Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 681.3

Обрядин

Георгий Валерьевич

«Методика проведения оперативного аудита систем защищенного документооборота»

АВТОРЕФЕРАТ

на соискание степени магистра технических наук
по специальности 1-98 80 01 «Методы и системы защиты информации, информационная безопасность»

_____

Научный руководитель

Маликов Владимир Викторович
кандидат технических наук, доцент

_____

Минск 2017

1 КРАТКОЕ ВВЕДЕНИЕ

Вопрос о необходимости автоматизации управления документооборотом давно перешел в практическую плоскость, и все больше предприятий внедряют у себя системы электронного документооборота (далее – СЭД), позволяя организациям уже на собственном опыте оценить преимущества новой технологии работы с документами. Однако и для тех немногих, кто считает автоматизацию документооборота пройденным этапом, возможно, в скором времени потребуется переосмыслить сделанный выбор и вновь погрузиться в проблему повышения эффективности системы защиты СЭД.

Основу для создания системы защищенного документооборота организации сегодня видят по-разному: одни - в повышении эффективности нормативно-правовых мер защиты информации, другие - в повышении эффективности технических мер по защите информации. Такое разделение точек зрения в вопросах защиты информации электронного документооборота определяется разной ролью и значимостью самих документов в деятельности организации, что зависит от размера организации, стиля управления, отрасли производства, общего уровня технологической зрелости и многих других факторов.

Защищенная СЭД должна обеспечивать сохранность и подлинность документов, безопасный доступ и протоколирование действий пользователей в условиях потенциальных угроз информационной безопасности.

Сохранность документов должна обеспечиваться в период всего времени жизненного цикла документа, а в случае его непредвиденной потери или порчи, СЭД должна иметь возможность его быстрого восстановления.

Механизмы защиты информации систем электронного документооборота реализуются на принципах комплексного подхода к организации защиты и учитывают разнообразие возможные угроз информационной безопасности СЭД, а также величину возможных потерь от реализованных угроз. Защита информации в СЭД не сводится только лишь к защите электронных документов и разграничению доступа к ним.

Актуальными задачами являются защита аппаратных средств и прочих устройств подсистем СЭД; защита сетевой среды, в которой функционирует СЭД, а так же защита каналов передачи данных и сетевого оборудования.

Эффективным способом защиты является создание системы управления информационной безопасностью (СЗИ), которая является современным процессом обеспечения безопасности информационных ресурсов организации, построенная на лучших мировых практиках.

Внедрение процессов оперативного аудита СЭД позволяет снизить или устранить риски информационной безопасности, повысить защищенность предприятия.

2 ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы магистерской диссертации

В настоящее время обеспечение защищенности современных систем защищенного документооборота является одной из приоритетных задач современного общества.

Анализ состояния указанной проблемы в мире показывает, что уровень ее научно – теоретической, практической реализации не в полной мере соответствует современным требованиям:

- отсутствует единый подход в вопросах эффективного управления системами защищенного документооборота с учетом специфики угроз и обеспечения адекватной их локализации;

- существующие методы оценки эффективности систем защищенного документооборота не позволяют полностью учитывать появление как новых, ранее не классифицированных видов угроз, так и новых средств, и систем безопасности в области информационной защиты.

Данная проблема приобретает сегодня особую значимость и для Республики Беларусь в связи с необходимостью проведения своевременных мероприятий по повышению надежности систем защищенного документооборота и обоснованию их экономической целесообразности.

Необходимость проведения исследования связана с тем, что надежность современных систем защищенного документооборота в первую очередь определяется эффективностью построения и управления такими системами.

Проведение оперативных аудитов и оценка эффективности систем защищенного документооборота позволяют проводить своевременные мероприятия по повышению их надежности и обоснованию экономической целесообразности.

Цель работы

Целью работы является разработка методики проведения оперативного аудита систем защищенного документооборота.

Задачи исследования

Основными задачами являются:

- изучение и классификация угроз системе защиты информации защищенного документооборота;

- исследование моделей управления системой защищенного документооборота;

- выбор и обоснование методов, средств для проведения оперативного аудита и оценки эффективности систем защищенного документооборота;

- повышение эффективности управления системой защищенного документооборота.

Объект исследования

Объектом исследования являются системы защищенного документооборота.

Предмет исследования

Предметом исследования являются нормативно-правовые, организационно-технические и технические методы и средства, способствующие повышению эффективности построения и управления системой защиты информации защищенного документооборота, а также методики проведения оперативных аудитов и оценки эффективности таких систем.

Научная новизна работы заключается в следующем:

1) Разработана методика оперативного аудита систем защищенного документооборота, позволяющая проводить оценку значимых угроз и проводить оценку реализованных мер защиты информации;

2) Предложена методика оценки рисков информационной безопасности, учитывающая объективные и субъективные дестабилизирующие факторы;

3) Предложена модель нарушителя информационной безопасности, которая характеризует 4 класса нарушителей.

4) Определены критерии оценки СЗИ СЭД.

Положения выносимые на защиту:

1. Модель управления системой зашиты информации СЭД, основанная на анализе модели угроз системе менеджмента информационной безопасности с учетом требований по нормативно-правовому, организационно-техническому и техническому обеспечению для управления безопасностью СЭД, позволяющая проводить оперативное управление системой защиты с прогнозированием потенциальных угроз такой системе и ликвидации их последствий.

