В.А. Бойправ, О.В. Бойправ, Л.Л. Утин

АСПЕКТЫ ОБЕСПЕЧЕНИЯ АУДИТА СИСТЕМ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ ЭЛЕКТРОСВЯЗИ

Минск
«Бестпринт»
2025

УДК 62-758.38

Бойправ, В. А. Аспекты обеспечения аудита систем менеджмента информационной безопасности организаций электросвязи / В. А. Бойправ, О. В. Бойправ, Л. Л. Утин. – Минск: Бестпринт, 2025. – 116 с., ISBN 978-985-7267-46-0.

В монографии приведены критерии и подходы к реализации этапов аудита систем менеджмента информационной безопасности организаций электросвязи Республики Беларусь. Представлен порядок действий в рамках подготовки к проведению и проведения аудита указанных систем, а также выполнения анализа его результатов. Описаны разработанные модель процесса обработки результатов аудита, программное средство для анкетирования руководителей подразделений и служб в ходе проведения аудита, а также модель процесса оценки рисков безопасности информационных систем организаций электросвязи.

Монография предназначена для инженерно-технических и научных работников в сфере инфокоммуникационных технологий, студентов старших курсов и магистрантов, обучающихся по специальности «Информационная безопасность», а также аспирантов, обучающихся по специальности «Методы и системы защиты информации, информационная безопасность».

Рекомендована Научно-техническим советом БГУИР, протокол № 2 от 30.09.2025.

Рецензенты:
декан факультета довузовской подготовки учреждения образования «Белорусская государственная академия связи», доктор военных наук, профессор *М.В. Пылинский*;
начальник кафедры связи военного факультета учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», кандидат военных наук *М.М. Латушко*.

ISBN 978-985-7267-46-0

ОГЛАВЛЕНИЕ

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

ЗИ – защита информации
ИБ – информационная безопасность
ИС – информационная система
КВОИ – критически важный объект информатизации
ОАЦ – Оперативно-аналитический центр при Президенте Республики Беларусь
СЗИ – система защиты информации
СМИБ – система менеджмента информационной безопасности
ТНПА – технический нормативный правовой акт

ВВЕДЕНИЕ

Светлой памяти отца
и ученика посвящается

Согласно данным, представленным Национальным статистическим комитетом Республики Беларусь [1], более 95 % организаций страны используют услуги доступа к сетям электросвязи в рамках своих бизнес-процессов: для эффективного поиска или предоставления информации, пользования ресурсами электронной почты, осуществления банковских операций, построения систем электронного документооборота, а также налаживания процессов обращения к элементам виртуальной инфраструктуры. Практический опыт работы Бойправа Владимира Андреевича в различных организациях электросвязи Республики Беларусь (трест «Белсвязьстрой», Министерство связи и информатизации, РУП «Белтелеком», СООО «СМУ Союзтелефонстрой») подтвердил, что размер прибыли подавляющего большинства организаций напрямую зависит от своевременности и качества предоставляемых ими услуг доступа к сетям электросвязи. Даже небольшие перерывы в связи, вызванные сбоями в работе аппаратуры, повреждениями в линиях передачи и другими причинами, приводят к прямым и косвенным затратам, срывам выгодных контрактов и потери репутации. В соответствии с Концепцией информационной безопасности Республики Беларусь [2], наиболее серьезная причина снижения эффективности функционирования сетей электросвязи, как составляющих информационной инфраструктуры, обусловлена угрозами информационной безопасности. Согласно Закону Республики Беларусь от 19 июля 2005 г. № 45-З «Об электросвязи» [3], деятельность в области электросвязи в Республике Беларусь осуществляется на основе принципов тайны телефонных и иных сообщений, устойчивости и управляемости сетей электросвязи. Выполнение этих требований невозможно без применения эффективной системы защиты информации. Указанная система в первую очередь должна быть направлена на недопущение внедрения в сеть электросвязи и функционирования в составе этой сети аппаратных и программных средств с уязвимостями и / или недеклалированными возможностями, с применением которых нарушители информационной безопасности могут решать следующие задачи:

– получать точные координаты расположения аппаратных средств сетей электросвязи;

– управлять режимами функционирования аппаратных средств сетей электросвязи;

– выводить из строя аппаратные средства сетей электросвязи;

– вносить изменения в алгоритмы функционирования программных средств сетей электросвязи;

– осуществлять скрытые дублирование, накопление и передачу информации, циркулирующей в сетях электросвязи;

– снижать скорость обмена информацией между узлами сеттей электросвязи;

– искажать информацию, передаваемую по сетям электросвязи.

Таким образом, защита сетей электросвязи от угроз информационной безопасности является ключевой задачей, направленной на поддержание высокого уровня качества услуг электросвязи и снижение рисков потерь прибыли организациями, использующими такие услуги. Эффективность эксплуатации системы защиты информации сопряжена с созданием системы менеджмента информационной безопасности, а непрерывность ее совершенствования – с проведением аудита системы менеджмента информационной безопасности [4]. В соответствии с изложенным, можно отметить, что аудит системы менеджмента информационной безопасности является одним из основополагающих процессов в обеспечении эффективности защиты информации и функционирования сетей электросвязи.

Вопросам информационной безопасности уделяется большое внимание не только в нашей стране, но и рамках межгосударственного сотрудничества. На заседании коллегии Евразийской экономической комиссии, состоявшемся 12 марта 2019 г., был утвержден и предложен к использованию в странах Евразийского экономического союза перечень международных стандартов и рекомендаций в области обеспечения информационной безопасности, в том числе, в части проведения аудита систем менеджмента информационной безопасности [5]. Следует отметить, что указанный перечень, несмотря на его обширность, не является достаточным для проведения аудита систем менеджмента информационной безопасности в организациях Республики Беларусь. Это объясняется тем, что в процессе аудита необходимо учитывать не только требования международных стандартов и рекомендаций, но и требования национальных технических нормативных правовых актов в сфере защиты информации (в том числе требования независимого регулятора в сфере информационно-телекоммуникационных технологий – Оперативно-аналитического центра при Президенте Республики Беларусь), а также требования национального законодательства в отношении деятельности аудируемой организации.

В связи с вышеизложенным, в настоящее время, актуальной научной задачей является адаптация научно-методического обеспечения,

регламентирующего построение системы менеджмента информационной безопасности организаций и реализацию процесса ее аудита, под требования национального законодательства и выработки критериев его проведения. Кроме того, под требования национального законодательства необходимо адаптировать средства автоматизации, разрабатываемые и внедряемые в целях снижения временных и человеческих ресурсов при реализации процесса аудита системы менеджмента информационной безопасности организации.

В монографии представлены результаты исследования, направленного совершенствование модели аудита СМИБ организаций электросвязи Республики Беларусь путем разработки новых методов и средств реализации этого процесса, адаптированных под требования национального законодательства. Объектом указанного исследования был аудит системы менеджмента информационной безопасности, а предметом – методы и средства, используемые в рамках такого процесса.

ГЛАВА 1
СОВРЕМЕННЫЕ ПОДХОДЫ К АУДИТУ СИСТЕМ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1 Организация деятельности в отрасли связи в Республике Беларусь

В Республике Беларусь деятельность организаций электросвязи независимо от их форм собственности и индивидуальных предпринимателей, работающих в области электросвязи, регулируется Министерством связи и информатизации [6]. В его состав входят 13 организаций (из них коммерческих государственной формы собственности – 5, финансируемых из бюджета – 2, открытых акционерных обществ – 5, закрытых акционерных обществ – 1). Курирование деятельности этих организаций выполняется министром связи и информатизации или его заместителями (рисунок 1.1).

В состав организаций РУП «Белпочта», РУП «Белтелеком», ОАО «Белсвязьстрой», ОАО «Белремстройсвязь» входят филиалы, общее количество которых равно 30. Филиалы РУП «Белпочта» включают 90 узлов почтовой связи, филиалы РУП «Белтелеком» – 59 узлов электросвязи, в том числе 23 зональных и 23 районных узла [7]. Наличие большого количества обособленных структурных подразделений, их территориальная разобщенность и значительная протяженность линейно-кабельных сооружений существенно затрудняет решение всех задач менеджмента и особенно задач по обеспечению информационной безопасности (ИБ) [8, 9].

В отличие от продукции большинства промышленный предприятий, продукция организаций электросвязи является невещественной (т. е. она не может накапливаться на складах предприятия или дилерских центров), а процессы производства и потребления этой продукции неотделимы один от другого [10, 11, 12]. Поэтому можно сделать вывод, что своевременность и качество предоставления услуг организациями электросвязи будет реализовано в случае обеспечения непрерывности их функционирования. При этом должны быть соблюдены следующие основные принципы [3, 13]:

- доступность услуг электросвязи общего пользования;
- приоритет прав и законных интересов пользователей услуг электросвязи;
- равенство прав на получение услуг электросвязи;
- тайна телефонных и иных сообщений;
- устойчивость и управляемость сетей электросвязи;
- единство обязательных для соблюдения технических требований в области электросвязи;

- бесперебойность функционирования ИС, используемых для предоставления услуг электросвязи;

- защита ИС, используемых для предоставления услуг электросвязи, с помощью средств, прошедших подтверждение соответствия требованиям технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY) в форме сертификации или декларирования соответствия.

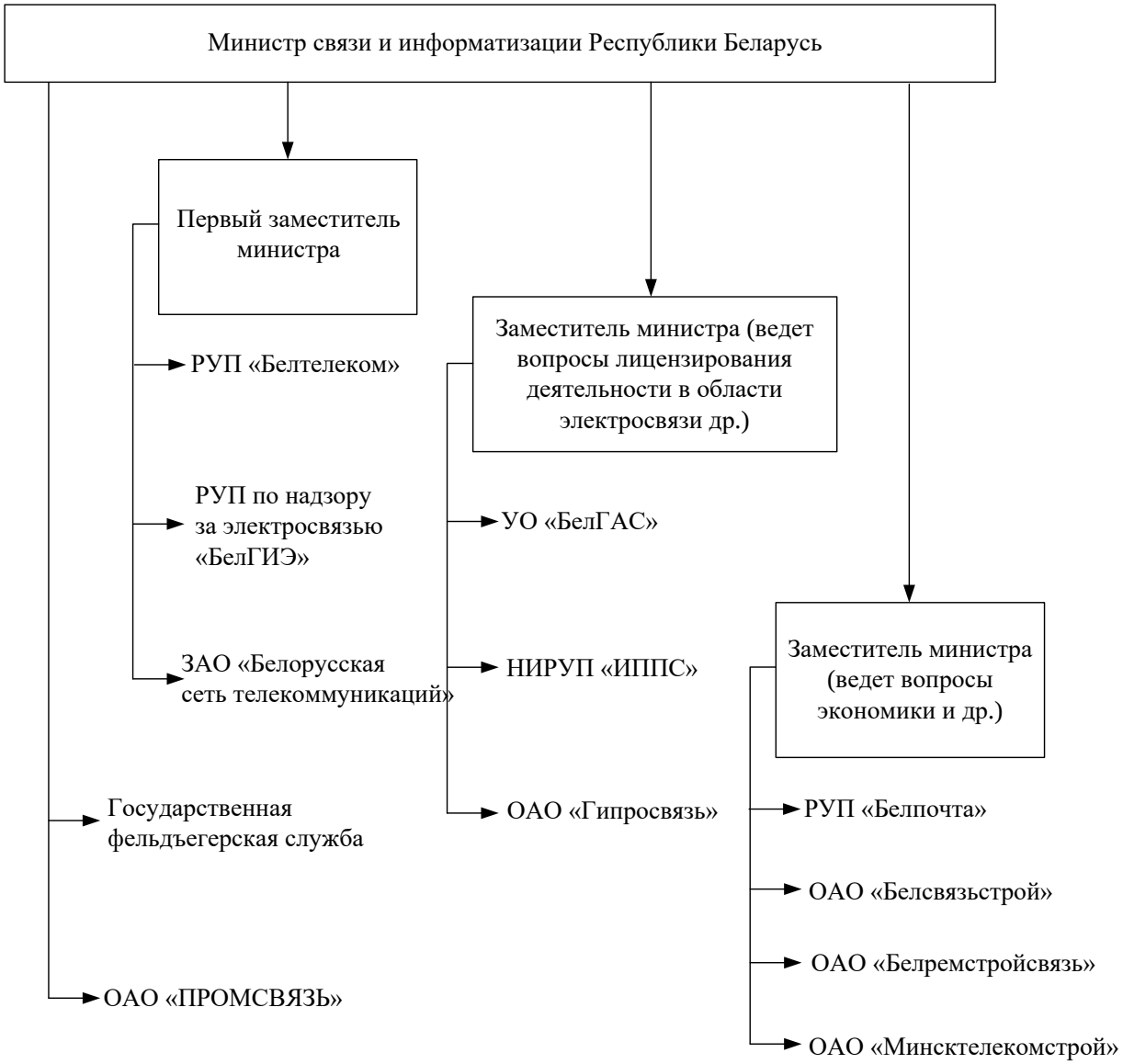

Рисунок 1.1. – Система курирования деятельности организаций, входящих в состав Министерства связи и информатизации Республики Беларусь

Государственное регулирование в области электросвязи осуществляется Президентом Республики Беларусь, Советом Министров Республики Беларусь, Министерством связи и информатизации Республики Беларусь, Оперативно-аналитическим Центром при Президенте Республики Беларусь (ОАЦ). Также на указанных субъектов возложена задача государственного регулирования

в области защиты информации (ЗИ), в том числе информации, передаваемой по сетям электросвязи [14].

Несмотря на большое количество государственных регуляторов в области ЗИ, основная работа в этой области выполняется ОАЦ, который имеет полномочия разрабатывать проекты технических нормативных правовых актов по вопросам технической и криптографической защиты информации, а также принимать (издавать) такие акты.

Следовательно, можно сделать вывод, что в Республике Беларусь при реализации процессов, связанных с ЗИ в организациях электросвязи, в первую очередь, необходимо руководствоваться документами (постановлениями, положениями и приказами) ОАЦ, так как данным субъектом осуществляется государственное регулирование как в области электросвязи, так и в области ЗИ. На начальном этапе любого процесса, связанного с разработкой мер по ЗИ, необходимо реализовывать анализ уязвимостей.

1.2 Модели угроз безопасности информационных систем организаций электросвязи и вектора атак, направленных на эти системы

Установлено, что основными причинами угроз безопасности ИС организаций электросвязи, могут быть следующие.

1. Побочные электромагнитные излучения средств и линий электросвязи.
2. Выход из строя средств и/или линий электросвязи ввиду их производственных дефектов (в том числе дефектов, обуславливающих их незащищенность от внешних факторов).
3. Нарушение работоспособности или ошибки в проектировании систем охранной и пожарной сигнализации, относящихся к комплексу средств безопасности критически важных объектов информатизации (КВОИ).
4. Полное или частичное несоблюдение требований к технической укрепленности ИС или их отдельных конструктивных элементов [15] (линий электросвязи, используемых для соединения КВОИ, расположенных в пределах разных контролируемых зон).
5. Некорректные подключение и настройка средств электросвязи.
6. Нарушение контрольно-пропускного режима в пределах контролируемой зоны ИС [16].
7. Нарушение порядка перемещения лиц, не относящихся к числу сотрудников организации, в пределах контролируемой зоны ИС.

8. Преднамеренное или непреднамеренное повреждение средств и линий электросвязи лицами из числа внутренних или внешних нарушителей.

9. Замедление процесса реализации мероприятий по устранению повреждений средств и линий электросвязи.

10. Разглашение сотрудниками организации сведений о местах расположения и технических характеристиках средств, линий и сооружений электросвязи как активов ИС, о заказчиках и ходе работ по строительству линий и сооружений электросвязи и пуско-наладке средств электросвязи.

11. Преднамеренное или непреднамеренное разглашение сотрудниками организации третьим лицам данных об абонентах из числа как физических, так и юридических лиц [17].

12. Преднамеренное или непреднамеренное разглашение сотрудниками организации третьим лицам данных об используемых в организации системах тарификации услуг электросвязи [18].

13. Побочные электромагнитные излучения средств вычислительной техники, используемых для создания, обработки и хранения электронных документов и баз данных, в которых содержится информация, распространение и (или) предоставление которой ограничено.

14. Невыполнение разграничения доступа к электронным документам и базам данных, в которых содержится информация, распространение и (или) предоставление которой ограничено.

15. Невыполнение шифрования электронных документов и баз данных, в которых содержится информация, распространение и (или) предоставление которой ограничено.

16. Несвоевременное обновление программных средств, относящихся к комплексу системе защиты информации (СЗИ).

17. Отсутствие или неиспользование выделенных помещений для проведения переговоров.

Таким образом, потенциальные угрозы ИС организаций электросвязи обусловлены:

- уязвимостями активов ИС;

- несоблюдением пользователями ИС требований о неразглашении сведений, связанных с особенностями их функционирования и эксплуатации и с содержанием обрабатываемой информации;

- несоответствием ИС требованиям, изложенным в актуальных нормативных правовых актах, связанных с обеспечением безопасности ИС (в частности, в Положении об обеспечении безопасности КВОИ и Положении о порядке технической защиты информации в информационных системах, предназначенных для обработки информации,

распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам).

Активы ИС могут быть условно разделены на следующие категории [19]:

- аппаратные;
- программные;
- аппаратно-программные;
- обрабатываемая информация;
- реализуемые информационные процессы.

На рисунке 1.2 представлен перечень активов ИС организаций электросвязи Республики Беларусь.

Рисунок 1.2. – Перечень активов ИС организаций электросвязи

Уязвимости аппаратных и аппаратно-программных активов рассматриваемых ИС связаны со следующими особенностями их реализации и эксплуатации:

- выход из строя ввиду производственных дефектов;
- некорректное подключение;
- несвоевременность устранения повреждений;
- незащищенность от побочного электромагнитного излучения.

Уязвимости программных активов со следующими их недостатками:

- ошибки в программных кодах, позволяющие злоумышленнику реализовать несанкционированный доступ в ИС либо внедрить вредоносное программное обеспечение;

- ошибки в программных кодах, приводящие к сбою процессов функционирования программных активов;

- некорректность настроек;

- несовместимость программных активов друг с другом (в том числе с операционными системами, используемыми для управления ИС).

Уязвимости информационных процессов, реализуемых в рамках рассматриваемых ИС, связаны как с представленными выше уязвимостями, так и с:

- несовершенством используемых алгоритмов шифрования;

- ошибками проектирования ИС и СЗИ.

Таким образом, источниками угроз безопасности ИС орагнизаций электросвязи являются:

1) лица, относящиеся к числу сотрудников организации (внутренние нарушители);

2) лица, не относящиеся к числу сотрудников организации (внешние нарушители);

3) неблагоприятные погодные условия и природные катаклизмы.

Результатом реализации угроз безопасности ИС, исходящих от внутренних или внешних нарушителей, является нарушение свойств конфиденциальности, целостности, доступности, подлинности и сохранности информации, обрабатываемой в этих системах.

Результат реализации угроз, источником которых являются неблагоприятные погодные условия и природные катаклизмы – нарушение свойств целостности и доступности информации, обрабатываемой в таких системах [20, 21, 22].

Для анализа векторов атак на ИС (в том числе ИС организаций электросвязи) необходимо использовать следующие классификационные признаки: 1) объект воздействия; 2) характер реализации; 3) продолжительность реализации; 4) путь реализации.

В зависимости от первого классификационного признака можно выделить следующие разновидности атак на ИС:

- атаки, направленные на аппаратные средства ИС;

- атаки, направленные на программные (аппаратно-программные) средства ИС;

- атаки, направленные на информационные технологии, реализуемые в ИС;

- атаки, направленные на информационные ресурсы.

В зависимости от второго классификационного признака можно выделить следующие разновидности атак на ИС:

- случайные;
- целенаправленные.

В зависимости от третьего классификационного признака можно выделить следующие разновидности атак на ИС:

- быстрые;
- медленные.

В зависимости от четвертого классификационного признака можно выделить следующие разновидности атак на ИС:

- реализуемые непосредственно (т. е. путем физического доступа);
- реализуемые опосредованно:
    - локально (через локальную сеть)
    - удаленно (через смежную или глобальную сеть).

Следует отметить, что, как правило, случайные атаки являются быстрыми, а целенаправленные – медленными.

Случайная и быстрая атака включает в себя следующие этапы: 1) разведка; 2) подготовка ресурсов; 3) доставка; 4) эксплуатация; 5) установка; 6) управление и контроль; 7) воздействие.

Процесс реализации целенаправленной и медленной атаки, как правило, включает в себя два дополнительных этапа по сравнению с процессом реализации случайной и быстрой атака. Такими этапами являются проектирование и предотвращение обнаружения. Наличие этапа проектирования в рамках атаки рассматриваемого типа основывается на том факте, что в ходе ее реализации нарушители информационной безопасности стремятся собрать как можно больше информации об объекте воздействия из социальной среды или других источников до момента подготовки ресурсов. Наличие этапа предотвращения обнаружения в рамках атаки рассматриваемого типа основывается на том факте, что нарушители информационной безопасности стремятся оставаться незамеченным с той целью, чтобы усложнить для пользователей атакованной ИС идентификацию атаки.

Таким образом, целенаправленная и медленная атака включает в себя следующие этапы: 1) проектирование; 2) разведка; 3) подготовка ресурсов; 4) доставка; 5) эксплуатация; 6) предотвращение обнаружения; 7) установка; 8) управление и контроль; 9) воздействие.

В совокупности причисленные этапы атак каждого из типов представляют собой вектор атаки.

В работе [23] определено, что в настоящее время наиболее вероятными атаками, направленными на ИС организаций электросвязи, используемые для предоставления услуг (в соответствии с прямым переводом текста указанной работы – телекоммуникационные системы) являются следующие:

- системная инсайдерская атака;
- DDoS-атака;
- сканирование портов;
- атака по бэкдор-каналу;
- атака, направленная на получение root-прав;
- атака на виртуальную машину или гипервизор.

В таблице 1.1 представлен результат анализа векторов указанных атак с использованием представленных классификационных признаков.

Таблица 1.1 – Результат анализа векторов потенциальных атак на ИС организаций электросвязи, используемые для предоставления услуг

Наименование атаки	Характер реализации	Продолжительность реализации	Объект воздействия	Путь реализации
1	2	3	4	5
Системная инсайдерская атака	Целенаправленная	Медленная	Аппаратные средства, программные (аппаратно-программные) средства, информационные технологии, информационные ресурсы	Непосредственно (физический доступ)
DDoS-атака	Целенаправленная	Медленная	Информационные технологии	Опосредованно удаленно (через смежную или глобальную сеть)

Продолжение таблицы 1.1

1	2	3	4	5
Сканирование портов	Целенаправленная	Медленная	Программные средства	Опосредованно удаленно (через смежную или глобальную сеть)
Атака по бэкдор-каналу	Целенаправленная	Медленная	Программные средства	Опосредованно удаленно (через смежную или глобальную сеть)
Атака, направленная на получение root-прав	Целенаправленная	Медленная	Программные средства	Опосредованно удаленно (через смежную или глобальную сеть)
Атака на виртуальную машину или гипервизор	Целенаправленная	Медленная	Программные средства	Опосредованно удаленно (через смежную или глобальную сеть)

Таким образом, на основе результатов проведенного анализа было установлено, что в настоящее время вектора потенциальных атак на ИС организаций электросвязи, используемые для предоставления услу, чаще всего направлены на программные средства и реализуются опосредованно удаленно (через смежную или глобальную сеть). Следует отметить, что при решении задачи, связанной с устранением уязвимостей ИС, необходимо использовать комплексный подход, включающий в себя применение не только технических и правовых, но и организационных мер по ЗИ [24, 25]. Решающая роль при решении этой задачи принадлежит аудиту системы менеджмента информационной безопасности (СМИБ), по результатам которого представляется возможным оценить эффективность функционирования системы защиты информации (СЗИ) в целом и при необходимости внести соответствующие корректировки в ее состав [26, 27].

1.3 Роль аудита систем менеджмента информационной безопасности в реализации процесса защиты информации

В Республике Беларусь обеспечение ИБ является одной из составляющих процесса обеспечения национальной безопасности [28]. В связи с этим реализация процесса ЗИ является одной из задач, которую нужно решать в целях обеспечения национальной безопасности. Указанный процесс является многоэтапным. Основными его этапами являются следующие:

1) создание СЗИ;

2) создание СМИБ;

3) проведение аудита СМИБ;

4) реализация действий корректирующего характера.

