. The processes of workflow systems analyzed based on which information flows and a typical architecture are distinguished. The task of information security management of WS poorly formalized. Based on the results of the study of this problem, the authors of the article proposed a formal model of ISSW. In the developed model, a matrix of binary relations is used, which determines the relationship between the set of information protection tools, the set of actual threats and the re-

quirements for information security systems in the WS. The proposed model allows to solve the problem of optimization of information protection tools, put into operation, and to ensure their minimum cost. The architecture of ISSW in the enterprise is developed. The interface, block diagram of algorithms of the developed ISSW. ISSW passed the test tests at the enterprise LLC "ITC SKON". The obtained results showed, that the use of the ISSW made it possible to improve the efficiency management of information security of WS.

Keywords: organization, workflow, control system, information security, means of protection, optimization methods, matrix of binary relations, flow diagram, information technologies.

Graphical abstract (Графическая аннотация)



*СЭД – система электронного документооборота; EDMS – electronic document management system.

Введение. Управление информационной безопасностью (ИБ) документооборота является значимым для коммерческой организации, корпорации или промышленного предприятия. Это обуславливается обработкой в системе электронного документооборота (СЭД) информации, которая является критически важной для деятельности организаций. Такая информация является категорированной, может содержать государственную и коммерческую тайну, персональные данные. Информационные ресурсы, задействованные в специальном делопроизводстве предприятия, нуждаются в особом обеспечении их безопасности; поддержании высокого уровня защищённости и стабильности показателей эффективности защитных механизмов. Однако изменяющаяся информационно-пространственная среда, в которой функционируют такие ресурсы, порождает факторы, способные снизить эффективность защиты данных и непрерывного функционирования СЭД.

Большинство предприятий в настоящее время используют СЭД, которые позволяют автоматизировать обработку документов и управление информационными активами. Согласно распределению реализованных проектов внедрения СЭД в России (с 2005 г. по декабрь 2017 г.), представленному в [27], наибольшее количество «фактов использования» имеют Directum – 24 %, DocVision – 18 %, ELMA – 17 % и Дело – 15 %. Наименьшие количественные показатели у 1С: Документооборот, ТЕЗИС – 6 %, MicrosoftSharePoint, NauDoc – 4 %, Е1 Ефрат, Documentum – 3 %. Выручка участников российского рынка СЭД значительно выросла в 2015–2016 гг.[27]. В общем случае конкретное предприятие может вести работу в нескольких СЭД для удовлетворения совокупности имеющихся функциональных требований. Однако это осложняет обеспечение и управление ИБ, в т.ч. на этапах анализа угроз и уязвимостей СЭД, а также разработки частных моделей угроз.

Исследования по проблемам управления ИБ электронного документооборота начали проводиться сравнительно недавно. Поэтому для решения задачи эффективного управления ИБ СЭД необходимо разработать новые подходы к управлению; модели управления и алгоритмы, способные эффективно реализовать такие управленческие механизмы. Об этом свидетельствуют работы ряда авторов [2, 8–10, 16, 18]. Таким образом, управление ИБ СЭД является актуальной проблемой в настоящее время, которую необходимо решать комплексно. Поэтому целью данной статьи был комплексный анализ указанной проблематики и разработка адекватных программно-технических решений, направленных на обеспечение ИБ СЭД.

Общая характеристика проблемы управления информационной безопасностью документооборота на предприятии. Вопросы обеспечения безопасности СЭД изучаются достаточно давно, однако проблема управления ИБ СЭД стала исследоваться сравнительно недавно. Исследования [2, 3, 12–14] показывают, что в настоящее время существуют различные средства защиты информации (СЗИ) СЭД и корпоративной среды. Однако ухудшение условий функционирования таких СЗИ в результате дестабилизирующих факторов, роста банка (номенклатуры) угроз осложняет процедуру управления ИБ и оценки состояния защищённости СЭД [1, 12]. Особенно это касается частных корпоративных информационных систем, в которых функционируют СЭД [16].

В настоящее время не существует средств управления ИБ СЭД, которые можно интегрировать в СЭД с целью усиления встроенных в них механизмов защиты. По результатам научных исследований [10, 16, 18, 19, 31] можно сделать вывод, что проблема управления ИБ СЭД предприятия сейчас не решена. Сама система управления ИБ СЭД является частной, однако должна быть интегрирована в систему управления информационной безопасностью (СУИБ) предприятия.

Выделим аспекты, которые охватывают процесс управления ИБ СЭД: планирование затрат на обеспечение ИБ (инвестиционная политика) [13]; планирование процедур ИБ, включая обновление и усовершенствование СЗИ, поддержание стабильного уровня защищённости информации, соблюдение выполнения требований политики ИБ предприятия; проведение внутренних проверок (аудита) на соответствие требованиям ИБ (внешние проверки проводятся по необходимости); противодействие утечкам информации; управление рисками и инцидентами [2, 6, 13, 14, 16, 28]; гибкая система управления событиями в СЭД и СУИБ [10, 15, 20].

Таким образом, проблема управления ИБ СЭД заключается в отсутствии комплексной методики управления ИБ, ориентированной на СЭД и информационные потоки, которыми они оперируют.

Анализ процессов, присущих системам электронного документооборота. Современные СЭД являются многозадачными. Организация документооборота и обработка документов в них выполняются на разных уровнях. Таким образом, необходимо выделить информационные процессы, присущие СЭД.

1. Бизнес-процессы – постановка целей, выделение тенденций развития, прогнозирование реструктуризации документооборота [7, 32].

2. Процессы обработки информации – сбор информации, обработка информации, формирование пакетов документов, анализ источников информации, модификация информационных активов [30].

3. Управленческие процессы – обновление баз данных и баз знаний в системе, формирование информационных активов предприятия, классификация информации, расстановка приоритетов значимости информации, принятие управленческих решений, стратегия обработки информации, политика управления документами [13].

Количество процессов в СЭД обычно большое, что порождает различные информационные потоки (ИП) – рисунок 1.

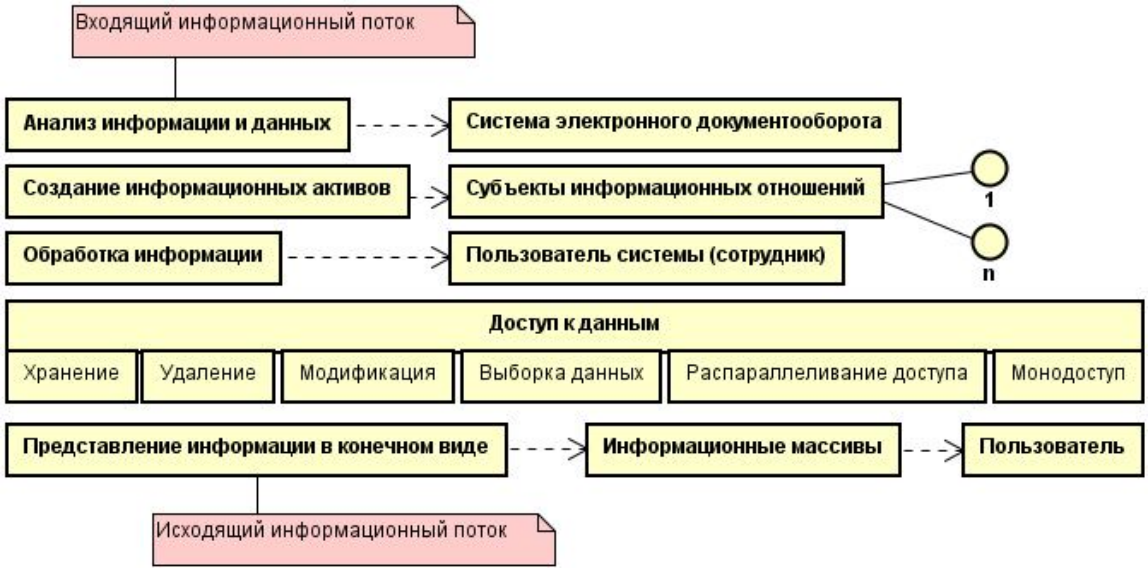


Рисунок 1 – Схема информационных потоков системы электронного документооборота

Входящим ИП является «анализ информации и данных», исходящим – «представление информации в конечном виде». Разработанная схема ИП позволяет определить отношение процесса к объекту или субъекту СЭД.