2. Методический подход по оценке эффективности систем защиты информации СЭД, основанный на анализе результатов оперативного аудита систем защиты информации СЭД с учетом разработанных показателей и критериев оценки эффективности защиты, позволяющий сотрудникам служб безопасности проводить оперативный аудит таких систем.

Личный вклад соискателя

Основные научные и практические результаты диссертационной работы, а также положения, выносимые на защиту, разработаны и получены автором.

Апробация диссертации

Методика оперативного аудита была внедрена в СЗИ ИС СЭД коммерческой организации.

Структура и объем диссертации

Работа состоит из перечня условных обозначений, введения, общей характеристики работы, четырех глав, заключения, библиографического списка и 1 приложения. Общий объем диссертационной работы составляет 114 страниц, из них 94 страницы основного текста, 37 иллюстраций на 19 страницах, 11 таблиц на 15 страницах, библиография из 33 наименований и 1 приложение на 20 страницах.

3 КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность темы исследования, поставлена цель и сформулированы задачи, описан объект и предмет исследования, указаны методы исследования, определена достоверность научных положений, сформулирована научная новизна и практическая значимость выносимых на защиту результатов.

В **общей характеристике** работы сформированы цели и задачи работы, связь работы с крупными научными программами и темами, охарактеризована научная значимость полученных результатов, изложены основные положения диссертации, выносимые на защиту, объяснен личный вклад автора и апробация результатов диссертации.

В **первой главе** рассматривается анализ угроз информационной безопасности СЭД. Приведены статистические данные по нарушению информационной безопасности, выражена динамика компьютерной преступности за прошлые годы.

Далее на рисунке 1 приведена классификация угроз информационной безопасности СЭД.

Рисунок 1 – Классификация угроз

В качестве антропогенного источника угроз можно рассматривать субъекта, имеющего доступ (санкционированный или несанкционированный) к работе со штатными средствами защищаемого объекта. Антропогенные источники угроз по отношению к информационной системе могут быть как внешними, так и внутренними.

Техногенные источники угроз напрямую зависят от свойств техники. Данные источники также могут быть как внешними, так и внутренними.

К внешним источникам относятся инфраструктурные элементы информационных систем: средства связи (телефонные линии, линии передачи данных и т.п.), сети инженерных коммуникаций (водоснабжение, канализация, отопление и пр.)

Также в главе 1 приведены статистические данные по методам обеспечения безопасности систем защищенного документооборота и классификация аппаратно-программных средств и систем защиты информации. Описанный основные направления исследований по системам защищенного документооборота.

На основании анализа статистических данных по угрозам информационной безопасности предприятий и современных методов защиты можно сделаны следующие выводы:

1. Выявление фактов компрометации баз данных СЭД предприятий, подделки ЭЦП, компрометации личных ключей ЭЦП пользователей, получения доступа к конфиденциальной информации, всеобщем внедрении СМДО – говорит о необходимости использования современных комплексных подходах защиты информации.

2. Являясь широко исследуемым и постоянно совершенствуемым, риск-ориентированный подход является приоритетным для управления информационной безопасностью в организациях. Данный подход позволяет добиться структуры, абсолютно уменьшающей вероятность возникновения угрозы активам предприятия, таким как СЭД

Во **второй главе** определены нормативно-правовые, организационно-технические и техническое меры для управления системой защищенного документооборота. С учетом выявленных угроз безопасности информации СЭД режим защиты должен формироваться как совокупность способов и мер защиты в информационной среде СЭД, поддерживающая ее инфраструктуру от случайных или преднамеренных воздействий естественного или искусственного характера, влекущих за собой нанесение ущерба владельцам или пользователям информации. Определена модель угроз системе менеджмента информационной безопасности. В таблице 1 приведены типовые угрозы СЭД.

Таблица 1 – Типовые угрозы СЭД

Вид	Угрозы
1	2
Физический ущерб	Пожар
	Ущерб, причиненный водой
	Загрязнение
	Крупная авария
	Разрушение оборудования или носителей
	Пыль, коррозия, замерзание
Природные явления	Климатическое явление
	Сейсмическое явление
	Вулканическое явление
	Метеорологическое явление
	Наводнение
Утрата важных сервисов	Авария системы кондиционирования воздуха или водоснабжения
	Нарушение энергоснабжения
	Отказ телекоммуникационного оборудования

Продолжение таблицы 1

1	2
Помехи вследствие излучения	Электромагнитное излучение
	Тепловое излучение
	Электромагнитные импульсы
Компрометация/ информации	Перехват компрометирующих сигналов помех
	Дистанционный шпионаж
	Прослушивание
	Кража носителей или документов
	Кража оборудования
	Поиск повторно используемых или забракованных носителей
	Раскрытие
	Данные из ненадежных источников
	Преступное использование аппаратных средств
	Преступное использование программного обеспечения
	Определение местонахождения
Технические неисправности	Отказ оборудования
	Неисправная работа оборудования
	Насыщение информационной системы
	Нарушение функционирования программного обеспечения
	Нарушение сопровождения информационной системы
Несанкционированные действия	Несанкционированное использование оборудования
	Мошенническое копирование программного обеспечения
	Использование контрафактного или скопированного программного обеспечения
	Искажение данных
	Незаконная обработка данных
Компрометация функций	Ошибка при использовании
	Злоупотребление правами
	Фальсификация прав
	Отказ в произведении действий
	Нарушение работоспособности персонала

Деятельность СЭД поддерживается входящей в ее состав информационной инфраструктурой (представлена на рисунке 2), которая обеспечивает реализацию технологий и может быть представлена в виде иерархии следующих основных уровней:

- физического (линии связи, аппаратные средства и пр.);
- сетевого оборудования (маршрутизаторы, коммутаторы, концентраторы и пр.);
- сетевых приложений и сервисов;
- операционных систем (ОС);
- систем управления базами данных (СУБД);
- технологических процессов и приложений;
- бизнес-процессов организации.