В таблице 1.2 представлены ссылки на документы, регламентирующие процесс реализации каждого из указанных этапов.

Таблица 1.2. – Ссылки на документы, регламентирующие процесс реализации каждого из этапов процесса ЗИ

Номер этапа	Ссылка (-и) на документ (-ы)
1	[29]
2	[30–36]
3	[4, 37–39]
4	[7–14]

Процесс создания СЗИ в соответствии с [7] представлен на рисунке 1.3 в виде графической нотации. На этом и последующих аналогичных рисунках использованы условные обозначения, предусмотренные в рамках системы BPMN (от англ. Business Process Model and Notation), применяемой для описания моделей различных бизнес-процессов.

Рисунок 1.3. – Графическая нотация процесса создания СЗИ в соответствии с Положением

Описание процесса, представленного на рисунке 1.3, может быть дополнено с помощью следующей математической нотации:

$$IPS = \{IPS \mid f\,(PSP, PSC)\},$$

где *IPS* – процесс построения СЗИ, свойства которого функционально зависят от следующих процессов: проектирование СЗИ (*PSP*); создание СЗИ (*PSC*).

Процессы, определяющие свойства процесса создания СЗИ могут быть описаны с помощью следующих математических нотаций.

$$PSP = \{PSP \mid f\,(isfs, \{isp \mid f\,(ipa, isc, uq, oisi)\}, \{trd \mid f\,(isc, ipsr, oisio, cmipr)\},$$

где *isfs* – совокупность сведений о структуре информационной системы (ИС) и информационных потоков;

isp – процесс разработки политики ИБ, свойства которого функционально зависят от:

ipa – совокупность целей и принципов ЗИ;

isc – перечень используемых типовых ИС;

uq – количество пользователей ИС;

oisi – наличие взаимодействия ИС с другими ИС;

trd – процесс разработки технического задания на построение СЗИ, свойства которого функционально зависят от перечня используемых типовых ИС, а также от:

ipsr – требования к СЗИ;

oisio – порядок взаимодействия ИС с другими ИС (при наличии такого взаимодействия);

cmipr – требования к криптографическим СЗИ.

$$PSC = \{PSC \mid f\,(\{tcmi \mid f\,(trc)\}, \{ipsdd \mid f\,(trc, ad, ib, mp, rdu, emu, ipmu, ism, iser, ckm)\})\}$$

где *tcmi* – процесс внедрения средств технической и криптографической ЗИ, свойства которого функционально зависят от содержания технического задания на построение СЗИ (*trc*);

ipsdd – процесс внедрения средств технической и криптографической ЗИ, свойства которого функционально зависят от содержания технического задания на построение СЗИ (*trc*), а также от применяемых принципов:

ad – разграничения доступа пользователей к объектам ИС;

ib – резервирования и уничтожения информации;
mp – защиты от вредоносного программного обеспечения;
rdu – использования съемных носителей информации;
emu – использования электронной почты;
ipmu – обновления средств ЗИ;
ism – мониторинга за функционированием ИС и СЗИ;
iser – осуществления контроля, реагирования на события информационной безопасности и ликвидации их последствий;
ckm – управления криптографическими ключами.

Из представленной математической нотации видно, что создание СЗИ является, по своей сути, многофакторным процессом, ряд факторов которого есть результат реализации дополнительных подпроцессов. В случае непринятия мер по совершенствованию СЗИ в процессе эксплуатации ее эффективность снижается. Это обусловлено ежегодным увеличением количества регистрируемых уязвимостей ИС, что наглядно продемонстрировано на рисунке 1.4 [40].

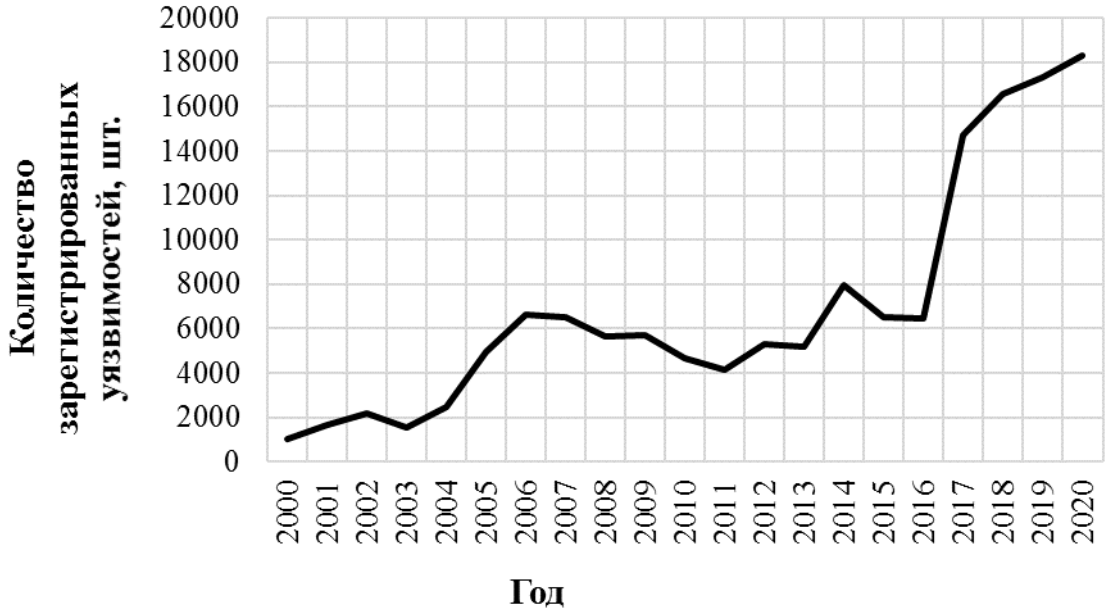

Рисунок 1.4. – Статистическая кривая динамики количества зарегистрированных уязвимостей за 2000–2020 годы

Повышение эффективности использования СЗИ в ходе ее эксплуатации обеспечивается за счет построения и реализации СМИБ [41, 42]. Графическая нотация процесса построения СМИБ представлена на рисунке 1.5.

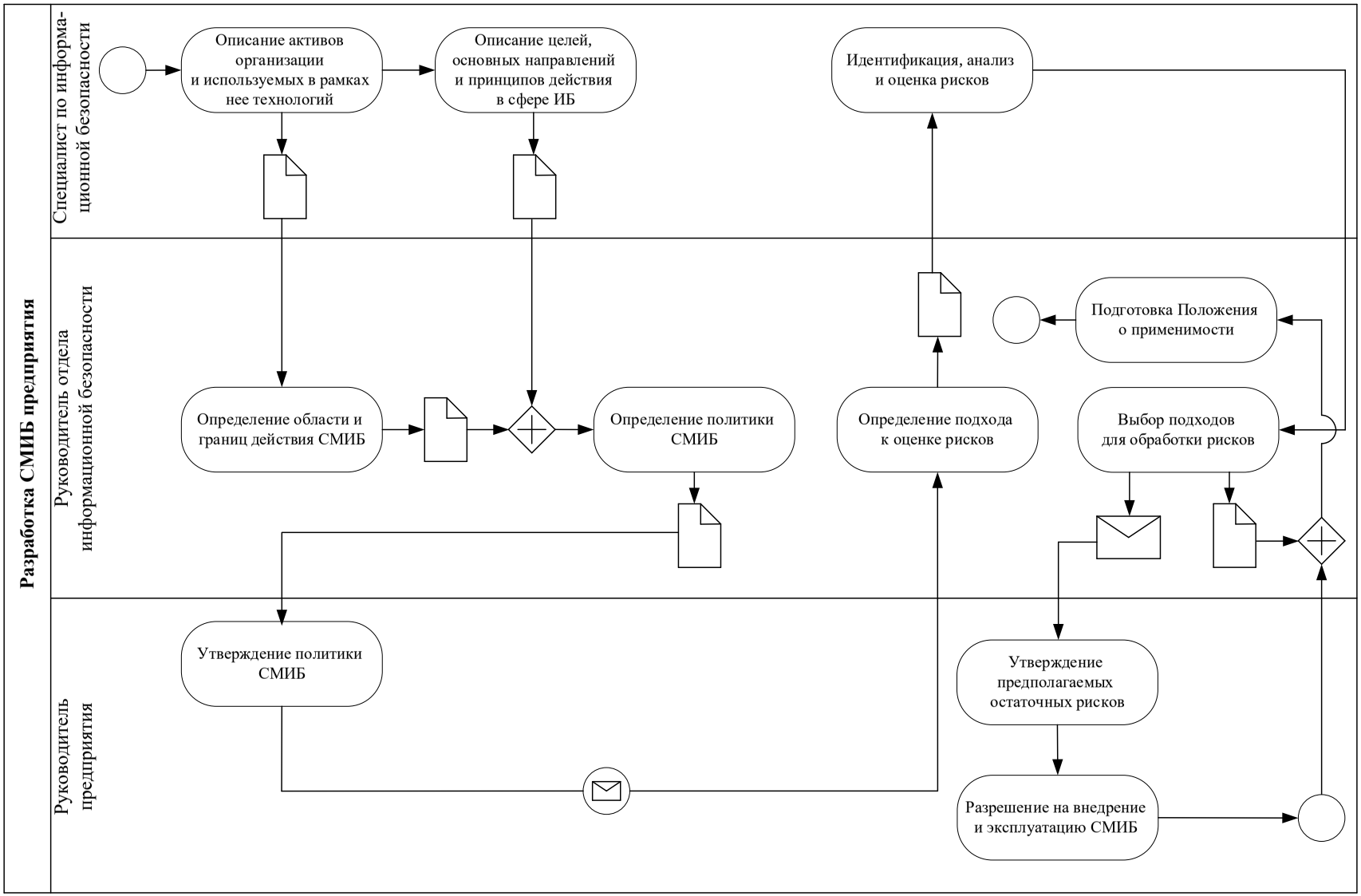

Рисунок 1.5. – Графическая нотация процесса построения СМИБ в соответствии с СТБ ISO/IEC 27001-2016

Описание представленного на рисунке 1.5 процесса может быть дополнено с помощью следующей математической нотации:

$$ISMS = \{ISMS \mid f(a, b, c, d, e, ch, p, g, jp)\},$$

где *ISMS* – процесс построения СМИБ, свойства которого функционально зависят от следующих процессов:

- определение области границ действия СМИБ (*a*);
- определение политики СМИБ (*b*);
- определение подходов к оценке рисков (*c*);
- идентификация рисков (*d*);
- анализ и оценка рисков (*e*);
- выбор вариантов обработки рисков (*ch*);
- выбор целей и мер управления для обработки рисков (*g*);
- подготовка Положения о применимости (*jp*).

Процессы, определяющие свойства процесса *ISMS*, могут быть описаны с помощью представленных ниже математических нотаций.

$$a = \{a \mid f(bc, oc, lc, ac, tc)\},$$

где *bc, oc, lc, ac, tc* – свойства, от которых функционально зависят свойства процесса *a* (соответственно характеристика бизнеса, характеристика организации, характеристика расположения организации, характеритсика активов организации, характеристика технологий, применяемых в организации).

$$b = \{b \mid f(conc, sr, rm)\},$$

где *conc, sr, rm* – свойства, от которых функционально зависят свойства процесса *b* (соответственно концепция организации в сфере ИБ, нормативно-правовые требования и договорные обязательства в сфере ИБ, стратегическое содержание менеджмента рисков организации).

$$c = \{c \mid f(\{m \mid f(oc, sr)\}, rc, rl)\},$$

где *m* – процесс определения методики оценки риска, подходящей для СМИБ, свойства которого функционально зависят от характеристики организации и нормативно-правовых требований в сфере ИБ;

rc – критерии принятия риска;

rl – приемлемые уровни риска.

$$d = \{d \mid f\,(ac, oai, ti, vi, ci)\},$$

где *ac, oai, ti, vi, ci* – свойства, от которых функционально зависят свойства процесса *d* (соответственно характеристика активов организации, сведения о владельцах активов организации, угрозы, которые могут воздействовать на активы организации, уязвимости активов организации, сведения о последствиях воздействия угроз на активы организации, связанных с нарушением свойств конфиденциальности, целостности и доступности этих активов).

$$e = \{e \mid f\,(od, p, rl)\},$$

где *od, p, rl* – свойства, от которых функционально зависят свойства процесса *e* (соответственно сведения об ущербе для деятельности организации в результате воздействия на ее активы угроз, вероятность сбоя обеспечения безопасности организации в результате воздействия на ее активы угроз, сведения об уровне риска).

$$ch \in \{ch_1, ch_2, ch_3, ch_4\},$$

f_1, f_2, f_3, f_4 – составляющие множества вариантов обработки рисков, среди которых необходимо сделать выбор наиболее подходящего для организации варианта (к этим вариантам соответственно относятся применение подходящих мер управления, принятие рисков, избегание рисков, передача рисков сторонним организациям).

$$g = \{g \mid f\,(rc, sr)\}.$$

$$jp = \{jp \mid f\,(ha, ia)\},$$

где *ha, ia* – свойства, от которых функционально зависят свойства процесса *jp* (соответственно факт утверждения руководителем организации предполагаемых остаточных рисков, факт получения разрешения от руководства на внедрение и эксплуатацию СМИБ).

Из представленных графической и математической нотаций следует, что процесс построения СМИБ основан на реализации следующих мероприятий:

- оценка рисков информационной безопасности в целях выбора адекватных методов и средств для обеспечения информационной безопасности;

- обеспечение комплексного подхода к менеджменту информационной безопасности;

- обоснование для пользователей ИС необходимости непрерывной реализации мер, направленных на обеспечение защиты информации, циркулирующей в этой системе;

- активное предупреждение и выявление инцидентов в сфере информационной безопасности;

- назначение ответственности за нарушение правил обеспечения информационной безопасности.

Согласно СТБ ISO/IEC 27002-2012 [4], весь процесс реализации СМИБ можно разбить на 11 шагов.

Шаг 1. Принятие руководством организации решения о создании СМИБ.

Шаг 2. Решение организационных аспектов информационной безопасности.

Шаг 3. Организация менеджмента активов.

Шаг 4. Обеспечение безопасности, связанной с персоналом.

Шаг 5. Обеспечение физической безопасности и защиты от воздействий окружающей среды.

Шаг 6. Организация менеджмента коммуникаций и работ.

Шаг 7. Организация управления доступом к информации, средствам обработки информации и процессам бизнеса.

Шаг 8. Определение порядка приобретения, разработки и эксплуатации информационных систем.

Шаг 9. Обеспечение менеджмента инцидентов ИБ.

Шаг 10. Обеспечение менеджмента непрерывности бизнеса.

Шаг 11. Обеспечение соответствия.

Эффективность СМИБ снижается по мере эксплуатации этой системы по той же причине, по которой по мере эксплуатации снижается эффективность СЗИ. Повышение эффективности СМИБ обеспечивается за счет аудита СМИБ, как еще одного этапа процесса ЗИ [43].

На рисунке 1.6 представлен алгоритм, отображающий взаимосвязь между основными этапами процесса ЗИ.

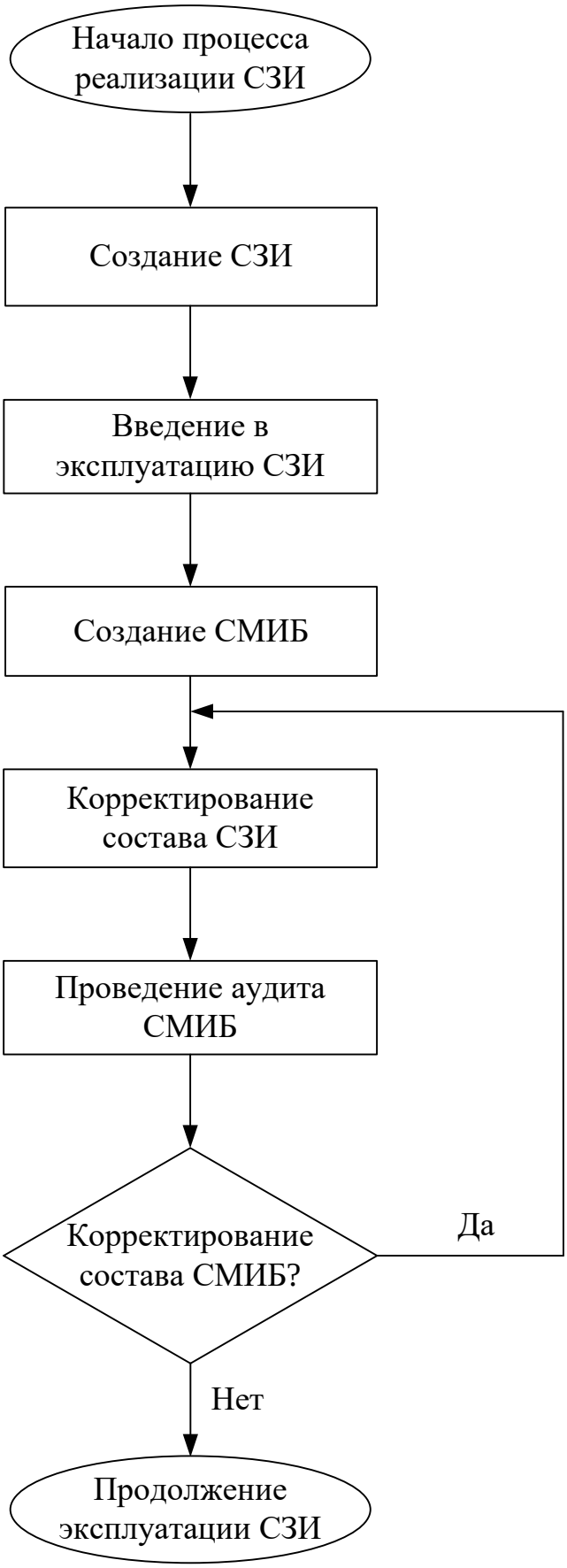

Рисунок 1.6. – Алгоритм реализации процесса ЗИ

Из рисунка 1.6 следует:

1) процесс ЗИ является процессом с обратной связью;

2) обратная связь процесса ЗИ направлена на поочередное повышение эффективности СМИБ и СЗИ, что в конечном итоге оказывает влияние на уровень обеспечиваемой с помощью этих систем защищенности информации;

3) обратная связь в процессе ЗИ есть результат реализации аудита СМИБ, как одного из этапов этого процесса.

Таким образом, аудит СМИБ является основополагающим в совокупности процессов по ЗИ, так как направлен на постоянное улучшение их эффективности [44, 45].

1.3 Анализ методов и средств проведения аудита системы менеджмента информационной безопасности

Путем проведения аудита СМИБ организации можно оценить текущее состояние самой этой системы, а также состояние безопасности принадлежащей аудируемой организации информации, распространение и (или) предоставление которой ограничено [46, 47]. По своей сути, аудит СМИБ является системным процессом получения объективных качественных или количественных оценок, характеризующих указанные состояния [48, 49].

Согласно ISO/IEC 27007:2020 «Информационная безопасность, кибербезопасность и защита конфиденциальности. Руководящие положения по проведению аудита систем менеджмента информационной безопасности» [4] процесс аудита СМИБ можно разбить на 5 шагов.

Шаг 1. Определить цели аудита.

Шаг 2. Разработать программу аудита.

Шаг 3. Реализовать программу аудита.

Шаг 4. Провести аудит согласно программе.

Шаг 5. Оценить компетентность аудиторов.

Порядок действий в рамках процесса реализации описанных шагов представлен в таблице 1.3.

Таблица 1.3. – Порядок действий в рамках процесса аудита системы менеджмента информационной безопасности

Номер шага	Действия, которые необходимо реализовать
1	Задокументировать описание целей аудита.
2	Определить роли и обязанности лица, осуществляющего менеджмент программы аудита. Определить компетентность лица, осуществляющего менеджмент программы аудита. Определить объем программы аудита. Идентифицировать и оценить риски программы аудита.
3	Определить цели, области и критерии для каждого конкретного аудита. Выбрать методы аудита. Сформировать группы по аудиту. Закрепить обязанности по проведению конкретного аудита за руководителем аудиторской группы.
3	Обеспечить управление выходными данными программы аудита. Обеспечить управление и поддержание записей программы аудита.
4	Установить первоначальный контакт с проверяемой организацией. Определить возможность проведения аудита. Выполнить анализ документов при подготовке к аудиту. Подготовить план аудита. Распределить работу между членами группы по аудиту. Выполнить анализ документов во время проведения аудита. Обеспечить обмен информацией в процессе проведения аудита. Определить роль и обязанности сопровождающих лиц и наблюдателей. Обеспечить сбор и верификацию информации. Сформировать выводы по результатам аудита. Подготовить заключения по результатам аудита. Провести заключительное совещание. Подготовить и разослать отчет по аудиту.
5	Определить компетентность аудитора для удовлетворения потребностей программы аудита. Оценить личные качества. Определить общие знания и навыки аудиторов системы менеджмента.

Из всех действий, представленных в таблице 1.3, основным является выбор метода проведения аудита СМИБ [50, с. 303]. Это обусловлено тем, что

выбор метода проведения аудита СМИБ определяет качество результатов последнего [51, 52].

Проведенный анализ литературных источников [31–35, 53, 54] показал, что на сегодняшний день можно выделить следующие методы проведения аудита СМИБ:

- экспертный (оценка степени соответствия СМИБ требованиям стандартов и нормативных правовых документов);
- активный (проведение анализа степени защищенности ИС с точки зрения злоумышленника, который обладает высокой квалификацией в исходной области).

Для повышения эффективности проведения аудита с помощью каждого из указанных методов в настоящее время разработано большое количество методик и средств [60, 61]. В таблице 1.4 представлен перечень этих методик и средств и соответствующих им методов аудита СМИБ.

Таблица 1.4. – Перечень методик и средств, используемых для проведения аудита СМИБ

Наименование методики (средства)	Метод аудита СМИБ, в ходе реализации которого используется методика (средство)
Методика CRAMM (CCTA Risk Analysis and Managment Method) и основанное на ней программное средство	Активный и экспертный метод
Методика FRAP (Facilitated Risk Analysis Process) и основанное на ней программное средство	Активный метод
Методика OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) и основанное на ней программное средство	Активный метод
Методика RiskWatch и основанное на ней программное средство	Экспертный метод
Методика COBRA и основанное на ней программное средство	Экспертный метод
Методика КОНДОР+ и основанное на ней программное средство	Экспертный метод

В таблице 1.5 представлены сведения об основных возможностях, которые могут быть обеспечены с использованием рассматриваемых методик.

Таблица 1.5. – Перечень возможностей, обеспечиваемых с использованием различных методик аудита СМИБ

	Методика CRAMM	Методика FRAP	Методика OCTAVE	Методика RiskWatch	Методика COBRA	Методика КОНДОР+
Оценка уровня информационных рисков	+	+	–	+	–	–
Оценка последствий от реализации угроз ИБ	+	+	+	–	–	–
Анализ состояния системы физической защиты ИС	–	–	–	+	–	–
Оценка соответствия ИС требованиям стандарта ISO 17799	+	–	–	+	+	+

На основании результатов анализа данных, представленных в таблицах 1.4 и 1.5 можно заключить, что большая часть современных методик и средств проведения аудита СМИБ связана с экспертным методом реализации этого процесса, в частности, с оценкой соответствия СМИБ требованиям стандартов.

Ниже приведено краткое описание указанных в таблицах 1.4 и 1.5 методик, на основе которого можно установить специфику каждой из них.

Методика CRAMM разработана в середине 80-х гг. XX в. Центральным агентством по компьютерам и телекоммуникациям Великобритании и является одной из первых методик, предложенных для использования в ходе аудита СМИБ коммерческих или правительственных

организаций [62]. На начальном этапе своего развития и использования эта методика основана выполнении проверки на соответствие ИС требованиям BS 7799 «Code of Practice for Information Security Management» и американского стандарта «Оранжевая книга», а также на выполнении комплексной (количественной и качественной) оценки рисков. На основе методики CRAMM разработано программное средство (рисунок 1.7), с помощью которого можно автоматизировать следующие процессы:

- идентификация активов ИС аудируемой организации;
- идентификация уязвимостей и угроз ИС, а также рисков ИБ аудируемой организации;
- оценка степени достаточности базовых мер для обеспечения ИБ;
- выбор оптимального с точки зрения стоимости набора контрмер для парирования рисков.