Внедрение СЭД осуществляется на основе экспертизы делопроизводственных структур предприятия [17, 26]. В результате экспертизы определяется объем годового документооборота, виды используемых документов, маршруты их движения и организация их хранения. Это позволяет выделить наиболее узкие места в системе документооборота предприятия, которые нуждаются в автоматизации. Типовая архитектура СЭД предприятия представлена на рисунке 2.

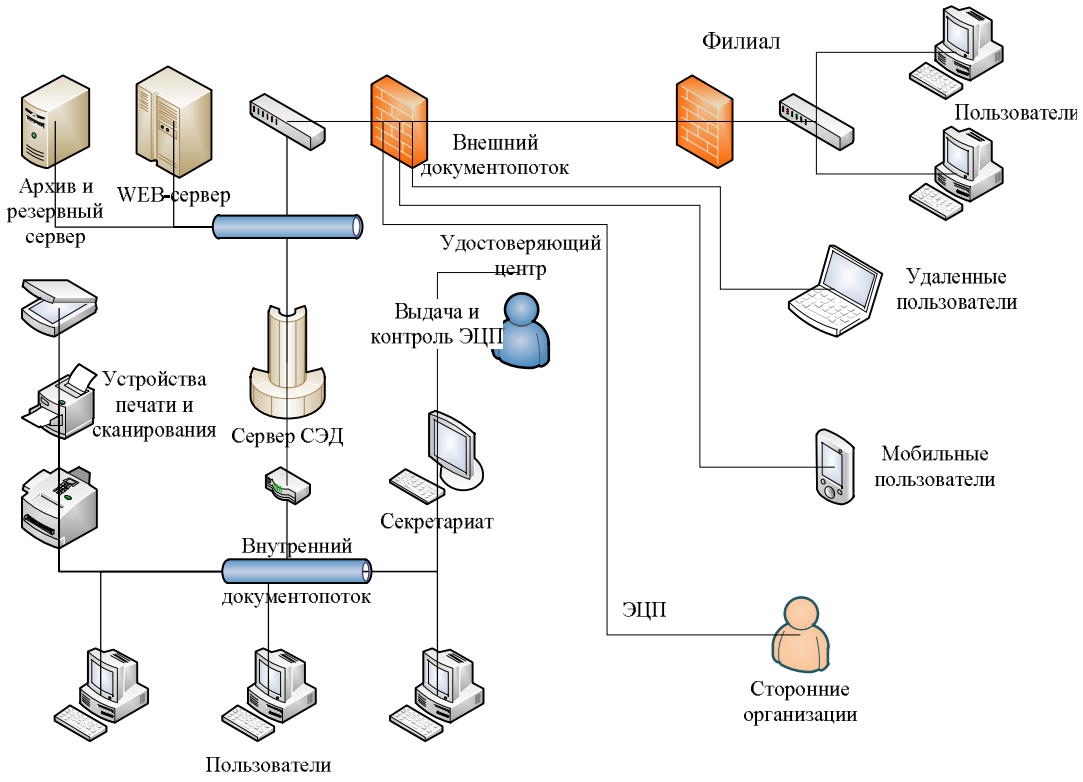


Рисунок 2 – Типовая архитектура СЭД предприятия

Принципами построения документооборота на предприятии являются разделение документопотока на внешний и внутренний, использование электронной цифровой подписи (ЭЦП) в юридически значимых электронных документах, согласование важных документов через секретариат, обязательное наличие архива в структуре документооборота, организация печати и сканирования документов в виде потока, централизованное управление документопотоком (рис. 2).

На основании схемы информационных потоков и типовой архитектуры СЭД (см. рис. 1, рис. 2), результатов исследований [4,15], с учетом требований методики [21], приказов [23-26], методического документа [22] авторами статьи разработана модель угроз безопасности СЭД (рис. 3). При разработке этой модели учитывались факторы, влияющие на архитектуру СЭД и локализацию угроз нарушения информационной безопасности. К таким факторам относятся наличие у предприятия филиалов, ЦОД, удалённых пользователей, сегментирование сети предприятия при помощи межсетевых экранов.

Модель угроз безопасности СЭД (рис. 3) включает в себя 10 типов угроз, распределённых по элементам СЭД предприятия, включая сетевую инфраструктуру. Так, наряду с угрозами нарушения конфиденциальности, целостности и доступности, для СЭД характерны угрозы получения несанкционированного доступа (НСД) к информации, угроза подмены ЭЦП, угроза отказа сетевого оборудования. По данным исследований [1, 7, 14, 28], наибольший ущерб для СЭД наносят угрозы нарушения целостности и угрозы, присущие центрам обработки данных (ЦОД), серверам СЭД и баз данных (БД). Среднему ущербу СЭД могут подвергнуть угрозы получения НСД к информации СЭД, к автоматизированным рабочим местам (АРМ) пользователей или файловому серверу [5, 11, 17, 29, 31].

Предложенная модель угроз позволяет проанализировать локализацию угроз – соотнести угрозы нарушения ИБ с определённым узлом СЭД.