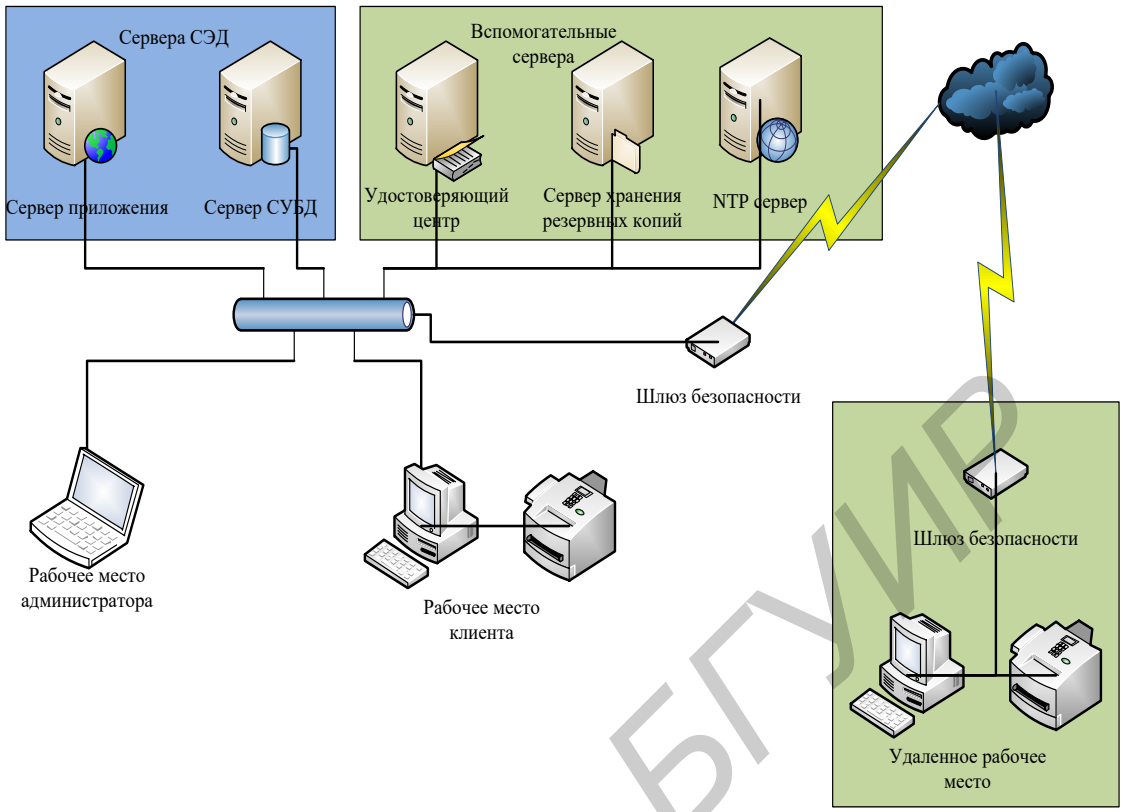

Рисунок 2 – Типовая инфраструктура СЭД

Определены модели управления системой защиты информации. На рисунке 3 приведена модель защиты информации.

