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

УДК 681.3

Макатерчик
Александр Васильевич

Методика оценки эффективности мероприятий обеспечения информационной безопасности инфокоммуникационных систем специального назначения»

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 2018

1 КРАТКОЕ ВВЕДЕНИЕ

В настоящее время в Республике Беларусь идет активная работа по реализации Государственной программы вооружения на период до 2020 года. Реализуются концептуальные положения и программы развития системы связи Вооруженных Сил на период до 2020 года, где одними из основных направлений ее совершенствования определены:

- совершенствование линий связи привязки узлов связи пунктов управления Вооруженных Сил Республики Беларусь к пунктам выделения каналов Министерства связи и информатизации;
- переход к цифровым методам передачи информации на основе современных технологий;
- создание на основных информационных направлениях высокоскоростных и устойчивых цифровых каналов;
- расширение предоставляемых услуг и сервисных функций.

Резкий рост информационных потоков, необходимость в предоставлении новых услуг и сервисов в интересах системы управления, ужесточение требований к информационному процессу в системах управления, непосредственно обеспечивающих управление на поле боя, постоянный рост территориальной распределенности и мобильности системы управления и ее отдельных элементов, взаимная интеграция и интеллектуализация систем автоматизации и связи ставят новые задачи перед системой связи.

Таким образом, необходимость проведения данного исследования обусловлена развитием современных систем связи, а также появлением новых угроз безопасности в таких системах, связанных с возможностью реализации злоумышленниками уязвимостей, результаты которых негативно влияют на обеспечение информационной безопасности государства и организаций различных форм собственности.

Целью работы является исследование, оценка эффективности и совершенствование подходов к обеспечению безопасности связи в инфокоммуникационных системах специального назначения.

Для достижения данной цели необходимо решение следующих задач:

1. Анализ статистических данных по обеспечению безопасности связи в инфокоммуникационных системах специального назначения.
2. Разработка моделей угроз системе менеджмента информационной безопасности, а также моделей управления системой зашиты информации в инфокоммуникационных системах специального назначения.
3. Разработка методики оценки эффективности систем защиты информации, а также практических рекомендаций по повышению эффективности защиты в инфокоммуникационных системах специального назначения

Проводимые в рамках настоящей диссертации исследования позволяют решить важную научную задачу, связанную с эффективным обеспечением безопасности связи в инфокоммуникационных системах специального назначения.

2 ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы магистерской диссертации

В настоящее время в Республике Беларусь идет активная работа по реализации Государственной программы вооружения на период до 2020 года. Реализуются концептуальные положения и программы развития системы связи Вооруженных Сил на период до 2020 года, где одними из основных направлений ее совершенствования определены:

- совершенствование линий связи привязки узлов связи пунктов управления Вооруженных Сил Республики Беларусь к пунктам выделения каналов Министерства связи и информатизации;
- переход к цифровым методам передачи информации на основе современных технологий;
- создание на основных информационных направлениях высокоскоростных и устойчивых цифровых каналов;
- расширение предоставляемых услуг и сервисных функций.

Резкий рост информационных потоков, необходимость в предоставлении новых услуг и сервисов в интересах системы управления, ужесточение требований к информационному процессу в системах управления, непосредственно обеспечивающих управление на поле боя, постоянный рост территориальной распределенности и мобильности системы управления и ее отдельных элементов, взаимная интеграция и интеллектуализация систем автоматизации и связи ставят новые задачи перед системой связи.

Таким образом, необходимость проведения данного исследования обусловлена развитием современных систем связи, а также появлением новых угроз безопасности в таких системах, связанных с возможностью реализации злоумышленниками уязвимостей, результаты которых негативно влияют на обеспечение информационной безопасности государства и организаций различных форм собственности.

Проведение оперативных аудитов и оценка эффективности мероприятий безопасности связи в инфокоммуникационных система специального назначения позволяют проводить своевременные мероприятия по повышению их надежности и обоснованию экономической целесообразности.

Цель работы

Целью работы является исследование, оценка эффективности и совершенствование подходов к обеспечению безопасности связи в инфокоммуникационных системах специального назначения.

Задачи исследования

Основными задачами являются:

1. Анализ статистических данных по обеспечению безопасности связи в инфокоммуникационных системах специального назначения.
2. Разработка моделей угроз системе менеджмента информационной безопасности, а также моделей управления системой зашиты информации в инфокоммуникационных системах специального назначения.
3. Разработка методики оценки эффективности систем защиты

информации, а также практических рекомендаций по повышению эффективности защиты в инфокоммуникационных системах специального назначения.