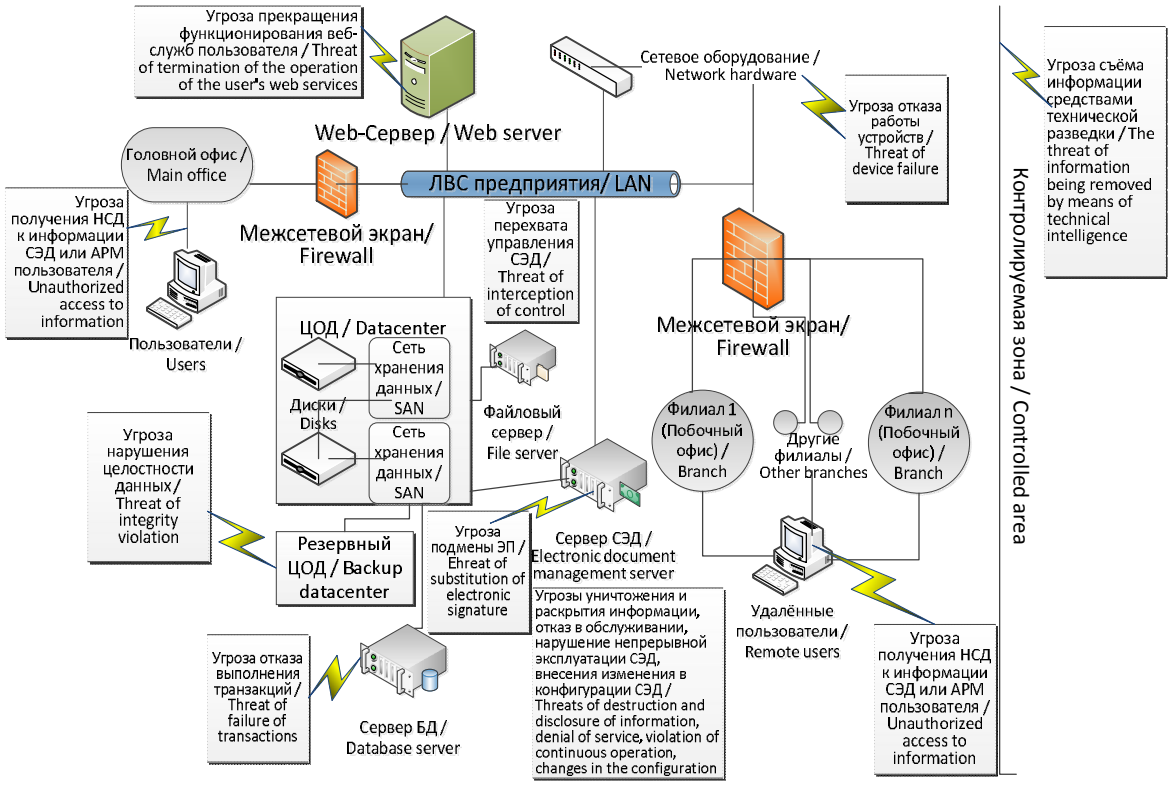


Рисунок 3 – Модель угроз безопасности СЭД предприятия (организации)

Формальная модель системы управления информационной безопасностью документооборота на предприятии. Модель управления безопасностью документооборота на предприятии можно представить в виде кортежа

$$X = (I,\ T,\ ECM,\ PC,\ ST,\ TH, SE,\ KO,\ LA),$$

где I – виды автоматизировано обрабатываемой информации, представленных вектором $I = (I_1, I_2, I_3, I_4, I_5)$, каждое из которых описывается базовыми значениями {*yes, no*} для I_1, I_2, I_3 и {1, 2, 3, 4} для I_4,I_5 (1– персональные данные, 2 – уровень ПДн, 3 – служебная тайна, 4 – класс ИС, 5 – коммерческая тайна);

T – тип предприятия, T = {*государственное*, *коммерческое*}; ECM – используемая СЭД, ECM = {“ДЕЛО”, “1С Документооборот”, “CompanyMedia”, “DocsVision”, “ТЕЗИС”, “Directrum”, “ELMA”};

PC – параметры сети предприятия $PC = (PC_1, PC_2, PC_3, PC_4)$, в котором PC_1 – число АРМ в сети предприятия, обрабатывающих конфиденциальную информацию, PC_2 – число филиалов, PC_3 – число удаленных пользователей; PC_4 – наличие взаимодействия со сторонними организациями, принимающее значения {*yes, no*} соответственно;

ST – этапы документооборота предприятия, на которых есть актуальные угрозы;

TH –угрозы безопасности документооборота;

SE – множество средств защиты $SE_i = (C_i, CE_i)$, где C_i – стоимость средства защиты для заданного количества параметров сети предприятия PC_i в зависимости от того, где применяется данное средство защиты, CE_i – стоимость технической поддержки в год;

KO – множество критериев оценки модели защищенного документооборота;

LA – требования к системе защиты, установленные нормативно-правовыми актами, а также отражающиеся в техническом задании заказчика.

Отношение между средствами защиты SE и множеством актуальных угроз TH, а также выполняемыми требованиями LA к защите описывается матрицей бинарных отношений M_n^t и L_k^t, где каждый элемент $m_j^i \in M_n^t$ и $l_c^i \in L_k^t$ отражает возможность перекрытия TH_j угрозы и выполнения LA_c требования SE_i средством защиты. При этом

$$m_j^i \begin{cases} 1, \text{если } TH_j \text{ перекрывается } SE_i \text{ средством защиты} \\ 0, \text{если } TH_j \text{ не перекрывается } SE_i \text{ средством защиты} \end{cases} \quad (1)$$

$$m_j^i \begin{cases} 1, \text{если } LA_c \text{ перекрывается } SE_i \text{ средством защиты} \\ 0, \text{если } LA_c \text{ не перекрывается } SE_i \text{ средством защиты} \end{cases} \quad (2)$$

Эффективность перекрытия n^* угроз и выполнения z^* требований системой защиты информации вычисляется как

$$ET = \frac{1}{n_*} \sum_{j=1}^{n^*} \sum_{i=1}^{SE} m_j^i \,, \tag{3}$$

$$EL = \frac{1}{z_*} \sum_{c=1}^{z^*} \sum_{i=1}^{SE} l_c^i \tag{4}$$

Эффективность защиты через частные критерии каждого средства защиты $\forall SE_i \in SE$ формализовано опишем вектором $EM = (KO_1, \ldots, KO_n)$, где KO_i – соответствующий критерий. Вектор EM будет считаться эталоном, если для любого $KO_i = 1$. Для сравнения вектора эффективности каждого из исследуемых средств защиты EF_{SEi} с эталоном будет использоваться метрика, на основе Евклидова расстояния E. Эффективность средства защиты вычисляется по формуле:

$$E(EM, EF_{SEi}) = \sqrt{\sum_{i=1}^{n} (EM_i - EF_{SEi})^2} \,. \tag{5}$$

Эффективными признаются те средства защиты, которые имеют минимальное значение E (EM, EF_{SEi}). Обязательным критерием является выполнение требований к защите и перекрытию угроз. При выборе хотя бы одного из критериев, сначала определяются те средства защиты информации, которые имеют максимальные значения соответствующих критериев. Если остались невыполненные требования, неперекрытые угрозы, то отсутствуют необходимые функции соответственно. Поэтому дальнейший выбор происходит только с учетом упущенных моментов и в последующих выборах. При этом в данной оценке не учитываются экономические показатели.

Затем необходимо решить следующую задачу оптимизации для t^* выбранных средств защиты: средства защиты информации должны перекрывать все актуальные угрозы, удовлетворять максимальному количеству требований по защите информации и при этом обеспечивать минимальную стоимость СЗИ:

$$\begin{cases} \sum_{i=1}^{t^*} (SE_i C_i + 5 SE_i CE_i) \to \min \\ \sum_{i=1}^{t^*} SE_i m_j^i = 1 \\ \sum_{i=1}^{t^*} SE_i l_j^i = 1 \end{cases} \tag{6}$$

Предложенное решение и результаты его тестовых испытаний. Описанная выше формализованная модель позволила определить архитектуру системы управления безопасностью документооборота на предприятии (рис.4). Эта система реализована на языке C# в виде программного комплекса.