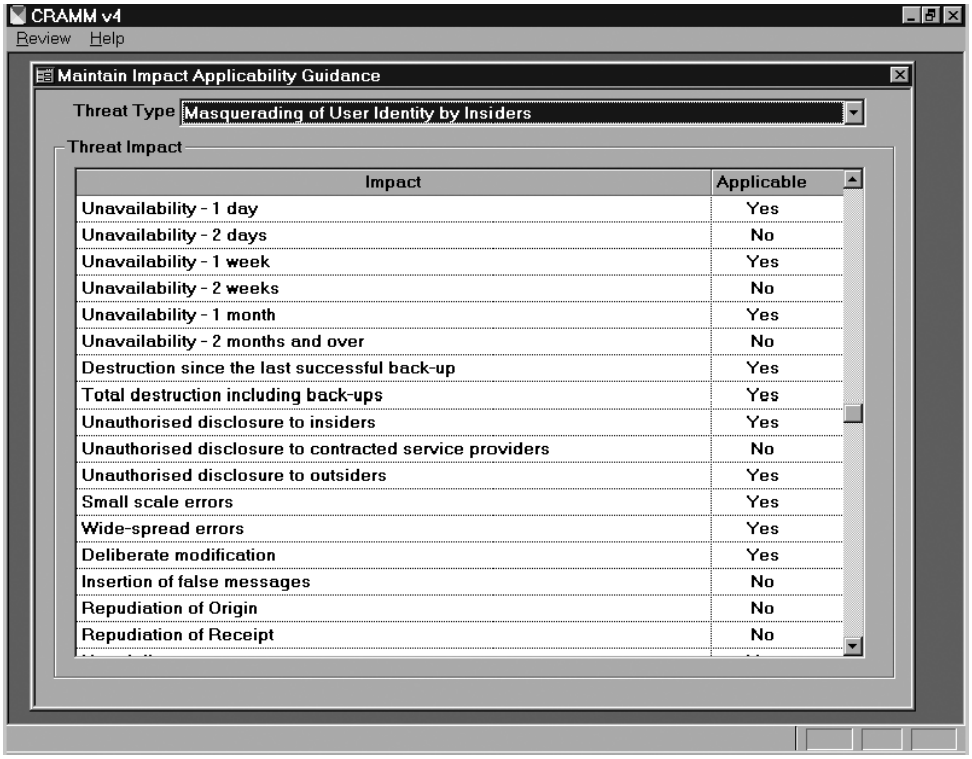

Рисунок 1.7. – Внешний вид окна программного средства, основанного на методике CRAMM [63]

Методика FRAP компании разработана американской компанией Peltier and Associates [64]. С помощью этой методики, так же, как и с помощью методики CRAMM, можно реализовать аудит СМИБ в рамках процесса управления рисками и поиска баланса между затратами средств на реализацию мероприятий по ЗИ и эффектом, получаемым в результате реализации этих мероприятий [65].

Методика OCTAVE разработана институтом Software Engineering Institute. Согласно этой методики, аудит проводится рабочей группой из числа сотрудников организации. Этот процесс заключается в выполнении всесторонней оценки последствий для организации от реализации различных угроз ИБ, а также в разработке (при необходимости) контрмер для парирования рисков ИБ, связанных с реализацией этих угроз [66].

Компания RiskWatch разработала многовекторную методику и основанное на ней семейство программных средств для проведения аудита СМИБ организаций [67]:

- RiskWatch for Physical Security (для анализа состояния системы физической защиты ИС);
- RiskWatch for Information Systems (для оценки уровня информационных рисков);
- HIPAA-WATCH for Healthcare Industry (для оценки соответствия ИС требованиям стандарта Healthcare Insurance Portability and Accountability Act);
- RiskWatch RW 17799 (для оценки соответствия ИС требованиям стандарта ISO 17799).

Методика COBRA разработана компанией C & A Systems Security Ltd. С помощью этой методики можно провести оценку степени соответствия ИС аудируемой организации требованиям стандарта ISO/IEC 17799:2005. Программное средство, основанное на рассматриваемой методике, представляет собой настраиваемый опросник (рисунок 1.8).

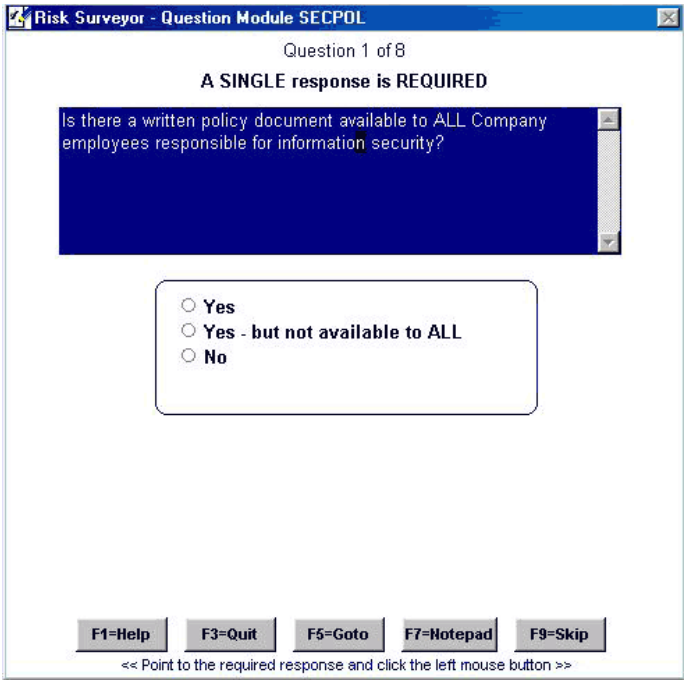

Рисунок 1.8. – Внешний вид окна основанного на методике COBRA программного средства с отображенным в нем вопросом

Методика КОНДОР+ разработана российской компанией Digital Security [68]. С помощью этой методики можно в рамках аудита СМИБ организации оценить степень соответствии ее политики ИБ требованиям ГОСТ Р ИСО/ИЭК 17799-2005. Программное средство, основанное на рассматриваемой методике, включает в себя базу анкетных вопросов, отвечая на которые аудитор имеет возможность формировать подробный отчет о состоянии политики ИБ проверяемой им организации (рисунок 1.9). В этом отчете содержится перечень положений политики ИБ, которые соответствуют требованиям ГОСТ Р ИСО/ИЭК 17799-2005, перечень положений, которые не соответствуют указанному стандарту, а также сведения об уровне риска ИБ, связанного с невыполнением не соответствующих требованиям стандарта положений политики ИБ [69].

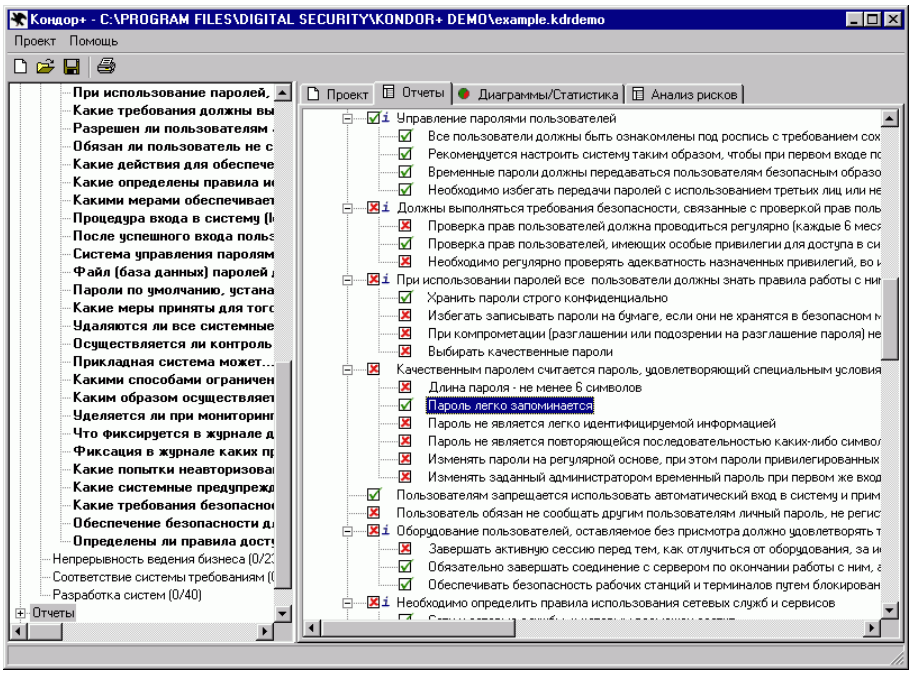

Рисунок 1.9. – Внешний вид окна основанного на методике КОНДОР+ программного средства с результатами ответа на анкетные вопросы

Таким образом, несмотря на наличие целого семейства международных стандартов ISO/IEC серии 27000, регламентирующих вопросы построения, менеджмента и аудита систем информационной безопасности, каждая страна разрабатывает собственные методы и средства оценки состояния ИБ, а также оценки эффективности СЗИ [70, 71, 72]. Это объясняет необходимость создания в Республики Беларусь собственных методик и программ аудита СМИБ базирующихся на национальном законодательстве, требованиях нормативных правовых документов, приказах и рекомендациях ОАЦ как независимого регулятора в области информационно-телекоммуникационных технологий [73].

1.4 Проблема проведения аудита систем менеджмента информационной безопасности организаций электросвязи Республики Беларусь

В Концепции информационной безопасности Республики Беларусь определено, что обеспечение информационной безопасности должно осуществляться в соответствии с государственной политикой в данной области, целью которой является достижение и поддержание такого уровня защищенности информационной сферы, который обеспечивает реализацию национальных интересов Республики Беларусь и ее прогрессивное развитие. Одна из ключевых задач достижения этой цели связана с осуществлением мониторинга, анализа и оценки состояния информационной безопасности, т. е. по сути с реализацией мероприятий по аудиту СМИБ.

На основе результатов анализа процессов, направленных на ЗИ, были установлены следующие проблемы.

1. В Республике Беларусь к настоящему времени не достаточно развита адаптированная модель процесса аудита СМИБ организаций, в которой были бы одновременно учтены принципы классификации информации, циркулирующей в пределах ИС, классификационные признаки последних, требования, изложенные в приказе ОАЦ от 20.02.2020 г. № 66, в Положении об отнесении объектов информатизации к критически важным и обеспечении безопасности КВОИ, утвержденное Указом Президента Республики Беларусь от 25 октября 2011 г. № 486 и в Положении об обеспечении безопасности КВОИ, утвержденном приказом ОАЦ от 12 октября 2018 г. № 151. В то же время указанных документов достаточно для того, чтобы выработать интегрированную схему указанного процесса.

2. Изложенные в современных международных стандартах рекомендации по построению СМИБ и проведению аудита этих систем носят общий характер и должны быть адаптированы для каждой группы конкретных предприятий с учетом специфики их деятельности и требований национальных нормативных, технических и правовых актов в сфере защиты информации [74, 75, 76, 77, 78, 79]. Процесс адаптации указанных рекомендаций целесообразно начинать с организаций, состояние информационной безопасности на которых напрямую определяет состояние национальной безопасности страны. К таким предприятиям относятся организации электросвязи, деятельность которых связана с разработкой, использованием и/или обслуживанием КВОИ.

Таким образом, научная задача представляемого исследования состояла в интегрировании требований нормативных технических правовых

актов (ТНПА) Республики Беларусь в сфере защиты информации и рекомендаций международных стандартов по проведению аудита СМИБ с целью выработки моделей реализации этого процесса для организаций электросвязи Республики Беларусь как одной из групп организаций, информационная безопасность которых напрямую определяет состояние национальной безопасности страны. Представленная научная задача может быть описана с помощью следующей математической нотации:

$$P = \{P \mid f\,(ir, (l = \{l \mid f(ipl, iscs, oaco, ciio)\}), z)\}, \qquad (1.1)$$

где P – процесс проведения аудита СМИБ в организациях электросвязи, свойства которого функционально зависят от:

ir – рекомендаций международных стандартов по проведению аудита СМИБ;

l – процесса интегрирования требования национального законодательства в сфере защиты информации, свойства которого функционально зависят от принципов классификации информации, изложенных в Законе Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации» (*ipl*), принципов классификации типовых информационных систем, изложенных в СТБ 34.101.30-2017 (*iscs*), требований по построению СЗИ, изложенных в приказе ОАЦ от 20 февраля 2020 г. № 66 с изменениями и дополнениями, утвержденными приказами Оперативно-аналитического центра при Президенте Республики Беларусь от 12 ноября 2021 г. № 195, от 29 декабря 2022 г. № 210, от 10 декабря 2024 г. № 259 (*oaco*), требований по обеспечению безопасности КВОИ, изложенных в Положении об отнесении объектов информатизации к критически важным и обеспечении безопасности КВОИ, утвержденное Указом Президента Республики Беларусь от 25 октября 2011 г. № 486 и в Положении об обеспечении безопасности КВОИ, утвержденном приказом ОАЦ от 12 октября 2018 г. № 151 (*ciio*);

z – требования законодательства Республики Беларусь, предъявляемых к порядку организации деятельности организаций электросвязи.

ГЛАВА 2
ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ АУДИТА СИСТЕМ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРИМЕРЕ ОРГАНИЗАЦИЙ ЭЛЕКТРОСВЯЗИ РЕСПУБЛИКИ БЕЛАРУСЬ

2.1 Анализ недостатков процесса аудита систем менеджмента информационной безопасности на примере организаций электросвязи Республики Беларусь

Установлено, что основными недостатками при проведении аудита СМИБ являются:

- наличие значительного количество разработанных стандартов (международных, государственных, отраслевых) в области ИБ, обуславливает способов их применения для обеспечения безопасности;
- необходимость выполнения интеграции принятых на территории Республики Беларусь международных стандартов, регламентирующих аудит СМИБ, и национальных ТПНА в сфере защиты информации и, как следствие, отсутствие единых критериев проведения аудита СМИБ базирующихся на национальных нормативных документах;
- противоречивость требований принятых на территории Республики Беларусь международных стандартов, регламентирующих аудит СМИБ, и требований национальных ТНПА в сфере защиты информации, что затрудняет как процесс интеграции документов указанных видов, так и процесс их одновременного использования в ходе проведения аудита СМИБ;
- исключение из процесса аудита СМИБ сотрудников и персонала, участвующих в создании информационной инфраструктуры (представителей проектных и строительных организаций);
- низкая заинтересованность руководителей организаций в процесс проведения аудита СМИБ и слабая их вовлеченность в этот процесс, вследствие чего руководители, как правило, ориентированы на снижение затрат как на регулярное проведение аудита СМИБ, так и на устранение обнаруженных в ходе аудита недостатков этой системы;
- высокий уровень затрат временных и человеческих ресурсов на проведение аудита СМИБ (как внутреннего, так и внешнего), что обусловлено как вышеперечисленными недостатками, так и отсутствием средств для автоматизации этого процесса.

Установлено, что в настоящее время основными принципами проведения аудита СМИБ является следующие [4, 80, 81, с. 75; 82, с. 32].

1. Принцип поэтапности. В соответствии с этим принципом процесс аудита должен быть структурирован в соответствии с требованиями, представленными в ISO/IEC 27007:2020 «Информационная безопасность, кибербезопасность и защита конфиденциальности. Руководящие положения по проведению аудита систем менеджмента информационной безопасности».

2. Принцип приоретизации. Согласно этого принципу, аудиту должны подлежать те активы, которые представляют наибольшую ценность для организации.

3. Принцип безупречности. Согласно этого принципу, аудиторам следует выполнять свою работу честно, старательно, беспристрастно и ответственно, оставаясь при этом справедливым и непредубежденным во всех своих действиях, устойчивым к любым влияниям, которые могут быть на них оказаны при выполнении аудита.

4. Принцип правдивого представления. Согласно этому принципу аудиторы обязаны представлять правдивые и точные отчеты. В отчетах следует отражать препятствия, встреченные в процессе аудита, а также неразрешенные мнения и разногласия между аудиторской группой и проверяемой организацией. Сообщения должны быть правдивыми, точными, объективными, своевременными, четкими и полными.

5. Принцип профессионализма. Согласно этому принципу аудиторам следует проявлять необходимую тщательность, уровень которой зависит от важности выполняемой задачи. В любых ситуациях, возникающих при проведении аудита, необходимо принимать профессиональные и обдуманные решения.

6. Принцип конфиденциальности. Согласно этому принципу аудиторам следует проявлять осторожность при использовании и защите информации, полученной в ходе выполнения своих обязанностей. Полученную информацию, нельзя использовать в корыстных целях аудитора, либо другим способом, который может нанести ущерб интересам аудируемой организации.

7. Принцип независимости. Согласно этому принципу аудиторам следует быть независимыми от деятельности аудируемой организации, действовать независимо от пристрастий и конфликта интересов. Заключения аудита должны быть объективны и основаны только на свидетельствах аудита.

8. Принцип основанности на свидетельстве. Согласно этому принципу аудиторы в процессепроведения аудита должны использовать рациональный метод достижения надежных и воспроизводимых заключений. Свидетельство аудита должно быть проверяемым иосновано на выборках

имеющейся информации, т.к. аудит проводится в ограниченный период времени и с ограниченными ресурсами.

9. Принцип риск-ориентированности. Согласно этому принципу аудиторы должны учитывать риски и возможности, которые могут оказать существенное влияние на планирование, проведение и отчетность по аудиту. Необходимо обеспечить уверенность, что аудит будет сфокусирован на вопросах, имеющих значение для заказчика.

Исходя из представленных недостатков, а также из результатов анализа организационных структур организаций электросвязи (см. раздел 1.1), были разработаны *новые принципы* проведения аудита СМИБ, направленные на совершенствование этого процесса, исключение характерных в настоящее время для него недостатков, а также на совершенствование существующих принципов проведения аудита СМИБ.

1. Принцип критеральности. Предложено использовать следующие документа для разработки критериев реализации аудита СМИБ организаций электросвязи Республики Беларусь:

- Закон Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации»;
- Закон Республики Беларусь от 19 июля 2010 г. № 170-З «О государственных секретах»;
- Положение об отнесении объектов информатизации к критически важным и обеспечении безопасности КВОИ, утвержденное Указом Президента Республики Беларусь от 25 октября 2011 г. № 486;
- Положение об обеспечении безопасности КВОИ, утвержденное приказом ОАЦ от 12 октября 2018 г. № 151;
- Постановление Совета Министров Республики Беларусь от 30.03.2012 № 293 «О некоторых вопросах безопасной эксплуатации и надежного функционирования критически важных объектов информатизации»;
- СТБ 34.101.30-2017 Информационные технологии. Методы и средства безопасности. Информационные системы. Классификация;
- Конституция Республики Беларусь;
- Закон Республики Беларусь от 19 июля 2005 г. № 45-З «Об электросвязи»;
- СТБ ISO/IEC 27001-2011 Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования;
- Положение о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, утвержденное приказом ОАЦ от 20 февраля 2020 г. № 66 с изменениями и

дополнениями, утвержденными приказами Оперативно-аналитического центра при Президенте Республики Беларусь от 12 ноября 2021 г. № 195, от 29 декабря 2022 г. № 210, от 10 декабря 2024 г. № 259.

Разработанные критерии реализации аудита СМИБ организаций электросвязи Республики Беларусь, основанные на указанных документах, описаны в разделе 2.2.

2. Принцип своевременности. В соответствии с этим принципом проведение аудита должно проводить как на регулярной, так и на внеплановой основе. Так как срок действия выдаваемых организациям Республики Беларусь сертификатов систем менеджмента качества составляет три года [83, 84, 85], то целесообразно реализовывать плановый аудит СМИБ организаций электросвязи Республики Беларусь с периодичностью один раз в три года. Внеплановое проведение аудита СМИБ целесообразно реализовывать после издания новых или внесения изменений и дополнений в нормативные документы в сфере ЗИ.

3. Принцип всеохватываемости. В соответствии с этим принципом в процессе аудита должны быть задействованы не только работники аудируемой организации, которые в рамках выполнения своих должностных обязанностей используют информационную систему (ИС), но и работники, которые обеспечивают создание и эксплуатацию инфраструктуры для этой системы.

4. Принцип единоначалия. В соответствии с этим принципом один из руководителей органов государственного управления или представителей руководства организаций электросвязи утверждает графики и регламенты проведения аудита СМИБ, а также принимать участие в реализации этого процесса и осуществлят его итоговый контроль. В случае, если аудит является внеплановым, то целесообразным представляется также организация его промежуточного контроля со стороны названных субъектов.

5. Принцип оптимизации. В соответствии с этим принципом необходимо принимать все возможные меры для сокращения временных и человеческих ресурсов на проведение аудита путем. Для этого необходимо использовать специальные программные средства для проведения аудита и опросные листы для сотрудников аудируемой организации, составленные на основе принципа разумной достаточности.

Применение предложенных принципов будет способствовать структурированности аудита СМИБ в организациях электросвязи Республики Беларусь.

Разработанные подходы к реализации этапов аудита СМИБ организаций электросвязи Республики Беларусь представлены в разделе 2.3.

2.2 Назначение критериев реализации аудита систем менеджмента информационной безопасности на примере организаций электросвязи Республики Беларусь

В таблице 2.1 представлено описание назначения основанных на представленных в разделе 2.1 критериев реализации аудита СМИБ организаций электросвязи Республики Беларусь.

Таблица 2.1. – Назначение критерией реализации аудита СМИБ организаций электросвязи Республики Беларусь

Наименования документов, регламентирующих критерии	Назначение критерия
1	2
Закон Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации» Закон Республики Беларусь от 19 июля 2010 г. № 170-З «О государственных секретах»	1. Наличие в организации информации, распространение и (или) предоставление которой ограничено. 2. Корректность применения основных терминов во внутренних документах организации, регулирующих ее деятельность, направленную на обеспечение ИБ.
Положение об отнесении объектов информатизации к критически важным и обеспечении безопасности КВОИ, утвержденное Указом Президента Республики Беларусь от 25 октября 2011 г. № 486	Наличие в организации ИС, относящихся к КВОИ, или выполнение сотрудниками организации работ на таких объектах
СТБ 34.101.30-2017 Информационные технологии. Методы и средства безопасности. Информационные системы. Классификация	Наличие в организации ИС, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам

Окончание таблицы 2.1.

1	2
Положение об обеспечении безопасности КВОИ, утвержденное приказом ОАЦ от 12 октября 2018 г. № 151. Постановление Совета Министров Республики Беларусь от 30.03.2012 № 293 «О некоторых вопросах безопасной эксплуатации и надежного функционирования критически важных объектов информатизации»	Наличие и корректность мер, применяемых для обеспечения безопасности КВОИ в ходе их эксплуатации (при их наличии в организации) или в ходе выполнения работ на таких объектах
Положение о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, утвержденное приказом ОАЦ от 20 февраля 2020 г. № 66 с изменениями и дополнениями, утвержденными приказами Оперативно-аналитического центра при Президенте Республики Беларусь от 12 ноября 2021 г. № 195, от 29 декабря 2022 г. № 210, от 10 декабря 2024 г. № 259	Наличие и корректность мер, применяемых для обеспечения безопасности данных, циркулирующих в ИС организации, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам (в том числе информации, составляющей тайну телефонных и иных сообщений, и баз данных операторов электросвязи (в соответствии со статьей 28 Конституции Республики Беларусь и статьями 54 и 56 закона Республики Беларусь от 19 июля 2005 г. № 45-З «Об электросвязи»)

2.3 Подходы к реализации этапов аудита систем менеджмента информационной безопасности на примере организаций электросвязи Республики Беларусь

В таблице 2.2 представлено описание разработанных подходов к реализации этапов аудита СМИБ организаций электросвязи Республики Беларусь, которое по своей сути является моделью процесса аудита СМИБ организаций электросвязи Республики Беларусь.

Таблица 2.2. – Подходы к реализации этапов аудита СМИБ

Номер этапа	Наименование этапа	Разработанный подход к выполнению этапа	Результаты этапа
1	2	3	4
1	Организация проведения аудита	Установление целей и задач проведения аудита в соответствии с его критериями (см. таблицу 2.1). Определение временных рамок аудита	План проведения аудита
2	Подготовка к проведению аудита	1. Установление перечня используемых в аудируемой организации КВОИ и ИС, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам.	1. Список аудируемых отделов (сотрудники которых при выполнении своих должностных обязанностей используют КВОИ или ИС, предназначенные для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам).