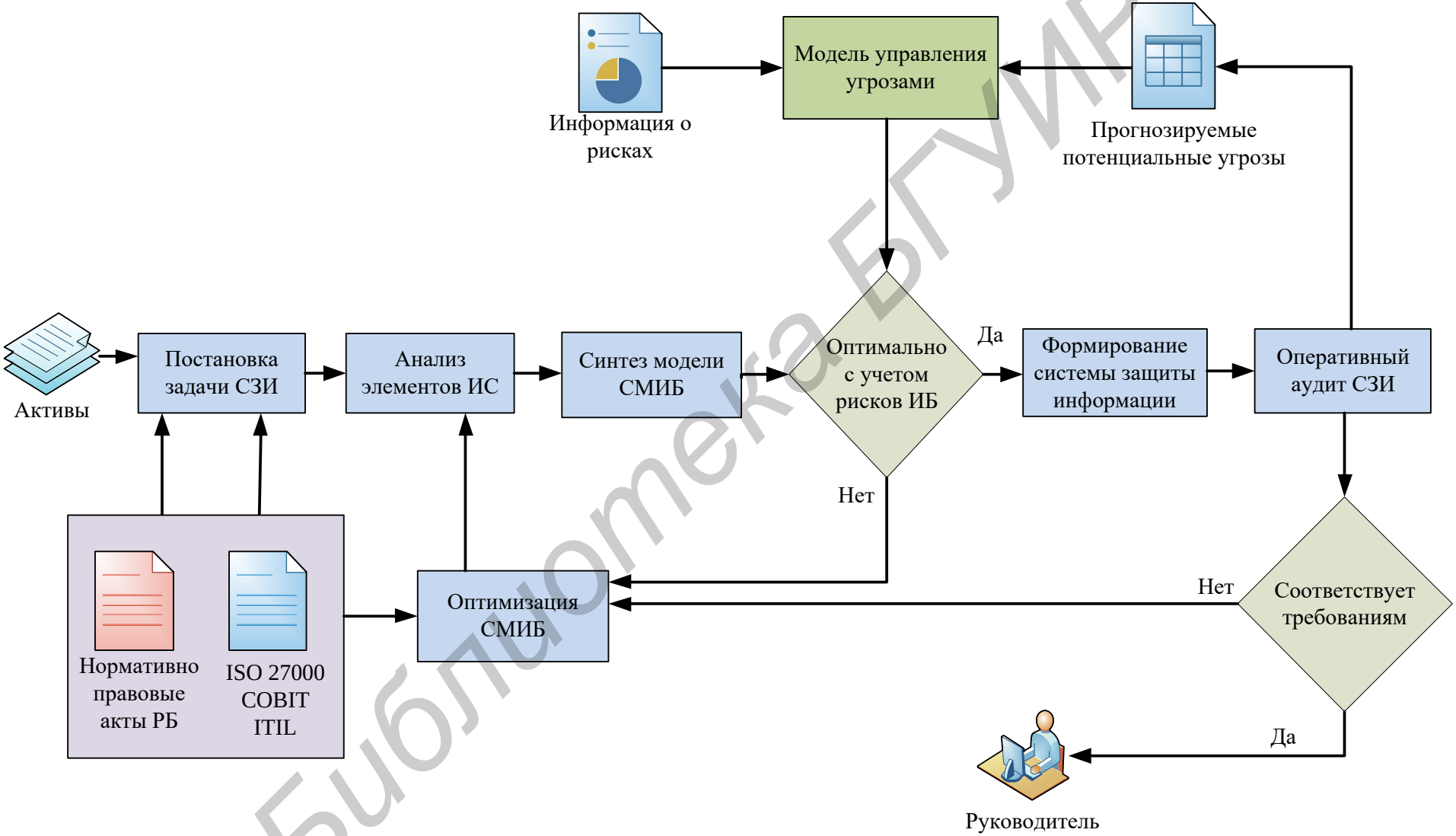

Рисунок 3 – Модель системы защиты информации

В **третьей главе** определено нормативно-правовое обеспечение аудитов СЭД, определен перечень стандартов, по которым должен проводится оперативный аудит СЭД. Далее описаны психологические особенности проведения аудитов. Определены 4 этапа энергитического процесса работы мозга:

- мозг передающего формирует идею, убеждение;
- посредством языка, интонации, жестов и мимики передающий передает убеждение до мозга получателя;
- получатель должен подготовиться к их восприятию;
- через некоторое время получатель готов реагировать.

Далее в третьей главе описаны типовые показатели и критерии эффективности систем защиты информации СЭД. Описаны методы оценки эффективности систем защиты информации СЭД. Затем в магистерской диссертации приведен обзор программного обеспечения, используемого для проведения оценки эффективности систем защиты информации, в обзоре используются такие средства как RA2 art of risk, vsRisk, Callio Secura 17799, CRAMM, RiskWatch, COBRA, Proteus и др.

Затем в третьей главе приведена методика оперативного аудита СЭД. На рисунке 4 приведена схема структуры защищаемых активов типовой СЭД.

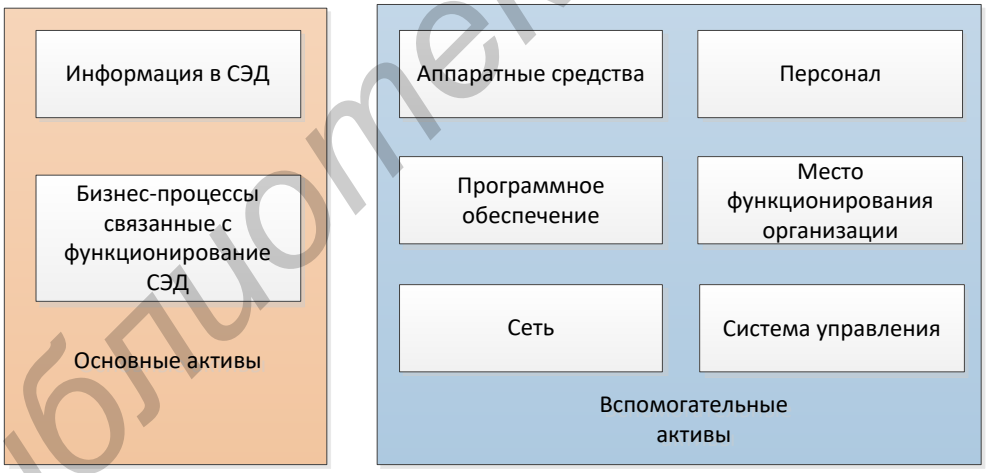

Рисунок 4 – Схема структуры защищаемых активов

Основными активами являются базовые бизнес-процессы документооборота организации и информация обрабатываемая в СЭД организации.

Основные активы бывают двух типов:

1) бизнес-процессы и бизнес-деятельность:

- процессы, утрата или ухудшение которых делает невозможным выполнение целевой задачи организации;
- процессы, модификация которых может значительно повлиять на выполнение назначения организации;
- процессы, которые необходимы организации для выполнения договорных,

правовых или регулирующих требований;

2)информация:

- информацию, необходимую для осуществления назначения или бизнеса организации;

- информацию личного характера, если она может быть определена особым образом, соответствующим национальным законам о неприкосновенности частной жизни;

К вспомогательным активам относятся активы, от функционирования которых зависят основные активы.