Объект исследования

Объектом исследования являются инфокоммуникационные системы специального назначения.

Предмет исследования

Предметом исследования являются организационно-технические и технические методики и средства, способствующие повышению эффективности защиты инфокоммуникационных систем специального назначения.

Научная новизна работы заключается в следующем:

1) Разработана методика оперативного аудита инфокоммуникационных систем специального назначения, позволяющая проводить оценку значимых угроз и реализованных мер защиты информации;

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

4) Определены критерии оценки СЗИ ИКССН.

Положения выносимые на защиту:

1. Модель управления системой зашиты информации ИКССН, основанная на анализе модели угроз системе менеджмента информационной безопасности с учетом требований по нормативно-правовому, организационно-техническому и техническому обеспечению для управления безопасностью ИКССН, 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 ИКССН, основанный на анализе результатов оперативного аудита систем защиты информации ИКССН 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 ИКССН одного из командований Вооруженных Сил.

Структура и объем диссертации

Работа состоит из перечня условных обозначений, введения, общей характеристики работы, четырех глав, заключения, библиографического списка. Общий объем диссертационной работы составляет 97 страниц, из них 85 страницы основного текста, 14 иллюстраций на 14 страницах, 25 таблиц на 19 страницах, библиография из 40 наименований.

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 ИКС СН. Приведены статистические данные по нарушению информационной безопасности, выражена динамика компьютерной преступности за прошлые годы.

Далее на рисунке 1 приведена классификация угроз информационной безопасности ИКССН.

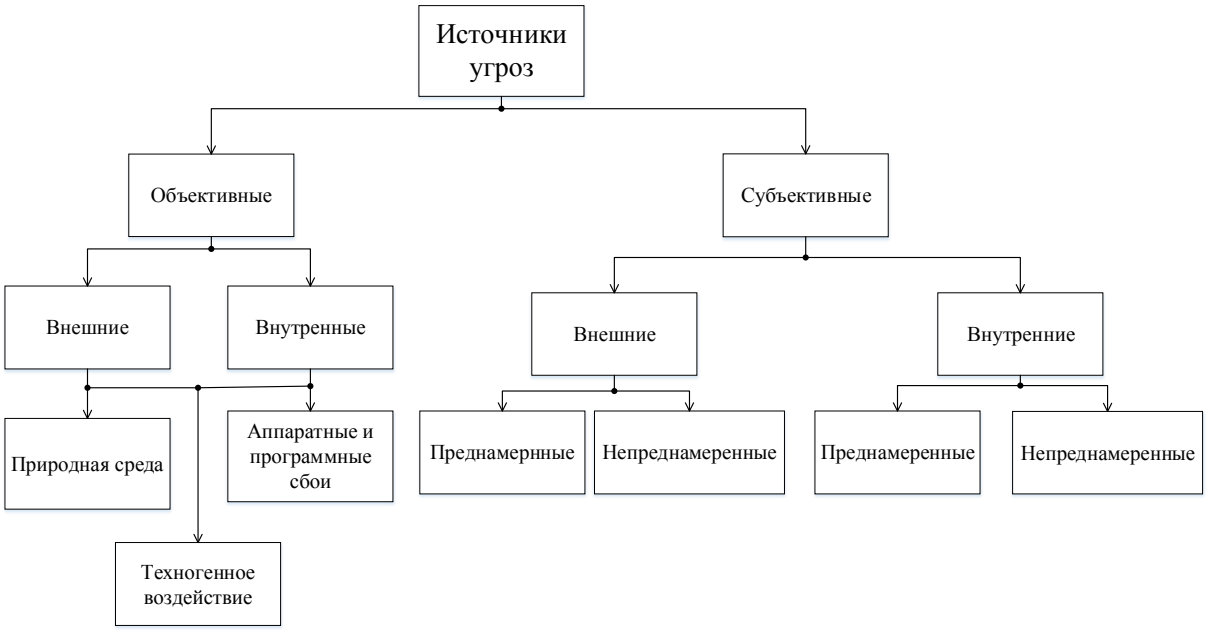

Рисунок 1 **– Классификация угроз**

Непреднамеренные угрозы возникают независимо от воли и желания людей. Данный тип угроз связан чаще всего с прямым природным или техногенным физическим воздействием на элементы системы связи и ведет к нарушению ее работы и (или) физическому повреждению (уничтожению) ее элементов.

Причиной возникновения угроз случайного характера могут быть как сбои вследствие конкретных ошибок оператора и прямых действий иных лиц

(например, неравномерное натяжение тросов антенны может привести к ее падению), так и случайные нарушения в работе системы (например, вследствие поломки оборудования, сбоя в работе программного обеспечения и т.д.)