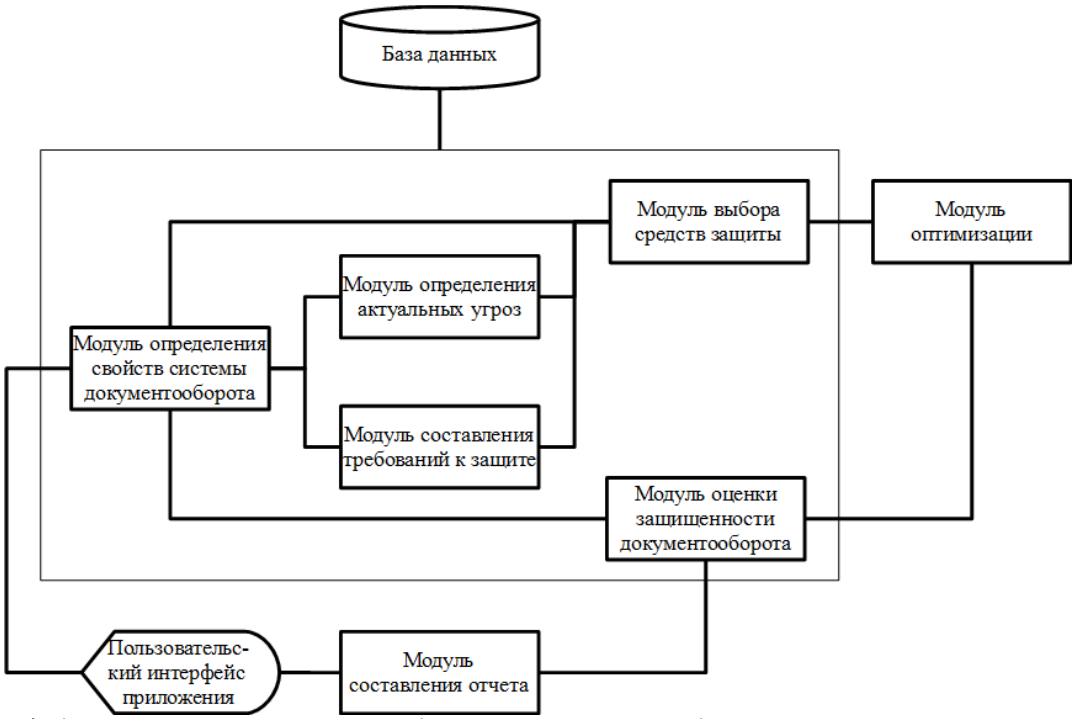


Рисунок 4 –Архитектура системы управления безопасностью документооборота на предприятии

Модуль составления требований к защите определяет набор требований, предъявляемых к обеспечению безопасности, на основе заданных свойств системы документооборота, а также дополнительных требований. Модуль определения актуальных угроз позволяет получить актуальные угрозы на основе свойств системы документооборота. Модуль выбора эффективных средств защиты формирует список средств защиты на основе критериев оценки. Конечный список средств защиты информации формируется на основе результатов оптимизации, проводимой модулем оптимизации.

Оценку защищённости документооборота на основе перекрытых угроз и выполненных требований производит модуль оценки защищённости. Модуль составления отчета формирует окончательные данные по выбранным средствам защиты и результаты оценки защищенности модели документооборота. Итоговые сведения о средствах защиты информации, а также результаты работы программных модулей приложения хранятся в базе данных.

Алгоритм функционирования предложенной системы представлен на рисунке 5.

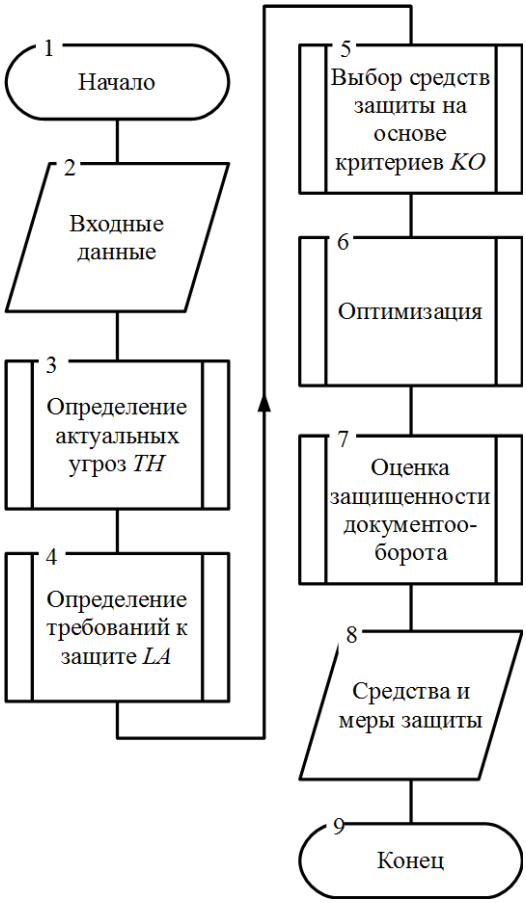


Рисунок 5 – Блок-схема алгоритма системы управления безопасностью документооборота на предприятии

Пользовательский интерфейс (рис. 6 и 7) осуществляет взаимодействие системы с пользователем: принимает данные, необходимые для определения свойств системы документооборота, а также выводит результаты работы в виде сформированного отчета, выдает справку о программе. Модуль определения свойств системы документооборота, на основе введенных данных пользователем, формирует список свойств системы документооборота: виды автоматизированно обрабатываемой информации, тип предприятия, используемая СЭД, параметры сети предприятия, необходимые критерии оценки.

С помощью разработанной системы управления безопасностью документооборота на 30-ти предприятиях были проведены экспериментальные исследования, направленные на повышение эффективности управления ИБ документооборота. Результаты исследований представлены на рисунках 8 и 9.

Результаты тестовых испытаний разработанной СУИБД показали возможность ее применения для управления ИБ СЭД. Использование СУИБД позволило повысить эффективность управления ИБ СЭД на предприятии до необходимого уровня – в среднем на 33 % «по угрозам» и на 30 % «по требованиям».

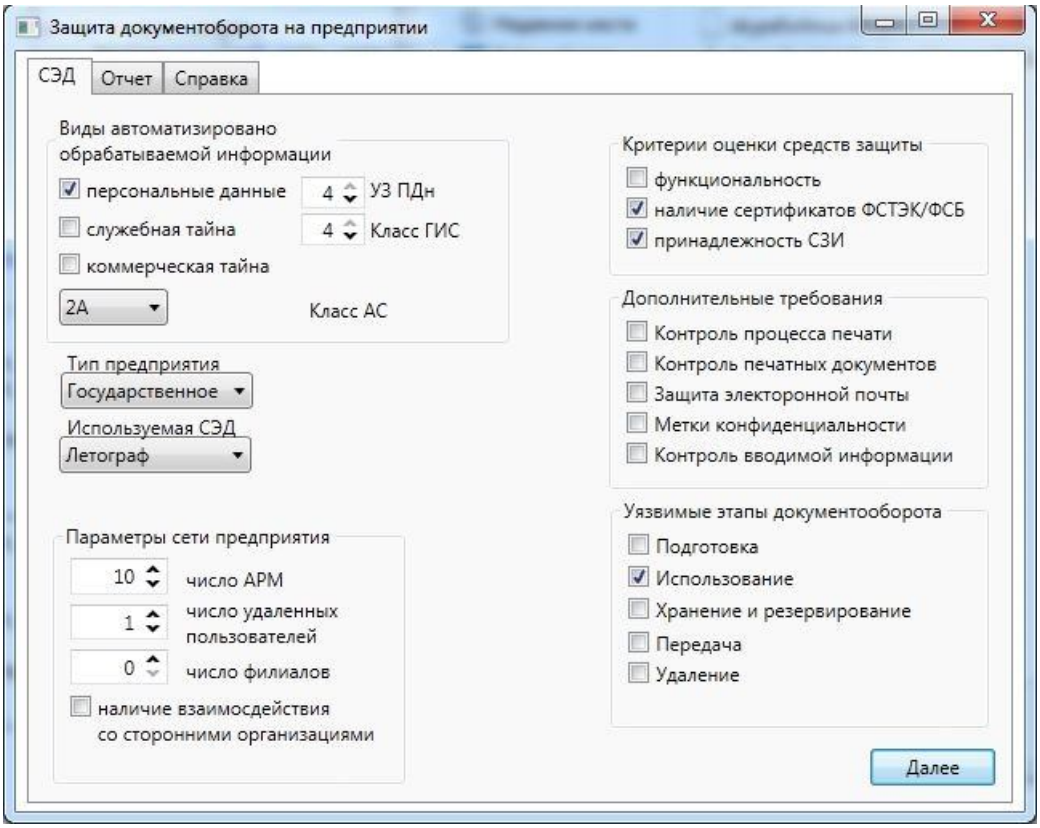


Рисунок 6 – Определение требований к системе документооборота на предприятии (копия «экранной формы» разработанного программного обеспечения)