Аппаратные средства включают в себя все физические элементы, поддерживающие бизнес-процессы.

Программное обеспечение состоит из всех программ, содействующих работе устройства по обработке данных.

Сеть состоит из всех телекоммуникационных устройств, используемых для соединения не скольких элементов информационной системы.

Персонал состоит из всех групп лиц, участвующих в работе СЭД.

Место функционирования организации включает в себя все площадки, имеющие отношение к области применения или части области применения, и физические средства, необходимые для ее функционирования

Далее определена **модель нарушителя СЭД.** Среда функционирования подразумевает описание модели потенциального нарушителя и среды функционирования, информация приведена в таблице 2.

Таблица 2 – Модель потенциального нарушителя

Источник угрозы	Мотивация	Действие угрозы
1	2	3
Хакер, взломщик	Вызов Самомнение Бунтарство Статус	- Хакерство - Социотехника - Проникновение в систему, взлом - Несанкционированный доступ
Лицо, совершающее компьютерное преступление	Разрушение информации Незаконное раскрытие информации Денежная выгода Несанкционированное изменение данных	-Компьютерное преступление (- Мошенническая деятельность (например, воспроизведение, выдача себя за другого, перехват) - Получение доступа обманным путем - Проникновение в систему
Промышленный шпионаж	Конкурентное преимущество Экономический шпионаж	- Получение информационного преимущества - Экономическая эксплуатация - Хищение информации - Покушение на неприкосновенность личной жизни - Социотехника - Проникновение в систему - Несанкционированный доступ к системе

Продолжение таблицы 2

1	2	3
Инсайдеры	Любопытство Самомнение Разведка Денежная выгода Месть Ненамеренные ошибки и упущения (	- Шантаж -Просмотр являющейся собственностью фирмы информации - Неправильное использование компьютера - Мошенничество и хищение - Информационный подкуп - Ввод фальсифицированных, искаженных данных - Перехват -Вредоносное программное обеспечение (

Модель методики оперативного аудита представляет собой структуру, связывающую информационную потребность с соответствующими объектами измерений и их атрибутами. В число объектов могут входить планируемые и реализованные процессы, процедуры, проекты и ресурсы. Модель методики оперативного аудита, как соответствующие атрибуты количественно оцениваются и преобразуются в показатели, служащие основой для принятия решений.

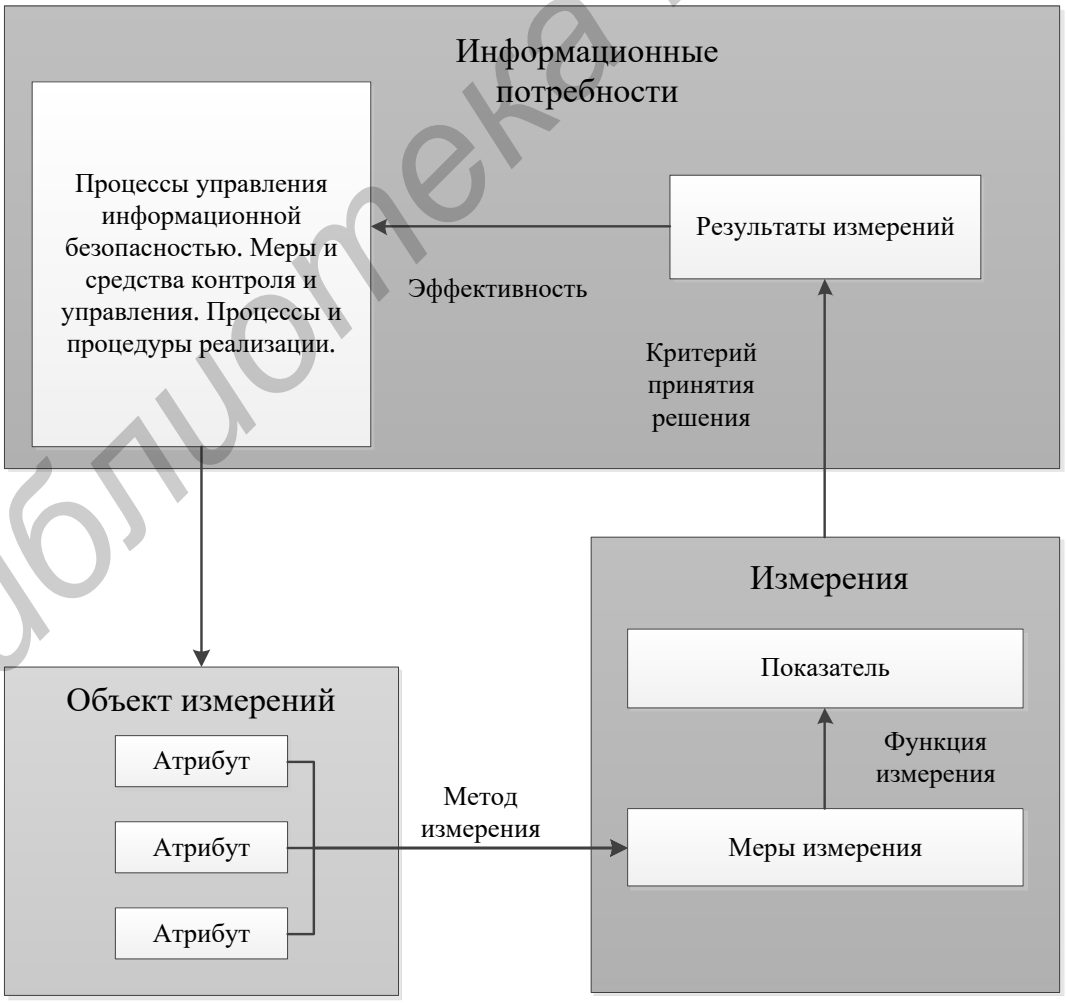

Рисунок 5 – Модель методики оперативного аудита

Далее в третьей главе приведен алгоритм проведения оперативного аудита СЭД, схема представлена на рисунке 6.