Преднамеренные угрозы, в отличие от непреднамеренных, могут быть созданы людьми, устройствами или процессами, действующими целенаправленно с целью дезорганизовать работу ИКССН. Преднамеренные угрозы, в свою очередь, подразделяются на пассивные и активные.

Пассивные угрозы связаны с несанкционированным доступом к информации с целью ее получения или изменения. Они наиболее опасны, так как их сложно своевременно обнаружить, и применить соответствующие меры для их нейтрализации.

Активные угрозы направлены на несанкционированное уничтожение и (или) изменение информации или попытки лишения доступа к информационным ресурсам легитимных пользователей.

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

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

1. Внедрение современных технологий в структуру ИКССН, выявление фактов и обоснованной возможности возникновения негативного воздействия на элементы ИКС СН, говорит о необходимости использования современных комплексных подходов для обеспечения защиты информации и безопасности связи в ИКССН.

2. Являясь широко исследуемым и постоянно совершенствуемым, риск-ориентированный подход является приоритетным для управления информационной безопасностью в ИКССН. Данный подход позволяет добиться структуры, абсолютно уменьшающей вероятность возникновения угрозы активам организаций , использующих собственные ИКССН.

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

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
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

Для последующей формулировки методики оценки эффективности мероприятий по обеспечению информационной безопасности в ИКС СН

сформирована модель реализации угроз информационной безопасности, которую можно представить в виде схемы, приведенной на рисунке 2.

Рисунок 2 – Модель реализации угроз безопасности связи

Разработана модель управления системой защиты информации. На рисунке 3 приведена модель защиты информации.