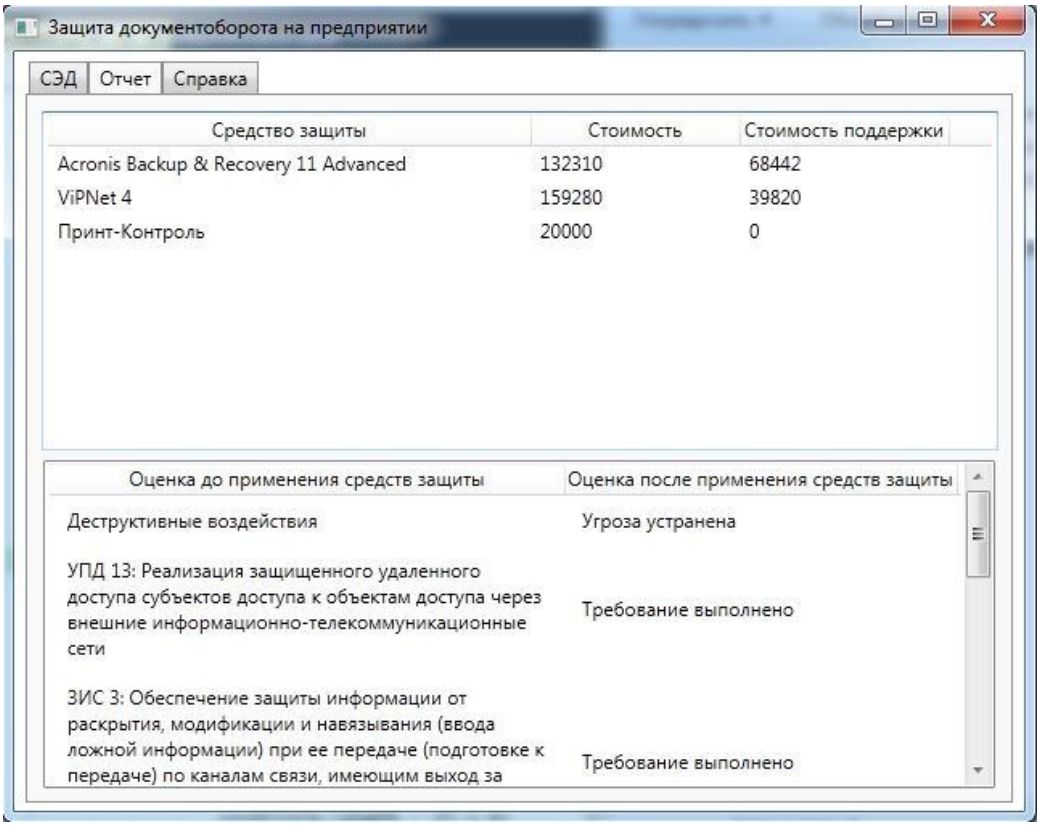


Рисунок 7 – Отчет о результатах работы программы (копия «экранной формы» разработанного программного обеспечения)

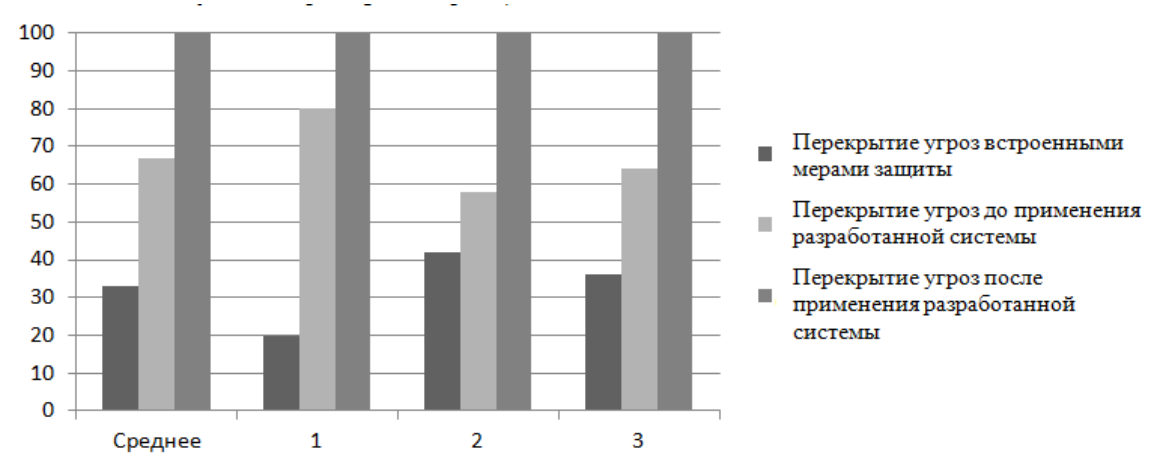


Рисунок 8 – Статистика перекрытия угроз: 1 – государственные предприятия, обрабатывающие персональные данные; 2 –государственные предприятия, обрабатывающие информацию, содержащую служебную тайну; 3 – коммерческие предприятия, обрабатывающие персональные данные и/или информацию, содержащую коммерческую тайну

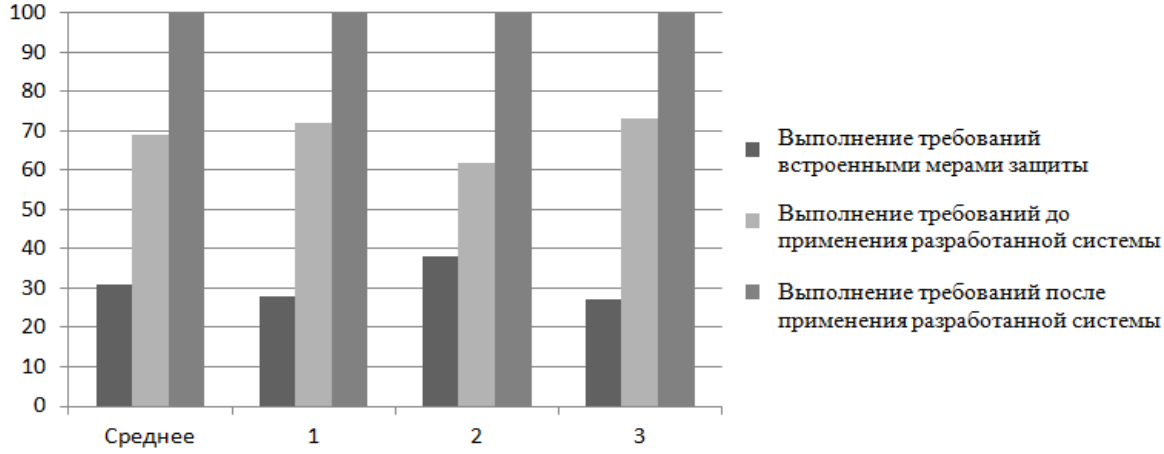


Рисунок 9 – Статистика выполнения требований: 1 – государственные предприятия, обрабатывающие персональные данные; 2 – государственные предприятия, обрабатывающие информацию, содержащую служебную тайну; 3 – коммерческие предприятия, обрабатывающие персональные данные и/или информацию, содержащую коммерческую тайну

Заключение. Разработана система управления безопасностью документооборота на предприятии, учитывающая тип, структуру, используемую СЭД, актуальные угрозы, требования к системе защиты. Компьютеризованная система, реализующая предложенную модель, позволяет подобрать средства защиты информации, перекрывающие все актуальные угрозы. При этом удовлетворяется максимальное количество требований по защите информации и обеспечивается минимальная стоимость СЗИ. Разработанная компьютеризованная система может применяться как компонент системы управления информационной безопасностью предприятия (организации).