Продолжение таблицы 2.2

1	2	3	4
2	Подготовка к проведению аудита	2. Выбор с целью проверки внутренних документов организации. 3. Составление перечня анкетных вопросов для руководителей и сотрудников аудируемых отделов на основе документов, представленных в разделе 2.1.	2. Список сопровождающих лиц, ответственных за обеспечение доступа аудитора к КВОИ организации или ИС, предназначенным для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам. 3. Контрольные листы со списком анкетных вопросов для руководителей и сотрудников аудируемых отделов.
3	Проведение аудита	1. Опрос руководителей и сотрудников аудируемых отделов с использованием подготовленных контрольных листов. 2. Анализ процесса работы (краткое интервьюирование) сотрудников аудируемых отделов. 3. Проверка выбранных на этапе 2 документов.	Свидетельства аудита, в которых представлены данные о результатах проведенного опроса, а также результаты анализа процесса работы сотрудников и проверки внутренних документов организации

Продолжение таблицы 2.2

1	2	3	4
4	Анализ данных, полученных в ходе проведения аудита	1. Построение моделей угроз ИБ, характерных для используемых в организации КВОИ или ИС, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам. 2. Проверка данных, представленных в свидетельствах, на соответствие критериям аудита.	1. Описание угроз ИБ. 2. Перечень несоответствий.
5	Подготовка отчета по результатам аудита	Структурирование в единый документ данных, полученных в ходе проведения аудита	Проект отчета о результатах проведения аудита
6	Завершение аудита	Проверка данных, представленных в проекте отчета о результатах проведения аудита, на соответствие плану аудита	Утверждение отчета о результатах проведения аудита у лица, ответственного за его итоговый контроль

ГЛАВА 3
МЕТОДЫ ПРОВЕДЕНИЯ АУДИТА СИСТЕМ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРИМЕРЕ ОРГАНИЗАЦИЙ ЭЛЕКТРОСВЯЗИ РЕСПУБЛИКИ БЕЛАРУСЬ

3.1 Подготовка к проведению аудита систем менеджмента информационной безопасности на примере организаций электросвязи Республики Беларусь

Подготовка к проведению аудита СМИБ организаций электросвязи Республики Беларусь заключается в реализации следующего:

1) категорировать организации электросвязи Республики Беларусь в зависимости от специфики их деятельности;

2) определить классы ИС, которые используют сотрудники организаций каждой из категорий для выполнения своих должностных обязанностей (в соответствии с СТБ 34.101.30-2017 Информационные технологии. Методы и средства безопасности. Информационные системы. Классификация и Положением о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, утвержденном приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66 с изменениями и дополнениями, утвержденными приказами Оперативно-аналитического центра при Президенте Республики Беларусь от 12 ноября 2021 г. № 195, от 29 декабря 2022 г. № 210, от 10 декабря 2024 г. № 259);

3) определить документы, на основании которых необходимо составить вопросы для анкетирования сотрудников организаций электросвязи каждой из категорий в ходе проведения аудита.

Предложено категорировать организации электросвязи Республики Беларусь в зависимости от специфики их деятельности, важности ИС, которые используют их сотрудники для выполнения своих должностных обязанностей, а также в зависимости от количества этих организаций. К организациям категории 1 предложено относить организации, занимающиеся строительством сетей и сооружений электросвязи, к организациям категории 2 – организации, занимающиеся предоставлением услуг электросвязи, к организациям категории 3 – организации, занимающиеся проектированием сетей и сооружений электросвязи, к организациям категории 4 – организации, являющиеся органами, осуществляющими государственное регулирование и управление в области электросвязи.

Таблица 3.1. – Особенности использования ИС и их активов сотрудниками организаций электросвязи Республики Беларусь различных категорий

Категория организации	Классы используемых ИС [86]	Наименование активов ИС, используемых сотрудниками организации [87]	Особенности использования активов ИС сотрудниками организации
1	2	3	4
1	6-гос*, 5-частн*, 5-гос*, 3-ин*, 3-юл*, 3-дсп*, КВОИ*	Аппаратно-программные ресурсы (средства и линии электросвязи)	Строительство и пуско-наладка
2	5-частн*, 5-гос*, 4-ин, 4-юл, 4-дсп, 3-ин* , 3-юл*, 3-дсп*, КВОИ*	Информация (базы данных)	Хранение и обработка персональных данных абонентов
		Аппаратно-программные ресурсы (средства электросвязи)	Обслуживание и эксплуатация
3	5-гос, 4-юл 4-дсп, 3-юл, 3-дсп	Информация (документы и базы данных)	Создание, хранение и обработка данных, касающихся архитектуры сетей электросвязи, включая сведения об аппаратно-программных средствах, используемых в таких сетях
4	5-гос, 4-юл 4-дсп, 3-юл, 3-дсп	Информация (документы и базы данных)	Создание, хранение и обработка данных об организационно-техническом обеспечении функционирования сетей электросвязи, использовании радиочастотного спектра, а также о мероприятиях по защите сетей электросвязи от несанкционированного доступа к ним и передаваемым сообщениям

*ИС, используемые для предоставления услуг электросвязи

Установлено, что количество организаций, отнесенных к категории 1, в настоящее время значительно превышает количество организаций, отнесенных к категориям 2–4 (таблица 3.2) [88, 89, 90].

Таблица 3.2. – Количество организаций электросвязи различных категорий

Категория организации	Количество организаций указанной категории
1	1765
2	380
3	47
4	4

Значительно большее количество организаций категории 1 по сравнению с количеством организаций категорий 2–4 обусловлено отменой лицензий на осуществление деятельности по строительству объектов электросвязи. Значительная часть организаций категории 1 ранее осуществляла строительство промышленных и жилых объектов, но сокращение финансирования этого сектора экономики вынудило их изменить направление своей деятельности. Возросшая конкуренция на рынке строительства объектов электросвязи способствует снижению стоимости выполняемых работ, но одновременно обуславливает увеличение рисков ИБ. Принцип отбора подрядных организаций на выполнения работ по строительству объектов электросвязи не включает требований по наличию собственной СМИБ и не предусматривает проведение проверки эффективности ее функционирования. Мелкие и средние строительные компании постоянно прибегают к практике приема на работу специалистов, набранных по рекламным объявлениям, для реализации конкретных объектов. Складывающаяся практика приводит к бесконтрольному допуску большого количества случайных людей к аппаратным активам ИС различных классов, в том числе относящихся к КВОИ, что обуславливает потенциальную угрозу безопасности этих систем и дает возможность вмешаться в процесс их функционирования или вывести из эксплуатации. В связи с вышеизложенным организации, занимающиеся строительством сетей и сооружений электросвязи, предложено отнести к организациям категории 1.

Увеличение организаций, получивших лицензии на предоставление услуг электросвязи (рисунок 3.1), и имеющаяся у их сотрудников возможность доступа к средствам электросвязи, с помощью которых обрабатываются данные абонентов, обуславливают необходимость отнесения этих организаций к категории 2.

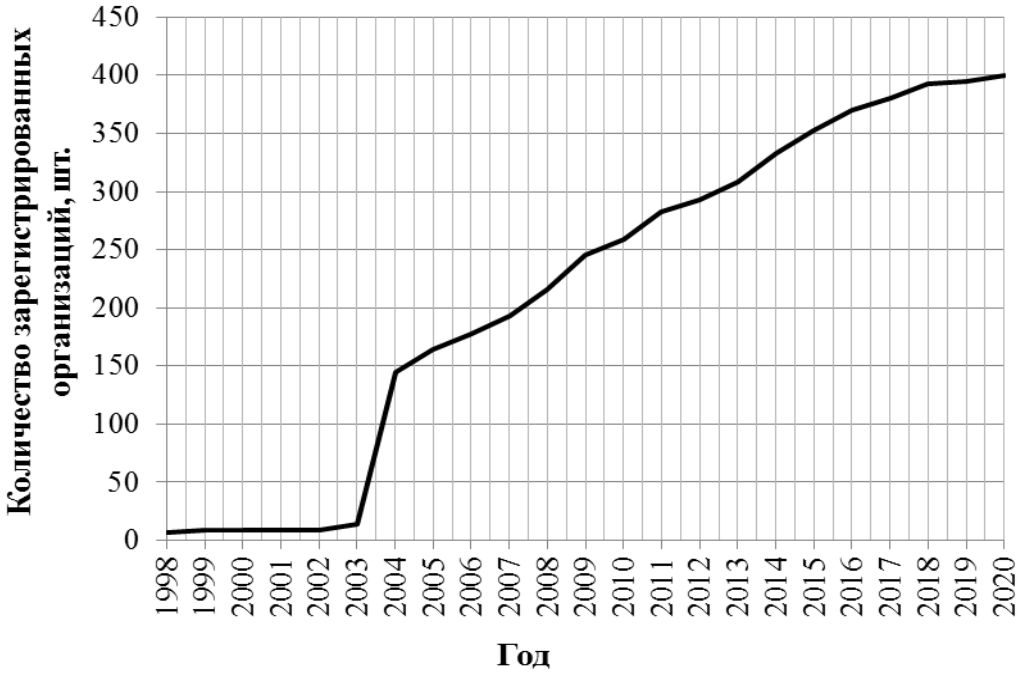

Рисунок 3.1. – Динамика изменения количества организаций, получивших лицензию на предоставление услуг электросвязи

Организации, занимающиеся проектированием объектов электросвязи, предложено отнести к категории 3 по причине того, что их сотрудники по сравнению с сотрудниками организаций категорий 1 и 2 имеют доступ к меньшему количеству активов ИС и не имеют доступа к КВОИ.

Органы государственного управления, занимающиеся регулированием в области электросвязи, отнесены к категории 4 из-за высокой квалификации сотрудников и наличия в их структуре специалистов по спецработе.

Категория организации электросвязи определяет перечень документов, на основании которых необходимо составлять анкетные вопросы для ее сотрудников, которые будут использованы при проведении аудита СМИБ такой организации.

Предложен следующий общий перечень документов для составления анкетных вопросов для сотрудников организаций электросвязи всех категорий.

1. СТБ ISO/IEC 27001-2016 Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

2. Положение об обеспечении безопасности критически важных объектов информатизации, утвержденное приказом ОАЦ от 12 октября 2018 г. № 151.

3. Положение о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено,

утвержденное приказом ОАЦ от 20 февраля 2020 г. № 66 с изменениями и дополнениями, утвержденными приказами Оперативно-аналитического центра при Президенте Республики Беларусь от 12 ноября 2021 г. № 195, от 29 декабря 2022 г. № 210, от 10 декабря 2024 г. № 259.

4. СТБ ISO/IEC 27000-2012 Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Основные положения и словарь.

5. Закон Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации».

6. Закон Республики Беларусь от 19 июля 2010 г. № 170-З «О государственных секретах».

7. Закон Республики Беларусь от 19 июля 2005 г. № 45-З «Об электросвязи».

8. Конституция Республики Беларусь.

9. ТКП 45-1.02-25-201-2014 Строительство. Проектная документация Состав и содержание.

Использование представленного перечня докментов будет способствовать соблюдению предложенного принципа критериальности в ходе проведения аудита СМИБ организаций электросвязи.

В таблице 3.3 определено, какие документы из приведенного перечня необходимо использовать для составления вопросов для анкетирования сотрудников организаций электросвязи каждой из категорий.

Таблица 3.3. – Перечень документов для составления вопросов для анкетирования сотрудников организаций электросвязи различных категорий

Категория организации электросвязи	Номер документа из приведенного перечня
1	1–7, 9
2	1, 3–8
3	1, 3–7
4	1, 3–7

Перечни анкетных вопросов, составленные в соответствии с указанными документами, представлены в разделе 3.2.

3.2 Проведение аудита систем менеджмента информационной безопасности организаций электросвязи Республики Беларусь

Как следует из таблицы 2.2, данные, которые должны быть получены при проведении аудита СМИБ, могут быть условно разделены на следующие группы:

- ответы сотрудников организации на анкетные вопросы, составленные на основании перечня документов, представленных в таблице 3.3 и систематизированные в контрольные листы;

- сведения об порядке реализации процесса работы с ИС, предназначенными для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам, полученные на основе результатов наблюдения за работой сотрудников аудируемых отделов;

- сведения о структуре внутренних документов организации, регламентирующих ее деятельность в сфере ИБ, а также о терминах, использованных для составления этих документах.

Сотрудники организаций электросвязи, которых следует отнести к кругу лиц, подлежащих опросу в ходе аудита СМИБ этих организаций:

- руководитель и главный инженер;

- начальник службы безопасности;

- старшие производители работ или начальники строительных участков (в случае, если аудируемая организация относится к категории 1);

- руководители подразделений и служб, специалисты которых работают с ИС, предназначенными для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам, полученные на основе результатов наблюдения за работой сотрудников аудируемых отделов (в случае, если аудируемая организация относится к категории 2, 3 или 4).

В приложении А представлены перечни вопросов, которые предложено включать в контрольные листы для анкетирования следующих лиц из числа сотрудников организаций электросвязи:

- руководители и главные инженеры организаций электросвязи категорий 1–4; .

- начальники службы безопасности организаций электросвязи категорий 1–4;

- старшие производители работ или начальники строительных участков организаций электросвязи категории 1.

Контрольные листы, предназначенные для анкетирования руководители подразделений и служб, специалисты которых работают с ИС, предназначенными для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам, должны включать в себя вопросы, сформулированные на основе перечня требований к системе защиты информации, подлежащих включению в частное техническое задание или задание по безопасности на ИС, представленного в Положении о порядке технической и криптографической

защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, утвержденное приказом ОАЦ от 20 февраля 2020 г. № 66 с изменениями и дополнениями, утвержденными приказами Оперативно-аналитического центра при Президенте Республики Беларусь от 12 ноября 2021 г. № 195, от 29 декабря 2022 г. № 210, от 10 декабря 2024 г. № 259.

Требования, изложенные в указанном Положении, по своей сути, определяют показатели безопасности информации, обрабатываемой с помощью таких ИС. Так как анкетирование руководители подразделений и служб направлено на установление факта выполнения (невыполнения) этих требований, то количество вопросов, ответы на которые необходимо получить от указанной категории лиц, составляет более 50 (по количеству требований, изложенных в Положении). В целях оптимизации и структурирования названного процесса выполнено следующее.

1. Условно разделены на 2 класса показатели безопасности, основанные на требованиях, изложенных в указанном Положении:

- общие показатели безопасности;
- частные показатели безопасности.

Для обозначения общих показателей безопасности предложено использование следующих наименований:

1) реализация организационных мер по защите информации;

2) использование средств технической и криптографической защиты информации;

3) обеспечение защиты информации в виртуальной инфраструктуре;

4) обеспечение защиты информации, передаваемой по каналам связи;

5) обеспечение защиты системы защиты информации.

Как видно из представленного перечня, каждый из общих показателей безопасности информации, обрабатываемой в ИС, соответствует определенной разновидности мероприятий по обеспечению безопасности информации, реализуемых в рамках такой системы.

Информация, обрабатываемая в ИС аудируемой организации, может характеризоваться как всеми, так и некоторыми из указанных общих показателей безопасности, в зависимости от класса такой системы (таблица 3.4).

Таблица 3.4. – Соответствие общих критериев безопасности, характерных для информации, обрабатываемой с помощью ИС, и классов этих систем

Класс (-ы) ИС	Порядковые номера общих критериев безопасности, характерных для информации, обрабатываемой с помощью ИС
4-ин	1, 2, 5
4-юл, 4-дсп	1–3, 5
3-ин, 3-юл, 3-дсп	1–5

2. Каждому из общих показателей безопасности поставлен в соответствие уникальный набор частных показателей безопасности. С помощью последних может быть установлена степень полноты выполнения требований, определяющих общие показатели безопасности информации, обрабатываемой в ИС аудируемой организации.

3. Разработаны 6 контрольных листов для анкетирования руководители подразделений и служб, специалисты которых работают с ИС, предназначенными для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам.

Разработанный контрольный лист № 1 включает в себя 1 вопрос и перечень вариантов ответа на него, по результатам которого можно установить, с ИС какого класса работают организации электросвязи. Содержание разработанного контрольного листа № 1 представлено ниже.

С информационной системой какого класса Вы работаете?

- 4-ин (вариант ответа 1);
- 4-юл (вариант ответа 2);
- 4-дсп (вариант ответа 3);
- 3-ин (вариант ответа 4);
- 3-юл (вариант ответа 5);
- 3-дсп (вариант ответа 6).

Контрольный лист № 2 включает в себя пункты для выбора, по результатам которого можно реализовать следующее:

- установить, какие из мероприятий, соответствующие общим показателям безопасности информации, реализуются в рамках ИС аудируемой организации;

- сгенерировать на основе контрольных листов №№ 3–7 пункты для выбора в виде перечня частных показателей безопасности информации, соответствующих выбранным общим показателям безопасности информации

Содержание контрольного листа № 2 зависит от ответа на вопрос из контрольного листа № 1. Предложены три вида контрольного листа № 2. На рисунке 3.2 представлен алгоритм проведения анкетирования с помощью

контрольного листа № 1, который отражает взаимосвязь между ответом на вопрос из контрольного листа № 1 и выбором вида контрольного листа № 2.

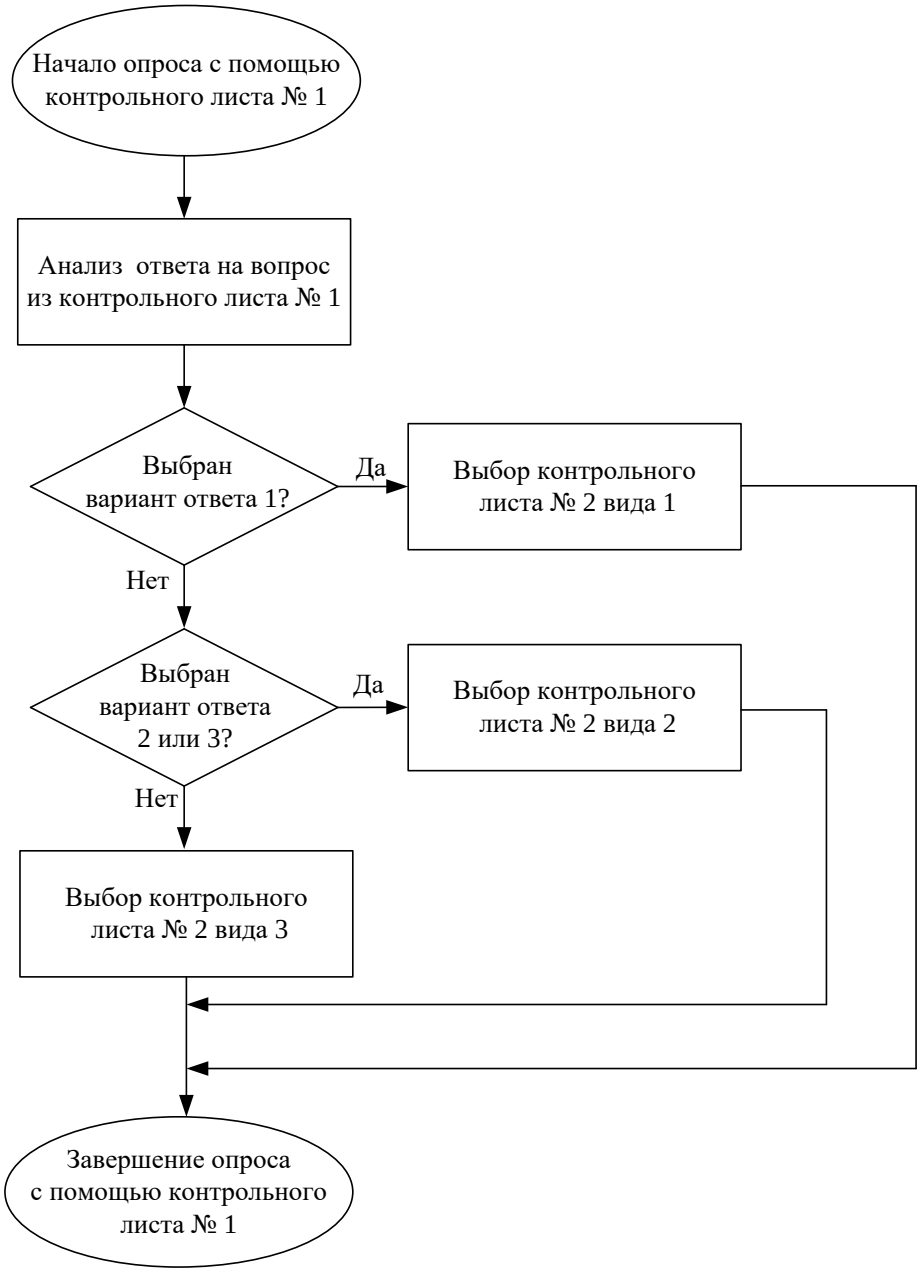

Рисунок 3.2. – Алгоритм проведения анкетирования с помощью контрольного листа № 1

В таблице 3.5 представлено содержание предложенных видов контрольного листа № 2.

Таблица 3.5. – Содержание контрольных листов № 2

Наименование вида контрольного листа	Содержание контрольного листа
1	Выберите реализуемые на Вашем предприятии разновидности мероприятий по защите информации, обрабатываемой в информационной системе. Реализация организационных мер по защите информации (вариант 1.1). Использование средств технической и криптографической защиты информации (вариант 1.2). Обеспечение защиты системы защиты информации (вариант 1.3).
2	Выберите реализуемые на Вашем предприятии разновидности мероприятий по защите информации, обрабатываемой в информационной системе. Реализация организационных мер по защите информации (вариант 2.1). Использование средств технической и криптографической защиты информации (вариант 2.2). Обеспечение защиты информации в виртуальной инфраструктуре (вариант 2.3). Обеспечение защиты системы защиты информации (вариант 2.4).
3	Выберите реализуемые на Вашем предприятии разновидности мероприятий по защите информации, обрабатываемой в информационной системе. Реализация организационных мер по защите информации (вариант 3.1). Использование средств технической и криптографической защиты информации (вариант 3.2). Обеспечение защиты информации в виртуальной инфраструктуре (вариант 3.3). Обеспечение защиты информации, передаваемой по каналам связи (вариант 3.4). Обеспечение защиты системы защиты информации (вариант 3.5).

Предложенные контрольные листы №№ 3–8 включают в себя пункты для выбора, по результатам которого можно установить степень соответствия ИС аудируемой организации требованиям, определяющим частные показатели безопасности информации, обрабатываемой с помощью этой системы. Содержание рассматриваемых контрольных листов представляет собой совокупность модулей (см. Приложение Б), номенклатура которых зависит от выбранного ответа на вопрос из контрольного листа № 1, т. е. от класса ИС, а также от номенклатуры выбранных в контрольном листе № 2 пунктов. Ниже на рисунке 3.3 представлен обобщенный алгоритм проведения анкетирования с помощью контрольного листа № 2, который отражает взаимосвязь между выбором пунктов из него и выбором модулей для формирования контрольных листов № 3–8. Использованные на рисунке 3.4 буквенные обозначения означают следующее: N – номер вида контрольного листа ($N \in \{1, 2, 3\}$); M – номер пункта для выбора в контрольном листе ($M \in \{1, 2, 3\} \mid N = 1; M \in \{1, 2, 3, 4\} \mid N = 2; M \in \{1, 2, 3, 4, 5\} \mid N = 2$); L – номер формируемого контрольного листа ($L \in \{3, 4, 5, 6, 7, 8\}$), который зависит от выбранного варианта ответа на вопрос из контрольного листа № 1. В таблице 3.6 представлена взаимосвязь между выбранным вариантом ответа на вопрос из контрольного листа № 1 и номером контрольного листа, формируемого по результатам выбора пунктов из контрольного листа № 2.

Таблица 3.6. – Таблица соответствия выбранного варианта ответа и номера контрольного листа

Выбранный вариант ответа на вопрос из контрольного листа № 1	Номер формируемого контрольного листа
Вариант ответа 1	3
Вариант ответа 2	4
Вариант ответа 3	5
Вариант ответа 4	6
Вариант ответа 5	7
Вариант ответа 6	8

Для систематизации сведений, которые аудитор получит в ходе анализа процесса работы (краткого интервьюирования) сотрудников аудируемых отделов организации, а также в ходе проверки ее внутренних документов, регламентирующих деятельность в сфере ИБ, предложено использовать контрольный лист, включающий в себя вопросы, перечень которых представлен в приложении В.