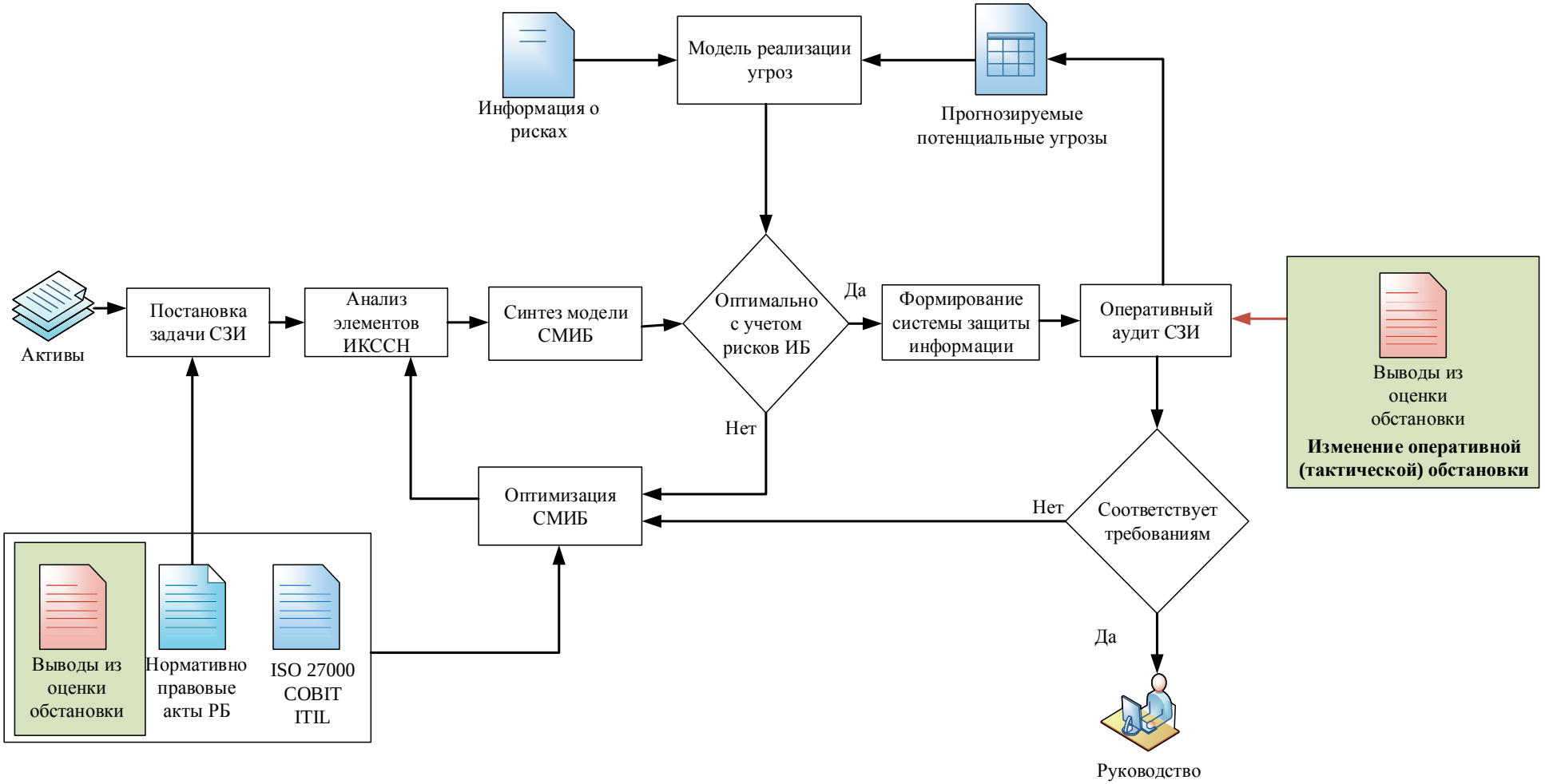

Рисунок 3 – Модель управления системой защиты информации в ИКС СН

В **третьей главе** определено нормативно-правовое обеспечение аудитов ИКССН, определен перечень стандартов, по которым должен проводится оперативный аудит ИКССН. Далее описаны психологические особенности проведения аудитов. Определены 4 этапа энергетического 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 ИКССН. Описаны методы оценки эффективности систем защиты информации ИКССН.

Сформулирована методика оперативного аудита ИКССН. Блок схема алгоритма проведения оперативного аудита представлена на рисунке 4.

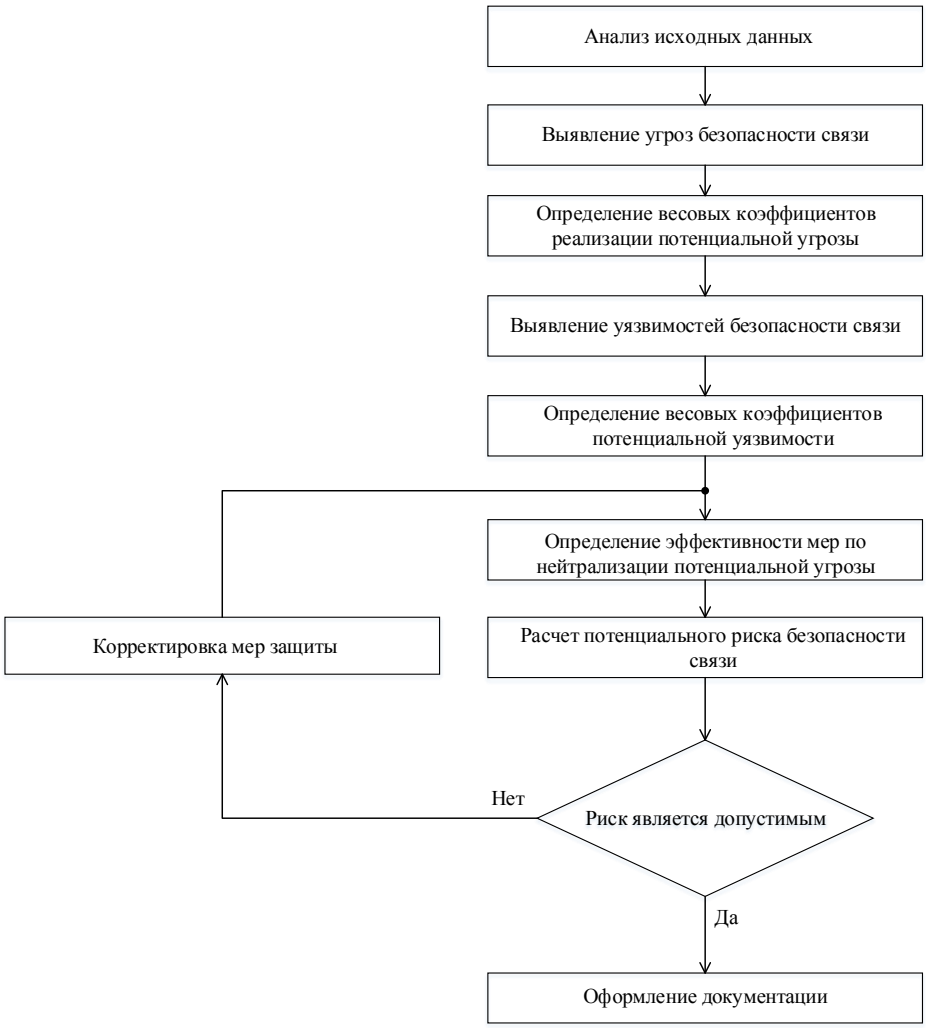

Рисунок 4 – Блок-схема разработанной методики

Анализ исходных данных

Перед началом определения численного значения риска безопасности связи, необходимо проанализировать исходные данные которые будут оказывать влияние на дальнейшие расчеты. Это такие данные как:

– местность, на которой расположены элементы анализируемая ИКС СН;

– количество радиорелейных линий;

– удаленность от средств РЭР армий иностранных государств;

– физическое состояние элементов ИКССН;

– наличие вблизи элементов ИКССН крупных промышленных предприятий;

– наличие диверсионно-разведывательных групп вблизи размещения фрагментов ИКССН;

– организация охраны и обороны вокруг ИКССН.

Выявление угроз

Для выявления угроз используется метод построения модели угроз рассмотренный выше. В качестве вспомогательной информации рекомендуется использовать перечень наиболее часто встречающихся угроз.

Важно не упустить из виду ни одной возможной угрозы, так как в результате возможно нарушение функционирования ИКССН.

При использовании материалов каталогов угроз или результатов ранее проводившихся оценок угроз следует иметь в виду, что угрозы постоянно меняются. После завершения выявления угроз составляют перечень выявленных угроз.

Определение весового коэффициента должно учитывать природу угрозы и особенности, присущие различным группам угроз, таких как:

1 Вероятность преднамеренных угроз зависит от мотивации, знаний, компетенции и ресурсов, доступных потенциальному злоумышленнику, а также от привлекательности активов для реализации атак;

2 Вероятность случайных угроз может оцениваться с использованием статистики и опыта. Вероятность таких угроз может зависеть от близости организации к источникам опасности. Также географическое положение средства связи оказывает влияние на возможность возникновения экстремальных погодных условий. Вероятность человеческих ошибок и поломки оборудования также должны быть оценены.

Для оценки вероятности рекомендуется применять экспертные мнения. Использование соответствующих накопленных данных для выявления событий или ситуаций, которые возникали в прошлом, дает возможность предположить вероятность их возникновения в будущем. Используемые данные должны соответствовать рассматриваемому типу оборудования. Если в прошлом риск возникал очень редко, то любая оценка вероятности будет весьма

неопределенной. Это особенно касается тех случаев, когда событие, ситуация или обстоятельство в прошлом никогда не возникали, что не позволяет обоснованно предполагать, что они не произойдут в будущем.

Уровни вероятности реализации угрозы и представлены в таблице 2.

Результатом этапа является определение вероятности («высокая», «средняя», «низкая») для каждого типа угроз.

Выявление уязвимостей предполагает идентификацию уязвимостей окружающей среды, процедур, персонала, аппаратных средств, ПО или средств связи, которые могли бы быть использованы источником угроз для нанесения ущерба системе связи.

Результаты построения модели уязвимостей представлен в таблицах 3 - 7.

Следует отметить, что некорректно внедренные или применяемые меры защиты могут сами по себе стать источниками появления уязвимостей.

Понятие «уязвимость» можно отнести к свойствам или атрибутам актива. Исходные данные идентификации уязвимостей следует получать от специалистов по разработке оборудования и информационных технологий, а также лиц, отвечающих за реализацию мер по защите безопасности связи. В качестве вспомогательной информации для идентификации уязвимостей может быть использован каталог типовых уязвимостей. Идентифицировать уязвимости следует исходя из перечня угроз и активов, определенных на ранних этапах оценки риска безопасности связи.

Таблица 2 – Вероятность реализации угрозы

Вероятность реализации	Описание
«Высокая» 0,6 - 0,9	Угроза, скорее всего, осуществится. Существуют инциденты, статистика или другая информация, указывающая на то, что угроза скорее всего, осуществиться, или могут существовать серьезные причины или мотивы для злоумышленника, чтобы осуществить такие действия. Ожидаемая частота реализации угрозы – еженедельно или чаще
«Средняя» 0,3 - 0,5	Возможно, эта угроза осуществится (в прошлом происходили инциденты), или существует статистика или другая информация, указывающая на то, что такие или подобные угрозы иногда осуществлялись прежде, или существуют признаки
«Низкая» 0,1 - 0,2	Маловероятно, что эта угроза осуществиться, не существует инцидентов, статистики, мотивов, которые указывали бы на то, что это может

Таблица 3 – Безопасность кадровых ресурсов

Уязвимость	Угроза, использующая уязвимость
Недостаточное обучение безопасности	Ошибки персонала
Неосведомленность в вопросах безопасности	Несанкционированное использование ПО
Немотивированный или недовольный персонал	Злоупотребление средствами обработки информации