Список литературы

1. Ажмухамедов И. М. Оценка состояния защищённости данных организации в условиях возможности реализации угроз информационной безопасности / И. М. Ажмухамедов, О. М. Князева // Прикаспийский журнал: управление и высокие технологии. – 2015. – № 3 (31). – С. 24–39 (http://hi-tech.asu.edu.ru/files/3(31)/24-39.pdf).

2. Аникин И. В. Методы оценки и управления рисками информационной безопасности в корпоративных информационных сетях / И. В. Аникин, Л. Ю. Емалетдинова, А. П. Кирпичников // Вестник Казанского технологического университета. – 2015. – Т. 18, № 6. – С. 195–197.

3. Бабенко А. А. Разработка системы управления аномальными событиями информационной безопасности / А. А. Бабенко, С. Ю. Микова, В. С. Оладько // Информационные системы и технологии. – 2017. – № 5 (103). – С. 108–116.

4. Богданов Н. Г. Администрирование безопасности корпоративных информационных систем на основе ролевого управления доступом / Н. Г. Богданов, П. В. Бочков, Н. Д. Нечаенко // Информационные системы и технологии. – 2015. – № 2 (88). – С. 124–130.

5. Брумштейн Ю. М. Медицинские данные организаций и пациентов: системный анализ категорий информации, угроз информационной безопасности, подходов к защите / Ю. М. Брумштейн, Е. О. Кузнецова, А. Д. Захаров // Методы компьютерной диагностики в биологии и медицине – 2017: мат-лы Всерос. школы-семинара. – Саратов : Саратовский источник, 2017. – С. 65–69.

6. Брумштейн Ю. М. Сравнительный анализ функциональности программных средств управления проектами, распространяемых по модели SaaS / Ю. М. Брумштейн, И. А. Дюдиков // Прикаспийский журнал: управление и высокие технологии. – 2014. – № 4. – С. 34–51 (http://hi-tech.asu.edu.ru/files/4(28)/34-51.pdf).

7. Брумштейн Ю. М. Анализ факторов, методов и модели управления рисками в процессе жизненного цикла медицинских информационных систем / Ю. М. Брумштейн // Известия ЮФУ. Технические науки. – 2014. – № 10 (159). – С. 186–194.

8. Буй Н. З. Информационная безопасность процесса регистрации android-устройства в системе управления корпоративной мобильностью / Н. З. Буй, А. Г. Кравец, Л. Т. Т. Нгуен // Вестник компьютерных и информационных технологий. – 2016. – № 8. – С. 34–43.

9. Гнеушев В. А. Моделирование сетевых атак злоумышленников в корпоративной информационной системе / В. А. Гнеушев, А. Г. Кравец, С. С. Козунова, А. А. Бабенко // Промышленные АСУ и контроллеры. – 2017. – № 6. – С. 51–60.

10. Досмухамедов Б. Р. Анализ угроз информации систем электронного документооборота / Б. Р. Досмухамедов // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. – 2009. – № 2. – С. 140–143.

11. Князева О. М. Управление качеством информационных систем на основе процессного подхода / О. М. Князева // Прикаспийский журнал: управление и высокие технологии. – 2016. – № 2. – С. 36–47 (http://hi-tech.asu.edu.ru/files/2(34)/36-47.pdf).

12. Козунова С. С. Information security model in the segment of corporate information system / С. С. Козунова, А. А. Бабенко // Информационные системы и технологии. – 2017. – № 1 (99). – С. 87–91.

13. Козунова С. С. Автоматизация управления инвестициями в информационную безопасность предприятия / С. С. Козунова, А. А. Бабенко // Вестник компьютерных и информационных технологий. – 2015. – № 3 (127). – С. 38–44.

14. Козунова С. С. Система оптимизации рисков инвестирования информационной безопасности промышленных предприятий / С. С. Козунова, А. А. Бабенко // Вестник компьютерных и информационных технологий. – 2016. – № 7 (145). – С. 22–29.

15. Козунова С. С. Менеджмент угроз информационной безопасности информационных систем / С. С. Козунова // Концепции фундаментальных и прикладных научных исследований : сб. ст. по мат-лам Междунар. науч.-практ. конф. (г. Уфа, 9 дек. 2017 г.) : в 6 ч. / отв. ред.: А. А. Сукиасян. – Стерлитамак, 2017. – Ч. 3. – С. 69–71.

16. Кравец А. Г. The Risk Management Model of Design Department's PDM Information System / А. Г. Кравец, С. С. Козунова // Creativity in Intelligent Technologies and Data Science. Second Conference, CIT&DS 2017 (Volgograd, Russia, September 12–14, 2017) : proceedings / ed. by A. Kravets, M. Shcherbakov, M. Kultsova, Peter Groumpos. – [Germany] : Springer International Publishing AG, 2017. – Pp. 490–500. – (Ser. Communications in Computer and Information Science; Vol. 754).

17. Кравец А. Д. Агрегация информации о перспективных технологиях на основе автоматической генерации интеллектуальных агентов мультиагентных систем / А. Д. Кравец, И. Ю. Петрова, А. Г. Кравец // Прикаспийский журнал: управление и высокие технологии. – 2015. – № 4. – С. 141–147 (http://hi-tech.asu.edu.ru/files/4(32)/141-148.pdf).

18. Кухарский А. Н. Информационная безопасность в аспекте защищенного электронного документооборота в информационных системах муниципальных образований / А. Н. Кухарский // Вестник ЗабГУ. – 2017. – Т. 23, № 7. – С. 86–90.

19. Лапина Е. В. О задаче моделирования информационного риска систем электронного документооборота / Е. В. Лапина // Решетневские чтения. – 2014. – Т. 2, № 18. – С. 318–320.

20. Ледовский М. В. Исследование различных способов построения алгоритмов метапланирования ресурсов центра обработки данных / М. В. Ледовский // International Journal of Open Information Technologies. – 2014. – Vol. 2, no. 8. – P. 6–9.

21. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. – Утв. зам. директора ФСТЭК России 14 февраля 2008 г. – Режим доступа: https://fstec.ru/component/attachments/download/290, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 06.04.2018).

22. Меры защиты информации в государственных информационных системах : методический документ. – Утв. ФСТЭК России от 11 февраля 2014 г. – Режим доступа: https://fstec.ru/component/attachments/download/675, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 06.04.2018).

23. Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах : приказ ФСТЭК России от 11 февраля 2013 г. № 17 (ред. от 15.02.2017). URL: http://fstec.ru/component/attachments/download/567, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 03.04.2018).

24. Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды : приказ ФСТЭК РФ №31 от 14 марта 2014 г. – Режим доступа: https://fstec.ru/component/ attachments/download/714, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения 02.04.2018).

25. Об утверждении Требований о защите информации, содержащейся в информационных системах общего пользования : приказ ФСБ РФ № 416, ФСТЭК РФ № 489 от 31 августа 2010 г. – Режим доступа: http://fstec.ru/component/attachments/download/283, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 03.04.2018).

26. Парамонов П. П. Методы и модели оценки инфраструктуры системы защиты информации в корпоративных сетях промышленных предприятий: монография / П. П. Парамонов, А. Г. Коробейников, И. Б. Троников, И. О. Жаринов ; под ред. П. П. Парамонова. – СПб : Студия «НП-Принт», 2012. – 115 с.