Ответы на представленные вопросы должны быть даны аудитором.

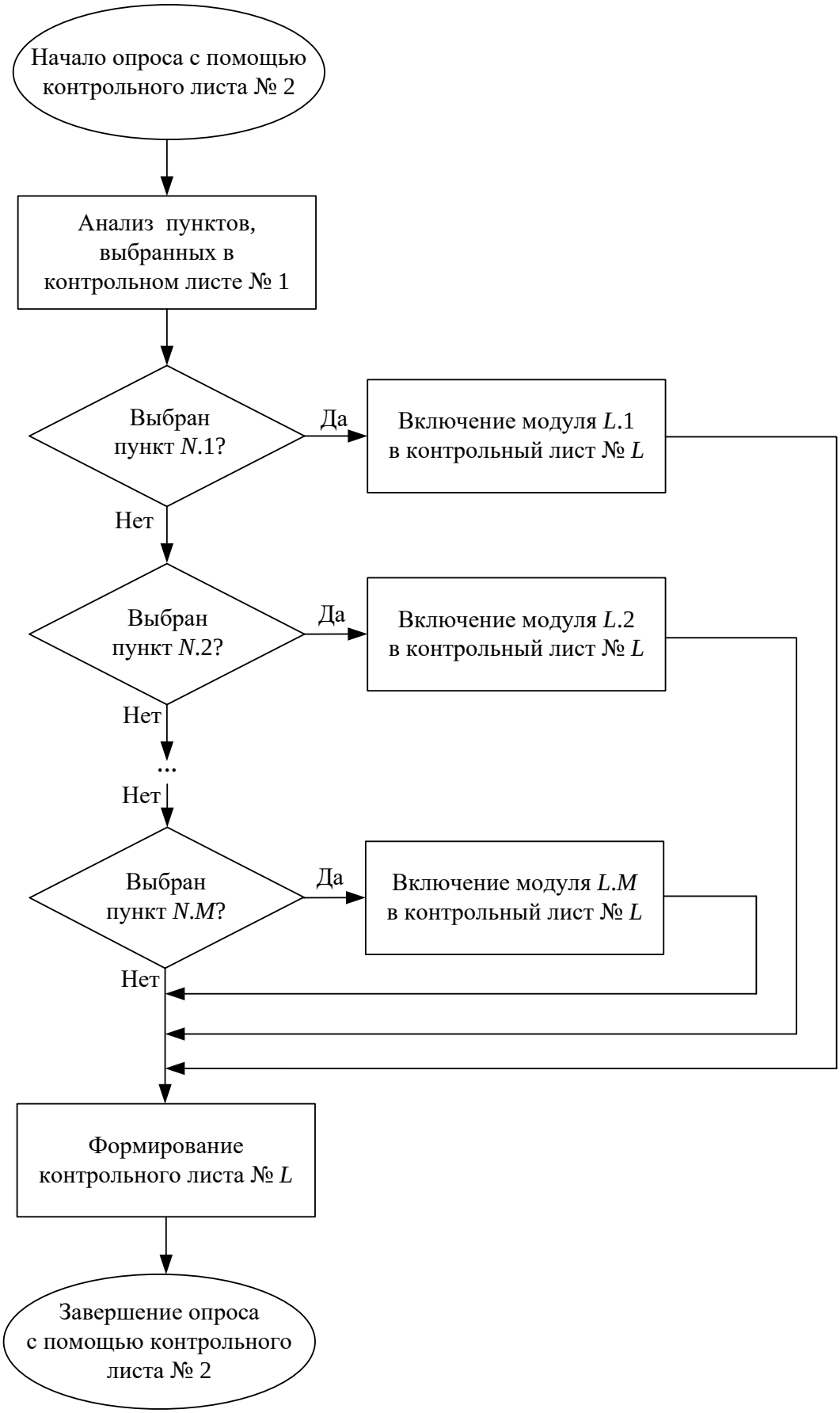

Рисунок 3.3. – Обобщенный алгоритм проведения анкетирования с помощью контрольного листа № 2

3.3 Анализ данных, полученных в ходе проведения аудита

Процесс анализа данных, полученных в ходе проведения аудита, рекомендуется начинать с оценки уязвимостей ИС, являющихся объектом аудита. Целесообразнее всего выполнять эту оценку с использованием стандарта CVSS v3 (от англ. Common Vulnerability Scoring System version 3), что обусловлено большим количеством предусмотренных в рамках него метрик уязвимости и соответствующих им характеристик, что позволяет обеспечить высокую точность ее оценки [91, 92]. Метрики, предусмотренные в стандартах CVSS, делятся на следующие виды [93]:

- базовые (совокупность характеристик уязвимости, не меняющихся со временем);
- временные (совокупность характеристик уязвимости, используемых для описания полноты имеющейся о ней информации, степени зрелости эксплуатирующего ее программного кода);
- контекстные (совокупность характеристик ИС, в которой обнаружена уязвимость).

В таблице 3.7 представлены характеристики, соответствующие метрикам указанных видов, а также описание этих характеристик [94].

Таблица 3.7. – Характеристики метрик, предусмотренных стандартом CVSS v3

Наименование метрик в зависимости от их вида	Наименование характеристики	Обозначение характеристики	Параметры характеристики
1	2	3	4
Базовые	Attack vector (вектор атаки)	AV	Network (N) Adjacent Network (A) Local (L) Physical (P)
	Attack complexity (сложность атаки)	AC	Low (L) High (H)
	Privileges required (требуемый уровень привилегий)	PR	High (H) Low (L) None (N)
	User interaction (необходимость взаимодействия с пользователем)	UI	None (N) Required (R)

Окончание таблицы 3.7

1	2	3	4
Базовые	Scope (границы эксплуатации)	S	Unchanged (U) Changed (C)
	Confidentiality impact, integrity impact, availability impact (метрики воздействия)	C I A	None (N) Medium (M) High (H)
Временные	Exploit code maturity (степень зрелости доступных средств эксплуатации уязвимости)	E	Not Defined (ND/X) High (H) Functional (F)[1] Proof-of-Concept (POC/P)[2] Unproven (U)[3]
	Remediation level (доступные средства устранения уязвимости)	RL	Not Defined (ND/X) Unavailable (U) Workaround (W)[4] Temporary Fix (TF/T)[5] Official Fix (OF/O)[6]
	Report confidence (степень доверия к информации об уязвимости)	RC	Not Defined (X) Unknown (U)[7] Reasonable (R)[8] Confirmed (C)[9]
Контекстные	Confidentiality requirement, integrity requirement, availability requirement (требования к безопасности)	CR IR AR	Not Defined (ND/X) High (H) Medium (M) Low (L)

[1] Имеется программный код для эксплуатации уязвимости
[2] Имеется сценарий реализации атаки
[3] Наличие программного кода для эксплуатации уязвимости не подтверждено
[4] Средства устранения уязвимости разработаны самой организацией (являются неофициальными)
[5] Средства устранения уязвимости являются временно официальными
[6] Средства устранения уязвимости являются официальными
[7] Описание причины уязвимости отсутствует
[8] Существуют отчеты об уязвимости, с помощью которых можно установить причины ее возникновения, а также выполнить ее оценку
[9] Наличие уязвимости подтверждено производителем продукта

В таблице 3.8 представлены вектора наиболее критичных уязвимостей ИС организаций электросвязи различных категорий.

Таблица 3.8. – Вектора потенциальных уязвимостей ИС, используемых сотрудниками организаций электросвязи различных категорий

Категория организации электросвязи	Вектора основных потенциальных уязвимостей ИС		
	Базовые метрики	Временные метрики	Контекстные метрики
1	AV:P/AC:L/PR:L/ UI:N/S:C/C:N/I:H/A:H	E:F/RL:W/ RC:X	CR:H/IR:M/ AR:M
2, 3, 4	AV:N/AC:H/PR:L/ UI:R/S:C/C:H/I:H/	E:F/RL:O/ RC:R	CR:H/IR:H/ AR:H

Установлено, что ИС организаций электросвязи, сфера деятельности которых сопряжена с проектированием, предоставлением услуг и государственным регулированием, характеризуются одинаковыми векторами наиболее критичных потенциальных уязвимостей, которые обусловлены уязвимостями программных активов.

На основании анализа полученных векторов потенциальных уязвимостей информационных систем и сетей организаций электросвязи бала выполнена их оценка [95]. В таблице 3.9 представлены результаты этой оценки.

Таблица 3.9. – Оценки потенциальных уязвимостей ИС, используемых работниками организаций электросвязи различных категорий

Категория организации электросвязи	Оценки основных потенциальных уязвимостей ИС		
	Базовые метрики	Временные метрики	Контекстные метрики
1	7,1	6,7	6,7
2, 3, 4	8,0	7,1	7,6

Из таблицы 3.9 следует, что в соответствии со стандартом CVSS v 3, потенциальные уязвимости ИС, используемых сотрудниками организаций электросвязи категорий 2–4 для выполнения своих должностных обязанностей, являются более критичными, чем потенциальные уязвимости ИС, используемых сотрудниками организаций электросвязи категории 1. Однако класс вторых из упомянутых ИС, выше, чем класс первых. В связи с этим для того, чтобы использовать стандарт CVSS v 3 для оценки уязвимостей ИС, используемых работниками организаций электросвязи для выполнения своих должностных обязанностей, необходимо использовать поправочные коэффициенты. Каждый из этих коэффициентов соответствует тяжести последствий, которые могут наступить в результате реализации угрозы, связанной с эксплуатацией уязвимости ИС, и зависит от:

- категории организации электросвязи;
- класса ИС, используемой работниками организации электросвязи;
- полученной в соответствии со стандартом CVSS v 3 оценки потенциальных уязвимостей ИС, используемой работниками организации электросвязи.

Указанные коэффициенты могут быть описаны с помощью следующей математической нотации:

$$coeff = f(cat, class, est),$$

где *coeff* – поправочный коэффициент;

cat – коэффициент, соответствующий категории организации электросвязи;

class – коэффициент, соответствующий классу ИС, используемой работниками организации электросвязи;

est – коэффициент, соответствующий полученной в соответствии со стандартом CVSS v 3 оценке потенциальных уязвимостей ИС, используемой работниками организации электросвязи.

Коэффициенты *cat, class, est* определяются с помощью метода экспертных оценок [96]. В таблицах 3.10–3.12 представлены значения этих коэффициентов.

Таблица 3.10. – Значения коэффициентов *cat*

Категория организации электросвязи	1	2	3	4
Значение коэффициента *cat*	1,0	0,5	0,5	0,5

Таблица 3.11. – Значения коэффициентов *class*

Класс (-ы) ИС	Значение коэффициента *class*
6-частн, 5-частн	0,1
6-гос, 5-гос	0,2
4-ин	0,7
4-юл	0,3
4-дсп	0,5
3-ин	0,8
3-юл	0,4
3-дсп	0,6
КВОИ	1,0

Таблица 3.12. – Значения коэффициентов *est*

Диапазон значений полученной в соответствии со стандартом CVSS v 3 оценки потенциальных уязвимостей ИС	Значение коэффициента *est*
[1,0; 2,0]	0,2
(2,0; 3,0]	0,3
(3,0; 4,0]	0,4
(4,0; 5,0]	0,5
(5,0; 6,0]	0,6
(6,0; 7,0]	0,7
(7,0; 8,0]	0,8
(8,0; 9,0]	0,9
(9,0; 10,0]	1,0

Значения итоговых оценок (*result*) уязвимостей ИС организации электросвязи должны быть вычислены согласно формуле:

$$result = CVSS \cdot (1 + cat \cdot class \cdot est),$$

где *CVSS* – значение, полученной с помощью [94] оценки, соответствующей базовым и контекстам метрикам.

Если *result* > 10, то этому параметру должно быть присвоено значение, равное 10. На рисунке 3.4 представлена схема алгоритма вычисления значения *result*.

На рисунке 3.5 представлена графическая нотация процесса проведения аудита СМИБ организаций электросвязи Республики Беларусь с помощью предложенных принципов, подходов и методов. Из представленной графической нотации следует, что путем использования предложенных принципов, подходов и методов в ходе проведения аудита СМИБ организаций электросвязи Республики Беларусь можно реализовать его в соответствии, как с международными стандартами, так и с ТНПА Республики Беларусь. Этот процесс может быть интегрирован с другими процессами по ЗИ (построение СЗИ в соответствии с Положением о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, утвержденным приказом ОАЦ от 20 февраля 2020 г. № 66 с изменениями и дополнениями, утвержденными приказами Оперативно-аналитического центра при Президенте Республики Беларусь от 12 ноября 2021 г. № 195, от 29 декабря 2022 г. № 210, от 10 декабря 2024 г. № 259, и построение и корректировка состава СМИБ

в соответствии с [29–35]). Содержание представленной на рисунке 3.6 графической нотации соответствует математической нотации (1.1), на основании чего можно заключить, что основная научная задача представляемого исследования решена.

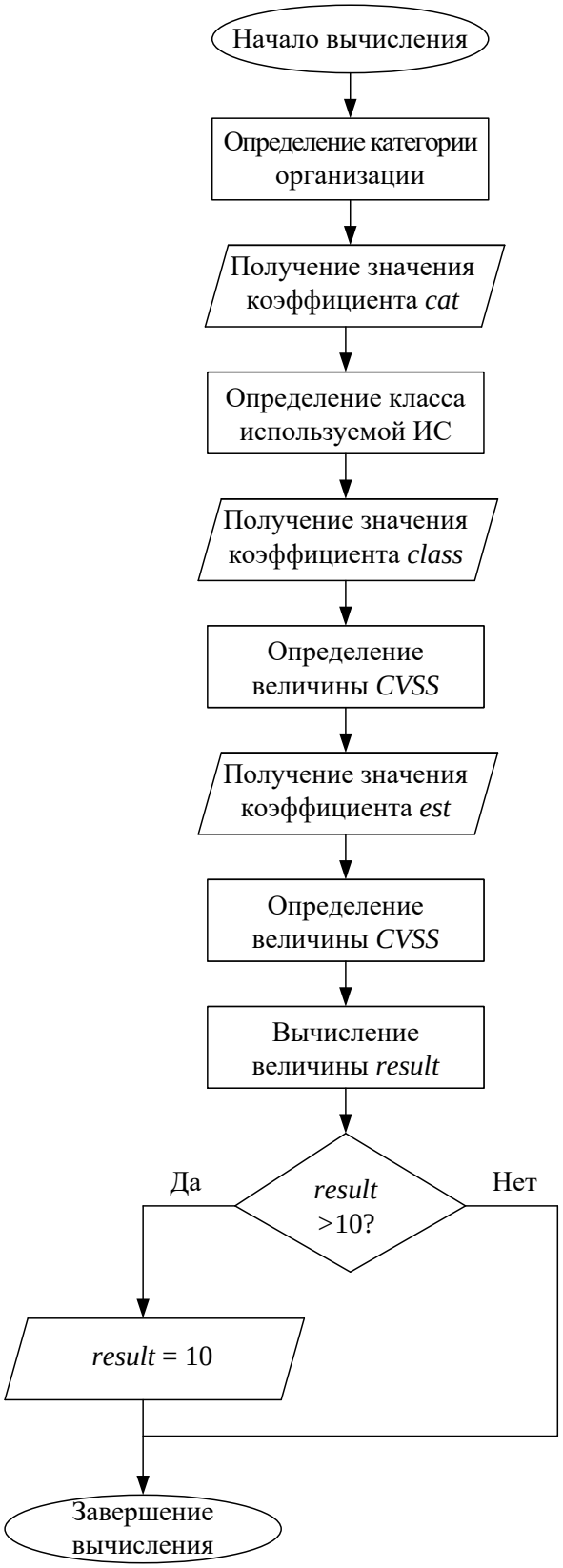

Рисунок 3.4. – Схема алгоритма вычисления значения *result*

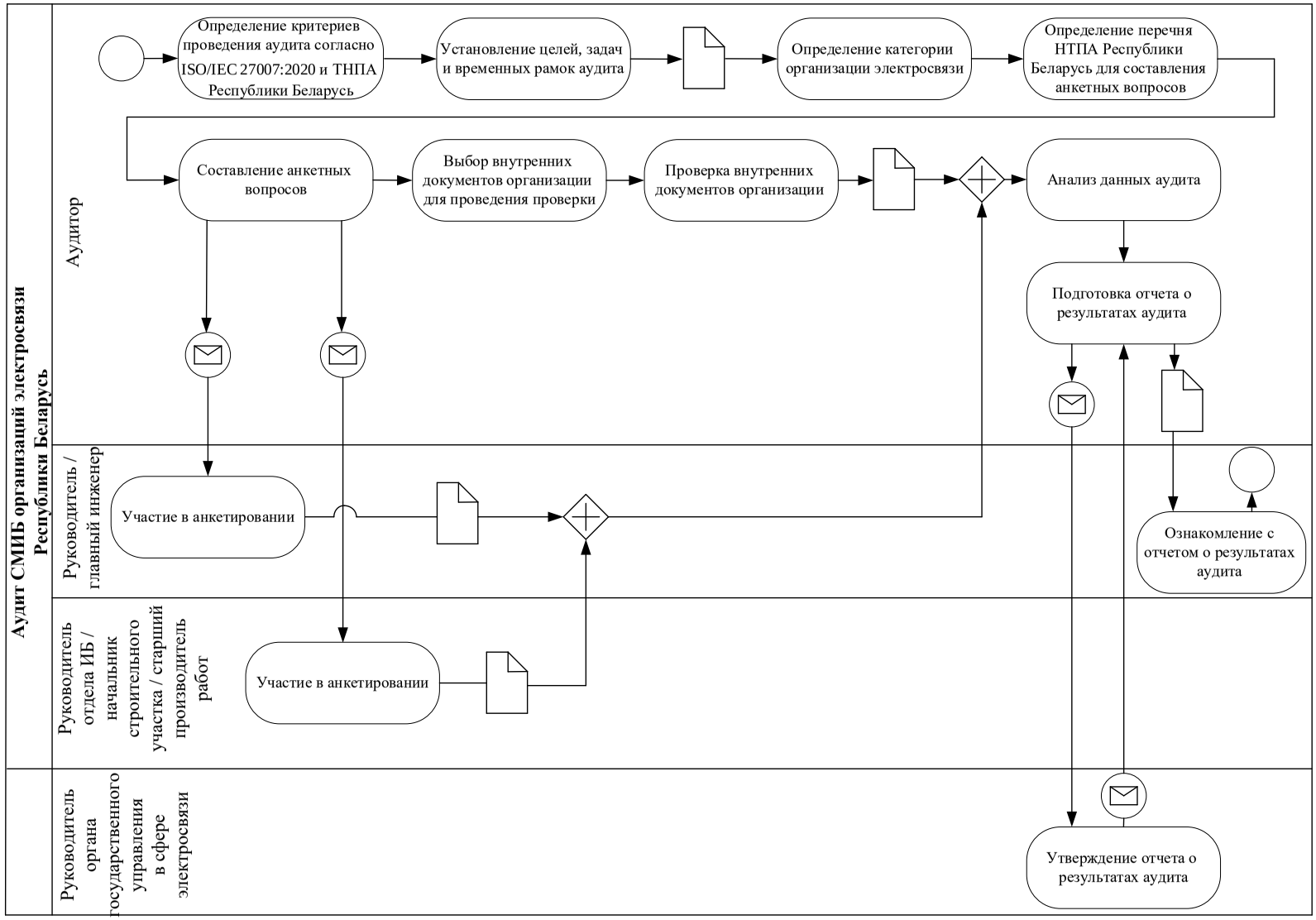

Рисунок 3.5 – Графическая нотация процесса проведения аудита СМИБ организаций электросвязи Республики Беларусь с помощью предложенных методов

ГЛАВА 4
СРЕДСТВА ОБЕСПЕЧЕНИЯ АУДИТА СИСТЕМ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ ЭЛЕКТРОСВЯЗИ РЕСПУБЛИКИ БЕЛАРУСЬ

4.1 Модель процесса обработки данных, полученных при проведении анкетирования руководителей, главных инженеров, начальников службы безопасности и старших производителей работ

Предложена модель процесса обработки результатов анкетирования руководителей и главных инженеров организаций электросвязи категорий 1–4 с помощью контрольных листов, представленных в Приложении А. Эта методика заключается в выполнении следующих действий.

1. Подсчет количества ответов «Да», данных руководителем организации и главным инженером на вопросы 1–4 из контрольного листа ($P_Р$ и $P_{ГИ}$ соответственно).

2. Подсчет количества ответов «Не знаю», данных руководителем организации на вопросы 1–8 из контрольного листа ($DK_Р$ и $DK_{ГИ}$ соответственно).

3. Сравнение ответов, данных руководителем и главным инженером организации на вопросы 5–7 из контрольного листа.

4. Сравнение ответов, данных руководителем и главным инженером организации на вопросы 5, 8 из контрольного листа.

5. Расчет коэффициента, определяющего степень выполнения общих положений из Положения о порядке технической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам, утвержденного приказом ОАЦ от 20 февраля 2020 г. № 66 с изменениями и дополнениями, утвержденными приказами Оперативно-аналитического центра при Президенте Республики Беларусь от 12 ноября 2021 г. № 195, от 29 декабря 2022 г. № 210, от 10 декабря 2024 г. № 259, на основе ответов на вопросы из контрольного листа, данных руководителем организации и главным инженером ($D_Р$ и $D_{ГИ}$ соответственно). Формулы, которые необходимо использовать для расчета, зависят от результатов, полученных в ходе выполнения действий по пп. 3, 4.

5.1 Если на вопрос 5 из контрольного листа дан ответ «Нет», а на вопросы 6 и 7 – ответы «Да» или если на вопросы 5 и 8 даны ответы «Да», то для расчета указанных коэффициентов или одного из них (если

описанное условие выполняется только для ответов, данных руководителем или главным инженером на вопросы из контрольного листа) следует использовать следующую формулу или одну из них:

$$D_{\text{Р}} = \frac{P_{\text{Р}} + 2}{Y_{\text{Р}}};$$

$$D_{\text{ГИ}} = \frac{P_{\text{ГИ}} + 2}{Y_{\text{ГИ}}},$$

где $Y_{\text{Р}}$ и $Y_{\text{ГИ}}$ – максимальное количество ответов «Да» на все вопросы из контрольного листа, предложенного для использования в целях анкетирования соответственно руководителей и главных инженеров организаций электросвязи категорий 1–4 (номера вопросов из указанного контрольного листа, на которые могут быть даны ответы «Да», – 1–4, 5, 8 или 1–4, 6, 7).

Значение второго слагаемого в выражениях, фигурирующих в числителях представленных формул (т. е. 2), соответствует количеству ответов «Да» на вопросы 5–8 из контрольного листа, предложенного для использования в целях анкетирования руководителей и главных инженеров организаций электросвязи категорий 1–4 (номера вопросов из указанного диапазона, на которые могут быть даны ответы «Да» одновременно – 6 и 7 или 5 и 8).

5.2 Если на вопрос 5 из контрольного листа дан ответ «Нет», на вопросы 6 и 7 соответственно «Да» и «Нет» или «Нет» и «Да», или на вопрос 5 дан ответ «Да», а на вопрос 8 – «Нет», то для расчета указанных коэффициентов или одного из них (если описанное условие выполняется только для ответов, данных руководителем или главным инженером на вопросы из контрольного листа) следует использовать следующие формулы или одну из них:

$$D_{\text{Р}} = \frac{P_{\text{Р}} + 1}{Y_{\text{Р}}};$$

$$D_{\text{ГИ}} = \frac{P_{\text{ГИ}} + 1}{Y_{\text{ГИ}}}.$$

Значение второго слагаемого в выражениях, фигурирующих в числителях представленных формул (т. е. 1), соответствует количеству ответов «Да» на вопросы 5–8 из контрольного листа, предложенного

для использования в целях анкетирования руководителей и главных инженеров организаций электросвязи категорий 1–4.