Таблица 4 – Физическая безопасность

Уязвимость	Угроза, использующая уязвимость
Размещение в зоне, подверженной затоплению	Затопление
Незащищенное хранение	Кража
Подверженность оборудования влажности, пыли и загрязнению	Запыление
Подверженность оборудования температурам	Нарушения температурного режима перепадами

Таблица 5 – Управление коммуникациями и операциями

Уязвимость	Угроза, использующая уязвимость
Сложный пользовательский интерфейс	Ошибка персонала
Отсутствие обновления ПО, используемого для защиты от вредоносного кода	Внесение вредоносного программного кода
Неконтролируемое копирование	Кража информации
Незащищенное соединение с сетью электросвязи общего пользования	Использование ПО неавторизованными пользователями

Таблица 6 – Контроль доступа

Уязвимость	Угроза, использующая уязвимость
Отсутствие политик чистых столов и чистых экранов	Потеря или повреждение информации
Отсутствие выхода из системы при завершении работы пользователем на рабочей станции	Использование ПО неавторизованным пользователем
Плохое управление паролями	Присвоение чужого пользовательского идентификатора

Таблица 7 – Приобретение, разработка и сопровождение информационных систем

Уязвимость	Угроза, использующая уязвимость
Плохо документированное ПО	Ошибки персонала технической поддержки
Хорошо известные дефекты в ПО	Использование ПО неавторизированными пользователями

Результатом завершения оценки уязвимостей должен быть перечень уязвимостей.

Следующим этапом аудита является определение весового коэффициента потенциальной уязвимости. Перед началом анализа влияния необходимо использовать следующую информацию:

– целевое назначение средства связи;

– критичность средства связи и данных;

– конфиденциальность средства связи и данных;

– ценность активов.

Основываясь на полученных данных, производится определение весового коэффициента потенциальной уязвимости.

Коэффициент может ранжироваться в следующем диапазоне: «высокое», «среднее», «низкое». Описание величин влияния приведено в таблице 3.7.

Результатом этапа является определение весового коэффициента потенциальной уязвимости.

Идентификация мер защиты должна проводиться с учетом уже реализованных или планируемых мер защиты. Действующие или планируемые меры защиты должны быть частью общего процесса, во избежание не вызываемых необходимостью затрат труда и средств, *т.* е. дублирования мер защиты.

Эксперт, выполняющий оценку риска, определяет, реализуются ли требования безопасности. Для идентификации существующих или планируемых мер защиты могут реализовываться следующие мероприятия:

– просмотр документов, содержащих информацию о мерах защиты. Если процессы задокументированы должным образом, то все существующие или планируемые средства защиты информации и состояние их реализации должны быть там доступны;

– определение совместно с пользователями и персоналом, отвечающим за безопасность связи, какие средства защиты информации действительно использованы для рассматриваемого станции;

– анализ фактически реализованных мер физической защиты;

– использование перечня типовых мер защиты информации.

Таблица 8 – Определение весового коэффициента потенциальной уязвимости.

Влияние	Определение
«Высокое» 0,6 - 0,9	Потеря конфиденциальности, целостности или доступности может привести к тяжелым или катастрофичным неблагоприятным последствиям, которые отразятся на функционировании средства связи.
«Среднее» 0,3 - 0,5	Потеря конфиденциальности, целостности или доступности может привести к серьезным неблагоприятным последствиям, которые отразятся на функционировании средства связи, при этом средство связи будет выполнять свои основные функции, но эффективность этих функций значительно снизится
«Низкое» 0,1 - 0,2	Потеря конфиденциальности, целостности или доступности может вызвать ограниченные неблагоприятные последствия, которые отразятся на функционировании средства связи, при этом средство связи будет выполнять свои основные функции, но эффективность этих функций заметно снизится.

В процессе идентификации уже действующих мер защиты необходимо проверить, правильно ли они функционируют. Если предполагается, что какое-либо средство защиты информации функционирует правильно, однако это не подтверждается в процессе осуществления деловых операций, то функционирование его может стать источником возможной уязвимости.

По результатам составляют перечень действующих и планируемых мер защиты с указанием статуса их реализации и использования.