27. Система электронного документооборота EnterpriseContentManagement. Управление корпоративной информацией. Обзор TAdviser. Российский рынок СЭД/ECM. – Режим доступа: http://www.tadviser.ru/index.php/ %D1%DD%C4, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 16.02.2018).

28. Соколов С. С. Методы и модели построения защищённой системы электронного документооборота в транспортно-логическом кластере / С. С. Соколов, А. С. Карпина, В. Д. Гаскаров // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. – 2016. – № 3. – С. 40–52.

29. Финогеев А. А. Анализ информационных рисков в системах обработки данных на основе «туманных» вычислений / А. А. Финогеев, А. Г. Финогеев, И. С. Нефедова, Е. А. Финогеев, В. А. Камаев // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. – 2015. – № 4. – С. 38–46.

30. Finogeev A. Methods and tools for secure sensor data transmission and data mining in energy SCADA system / A. Finogeev, L. Fionova, A. Finogeev, I. Nefedova, E. Finogeev, T. Q. Vinh, V. Kamaev // Communications in Computer and Information Science. – 2015. – Vol. 535. – P. 474–484.

31. Шевцов В. Ю. Особенности защищённого документооборота на предприятии / В. Ю. Шевцов, А. А. Бабенко, С. С. Козунова // Актуальные вопросы информационной безопасности регионов в условиях глобализации информационного пространтсва : матер. V Всерос. науч.-практ. конф. (г. Волгоград, 22–23 апр. 2016 г.). – Волгоград : Волгоградский гос. ун-т, 2016. – С. 237–341.

32. Щербаков М. В. A Method and IR4I Index Indicating the Readiness of Business Processes for Data Science Solutions / М. В. Щербаков, P. P. Groumpos, А. Г. Кравец // Creativity in Intelligent Technologies and Data Science. Second Conference, CIT&DS 2017 (Volgograd, Russia, September 12–14, 2017) : proceedings / ed. by A. Kravets, M. Shcherbakov, M. Kultsova, Peter Groumpo. – [Germany] : Springer International Publishing AG, 2017. – P. 21–34. – (Ser. Communications in Computer and Information Science ; vol. 754).

References

1. Azhmukhamedov I. M., Knyazeva O. M. Otsenka sostoyaniya zashchishchennosti dannykh organizatsii v usloviyakh vozmozhnosti realizatsii ugroz informatsionnoy bezopasnosti [Assessment of status for data security of organization in conditions of realization possibility for information security threats]. *Prikaspiyskiy zhurnal: uptavlenie I vysokie teknologii* [Caspian Journal: Control and High Technologies], 2015, no. 3 (31), pp. 24–39 (http://hi-tech.asu.edu.ru/files/ 3(31)/24-39.pdf).

2. Anikin I. V., Emaletdinova l. Yu., Kirpichnikov A. P. Metody otsenki i upravleniya riskami informatsionnoy bezopasnosti v korporativnykh setyakh [Methods for assessing and managing information security risks in corporate information networks]. *Vestnik Kazanskogo tekhnologicheskogo universiteta* [Bulletin of Kazan Technological University], 2015, vol. 18, no. 6, pp. 195–197.

3. Babenko A. A., Mikova S. Yu., Oladko V. S. Razrabotka sistemy upravleniya anomalnymi sobytiyami informatsionnoy bezopasnosti [Development of information security's abnormal events control system. Information Systems and Technologies]. *Informatsionnye sistemy i tekhnologii* [Scientific and Technical Journal], 2017, no. 5, pp. 108–116.

4. Bogdanov N. G., Bochkov P. V., Nechaenko N. D. Administrirovanye bezopasnosti korporativnykh informatsionnykh system na osnove rolevogo upravleniya dostupom [Security administration corporate information systems based on role of access]. *Informatsionnye sistemy i tekhnologii* [Information Systems and Technologies], 2015, no. 2 (88), pp. 124–130.

5. Brumshteyn Yu. M., Kuznetsova E. O., Zakharov A. D. Meditsinskie dannye organizatsiy i patsientov: sistemnyy analiz kategoriy informatsii, ugroz informatsionnoy bezopasnosti, podkhodov k zashchite [Medical data of organizations and patients: a system analysis of information categories, threats to information security, approaches to protection]. *Metody kompyuternoy diagnostiki v biologii i meditsine – 2017: mat-ly Vseros. shkoly-seminara* [Methods of Computer Diagnostics in Biology and Medicine – 2017. Proceedings of the All-Russian School-Seminar], Saratov, Saratovskiy istochnik Publ., 2017, pp. 65–69.

6. Brumshteyn Yu. M., Dyudikov I. A. Sravnitelnyy analiz funktsionalnosti programmnykh sredstv upravleniya proektami, rasprostranyaemykh po modeli SAAS [Comparative analysis of the functionality of software project management tools distributed by the SaaS model]. *Prikaspiyskiy zhurnal: uptavlenie I vysokie teknologii* [Caspian Journal: Control and High Technologies], 2014, no. 4. pp. 34–51 (http://hi-tech.asu.edu.ru/files/4(28)/34-51.pdf).

7. Brumsteyn Yu. M., Siver O. V. Analiz faktorov, metodov i modeley upravleniya riskami v protsesse zhiznennogo tsikla meditsinskikh informatsionnykh sistem [System analysis of risks in process of medical information systems life cycle]. *Izvestiya UFU. Tekhnicheskie nauki* [Proceedings of the SFedU. Engineering Sciences], 2014, no. 10 (159), pp. 186–194.

8. Bui N. D., Kravets A. G., Nguyen L. T. T. Informatsionnaya bezopasnost protsessa registratsii android-ustroystv v sisteme upravleniya korporativnoy mobilnosti [Information security of the android-device enrollment process in enterprise mobility management system]. Vestnik kompyuternykh i infornatsionnykh tekhnologii [Bulletin of the Computer and Information Technologies], 2016, no. 8, pp. 34–43.

9. Gneushev V. A., Kravets A. G., Kozunova S. S., Babenko A. A. Modelirovanie setevykh atak zloumyshlennikov v korporativnoy informatsionnoy sisteme [Modeling network attack of attacker in the corporate information system]. *Promyshlennye ASU i kontrollery* [Industrial Control Systems and Controllers], 2017, no. 6, pp. 51–60.

10. Dosmukhamedov B. R. Analiz ugroz informatsii system elektronnogo dokumentooborota [The analysis of threats of the information of systems of the electronic document circulation]. *Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Seriya: Upravlenie, vychislitelnaya tekhnika i informatika* [Bulletin of the Astrakhan State Technical University. Series: Management, Computer Facilities and Informatics], 2009, no. 2, pp. 140–143.

11. Knyazeva O. M. Управление качеством информационных систем на основе процессного подхода [Quality management of information systems based on the process approach]. *Prikaspiyskiy zhurnal: uptavlenie I vysokie teknologii* [Caspian Journal: Control and High Technologies], 2016, no. 2 (34), pp. 36–47 (http://hi-tech.asu.edu.ru/files/2(34)/36-47.pdf).

12. Kozunova S. S., Babenko A. A. Information security model in the segment of corporate information system [Information security model in the segment of corporate information system]. *Informatsionnye sistemy i tekhnologii* [Information Systems and Technologies], 2017, no. 1, pp. 87–91.

13. Kozunova S. S., Babenko A. A. Avtomatizatsiya upravleniya investitsiyami v informatsionnuyu bezopasnost predpriyatiya [Automating management of investment in information security for business]. *Vestnik kompyuternykh i infornatsionnykh tekhnologiy* [Bulletin of the Computer and Information Technologies], 2015, no. 3, pp. 38–44.