Анализ полученной документации СЭД

На данном этапе проводится анализ документации на СЗИ СЭД, СЭД, Политики информационной безопасности организации, частных политик информационной безопасности СЭД, Технического задания СЭД, Задания по безопасности СЗИ СЭД.

Декомпозиция по модулям

На этапе декомпозиции по модулям, необходимо разделить систему СЭД на логические модули согласно таблице 2.2, где определены уязвимости и угрозы типовой СЭД. Предлагается использование декомпозиции со следующими элементами СЭД:

- Персонал;
- Аппаратные средства;
- Программные средства;
- Сеть;
- Место функционирования;
- Система управления

Формирование проверяемых требований информационной безопасности

На данном этапе перед аудиторами ставиться задача сформировать конечные проверяемые требования к СЗИ СЭД и СЭД. Данные требования обусловлены руководящими нормативно-правовыми актами госрегулятора, стандартами информационной безопасности, политикой информационной безопасности организации, частными подполитиками на СЭД, требованиями ТЗ либо ЗБ.

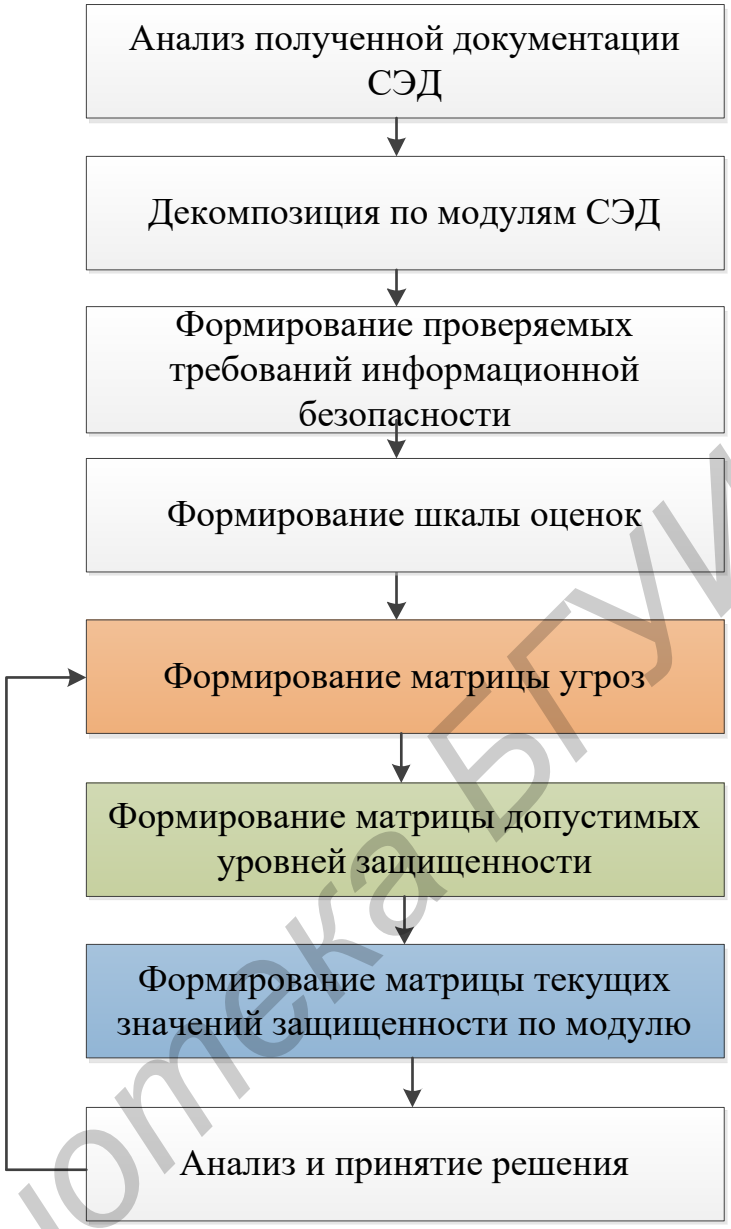

Рисунок 6 – Алгоритм методики проведения оперативного аудита СЭД

Формирование шкалы оценок

На данном этапе группа аудиторов формирует шкалу оценок, необходимую для проведения оценки соответствия защитных мер, требованиям предъявляемым документацией по информационной безопасности

Формирование матрицы угроз

Следующим этапом является формирования матрицы угроз, алгоритм формирования матрицы изображен на рисунке 7.