Окончательное определение риска осуществляется путем расчета показателя

$$R = \frac{\sum_{j=1}^{J}\sum_{i=1}^{I}\sum_{n=1}^{N}(P_i \cdot U_i)\cdot(D_{ij} \cdot V_{ij})\cdot(1-K_{jn})}{\sum_{j=1}^{J}\sum_{i=1}^{I}\sum_{n=1}^{N}U_i \cdot V_{ij}}, \qquad (1)$$

где R – численная величина риска безопасности связи;

I – количество уязвимостей;

J – количество угроз;

N – количество мер по обеспечению безопасности связи;

P_i – весомый коэффициент реализации потенциальной угрозы;

U_i – возможность реализации потенциальной угрозы;

D_{ij} – весомый коэффициент потенциальной уязвимости;

V_{ij} – возможность реализации потенциальной уязвимости;

K_{in} – возможность нейтрализации угроз.

Результаты расчета потенциального риска безопасности сравниваются с допустимым риском. Описание уровней допустимого риска для ИКС СН развернутых в интересах Вооружённых Сил представлено в таблице 8, в которой приведена шкала риска, с рейтингом риска («высокий», «средний» и «низкий»). Данный рейтинг представляет степень или уровень риска, при функционировании ИКССН, если будет реализована некоторая угроза. На этой шкале риска также предлагаются действия, которые необходимо предпринять для данного уровня риска.

По результатам данного сравнения делается вывод, что если риск допустимым, то следующим этапом становиться оформление документов по оценке эффективности системы защиты информации. Если риск превышает допустимый уровень, то необходимо корректировка мер защиты, после чего необходимо еще раз пройти процедуру расчета потенциального риска безопасности связи.

С использование сформулированной методики проведен оперативный аудит в части касаемо временно развертываемого в период проведения мероприятий подготовки войск фрагмента ИКССН (ряд точных сведений не приводятся из соображений конфиденциальности).

Полная информация о результатах аудита и порядке расчета не приводится по требованиям владельца ИКССН.

Итоговое значения для анализируемого объекта были оценены по выше предложенной методике, как «средний».

Таблица 8 – Предлагаемая шкала риска и необходимых действий

Уровень риска	Описание риска и необходимых действий
«Высокий» 0,5 - 0,9	Если в результате обследования риск оценен как высокий, необходимо быстро реализовать корректирующие меры. Существующая система может продолжать функционировать, но корректирующие действия должны быть произведены незамедлительна
«Средний» 0,2 - 0,5	Если в результате обследования риск оценен как средний, необходимы корректирующие меры, которые должны лечь в основу план снижения рисков, чтобы реализовать эти действия в разумные сроки
«Низкий» 0,01 - 0,2	Если в результате обследования риск оценен как низкий, необходимо на уровне руководства организации определить следует ли реализовывать корректирующие действия или следует принять риск

В **четвертой главе** описан процесс опробования методики оперативного аудита ИКССН на существующей системе.

Опробование методики оперативного аудита проводилось на базе Организации (название заменено на условное по причине соблюдения конфиденциальности), в качестве объекта аудита использовалась СЭД данной организации.

Опробованием методики оперативного аудита ИКССН проводилась путем проведения и последующего сравнения результатов аудита, осуществленного по двум методикам: разработанной в ходе данной работы и имеющейся у заказчика. Для проведения аудита сформированы 2 группы по 4 эксперта, являющиеся специалистами в области защиты информации.

Таблица 9 – исходные данные объекта аудита

Наименование параметра	Значение параметра
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 от 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 ИКС СН
Наличие DLP	Нет
Количество серверов	5
Класс объекта информатизации	А2

Выводы по результатам аудита выполненного по типовой методике: В результате оценки реальной эффективности, часть параметров близка к порогу допустимого значения эффективности, следовательно владельцам активов необходимо более детально проанализировать тенденцию изменения параметра и принять меры.

В ходе работы по экспериментальной методике вторая группа экспертов с целью объективности сравнения придерживалась аналогичных подходов к проведению аудита.

В ходе работы экспертами выполнена расстановка весовых коэффициентов, определена вероятность реализации уязвимостей и угроз, а также вероятность их нейтрализации.

С использованием формулы 1 получен результат равный 0,001106, что по таблице 8 классифицируется как «низкий» уровень риска. И соответственно необходимо на уровне руководства организации определить следует ли реализовывать корректирующие действия или следует принять риск.

Разработанная методика позволяет получить количественную оценку эффективности функционирования СЗИ ИКС СН.

При проведении аудита отмечено, что на первых этапах аудита трудозатраты обоих рабочих групп примерно одинаковы. Но в ходе проведении штабной тренировки экспертами была отмечена высокая оперативность получения оценки эффективности мероприятий по обеспечению информационной безопасности применяемых в качестве ответных действий по вводным.

Исходя из практических рекомендаций по совершению оперативного аудита, методам оценки эффективности СЗИ можно сделать следующие выводы:

1. Опробована методика оперативного аудита и оценки защищенности СЗИ типовой ИКССН. В ходе опробования на существующей системе были получены пригодные для анализа результаты. Оценена эффективность принимаемых мер защиты информации. Выработаны рекомендации.