5.3 При всех остальных комбинациях ответов на вопросы 5–7 или на вопросы 5 и 8 указанные коэффициенты или один из них (если описанное условие выполняется только для ответов, данных руководителем или главным инженером на вопросы из контрольного листа) следует использовать следующие формулы или одну из них:

$$D_{\text{Р}} = \frac{P_{\text{Р}}}{Y_{\text{Р}}};$$

$$D_{\text{ГИ}} = \frac{P_{\text{ГИ}}}{Y_{\text{ГИ}}}.$$

6. Расчет доли ответов «Не знаю», данных руководителем и главным инженером организации на вопросы 1–8 из контрольного листа ($A_{DK_{\text{Р}}}$ и $A_{DK_{\text{ГИ}}}$ соответственно), которая показывает уровень неосведомленности указанных лиц по вопросам обеспечения внутренней деятельности организации, связанной с ее ИБ:

$$A_{DK_{\text{Р}}} = \frac{DK_{\text{Р}}}{Q_{\text{РГИ}}};$$

$$A_{DK_{\text{ГИ}}} = \frac{DK_{\text{ГИ}}}{Q_{\text{РГИ}}}.$$

где $Q_{\text{РГИ}}$ – количество вопросов из контрольного листа, предложенного для использования в целях анкетирования руководителей и главных инженеров организаций электросвязи категорий 1–4.

7. Расчет уровня неосведомленности руководителя и главного инженера организации по вопросам обеспечения ИБ ($U_{\text{Р}}$ и $U_{\text{ГИ}}$ соответственно):

$$U_{\text{Р}} = \frac{NM_{\text{Р}}}{Q_{\text{РГИ}}};$$

$$U_{\text{ГИ}} = \frac{NM_{\text{ГИ}}}{Q_{\text{РГИ}}}.$$

8. Расчет коэффициента согласованности уровней осведомленности руководителя и главного инженера организации по вопросам обеспечения ее ИБ (K_A):

$$K_A = \frac{P}{Y_{MAX}},$$

где P – количество вопросов, на которые и руководитель, и главный инженер организации дали ответ «Да»;

Y_{MAX} – максимальное количестве ответов «Да» на все вопросы из контрольного листа, предложенного для использования в целях анкетирования руководителей и главных инженеров организаций электросвязи категорий 1–4.

Использование разработанной методики анкетирования руководителей и главных инженеров организации в ходе проведения аудита СМИБ способствует соблюдению предложенного принципа единоначалия.

Обработку результатов анкетирования начальника службы безопасности и старших производителей работ (начальников строительных участков) предложено проводить путем подсчета количества вопросов из контрольных листов, представленных в Приложении А, на которые указанные лица дали ответ «Да» в ходе анкетирования.

На основе результатов такого подсчета необходимо вычислить:

– $D_{НСБ}$ – коэффициент, определяющий степень выполнения требований по проектированию и созданию системы защиты информации, изложенных в Положении о порядке технической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам, утвержденного приказом ОАЦ от 30 августа 2013 г. № 62 (в редакции приказа ОАЦ от 11 октября 2017 г. № 64);

– $D_{НСУ}$ – коэффициент, определяющий степень выполнения требований, изложенных в Положении об обеспечении безопасности КВОИ, утвержденном приказом ОАЦ от 12 октября 2018 г. № 151, а также в ТКП 45-1.02-25-201-2014 Строительство. Проектная документация Состав и содержание.

Для этого необходимо использовать следующие формулы:

$$D_{НСБ} = \frac{P_{НСБ}}{N_{НСБ}};$$

$$D_{НСУ} = \frac{P_{НСУ}}{N_{НСУ}},$$

где $P_{НСБ}$ и $P_{НСУ}$ – количество вопросов, на которые соответственно начальник службы безопасности и старший производитель работ (начальник строительного участка) дали ответ «Да»;

$N_{НСБ}$ и $N_{НСУ}$ – количество вопросов, на которые соответственно начальник службы безопасности и старший производитель работ

(начальник строительного участка) должны были ответить в ходе анкетирования.

Результаты обработки данных, полученных в ходе проведения аудита, должны быть использованы аудитором в ходе построения матрицы причинно-следственных связей между уязвимостями и угрозами безопасности информации (см. раздел 4.3) [97].

Использование разработанной методики анкетирования начальника службы безопасности и старших производителей работ (начальников строительных участков) организации в ходе проведения аудита СМИБ способствует соблюдению предложенного принципа всеохватываемости.

Методика анкетирования старших производителей работ и начальников строительных участков была внедрена в СООО «СМУ Союзтелефонстрой». В результате внедрения указанной методики удалось сократить на 35–40 % продолжительность процесса проведения внутреннего аудита систем менеджмента информационной безопасности и на 50 % – количество работников, задействованных в поцессе обработки результатов аудита, о чем свидетельствует соответствующий документ (Приложение Г). На основе этого можно заключить, что использование разработанной методики в ходе проведения аудита СМИБ организации будет способствоввать соблюдению предложенного принципа оптимизации.

4.2 Программное средство для анкетирования руководителей подразделений и служб организаций электросвязи в ходе проведения аудита

Так как контрольные листы, предложенные для анкетирования руководителей подразделений и служб, специалисты которых работают с ИС, предназначенными для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам, характеризуются наибольшим объемом по сравнению с другими предложенными контрольными листами, то разработано специальное программное средство, с помощью которого можно ускорить и упорядочить процесс анкетирования с применением таких листов. Разработанное программное средство функционирует в соответствии с алгоритмами, представленными на рисунках 3.3 и 3.4 в подразделе 3.2.1 и может быть применено при проведении аудита СМИБ не только организаций электросвязи Республики Беларусь, но и организаций других видов деятельности, на которых используются ИС, предназначенные для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам. С помощью разработанного

программного средства может быть оценена степень соответствия системы защиты информации ИС организации требованиям Положения о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, утвержденного приказом ОАЦ от 20 февраля 2020 г. № 66 с изменениями и дополнениями, утвержденными приказами Оперативно-аналитического центра при Президенте Республики Беларусь от 12 ноября 2021 г. № 195, от 29 декабря 2022 г. № 210, от 10 декабря 2024 г. № 259, а также могут быть систематизированы рекомендации по улучшению этой системы.

Для разработки программного средства использован язык программирования JavaScript. Разработанное программное средство представляет собой совокупность файлов формата html, в связи с чем в отличие от аналогов [61–66, 98, 99] оно не требует установки и может быть запущено и использовано на всех рабочих станциях, оснащенных Интернет-браузером. В таблице 4.1 представлены имена файлов, входящих в состав разработанного программного средства, а также сведения об этих файлах.

Таблица 4.1 – Сведения о файлах, входящих в состав разработанного программного средства

№ п/п	Имя файла	Размер файла, КБ	Сведения о назначении файла
1	2	2	4
1	index.html	2	Файл для запуска программного средства
2	opros.html	3	Файл, содержащий контрольный лист № 1
3	3dsp.html	31	Файл, содержащий контрольный лист № 2 вида 1, скрытые по умолчанию модули 3.1, 3.2, 3.3 и предназначенный для формирования контрольного листа № 3 и обработки результатов выбора пунктов (частных показателей безопасности информации) из этого контрольного листа
4	3pd.html	27	Файл, содержащий контрольный лист № 2 вида 2, скрытые по умолчанию модули 4.1, 4.2, 4.3,4.4 и предназначенный для формирования контрольного листа № 4 и обработки результатов выбора пунктов (частных показателей безопасности информации) из этого контрольного листа

Продолжение таблицы 4.1

1	2	2	4
5	3ul.html	29	Файл, содержащий контрольный лист № 2 вида 2, скрытые по умолчанию модули 5.1, 5.2, 5.3, 5.4 и предназначенный для формирования контрольного листа № 5 и обработки результатов выбора пунктов (частных показателей безопасности информации) из этого контрольного листа
6	4dsp.html	22	Файл, содержащий контрольный лист № 2 вида 3, скрытые по умолчанию модули 6.1, 6.2, 6.3, 6.4, 6.5 и предназначенный для формирования контрольного листа № 6 и обработки результатов выбора пунктов (частных показателей безопасности информации) из этого контрольного листа
7	4pd.html	18	Файл, содержащий контрольный лист № 2 вида 3, скрытые по умолчанию модули 7.1, 7.2, 7.3, 7.4, 7.5 и предназначенный для формирования контрольного листа № 7 и обработки результатов выбора пунктов (частных показателей безопасности информации) из этого контрольного листа
8	4ul.html	20	Файл, содержащий контрольный лист № 2 вида 3, скрытые по умолчанию модули 8.1, 8.2, 8.3, 8.4, 8.5 и предназначенный для формирования контрольного листа № 8 и обработки результатов выбора пунктов (частных показателей безопасности информации) из этого контрольного листа

На рисунках 4.1–4.9 представлен внешний вид фрагментов диалоговых окон файлов разработанного программного средства.

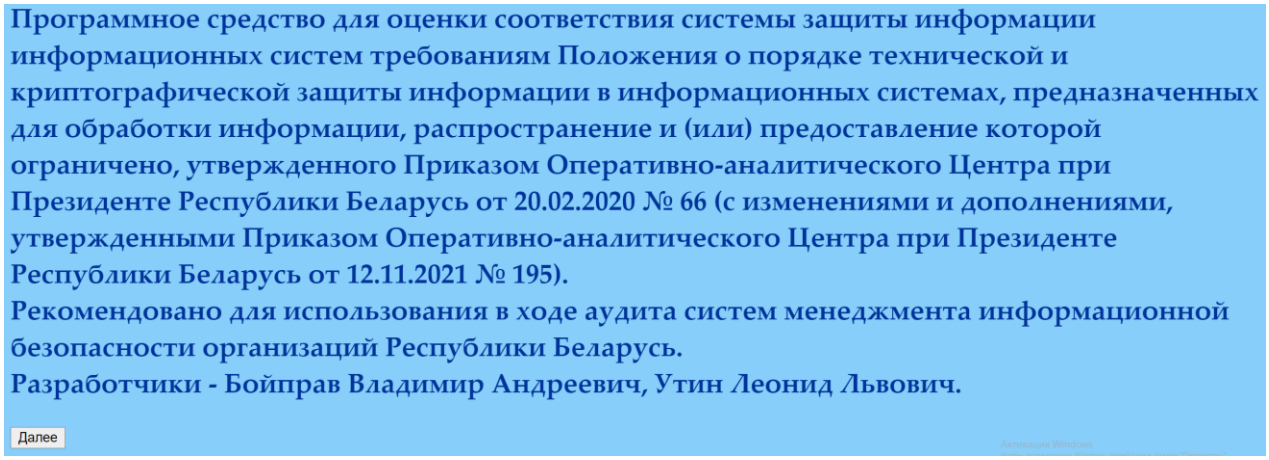

Рисунок 4.1. – Внешний вид фрагмента диалогового окна «index.html»

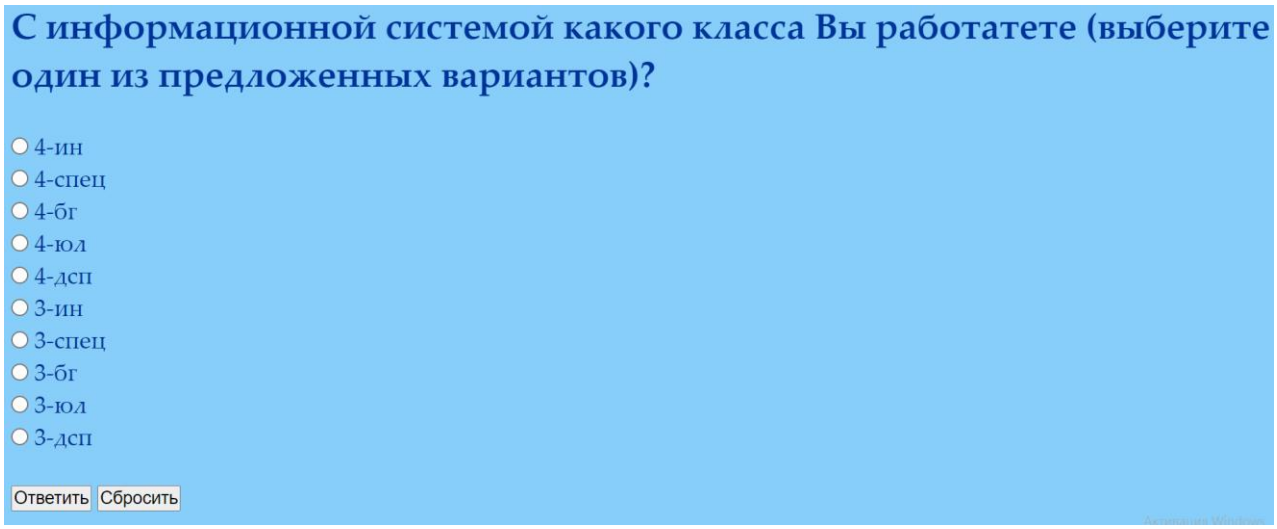

Рисунок 4.2. – Внешний вид фрагмента диалогового окна «opros.html»

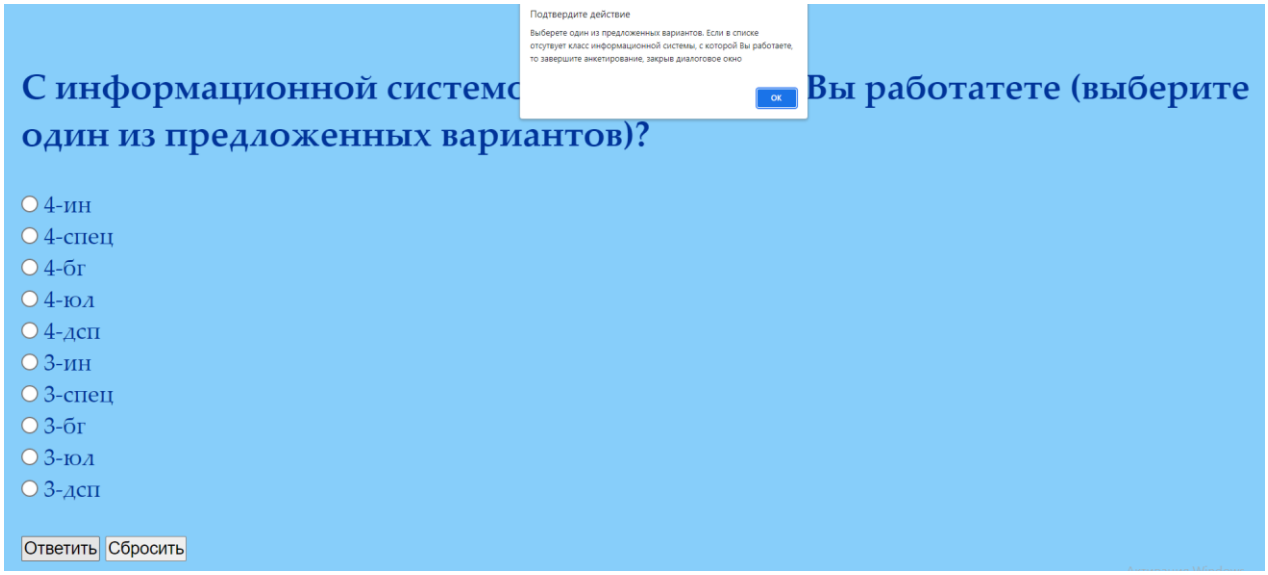

Рисунок 4.3. – Внешний вид фрагмента диалогового окна «index.html» после нажатия кнопки «Ответить» при условии не сделанного выбора класса информационной системы

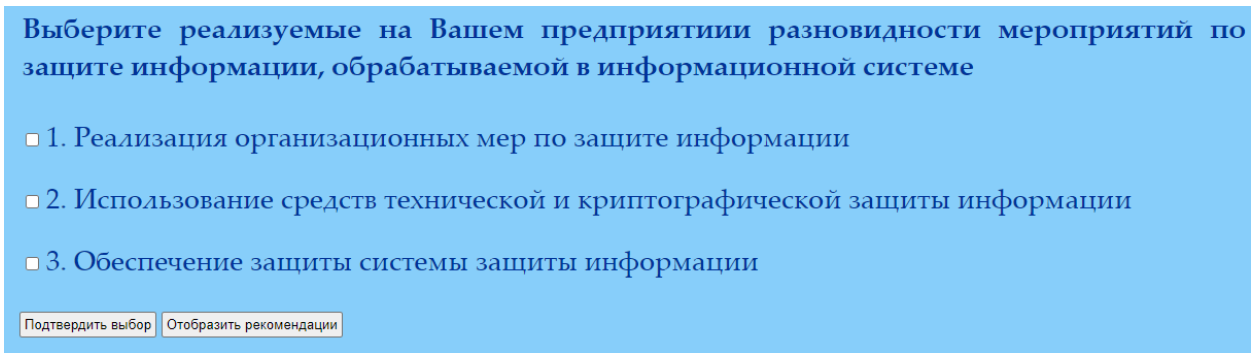

Рисунок 4.4. – Внешний вид фрагмента диалогового окна «4pd.html»

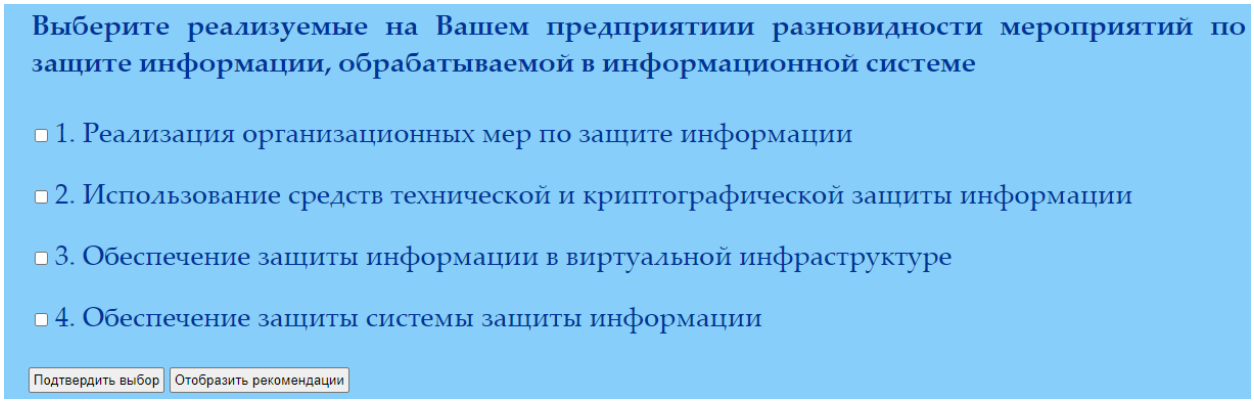

Рисунок 4.5. – Внешний вид фрагмента диалоговых окон «4ul.html» и «4dsp.html»

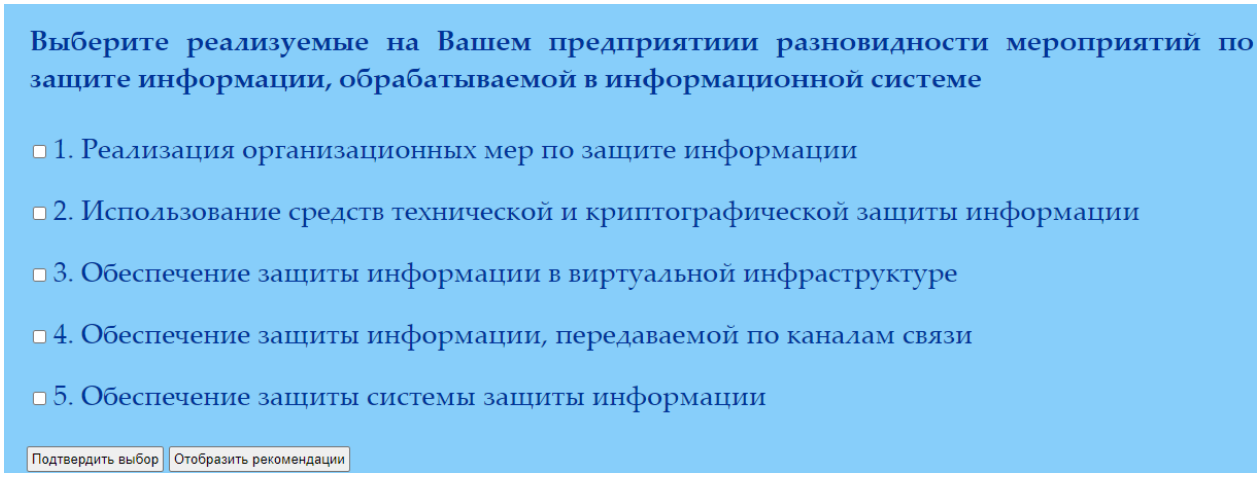

Рисунок 4.6. – Внешний вид фрагмента диалоговых окон «3pd.html», «3ul.html» и «3dsp.html»

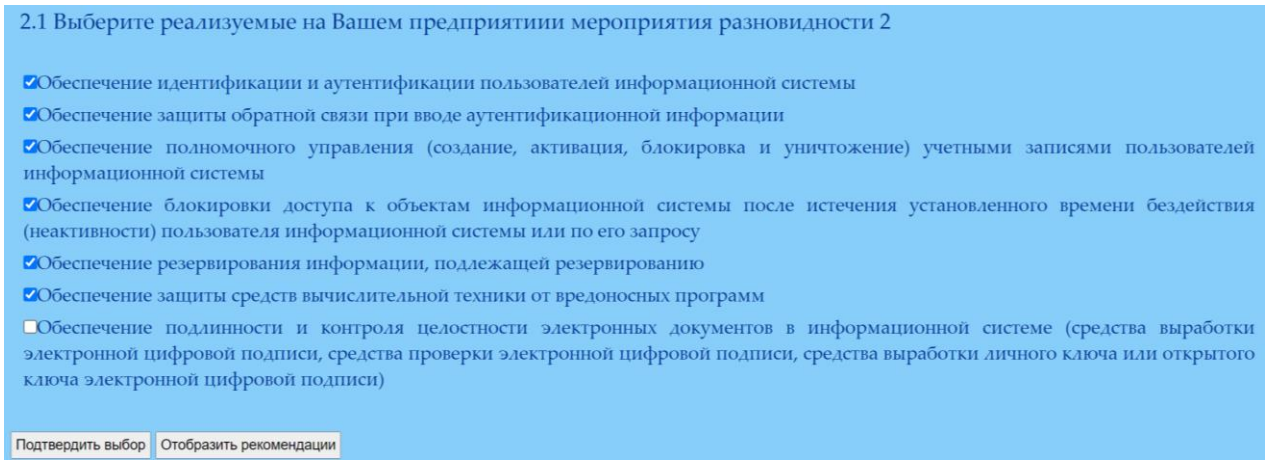

Рисунок 4.7. – Внешний вид фрагмента диалогового окна «3dsp.html» после выбора реализуемых на предприятии разновидностей мероприятий по защите информации и нажатия на кнопку «Подтвердить выбор»

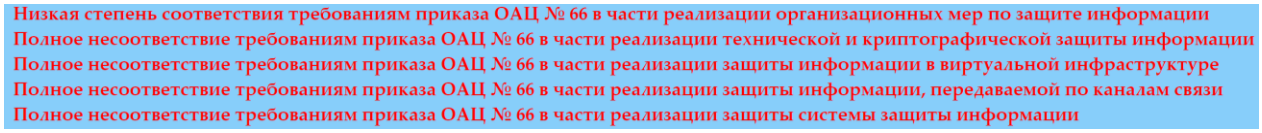

Рисунок 4.8. – Внешний вид фрагмента диалогового окна «3dsp.html» после нажатия на кнопку «Подтвердить выбор» при условии сделанного выбора пунктов

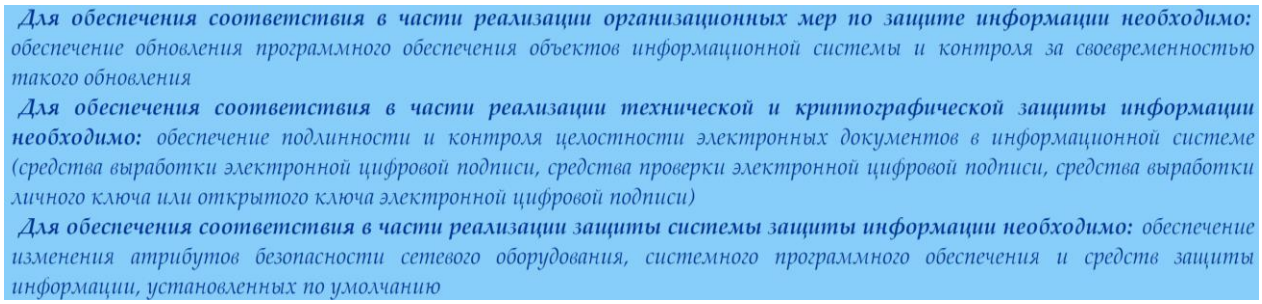

Рисунок 4.9. – Внешний вид фрагмента диалогового окна «3dsp.html» после нажатия на кнопку «Отобразить рекомендации»

Степени соответствия системы защиты информации ИС требованиям Положения о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, утвержденного приказом ОАЦ от 20 февраля 2020 г. № 66 с изменениями и дополнениями, утвержденными приказами Оперативно-аналитического центра при Президенте Республики Беларусь от 12 ноября 2021 г. № 195, от 29 декабря 2022 г. № 210, от 10 декабря 2024 г. № 259, которые могут быть установлены в результате использования разработанного программного средства, проранжированы по пяти уровням:

- полное несоответствие;
- низкая степень соответствия;
- средняя степень соответствия;
- высокая степень соответствия;
- полное соответствие.