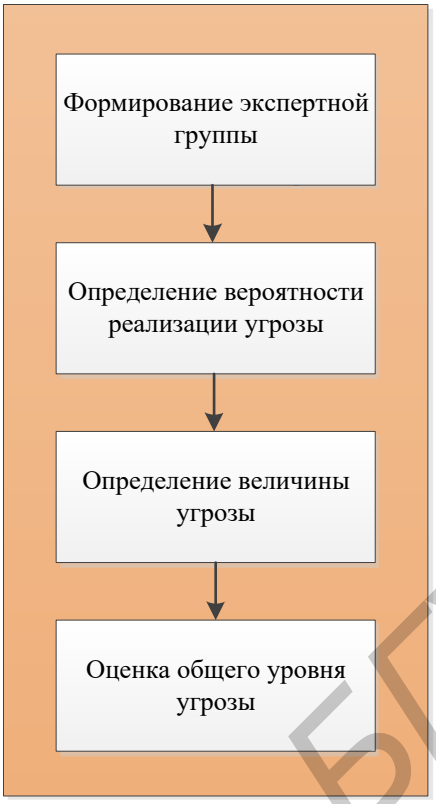

Рисунок 7 – Формирование матрицы угроз

Вероятность угрозы определяется методом экспертной оценки. Величина угрозы представляет собой произведение вероятность угрозы на величину значимости угрозы.

$$q_i = p_i \cdot v_i \quad (1)$$

Оценка общего уровня ущерба производится по формуле 2 где S стоимость ресурса.

$$P_i = q_i \cdot S_i \quad (2)$$

Формирование матрицы допустимых значений

Следующим этапом является формирование матрицы допустимых значений эффективности СЗИ СЭД, алгоритм изображен на рисунке 8.

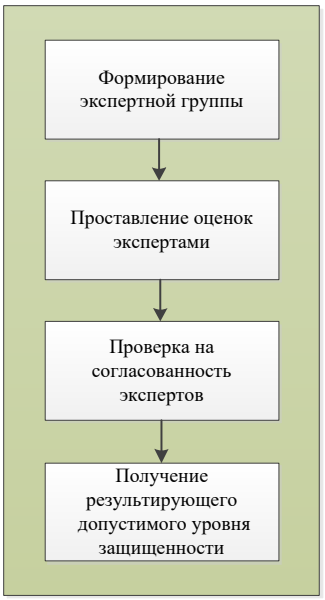

Рисунок 8 – Алгоритм формирования матрицы допустимых значений

В случае, если допустимые значения показателей эффективности отдельных компонентов системы определяются числовым значения они будут определяться экспертным методом. Эксперты по очереди будут проставлять значения показателя. Затем будет проводиться анализ этих оценок, определятся результирующее значение по формуле 3 и коэффициенты согласованности экспертов по формуле 4.

$$\text{Ид} = \sum_{i=1}^{n} \frac{\text{Ид}_i}{n}, \tag{3}$$

где n – число экспертов.

$$\sigma_i = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(\text{Ид}_i - \text{Ид})^2} \tag{4}$$

Далее необходимо убедится в отсутствии грубых ошибок, для этого должно выполняться условие:

$$\left|\text{Ид}_i - \text{Ид}\right| \le 3\sigma_i. \tag{5}$$

В случае обнаружения «грубых» ошибок, эти ошибки обсуждаются в группе экспертов, а затем проводится выбор значений параметров. Далее необходимо просчитать согласованность групповой экспертной оценки с помощью коэффициента вариации, который рассчитывается по формуле 6.

$$\delta_i = \frac{\sigma_i}{\text{Ид}} \tag{6}$$

Эмпирически, согласованность экспертных оценок считается высокой если $\delta_i \le 0{,}1$; выше средней – $0{,}1 \le \delta_i \le 0{,}2$; средней – $0{,}2 \le \delta_i \le 0{,}3$; ниже средней $0{,}3 \le \delta_i \le 0{,}5$; низкой если $\delta_i \ge 0{,}5$.

Формирование матрицы текущих значений

Текущие значения эффективности СЗИ СЭД формируются экспертным методом. На предварительном этапе необходимо сформировать набор критериев, необходимых для проведения оценки показателей атрибутов безопасности объекта. Далее экспертная группа совместно с владельцами активов проводит процесс оценки значений показателей атрибутов безопасности. Следующим этапом является формирование результирующего значения реального уровня защищенности. Схема алгоритма приведена на рисунке 9.

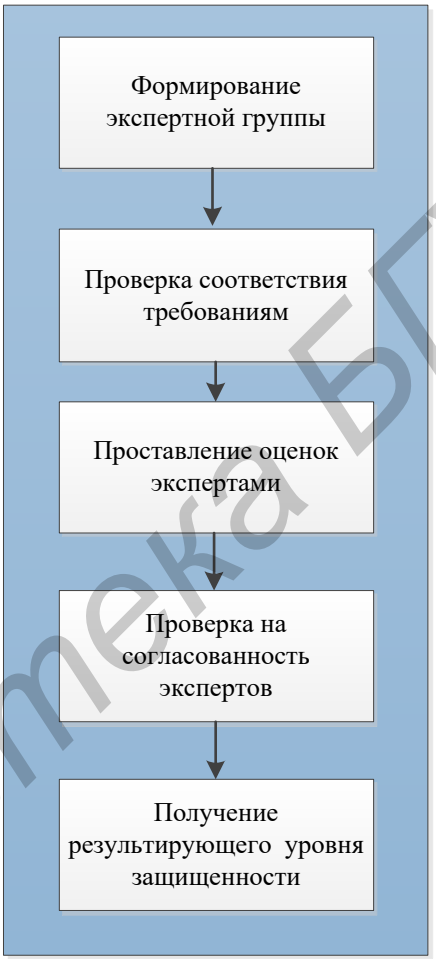

Рисунок 9 – Алгоритм получения результирующего уровня защищенности

Анализ и принятие решения

На данном этапе анализируется текущий уровень защищенности, сравнивается с допустимым значением и принимается решение о возможности повышения эффективности.