2. Предложенная методика оперативного аудита позволяет оперативно отслеживать эффективность функционирования СЗИ и оценивать эффективность мероприятий по обеспечению информационной безопасности в ИКС СН.

3. Эффективность создаваемой СЗИ определяется учетом требований безопасности информации на стадии проектирования информационной системы. Подходы к созданию и аттестации СЗИ должны обеспечивать объективную, достоверную и повторяемую оценку соответствия СЗИ установленным для нее требованиям в соответствии с процедурами, критериями и методологией, установленными в нормативных документах. Устойчивое выполнение ИКССН своих задач обеспечивается своевременной и периодической актуализацией модели угроз и модернизацией СЗИ с учетом рисков.

4. Совершенствование СЗИ представляет собой комплексный подход к управлению системой информационной безопасности, основными стадиями которого являются:

- подготовка к совершенствованию СЗИ;
- совершенствование СЗИ (проектирование, внедрение, опытная эксплуатация);
- внешний аудит СЗИ.

ЗАКЛЮЧЕНИЕ

Основные научные результаты диссертации

1. Проведен анализ статистических данных по угрозам информационной безопасности и современных методов защиты инфокоммуникационных систем специального назначения 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 методика оперативного аудита ИКССН и опробована на существующей ИКССН.

Рекомендации по практическому использованию результатов

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

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

3. Предложенная методика оперативного аудита позволяет отслеживать эффективность функционирования СЗИ и оценивать эффективность мероприятий по обеспечению информационной безопасности в ИКС СН.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1-А. Макатерчик А. В., Маликов В. В. Численное определение рисков безопасности связи для элемента инфокоммуникационных систем специального назначения. / В.В.Маликов, А.В. Макатерчик // Управление информационными ресурсами : материалы XIII Междунар. науч.-практ. конф., Минск, 9 дек. 2016 г. - Минск : Акад. упр. при Президенте Респ. Беларусь, 2016. - 420 с.

2-А. Маликов В.В., Бабич М.А., Макатерчик А.В. актуальные вопросы создания республиканской системы мониторинга общественной безопасности. / В.В.Маликов, М.А.Бабич, А.В. Макатерчик // Актуальные проблемы обеспечения общественной безопасности в Республике Беларусь: теория и практика: Тезисы докладов XIX Республиканской научно-практической конференции, 3 мая 2017 г., Минск. Минск: ВАРБ, 2017. – в 2 ч. 516 с.

3-А. Маликов В.В., Бабич М.А., Макатерчик А.В. Оценка эффективности работы DLP-системы по защите конфиденциальной информации от утечки по техническим каналам / В.В.Маликов, М.А.Бабич, А.В. Макатерчик // Комплексная защита информации : материалы XXII науч.-практ. конф., Полоцк, 16-19 мая 2017 г. / Полоц. Гос. ун-т ; отв. за вып. С.Н. Касанин. – Новополоцк: Полоц. гос. ун-т, 2017. – 282 с.

4-А Макатерчик А.В. Численное определение рисков безопасности связи для элемента инфокоммуникационных систем специального назначения. /А.В.Макатерчик // 53-я научная конференция аспирантов, магистрантов и студентов БГУИР : Тезисы докладов 53-й научной конференции аспирантов, магистрантов и студентов БГУИР, 5 мая 2017 г., Минск. Минск: БГУИР, 2017. – 446 с.

5-А. Макатерчик А.В. Численное определение рисков безопасности связи инфокоммуникационной системы специального назначения. /А.В.Макатерчик // Технические средства защиты информации: Тезисы докладов XV Белорусско-российской научно-технической конференции, 6 июня 2017 г., Минск. Минск: БГУИР, 2017. – 116 с.

6-А. Маликов В.В., Бабич М.А., Макатерчик А.В. Исследование стеганографических технологий модификации конфиденциальной информации. / В.В.Маликов, М.А.Бабич, А.В. Макатерчик // Технические средства защиты информации: Тезисы докладов XV Белорусско-российской научно-технической конференции, 6 июня 2017 г., Минск. Минск: БГУИР, 2017. – 116 с.

7-А. Макатерчик А.В., Романовский С.В. Математическая модель расчета вероятности рисков безопасности связи в инфокоммуникационных системах специального назначения. /А.В.Макатерчик, С.В.Романовский // Современные средства связи: Материалы XXII Международной научно-технической конференции, 19-20 октября 2017 г., Минск. Минск: БГАС, 2017. – 436 с.