14. Kozunova S. S., Babenko A. A. Sistema optimizatsii riskov investirovaniya informatsionnoy bezopasnosti promyshlennykh predpriyatiy [Optimize risks system of information security of industrial enterprises]. *Vestnik kompyuternykh i infornatsionnykh tekhnologiy* [Bulletin of the Computer and Information Technologies], 2016, no. 7, pp. 22–29.

15. Kozunova S. S. Menedzhment ugroz informatsionnoy bezopasnosti informatsionnykh system [Information Security Threat Management for Information Systems]. *Kontseptsii fundamentalnykh i prikladnykh nauchnykh issledovaniy : sb. st. po matlam Mezhdunar. nauch.-prakt. konf. (g. Ufa, 9 dek. 2017 g.)* [Concepts of Fundamental and Applied Scientific Research. Proceedings by Mateials International Scientific and Practical Conference (Ufa, 9 December, 2017)], Sterlitamak, 2017, part 3, pp. 69–71.

16. Kravets A. G., Kozunova S. S. *The Risk Management Model of Design Department's PDM Information System. Creativity in Intelligent Technologies and Data Science. Second Conference, CIT&DS 2017 (Volgograd, Russia, September 12–14, 2017).* Proceedings, [Germany], Springer International Publishing AG, 2017, pp. 490–500. (Ser. Communications in Computer and Information Science ; Vol. 754).

17. Kravets A. D., Petrova I. Yu., Kravets A. G. Agregatsiya informatsii o perspektivnykh tekhnologiyakh na osnove avtomaticheskikh generatsiy intellektualnykh agentov multiagentnykh sistem [Aggregation of information on advanced technologies on the basis of automatic generation of intelligent agents of multi-agent systems]. *Prikaspiyskiy zhurnal: uptavlenie i vysokie teknologii* [Caspian Journal: Control and High Technologies], 2015, no. 4 pp. 141–147.

18. Kukharskiy A. N. Informatsionnaya bezopasnost v aspekt zashchishchennogo elektronnogo dokumentooborota v informatsionnykh sistemakh munitsipalnykh obrazovaniy [Information security in the aspect of secure electronic document management in information systems of municipalities]. *Vestnik ZabGU* [Bulletin of the Transbaikal State University], 2017, vol. 23, no. 7, pp. 86–90. DOI: 10.21209/2227924520172378690.

19. Lapina Ye. V. O zadache modelirovaniya informatsionnogo riska system elektronnogo dokumentooborota [On the problem of modeling information risks workflow systems]. *Reshetnevskie chteniya* [Reshetnev's readings], 2014, vol. 2, no. 18, pp. 318–320.

20. Ledovskiy M. V. Issledovanie razlichnykh sposobov postroeniya algoritmov metaplanirovaniya resursov tsentra obrabotki dannykh [On research of various techniques of data center resource meta-scheduler algorithms]. *International Journal of Open Information Technologies*, 2014, vol. 2, no. 8, pp. 6–9.

21. *Metodika opredeleniya aktualnykh ugroz bezopasnosti personalnykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personalnykh dannykh* [Methods of Detecting Pressing Threats to Personal Data Security during Their Processing in the Information Systems of Personal Data]. Appointed on February 14, 2008. Available at: https://fstec.ru/component/attachments/download/290 (accessed: 06.04.2018).

22. *Mery zashchiy informatsii v gosudarstvennykh informatsionnykh sistemakh* : metodicheskiy dokument [Measures to protect information in public information systems: a policy document]. Approved by FSTEK Rossii on February 11 2014. Available at: https://fstec.ru/component/attachments/download/675 (accessed: 17.04.2018).

23. On approval of Requirements to defense of information not classified as state secret and contained in state information systems. Order of Federal Service of Technical and Export Control of Russia of February 11, 2013. Available at: http://fstec.ru/component/attachments/download/567 (accessed: 03.04.2018).

24. On the approval of the requirements to ensure the protection of information in automated control systems for production and technological processes in critical facilities, potentially hazardous facilities, as well as objects that present a heightened danger to human life and health and the environment. Order of FSTEC RF no. 31 of March 14, 2014. Available at: https://fstec.ru/component/attachments/download/714 (accessed: 02.04.2018).

25. On the approval of Requirements to defense of information contained in public information systems. Order of the Federal Security Service of the Russian Federation no. 416, the Federal Service for Technical and Export Control no. 489 dated August 31, 2010. Available at: http://fstec.ru/component/attachments/download/283 (accessed: 03.04.2018).

26. Paramonov P. P., Korobeynikov A. G., Tronikov I. B., Zharinov I. O. *Metody i modeli otsenki infrastruktury sistemy zachity informatыii v korporativnykh setyakh promyshlennykh predpriyatiy* [Methods and models for assessing the infrastructure of information security systems in corporate networks of industrial enterprises: monograph], Saint Petersburg, Studio "NP-Print" Publ., 2012. 115 p.

27. Sistema elektronnogo dokumentooborota EnterpriseContentManagement. Upravlenie korporativnoy in-formatsiey. Obzor TAdviser. Rossiyskiy rynok SED/ECM [System of workflow Enterprise Content Management. Management of corporate information. TAdviser Overview. The Russian market of SED/ECM]. Avaliable at: http://www.tadviser.ru/index.php/%D1%DD%C4 (accessed: 16.02.2018).

28. Sokolov S. S., Karpina A. S., Gaskarov V. D. Metody i modely postroeniya zachichennoy sistemy elektronnogo dokumentooborota v transportno-logicheskom klastere [Methods and models of designing the secure system of electronic document management in transport logistic cluster]. Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Seria. Upravlenie, vychislitelnaya tekhnika i informatika [Bulletin of the Astrakhan State Technical University. Series: Management, Computer Facilities and Informatics], 2016, no. 3, pp. 40–52.

29. Finogeev A. A., Finogeev A. G., Nefedova I. S., Finogeev Ye. A., Kamaev V. A. Analiz informatsionnykh riskov v sistemakh obrabotki dannykh na osnove "tumannykh" vychisleniy [Analysis of information risks in the system of distributed monitoring based on the fog computing model]. Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Seria. Upravlenie, vychislitelnaya tekhnika i informatika [Bulletin of the Astrakhan State Technical University. Series: Management, Computer Facilities and Informatics], 2015, no. 4, pp. 38–46.

30. Finogeev A., Fionova L., Finogeev A., Nefedova I., Finogeev Ye., Vinkh T.Q., Kamaev V. Methods and tools for secure sensor data transmission and data mining in energy SCADA system. *Communications in Computer and Information Science*, 2015, vol. 535, pp. 474–484.

31. Shevtsov V. Yu., Babenko A. A., Kozunova S. S. Osobennosti zashchishchennogo dokumentooborota na predpriyatii [Features secure document management for the enterprise]. *Aktualnye voprosy informatsionnoy bezopasnosti regionov v usloviyakh globalizatsii informatsionnogo prostrantsva : mater. V Vseros. nauch.-prakt. konf. (g. Volgograd, 22–23 apr. 2016 g.)* [Topical Issues of Regional Information Security in the Context of Globalization of the Information Space. Proceedings of the V All-Russian Scientific and Practical Conference (Volgograd, 22–23 apr. 2016)], Volgograd, Volgograd State University Publ. House, 2016, pp. 237–341.

32. Shcherbakov M. V., Groumpos P. P., Kravets A. G. A Method and IR4I Index Indicating the Readiness of Business Processes for Data Science Solutions. *Creativity in Intelligent Technologies and Data Science. Second Conference, CIT&DS 2017 (Volgograd, Russia, September 12–14, 2017). Proceedings*. [Germany], Springer International Publishing AG, 2017, pp. 21–34. (Ser. Communications in Computer and Information Science; vol. 754).