В **третьей главе** описан процесс опробования методики оперативного аудита СЭД на существующей системе предприятия.

Опробование методики оперативного аудита проводилось на базе Организации, в качестве объекта аудита использовалась СЭД данной организации.

Опробованием методики оперативного аудита СЭД занимались 4 эксперта, являющиеся специалистами в области защиты информации.

Таблица 3 – Исходные данные объекта аудита

Наименование параметра	Значение параметра
1	2
Форма юридического лица	Унитарное предприятие
Режим коммерческой тайны	Установлен
Численность персонала	100 человек
Наличие СКУД	Периметр контролируется СКУД
Наличие в штате организации специалистов по информационной безопасности	5
Электропитание	2 ввода электроэнергии с независимых источников
Наличие вредных факторов микроклимата	Нет
Выход в сети общего пользования	Нет
Использование лицензионного ПО	100%
Документация на систему	Политика информационной безопасности Организации Подполитики и инструкции по информационной безопасности Техническое задание содержащее требования по защите информации СЭД
Наличие DLP	Нет
Наличие SIEM	
Количество серверов	5
Класс объекта информатизации	А2

Первым этапом проведения оперативного аудита является анализ полученной документации. В результате анализа политики информационной безопасности Организации, подполитики и инструкциий по информационной безопасности, технического задания СЭД экспертной группой сформирован список требований подлежащих аудиту.

Следующим этапом проведения оперативного аудита является декомпозиция системы на логические элементы. Предлагается использование декомпозиции со следующими элементами СЭД:

- Персонал;
- Аппаратные средства;

- Программные средства;
- Сеть;
- Место функционирования;
- Система управления

Согласно алгоритму оперативно аудита после формирования требований подвергаемых проверке, экспертной группе необходимо сформировать шкалу оценок, в таблице 4 приведена шкала.

Таблица 4 – Количественная оценка компонентов

Оценка	Интерпретация
0	компонент не существует
0,25	компонент существует, но не выполняется
0,5	компонент существует, выполняется, но есть существенные замечания
0,75	компонент существует, выполняется, но есть несущественные замечания
1	компонент полностью соответствует требованиям

Общая оценка аудита компонента рассчитывается по формуле:

$$A=(N_1+N_2+\ldots+N_n)/M \quad (7)$$

где:

$N_1 \ldots N_n$–оценки компонентов аудита;

M– количество компонентов.

Далее необходимо сформировать матрицу угроз СЭД согласно методике оперативного аудита. Матрица уязвимостей, угроз и величины угроз построена.

Следующим этапом является проверка соответствия требований информационной безопасности объекта оценки. Эксперты проверяют последовательно все компоненты аудита, проставляют свои оценки согласно шкале определенной в таблице 4.

Далее необходимо провести оценку допустимого уровня эффективности. Он проводится согласно алгоритму описанному методике оперативного аудита. Затем проводится оценка реального уровня эффективности, результаты

приведены в таблице. Далее перед экспертами стоит задача сравнения реального уровня эффективности с допустимым уровнем эффективности. В случае недопустимых значений группой экспертов вырабатываются меры по увеличению эффективности СЗИ СЭД.

ЗАКЛЮЧЕНИЕ

Основные научные результаты диссертации

1. Проведен анализ статистических данных по угрозам информационной безопасности и современных методов защиты систем электронного документооборота на основе которого показано, что основным каналом утечек информации является персонал организации, а также нерациональный выбор способов хранения, передачи и обработки информации. Обозначено, что, являясь широко исследуемым и постоянно совершенствуемым, риск-ориентированных подход является приоритетным для управления информационной безопасностью организаций.

2. Исследованы основные технические нормативно-правовые документы по информационной безопасности кредитно-финансовых организаций. На примере ISO/IEC 27001:2013, COBIT и ITSM проведен сравнительный анализ подходов к обеспечению защиты организаций.

3. Показаны преимущества и недостатки основных походов по определению оценки эффективности СЗИ.

4. Сформулирована модель управления системой защиты информации СЭД, основанная на анализе модели угроз системе менеджмента информационной безопасности с учетом требования документации, позволяющая проводить оперативное управление системой защиты информации.

5. Сформулирована методика оперативного аудита систем защищённого документооборота и опробована на существующей СЭД.

Рекомендации по практическому использованию результатов

1. Практические рекомендации по совершенствованию системы управления информационной безопасности СЭД могут быть применены при построении систем защиты информации.

2. Предложенный подход по оценке эффективности систем защиты информации СЭД позволяет сотрудникам служб безопасности проводить оперативный аудит таких систем, оценку реальных и прогнозирования потенциальных угроз, а также обеспечение их оперативной локализации и ликвидации.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1-А. В.В. Маликов, Исследование сетевых сервисов/ресурсов кредитно-финансовых организаций на предмет проведения DoS / DDoS-атак /В.В. Маликов, М.А. Бабич, Г.В. Обрядин // Технические средства защиты информации: тезисы докладов 14–ой Белорусско–российской НТК, Минск, 25 – 26 мая 2016 г. / БГУИР; редкол.: Л.М. Лыньков [и др.]. – Мн.: БГУИР, 2016. – С. 35.