Уровни степени соответствия системы защиты информации ИС требованиям указанного выше Положения устанавливаются по каждому из общих показателей безопасности последней (см. представленный выше рисунок 4.6). Например, система защиты информации ИС может характеризоваться средней степенью соответствия требованиям Положения в части реализации организационных мер по защите информации, но при этом полностью не соответствовать требованиям Положения в части реализации технической и криптографической защиты информации, защиты

информации в виртуальной инфраструктуре, защиты информации, передаваемой по каналам связи, защиты системы защиты информации.

Уровень степени соответствия системы защиты информации ИС по общему показателю безопасности зависит от количества выбранных анкетируемым сотрудником частных показателей безопасности, на которых основаны контрольные листы №№ 3–8.

В таблице 4.2 представлены сведения о взаимосвязи между уровнем степени соответствия системы защиты информации ИС по общему показателю безопасности и количеством выбранных анкетируемым сотрудником частных показателей безопасности (*PM*).

В таблице 4.2 использованы следующие обозначения:

- *MAX* – количество частных показателей безопасности, на основе которых составлен контрольный лист для анкетирования и которые соответствуют определенному общему показателю безопасности;

- *MV* – медианное значение среди множества значений, отражающих количество частных показателей безопасности, на основе которых составлены все контрольные листы для анкетирования, и каждый из которых соответствует определенному общему показателю безопасности.

Значение *MV* определяется на основе совокупности следующих условий:

$$\begin{cases} MV \in \{GV_1, GV_2, ..., GV_m, ..., GV_r\}; \\ MV = GV_m; \\ m = \dfrac{r}{2}, \text{ если } r - \text{четное число}; \\ m = \dfrac{r+1}{2}, \text{ если } r - \text{нечетное число}, \end{cases}$$

где $GV_1, GV_2, ..., GV_m, ..., GV_r$ – проранжированные по возрастанию значения количества частных показателей безопасности, каждый из которых соответствует определенному общему показателю безопасности;

GV_m – значение, которое является медианным во множестве $GV_1, GV_2, ..., GV_m, ..., GV_r$;

m – порядковый номер значения, которое является медианным во множестве $GV_1, GV_2, ..., GV_m, ..., GV_r$;

r – суммарное количество общих показателей безопасности во множестве $GV_1, GV_2, ..., GV_m, ..., GV_r$.

Таблица 4.2. – Взаимосвязь между уровнем степени соответствия системы защиты информации ИС по общему показателю безопасности и *PM*

Уровень соответствия	Значения *PM*
Полное несоответствие	0
Низкая степень соответствия	$\begin{cases} 0 < PM < \dfrac{MAX - 1}{2}, \text{ если } MAX - \text{нечетное число} \cap MAX \le MV; \\ 0 < PM < \dfrac{MAX}{2}, \text{ если } MAX - \text{четное число}; \\ 0 < PM < \dfrac{MAX + 1}{2}, \text{ если } MAX - \text{нечетное число} \cap MAX > MV. \end{cases}$
Средняя степень соответствия	$\begin{cases} \dfrac{MAX - 1}{2}, \text{ если } MAX - \text{нечетное число} \cap MAX \le MV; \\ \dfrac{MAX}{2}, \text{ если } MAX - \text{четное число}; \\ \dfrac{MAX + 1}{2}, \text{ если } MAX - \text{нечетное число} \cap MAX > MV. \end{cases}$
Высокая степень соответствия	$\begin{cases} MAX - 1, \text{ если } MAX \le MV; \\ MAX - 2, \text{ если } MAX > MV \end{cases}$
Полное соответствие	*MAX*

Разработанное программное средство зарегистрировано в установленном порядке в Государственном предприятии «Национальный центр интеллектуальной собственности». В приложении Д представлена копия свидетельства о регистрации этого средства. Разработанное программное средство было апробировано в филиале «Междугородная связь» РУП «Белетелеком», о чем свидетельствует соответствующий документ (Приложение Е). По результатам апробации установленно что использование этого средства позволяет сократить на 20–30 % финансирование затрат на реализацию процесса проведения аудита СМИБ организации.

Таким образом, использование разработанного программного средства в ходе проведения аудита СМИБ будет способствовать соблюдению предложенного принципа оптимизации.

4.3 Модель процесса оценки рисков безопасности информационных систем организаций электросвязи

Предложена математическая модель оценки рисков ИБ организаций электросвязи Республики Беларусь. Она основана на следующих параметрах.

1. Весовой коэффициент, соответствующий классу ИС, с которыми работают сотрудники аудируемой организации электросвязи (согласно таблице 2.10).

2. Годовая стоимость аппаратных, программных или аппаратно-программных активов ИС, которые могут быть подвержены воздействию угроз. Величина этого параметра есть частное от деления цены этих активов на гарантийный срок их службы, измеряемый в годах.

3. Величина относительной ценности активов ИС, которые могут быть подвержены воздействию угроз (данный параметр может принимать значение в интервале (0;1]). Предложено определять данный параметр на основе результатов частной и экспертной оценок указанных активов. Частная оценка каждого из активов выполняется начальником строительного участка или старшим производителем работ (в случае если аудируемая организация является организацией категории 1) или руководителем подразделения и службы, специалисты которого (-ой) работают с ИС, предназначенными для обработки информации, распространение и (или) предоставление которой ограничено (в случае если аудируемая организация относится к организации категории 2, 3 или 4). Экспертная оценка выполняется группой аудиторов. Суть таких оценок заключается в присваивании указанными лицами определенной величины относительной ценности каждому из активов ИС.

Величину относительной ценности каждого активов ИС предложено вычислять на основе следующей формулы:

$$RV = \frac{\frac{\sum_{i=1}^{n_c} S_i \cdot RV_{ci}}{n_c} + \frac{\sum_{j=1}^{n_a} RV_{aj}}{n_a}}{2},$$

где S_i – коэффициент, соответствующий стажу работы сотрудника, выполнявшего частную оценку актива ИС ($S = 0{,}8$, если стаж работы указанного сотрудника в организации менее 1 года; $S = 1$, если стаж работы указанного сотрудника в организации от 1 до 5 лет; $S = 1{,}2$, если стаж работы указанного сотрудника в организации более 5 лет) [100, 101];

RV_{ci} – величина относительной ценности актива ИС, присвоенная i-м сотрудником, выполнявшим частную оценку этого актива;

RV_{aj} – величина относительной ценности актива ИС, присвоенная j-м

аудитором, выполнявшим экспертную оценку этого актива;

n_c – количество сотрудников, выполнявших частную оценку актива ИС;

n_a – количество аудиторов, выполнявших экспертную оценку актива ИС.

4. Вероятность возникновения угроз, получаемая на основе матрицы причинно-следственных связей между уязвимостями и угрозами. Эти матрицы должны быть построены начальником службы безопасности, начальником подразделения или службы аудируемой организации электросвязи, специалисты которого (-ой) работают с ИС, предназначенными для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам, а также аудитором. Таблица 4.3 – форма матрицы причинно-следственных связей между уязвимостями и угрозами.

Таблица 4.3. – Общий вид формы матрицы причинно-следственных связей между уязвимостями и угрозами

	Наименование уязвимости 1	Наименование уязвимости 2	…	Наименование уязвимости *n*
Наименование угрозы 1	Связь отсутствует / слабая / несильная / сильная	Связь отсутствует / слабая / несильная / сильная	…	Связь отсутствует / слабая / несильная / сильная
…			…	
Наименование угрозы *n*	Связь отсутствует / слабая / несильная / сильная	Связь отсутствует / слабая / несильная / Сильная	…	Связь отсутствует / слабая / несильная / сильная

Если связь между угрозой и уязвимостью отсутствует, то в ячейку, находящуюся на пересечении строки матрицы, в которой указано наименование угрозы, и столбца матрицы, в котором указано наименование уязвимости, заносится значение 0, если связь слабая, то в эту ячейку заносится значение 0,2, если связь несильная – то значение 0,5, если связь сильная – то значение 1.

Вероятность возникновения угрозы, определяемая на основе матрицы причинно-следственных связей между уязвимостями и угрозами, построенной руководителем подразделения или службы аудируемой организации, есть среднее арифметическое от значений, занесенных в ячейки строки, в которой указано наименование этой угрозы, умноженное на коэффициент *S*, соответствующий стажу работы сотрудника, выполнявшего построение матрицы.

Начальник службы безопасности и руководитель подразделения или службы аудируемой организации электросвязи должны строить матрицу

причинно-следственных связей между уязвимостями и угрозами на основе их опыта эксплуатации ИС.

Вероятность возникновения угрозы, определяемая на основе матрицы причинно-следственных связей между уязвимостями и угрозами, построенной аудитором, есть среднее арифметическое от значений, занесенных в ячейки строки. Аудитор должен строить матрицу причинно-следственных связей между уязвимостями и угрозами на основе результатов обработки ответов, которые были даны сотрудниками аудируемой организации электросвязи на вопросы из контрольных листов. При этом аудитором могут быть определены следующие уязвимости:

- уязвимости, связанные с невыполнением общих положений и требований по проектированию и созданию системы защиты информации из Положения о порядке технической защиты информации в ИС, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам, утвержденного приказом ОАЦ от 20 февраля 2020 г. № 66 с изменениями и дополнениями, утвержденными приказами Оперативно-аналитического центра при Президенте Республики Беларусь от 12 ноября 2021 г. № 195, от 29 декабря 2022 г. № 210, от 10 декабря 2024 г. № 259;

- уязвимости, связанные с невыполнением требований, изложенных в Положении об обеспечении безопасности КВОИ, утвержденном приказом ОАЦ от 12 октября 2018 г. № 151, а также в ТКП 45-1.02-25-201-2014 Строительство. Проектная документация Состав и содержание;

- уязвимости, связанные с различием в уровнях осведомленности руководителя и главного инженера организации по вопросам обеспечения ее ИБ;

- уязвимости, связанные с неосведомленностью начальника службы безопасности, начальника строительного участка (старшего производителя работ), начальника подразделения или службы, специалисты которого (-ой) работают с ИС, предназначенными для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам, по вопросам обеспечения безопасности таких систем, а также КВОИ.

Риск безопасности ИС организации – это произведение параметров, представленных в пп. 1–4 [102, 103].

ЗАКЛЮЧЕНИЕ

Усовершенствованы методы и средства обеспечения аудита СМИБ организаций электросвязи Республики Беларусь. В частности, определены новые принципы, критерии и подходы к реализации аудита СМИБ указанных организаций, а также выполнено следующее.

1. В рамках подготовительного этапа аудита СМИБ организации электросвязи Республики Беларусь предложено определять, к какой категории относится эта организация в зависимости совокупности их особенностей:

- специфики деятельности (строительство, предоставление услуг электросвязи, проектирование сетей электросвязи, управление и регулирование деятельности организаций электросвязи);
- количество классов ИС, к которым могут получать доступ сотрудники организаций электросвязи.

Показано, что количество классов ИС, к которым могут получать доступ сотрудники организаций электросвязи, зависит от специфики деятельности последних. Установлено, что сотрудники организаций, занимающихся строительством объектов электросвязи (организаций категории 1), в процессе выполнения своих должностных обязанностей имеют право получать доступ к активам наибольшего количества ИС, значимых для государства (в частности, и к КВОИ). В связи с этим в ходе аудита СМИБ таких организаций необходимо руководствоваться бóльшим количеством документов, чем в ходе реализации аналогичных мероприятий по отношению к организациям категорий 2–4. Разработаны контрольные листы для анкетирования сотрудников организаций электросвязи каждой из указанных категорий (руководитель и главный инженер организации, начальник службы безопасности, начальник строительного участка (старший производитель работ), которые предложено использования в ходе проведения аудита СМИБ этих организаций [104–108].

2. Разработано математическое и программное обеспечение для проведения аудита СМИБ организаций электросвязи Республики Беларусь категорий 1–4 и обработки его результатов. Оно основано на использовании системы коэффициентов, вычисляемых с применением результатов анкетирования сотрудников аудируемой организации, которые задействованы в процессе аудита (руководитель и главный инженер организации, начальник службы безопасности, начальник строительного участка (старший производитель работ), начальники подразделений или служб, сотрудники которых работают с ИС), а также на использовании системы весовых коэффициентов, которые зависят от категории этой организации [105, 109–121].

По результатам апорбации и внедрения разработанных усовершенствованных методов и средств установлено, что их использование в ходе проведения аудита СМИБ организаций способсвует сокращению до 40 % продолжительности этого процесса и до 50 % – количества работников, привлекаемых к его реализации.

Предложенная усовершенствованная методика аудита СМИБ организаций электросвязи основана на требованиях национального законодательства в сфере ИБ и может быть использована для проведения как внутреннего, так и внешнего аудита СМИБ организаций электросвязи Республики Беларусь, работающих с ИС различных классов. Эта методика была апробирована в ОАО «Белсвязьстрой». Методика анкетирования старших производителей работ и начальников строительных участков, входящая в состав предложенной методики, была внедрена в СООО «СМУ Союзтелефонстрой» и рекомендована для использования в ходе аудита СМИБ всех организаций, в рамках которых реализуются процессы по созданию инфраструктуры для сетей электросвязи.

С помощью разработанного программного средства может быть реализована оценка степени соответствия СЗИ организаций Республики Беларусь требованиям Положения о порядке технической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам, утвержденного приказами Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66 с изменениями и дополнениями, утвержденными приказами Оперативно-аналитического центра при Президенте Республики Беларусь от 12 ноября 2021 г. № 195, от 29 декабря 2022 г. № 210, от 10 декабря 2024 г. № 259. Это программное средство было апробировано в филиале «Междугородная связь» РУП «Белтелеком» и рекомендовано для использования в ходе аудита СМИБ всех организаций, в рамках которых используются ИС, предназначенные для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Анализ рынка услуг передачи данных в 2020 году [Электронный ресурс]. – Режим доступа: https://oac.gov.by/news/internet/service-market-analysisю. – Дата доступа: 01.09.2021.

2. Концепция информационной безопасности Республики Беларусь, утвержденная Постановлением Совета Безопасности Республики Беларусь 18 марта 2019 года № 1 // Нац. реестр правовых актов Респ. Беларусь. – 2010. – № 184. – 7/4247. – 20 с.

3. Об электросвязи : Закон Респ. Беларусь от 19 июля 2005 г. № 45-З : с изм. и доп. от 1 июля 2014 г. № 172-З // Нац. реестр правовых актов Респ. Беларусь. – 2010. – № 184. – 2/1724. – 45 с.

4. Информационная безопасность, кибербезопасность и защита конфиденциальности. Руководящие положения по проведению аудита систем менеджмента информационной безопасности : ISO/IEC 27007:2020 ; введ. 21.01.2020. – Минск : Госстандарт Республики Беларусь, 2020. – 46 с.

5. Национальный правовой Интернет-портал Республики Беларусь [Электронный ресурс]. – Режим доступа: https://pravo.by/document/?guid=3871&p0=F01900068. – Дата доступа: 01.09.2021.

6. О совершенствовании контрольной (надзорной) деятельности в Республике Беларусь : Указ Президента Респ. Беларусь от 16 окт. 2009 г. № 510. // Нац. реестр правовых актов Респ. Беларусь. – 18.10.2017. – 1/17314. – 28 с.

7. О компании | Белтелеком [Электронный ресурс]. – Режим доступа: https://beltelecom.by/about. – Дата доступа: 01.09.2021.

8. Ga, L. Discussion of Carrier Network and Information System Security Management and Control Techniques / L. Ga // Telecommunications Science. – 2011. – Vol. 27, iss. 1. – P. 110–118.

9. Proactive approach for security of the infocommunication network based on vulnerability assessment / M. Yevdokymenko [et al.] // 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T). – Kharkiv, Ukraine, 9–12 Oct. 2018. – DOI: 10.1109/INFOCOMMST.2018.8632079.

10. Кузовкова, Т. А. Научные основы экономики отрасли инфокоммуникаций / Т. А. Кузовкова, Н. Е. Зоря // T-Comm: телекоммуникации и транспорт. – 2012. – № 12. – С. 43–45.

11. Туякова, З. С. Содержание и структура бизнес-процессов телекоммуникационных компаний как объектов управленческого учета / З. С. Туякова, Т. В. Черемушникова // Вестник Оренбургского государственного университета. – 2012. – № 13. – С. 369–375.

12. Забродская, К. А. Инфокоммуникационные услуги: сущность, особенности, классификация / К. А. Забродская // Вестник связи. – 2013. – № 5. – С. 27–31.

13. Приказ Оперативно-Аналитического Центра при Президенте Республики Беларусь от 2 августа 2010 г. № 60 «Об утверждении Положения о порядке определения уполномоченных поставщиков интернет-услуг». – 2010. – 6 с.

14 Об информатизации, информации и защите информации : Закон Респ. Беларусь от 10 ноября 2008 г. № 455-З : с изм. и доп. от 4 янв. 2014 г. № 102-З, от 11 мая 2016 г. № 362-З // Нац. реестр правовых актов Респ. Беларусь. – 2008. – № 279. – 2/1552. – 14 с.

15. Техническая укрепленность объектов. Правила проектирования = Тэхнічная ўмацаванасць аб'ектаў. Правілы праектавання : Рабочий проект ТКП МВД Респ. Беларусь. – Минск : Министерство внутренних дел Республики Беларусь, 2014. – 68 с.

16. Постановление Комитета государственной безопасности Республики Беларусь от 30 сентября 2016 года № 24/268 «Об утверждении Положения о профилактических, режимных и организационных мерах предупреждения террористической деятельности и минимизации ее последствий на критически важных объектах Республики Беларусь». – 2016. – 8/31428. – 5 с.

17. Alexandrova, M. Risk factors in IT outsourcing partnerships: Vendors' perspective / M. Alexandrova // Global Business Review. – 2015. – Vol. 16(5). – P. 747–759.

18. Javaid, M. I. A comprehensive people process and technology (PPT) application model for Information Systems (IS) risk management in small/medium enterprises (SME) / M. I. Javaid, M. M. W. Iqbal // International Conference on Communication Technologies ComTech 2017. – 2017. P. 78–90.

19. Asset identification in information security risk assessment: a business practice approach / P. Shedden [et al.]. – 2016. – Communications of the Association of Information Systems. – Vol. 39 (15). – P. 297–320.

20. Egoshin, N. S. A model of threats to the confidentiality of information processed in cyberspace based on the information flows model / N. S. Egoshin, A. A. Konev, A. A. Shelupanov // Symmetry. – 2020. – Vol. 12 (11). – P. 1–18. – DOI: 10.3390/sym12111840.

21. Shaked, A. Model-based threat and risk assessment for systems design / A. Shaked, Y. Reich // Proceedings of the 7th International Conference on Information Systems Security and Privacy. – 2021. – P. 331–338.

22. Ahmad, A. A Case analysis of information systems and security incident responses / A. Ahmad, S. B. Maynard, G. Shanks // International Journal of Information Management. – 2015. – Vol. 35 (6). – P. 717–723.

23 Japertas, S. Method of Early Staged Cyber Attacks Detection in IT and Telecommunication Networks / S. Japertas, T. Baksys // Elektronika ir elektrotechnika. – 2018. – Vol. 24, No. 3. – P. 68–77

24. Singh, A. N. Identifying factors of organizational information security management / A. N. Singh, M. P. Gupta, A. Ojha // Journal of Enterprise Information Management– 2016. – Vol. 27 (5). – P. 644–667.

25. Cherdantseva, Y. Information security and information assurance : discussion about the meaning, scope, and goals / Y. Cherdantseva, J. Hilton // Organizational, legal, and technological dimensions of information system administration. – 2014. – P. 167–198.

26. The relationship between internal audit and information security: An exploratory investigation / P. J. Steinbart [et al.] // International Journal of Accounting Information Systems. – 2011. – Vol. 13. – P. 228–243.

27. Havelka D. Internal information technology audit process quality: Theory development using structured group processes / D. Havelka, J. W. Merhout // International Journal of Accounting Information Systems. – 2013. – Vol. 14, no. 3. – P. 165–192.

28. Концепция национальной безопасности Республики Беларусь, утвержденная Указом Президента Республики Беларусь от 9 ноября 2010 года № 575 // Нац. реестр правовых актов Респ. Беларусь. – 2010. – № 276. – 1/12080. – 21 с.

29. Приказ Оперативно-Аналитического Центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66 «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449» с изменениями и дополнениями, утвержденными Приказами Оперативно-аналитического центра при Президенте Республики Беларусь от 12 ноября 2021 г. № 195, от 29 декабря 2022 г. № 210, от 10 декабря 2024 г. № 259. – 2021. – 53 с.

30. Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Основные положения и словарь = Інфармацыйныя тэхналогіі. Метады забеспячэння бяспекі. Сістэмы менеджменту інфармацыйнай бяспекі. Асноўныя палажэнні і слоўнік : СТБ ISO/IEC 27000-2012 ; введ. 01.01.13. – Минск : Госстандарт Республики Беларусь, 2012. – 24 с.

31. Информационные технологии. Методы обеспечения безопасности. Кодекс практики менеджмента информационной безопасности = Інфармацыйныя тэхналогіі. Метады забеспячэння бяспекі. Кодэкс практыкі менеджменту інфармацыйнай бяспекі : СТБ ISO/IEC 27002-2012 ; введ. 01.01.2013. – Минск : Госстандарт Республики Беларусь, 2012. – 96 с.

32. Информационные технологии. Методы обеспечения безопасности. Руководство по внедрению систем менеджмента информационной безопасности = Інфармацыйныя тэхналогіі. Метады забеспячэння бяспекі. Кіраўніцтва па ўкараненні сістэм менеджменту інфармацыйнай бяспекі : СТБ ISO/IEC 27003-2014 ; введ. 01.02.2015. – Минск : Госстандарт Республики Беларусь, 2012. – 96 с.

33. Информационные технологии. Методы обеспечения безопасности. Менеджмент рисков информационной безопасности = Інфармацыйныя тэхналогіі. Метады забеспячэння бяспекі. Менеджмент рызык інфармацыйнай бяспекі : СТБ ISO/IEC 27005-2012 ; введ. 01.01.2013. – Минск : Госстандарт Республики Беларусь, 2012. – 68 с.

34. Информационные технологии. Методы обеспечения безопасности. Менеджмент информационной безопасности. Измерения = Інфармацыйныя тэхналогіі. Метады забеспячэння бяспекі. Менеджмент інфармацыйнай бяспекі. Вымярэнні : СТБ ISO/IEC 27004-2014 ; введ. 01.02.2015 Минск : Госстандарт Республики Беларусь, 2014. – 96 с.

35. Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования = Інфармацыйныя тэхналогіі. Метады забеспячэння бяспекі. Сістэмы менеджменту інфармацыйнай бяспекі. Патрабаванні : СТБ ISO/IEC 27001-2016 ; введ. 01.10.2016. . – Минск : Госстандарт Республики Беларусь, 2016. – 28 с.

36. Методические рекомендации по обеспечению информационной безопасности. Система менеджмента информационной безопасности [Электронный ресурс]. – Режим доступа: https://oac.gov.by/public/content/files/files/metod_recomend.docx. – Дата доступа: 01.09.2021.

37. Информационные технологии. Средства обеспечения безопасности. Требования для органов, выполняющих аудит и сертификацию систем менеджмента информационной безопасности = Інфармацыйныя тэхналогіі. Сродкі забеспячэння бяспекі. Патрабаванні для органаў, якія выконваюць аўдыт і сертыфікацыю сістэм менеджменту інфармацыйнай бяспекі : СТБ ISO/IEC 27006-2018 ; введ. 01.05.2018. – Минск : Госстандарт Республики Беларусь, 2012. – 46 с.

38. Информационные технологии. Методы обеспечения безопасности. Менеджмент инцидентов в области информационной безопасности = Інфармацыйныя тэхналогіі. Метады забеспячэння бяспекі. Менеджмент інцыдэнтаў у галіне інфармацыйнай бяспекі : СТБ ISO/IEC 27011-2017 ; введ. 01.03.2018 – Минск : Госстандарт Республики Беларусь, 2017. – 56 с.

39. Информационные технологии. Методы обеспечения безопасности. Оценка безопасности автоматизированных систем= Інфармацыйныя

тэхналогіі. Метады забеспячэння бяспекі. Ацэнка бяспекі аўтаматызаваных сістэм : СТБ ISO/IEC 27035-2017 ; введ. 01.03.2018. – Минск : Госстандарт Республики Беларусь, 2017. – 80 с.

40. Vulnerability distribution of CVE security vulnerabilities by types [Электронный ресурс]. – Режим доступа: https://www.cvedetails.com/ vulnerabilities-by-types.php. – Дата доступа: 01.09.2021.

41. Лившиц, И. И. Модель интегрированной системы менеджмента для обеспечения безопасности сложных объектов / И. И. Лившиц, Р. Р. Фаткиева // Вопросы кибербезопасности. – 2018. – № 1 (25). – С. 64–71.

42. Лившиц, И. И. Применение модели СМИБ для оценки защищенности интегрированных систем менеджмента / И. И. Лившиц // Труды СПИИРАН. – 2013. – № 8 (31). – С. 147–162.

43. Surcel, T. The Information Security Management System, Development and Audit / T. Surcel, C. Amancei // Informatica Economică. – 2007. – No. 4 (44). – P. 111–114.

44. Livshitz I. Evaluation of IT security – Genesis and its State-of-Art / I. Livshitz, A. Neklyudov, P. Lontsikh // Journal of Physics. – 2018. – 042029. – DOI: 10.1088/1742-6596/1015/4/042029.

45. Шаго Ф. Н. Модель и методика оценки системы менеджмента информационной безопасности : дис. ... канд. техн. наук : 05.13.19 / Ф. Н. Шаго. – СПб., 2014. –111 л.

46. Макаренко, С. И. Аудит информационной безопасности: основные этапы, концептуальные основы, классификация мероприятий / С. И. Макаренко // Системы управления, связи и безопасности. – 2018. – № 1. – С. 1–29.

47. Филяк, П. Ю. Обеспечение информационной безопасности организации на основе системы менеджмента информационной безопасности / П. Ю. Филяк, В. М. Шварев // Информация и безопасность. – 2015. – № 4. – С. 580–583.

48. Хлестова, Д. Р. Аудит информационной безопасности в организации / Д. Р. Хлестова, Ф. Т. Байрушин // Символ науки. – 2016. – № 11-3 (23). – С. 175–177.

49. Кравчук, Д. И. Аудит безопасности корпоративных информационных систем / Д. И. Кравчук, Д. А. Коркушко // Молодой ученый. – 2015. – № 10. – С. 755.

50. Гапоненко А.Л., Панкрухин А.П. Стратегическое управление. – М. : Омега-Л, 2008. – 464 с.

51. Управление качеством систем менеджмента информационной безопасности / А. В. Красов [и др.]. – СПб: СПбГУТ, 2016. – 75 с

52. Лившиц, И. И. Практическая оценка результативности СМИБ в соответствии с требованиями различных систем стандартизации – ИСО 27001 и СТО Газпром / И. И. Лившиц, А. В. Полещук // Труды СПИИРАН. – 2010. – № 3 (40). С. 33–44.

53. Model-based qualitative risk assessment for availability of it infrastructures / E. Zambon // Software System Modeling. – 2011. – Vol. 10(4). – P. 553–580.

54. A situation awareness model for information security risk management / J. Webb [et al.]. // Computers & Security. – 2014. – Vol. 44. – P. 1–15.

55. Просянников, Р. Е. Избавиться от заблуждений. Виды аудита информационной безопасности / Р. Е. Просянников// Connect! Мир связи. – 2004. – № 12. – С. 148–151

56. Фомин, А. А. Исследование и оптимизация алгоритмов аудита информационной безопасности организации / А. А. Фомин // Вопросы защиты информации. – 2009. – № 3 (86). – С. 57–63.

57. Иванова, Н. В. Метод аудита информационной безопасности информационных систем / Н. В. Иванова, О. Ю. Коробулина // Известия Петербургского университета путей сообщения. – 2010. – № 4. – С. 60–66.

58. Шаго, Ф. Н. Методика оптимизации планирования аудита системы менеджмента информационной безопасности / Ф. Н. Шаго, И. А. Зикратов // Научно-технический вестник информационных технологий, механики и оптики. – 2014. – № 2 (90). – С. 111–117.

59. Вакуленко, А. А. Инструменты выбора метода аудита информационной безопасности предприятия / А. А. Вакуленко, Н. С. Сорокопудов // Научный журнал НИУ ИТМО. Экономика и экологический менеджмент. – 2019. – № 3. – С. 163–169.

60. Pandey, S. K. A comparative study of risk assessment methodologies for information systems / S. K. Pandey, K. Mustafa // Bulletin of Electrical Engineering and Informatics. – 2012. – Vol. 1, no. 2. – P. 111–122.

61. Information security risk assessment / I. Kuzminykh [et al.] // Encyclopedia. – 2021. – Vol. 1(3). – P. 602–617.

62. Cramm – ENISA [Электронный ресурс]. – Режим доступа: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_cramm.html. – Дата доступа: 01.09.2021.

63. Возможности RiskWatch [Электронный ресурс]. – Режим доступа: https://studfile.net/preview/6177197/page:12/. – Дата доступа: 01.09.2021.

64. Welcome to William J. Peltier and Associates. Structural Engineering in Atlanta, Georgia [Электронный ресурс]. – http://www.williamjpeltier.com/. – Дата доступа: 01.09.2021.

65. Risk Analysis using FRAP: is it just Silo Thinking? – Analytica [Электронный ресурс]. – Режим доступа: https://lumina.com/risk-analysis-using-frap-is-it-just-silo-thinking/. – Дата доступа: 01.09.2021.

66. Octave – ENISA [Электронный ресурс]. – Режим доступа: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_octave.html. – Дата доступа: 01.09.2021.

67. Risk Assessment Platform: RiskWatch International [Электронный ресурс]. – Режим доступа: https://riskwatch.com/. – Дата доступа: 01.09.2021.

68. Информационная безопасность и анализ защищенности, консалтинг [Электронный ресурс]. – Режим доступа: https://dsec.ru/. – Дата доступа: 01.09.2021.

69. Программные средства проверки политики безопасности на соответствие ISO 17799 [Электронный ресурс]. – Режим доступа: https://www.ixbt.com/cm/iso17799-cobra-kondor012004.shtml. – Дата доступа: 01.09.2021.

70. Da Veiga, A. A framework and assessment instrument for information security culture / A. Da Veiga, J. Eloff // Computers & Security. – 2010. – Vol. 29, iss.2. – P. 196–207.

71. SECURQUAL: An instrument for evaluating the effectiveness of enterprise information security programs / P. J. Steinbart [et al.]. // Journal of Information Systems. – 2015. – Vol. 30(1). – P. 71–92.

72. Goodliff, P. B. CHEAT an approach to incorporating human factors in cyber security assessments / P. B. Goodliff, A. J. Widdowson // 10th IET System Safety and Cyber-Security Conference. – 2015. – Vol. 5, no. 5. – DOI: 10.1049/cp.2015.0298.

73. Независимый регулятор [Электронный ресурс]. – Режим доступа: https://oac.gov.by/activity/ict-development-and-services/independent-regulator. – Дата доступа: 01.09.2021.

74. Лившиц, И. И. Оценка защищенности объектов топливно-энергетического комплекса / И. И. Лившиц // Энергобезопасность и энергосбережение. – 2015.– № 5. – С. 5–10.

75. Лившиц, И. И. Методический подход к оценке защищенности информации в телекоммуникационных системах на основе анализа их доступности / И. И. Лившиц, В. В. Маликов // Вестник связи. – 2015. – № 2. – С. 57–61.

76. Лившиц, И. И. Оценка методических подходов для формирования систем безопасности сложных промышленных объектов топливно-энергетического комплекса / И. И. Лившиц // Вопросы защиты информации. – 2016. – № 1. – С. 56–61.

77. Лившиц, И. И. Подходы к применению модели интегрированной системы менеджмента для проведения аудитов сложных промышленных объектов – аэропортовых комплексов / И. И. Лившиц // Труды СПИИРАН. – 2014. – № 6. – С. 72–94.

78. Ясенев, В. Н. О концепции проведения аудита информационной безопасности в вузе / В. Н. Ясенев, А. В. Дорожкин, А. Л. Сочков // Учет. Анализ. Аудит. – 2019. – № 6. – С. 24–33.

79. Мартынов, А. Управление информационной безопасностью в банках. Особенности, реализация, аудит / А. Мартынов // Информационная безопасность. – 2007. – № 2. – С. 40–44.

80. Guidelines for auditing management systems = Руководящие указания по аудиту систем менеджмента : ISO 19011:2018 ; введ. 03.07.2018. – 56 с.

81. Principles of auditing. An introduction to international standards on auditing / R. Hayes [et al.]. – Pearson Education Limited, 2005. – 713 p.

82. Gantz, S. D. The Basics of IT Audit. Purposes, Processes, and Practical Information / S. D. Gantz. – Waltham : Elsevier Science, 2013. – 337 p.

83. Технический институт сертификации и испытаний. [Электронный ресурс]. – Режим доступа: http://www.tisi.by/stb_smk_process.html. – Дата доступа:15.08.2021.

84. Бойправ, В. А. Роль метрологической службы при сертификации системы менеджмента качества на предприятии / В. А. Бойправ // Метрология и приборостроение. – 2004. – № 1. – С. 29–31.

85. Лившиц, И. И. Менеджмент информационной безопасности / И. И. Лившиц // Стандарты и качество. – 2017. – № 9. – С. 48–52.

86. Информационные технологии. Методы и средства безопасности. Информационные системы. Классификация = Інфармацыйныя тэхналогіі. Метады і сродкі бяспекі. Інфармацыйныя сістэмы. Класіфікацыя : СТБ 34.101.30-2017 ; введ. 28.03.19. – Минск : Госстандарт Республики Беларусь, 2017. – 12 с.

87. Информационные технологии и безопасность. Безопасная эксплуатация и надежное функционирование критически важных объектов информатизации. Общие требования = Інфармацыйныя тэхналогіі і бяспека. Бяспечная эксплуатацыя і надзейнае функцыянаванне крытычна важных аб'ектаў інфарматызацыі : ТКП 483-2013 (01019). – Введ. 17.07.2013. – Минск : ОАЦ, 2013. – 6 с.

88. Белорусский бизнес. – [Электронный ресурс]. – Режим доступа: http://www.bizby.ru. – Дата доступа: 16.08.2019.

89. Информационно-справочный портал. – [Электронный ресурс]. – Режим доступа: http://www.belarusinfo.by. – Дата доступа: 16.08.2019.

90. Единый реестр лицензий. – [Электронный ресурс]. – Режим доступа: license.gov.by. – Дата доступа: 01.09.2021.

91. Common vulnerability scoring system / P. Mell [et al.] // IEEE Security & Privacy. – 2006. – Vol. 4, iss. 6. – P. 85–89.

92. Walkowski, M. Vulnerability management models using a common vulnerability scoring system / M. Walkowski, J. Oko, S. Sujecki // Applied Science. – 2021. – Vol. 11. – DOI: 10.3390/app11188735.

93. Ruohonen, J. A look at the time delays in CVSS vulnerability scoring / J. Ruohonen // Applied Computing and Informatics. – 2019. – Vol. 15, iss. 2. – P. 129–135.

94. CVSS v3.1 Specification Document [Электронный ресурс]. – Режим доступа: https://www.first.org/cvss/specification-document. – Дата доступа: 01.09.2021.

95. NVD – CVSS v3 Calculator [Электронный ресурс]. – Режим доступа: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator. – Дата доступа: 01.09.2021.

96. Мизиковский, И. Е. Методика экспертной оценки содержания и эксплуатации оборудования / И. Е. Мизиковский. – Аудит и финансовый анализ. – 2011. – № 4. – С. 1–3.

97. Сагитова, В. В. Применение метода экспертных оценок для автоматизации аудита информационных систем персональных данных / В. В. Сагитова, В. И. Васильев // Вестник УГАТУ. – 2017. – Т. 21, № 3 (73). – С. 105–112.

98. Van der Nest, D. P. The use of generalised audit software by internal audit functions in a developing country: a maturity level assessment / D. P. van der Nest, L. Smidt, D. Lubbe // Risk Governance and Control: Financial Markets & Institutions. – 2017. – Vol. 7(4-2). – P. 189–202.

99. Lehmann C. M. Integrating generalized audit software and teaching fraud detection in information systems auditing courses / C. M. Lehmann // Journal of Forensic & Investigative Accounting. – 2012. – Vol. 4, iss. 1. – P. 319–368.

100. Якимова, З. В. Динамика уровня вовлеченности персонала в зависимости от стажа работы в организации / З. В. Якимова, А. С. Пушкина // АНИ: экономика и управление. – 2018. – № 1 (22). – С. 283–286.

101. Spears, J. L. User participation in information systems security risk management / J. L. Spears, H. Barki // MIS Quarterly. – 2010. – Vol. 34 (3). P. 503-A5.

102. Ажмухамедов, И. М. Решение задач обеспечения информационной безопасности на основе системного анализа и нечеткого когнитивного моделирования / И. М. Ажмухамедов. – Астрахань, 2012. – 344 с.

103. Мизиковский, И. Е. Методика экспертной оценки содержания и эксплуатации оборудования / И. Е. Мизиковский. – Аудит и финансовый анализ. – 2011. – № 4. – С. 1–3.

104. Бойправ, В. А. Программное средство для проведения аудита системы защиты информации организации / В. А. Бойправ, В. В. Ковалев, Л. Л. Утин // Доклады БГУИР. – 2018. – № 5 (115). – С. 44–49.

105. Бойправ, В. А. Методика и программное средство для проведения аудита систем менеджмента информационной безопасности / В. А. Бойправ, Л. Л. Утин // Информатика. – 2022. – № 19 (4). – С. 42–52.

106. Утин, Л. Л. О некоторых нормативно-правовых коллизиях аудита информационной безопасности в организациях электросвязи / Л. Л. Утин, В. А. Бойправ // Комплексная защита информации : матер. докл. XXII науч.-практ. конф., Полоцк, 16–19 мая 2017 г. ; редкол. : Ю. С. Харин [и др.] – Полоцк : УО «ПГУ», 2016. – С. 218–220.

107. Бойправ, В. А. Актуализация разработки программного средства для проведения аудита системы защиты информации организаций электросвязи / В. А. Бойправ, Л. Л. Утин, В. В. Ковалев // Управление информационными ресурсами : матер. XIII Междунар. научно-практ. конф., Минск, 9 декабря 2016 г. / редкол.: А. В. Ивановский, Б. В. Новыш. – Минск : Академия управления при Президенте Республики Беларусь, 2016. – С. 181–182.

108. Бойправ, В. А. Обеспечение безопасности инфокоммуникационных сетей на этапе их проектирования и строительства / В. А. Бойправ, Л. Л. Утин // Управление информационными ресурсами : матер. XIV Междунар. научн.-практ. конф., Минск, 20 дек. 2017 г. / Акад. упр. при Президенте Респ. Беларусь ; редкол.: А. В. Ивановский [и др.]. – Минск: Академия управления при Президенте Республики Беларусь, 2017. – С. 156–157.

109. Бойправ, В. А. Принципы реализации методики аудита системы менеджмента защиты информации в организациях электросвязи / В. А. Бойправ, Л. Л. Утин // Доклады БГУИР. – 2016. – № 6 (100). – С. 94–99.

110. Бойправ, В. А. Особенности подготовительного этапа аудита системы менеджмента защиты информации в организациях электросвязи / В. А. Бойправ, Л. Л. Утин // Доклады БГУИР. – 2018. – № 1 (111). – С. 43–50.

111.Бойправ, В. А. Анализ мероприятий по аудиту системы безопасности филиала «Минская городская телефонная сеть» РУП «Белтелеком» / В. А. Бойправ, О. В. Бойправ, Л. М. Лыньков // Современные средства связи :

матер. XVII Междунар. науч.-техн. конф., Минск, 16–18 окт. 2012 г. / ВГКС ; редкол.: А. О. Зеневич [и др.]. – Минск : УО ВГКС, 2012. – С. 249.

112. Бойправ, В. А. Проведение аудита системы информационной безопасности на предприятии отрасли связи / В. А. Бойправ, О. В. Бойправ, Л. М. Лыньков // Управление информационными ресурсами : матер. IX Междунар. науч.-практ. конф., Минск, 21 ноя. 2012 г. / Акад. упр. при Президенте Респ. Беларусь ; редкол. А. В. Ивановский [и др.]. – Минск, 2012. – С. 69–70.

113. Бойправ, В. А. Методика обеспечения информационной безопасности на предприятии отрасли связи / В. А. Бойправ, О. В. Бойправ, Л. М. Лыньков // Телекоммуникации : сети и технологии, алгебраическое кодирование и безопасность данных : матер. междунар. науч.-техн. семинара, Минск, янв.–дек. 2012 г. / Бел. гос. ун-т информатики и радиоэлектроники ; редкол. : В. К. Конопелько [и др.]. – Минск : БГУИР, 2012. – С. 83–86.

114. Бойправ, В. А. Подходы к разработке систем менеджмента информационной безопасности в телекоммуникационных организациях в контексте концепции национальной безопасности Республики Беларусь / В. А. Бойправ, Л. Л. Утин // Технологии информатизации и управления : сб. науч. ст. – Вып. 3. В 2 кн. Кн. 1 / под ред. А. М. Кадана, Е. А. Свирского. – Минск : РИВШ, 2017. – С. 9–12.

115. Бойправ, В. А. Методика обработки результатов аудита системы менеджмента защиты информации организаций электросвязи / В. А. Бойправ, Л. Л. Утин // Современные средства связи : матер. XXII Междунар. науч.-техн. конф., Минск, 19–20 окт. 2017 г. / ВГКС ; редкол. : А. О. Зеневич [и др.]. – Минск : УО ВГКС, 2017. – С. 253–254.

116. Бойправ, В. А. Оценка потенциальных уязвимостей информационных систем и сетей организаций электросвязи / В. А. Бойправ, Л. Л. Утин // Кодирование и цифровая обработка сигналов в инфокоммуникациях : матер. междунар. научно-практ. конф., Минск, 4 апреля 2019 г. / Бел. гос. ун-т информатики и радиоэлектроники ; редкол. : В. К. Конопелько, В. Ю. Цветков, Л. А. Шичко. – Минск : БГУИР, 2019. – С. 104–108.

117. Бойправ В. А. Оценка состояния защищенности информации на телекоммуникационных предприятиях с учетом требований законодательства Республики Беларусь / В. А. Бойправ, Л. Л. Утин // Технические средства защиты информации : тез. докл. XIV Бел.-росс. науч.-техн. конф., Минск, 25–26 мая 2016 г. ; редкол. : Л. М. Лыньков [и др.]. – Минск: БГУИР, 2016. – С. 24–25.

118. Бойправ, В. А. Особенности анкетирования сотрудников организаций электросвязи при проведении аудита системы менеджмента защиты информации / В. А. Бойправ, Л. Л. Утин, В. В. Ковалёв //

Технические средства защиты информации : тез. докл. XV Бел.-росс. науч.-техн. конф., Минск, 6 июня 2017 г. ; редкол. : Т. В. Борботько [и др.]. – Минск : БГУИР, 2017. – С. 13–14.

119. Бойправ, В. А. Особенности математической модели методики оценки рисков информационной безопасности предприятий отрасли связи / В. А. Бойправ, Л. Л. Утин // Технические средства защиты информации : тез. докл. XVI Бел.-росс. науч.-техн. конф., Минск, 5 июня 2018 г. ; редкол. : Т. В. Борботько [и др.]. – Минск : БГУИР, 2018. – С. 22.

120 Бойправ, В. А. Интегрированная модель аудита систем менеджмента информационной безопасности предприятий отрасли связи Республики Беларусь / В. А. Бойправ, Л. Л. Утин // Технические средства защиты информации : тез. докл. XIX Бел.-росс. науч.-техн. конф., Минск, 8 июня 2021 г. ; редкол. : Т. В. Борботько [и др.]. – Минск : БГУИР, 2021. – С. 19–20.

121. Свидетельство о регистрации компьютерной программы № 1447. Программное средство для аудита систем менеджмента информационной безопасности организаций Республики Беларусь : заявлено 03.09.2021 : опубл. 14.10.2021 / Бойправ В. А., Утин Л. Л.

ПРИЛОЖЕНИЕ А

Перечни вопросов для анкетирования сотрудников организаций электросвязи Республики Беларусь при проведении аудита СМИБ этих организаций

Перечень вопросов для анкетирования руководителей и главных инженеров организаций электросвязи категорий 1–4

1. Внедрена и используется ли в Вашей организации политика ИБ?
2. Назначено ли в Вашей организации лицо, на которое возложены обязанности по контролю за соблюдением положений политики ИБ? (Если лицо назначено, указать его должность)
3. Организуются ли на регулярной основе для субъектов ИС, используемой в Вашей организации для обработки информации распространение и (или) предоставление к которой ограничено (далее – ИС), курсы повышения квалификации по вопросам обеспечения ИБ этих систем?
4. Осведомляются ли увольняемые сотрудники Вашей организации, которые имели доступ к информации, распространение и (или) предоставление к которой ограничено, об ответственности, к которой они могут быть привлечены вследствие разглашения этой информации третьим лицам?
5. Проектирование и внедрение системы защиты информации ИС, а также политики ИБ реализовывалась силами Ваших сотрудников?
6. Если для реализации мероприятий, указанных в предыдущем вопросе, привлекались (привлекаются) сотрудники сторонних организаций, то устанавливалась (устанавливается) ли ответственность сторон по обеспечению безопасности ИС?
7. Если для реализации мероприятий, указанных в вопросе 5, привлекались (привлекаются) сотрудники сторонних организаций, то имеют ли эти организации специальные разрешения (лицензии) на деятельность по технической и (или) криптографической защите информации в части соответствующих составляющих данный вид деятельности работ и услуг?
8. Есть ли в штате Вашей организации сотрудники, имеющие квалификацию специалиста по защите информации или прошедшие переподготовку по специальности «Защита информации»?

Перечень вопросов для анкетирования начальников службы безопасности организаций электросвязи категорий 1–4

1. Выполнена ли классификация информации, хранящейся и обрабатываемой в ИС Вашей организации, в соответствии с законом Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации»?

2. Выполнена ли классификация ИС, доступ к которым имеют сотрудники Вашей организации?

3. Если ответ на предыдущий вопрос положительный, то осведомлены ли сотрудники Вашей организации, которые имеют доступ к ИС, о том, к какому классу относятся эти системы и информация какой категории обрабатывается ими?

4. Выполняется ли в Вашей организации классификация активов ИС, доступ к которым имеют сотрудники?

5. Можете ли Вы сказать, что система защиты информации в Вашей организации представляет собой совокупность организационных, технических и правовых мер?

6. Известно ли Вам, на кого из сотрудников Вашей организации возложены обязанности по контролю за соблюдением положений политики ИБ?

7. Если мероприятия по контролю за соблюдением положений политики ИБ выполняются, то входит ли в их перечень проверка знаний сотрудников об их обязанностях по обеспечению защиты информации, используемой ими, или безопасности ИС, доступ к которым они получают?

8. Корректируется ли в Вашей организации СМИБ и политика ИБ?

9. Имеются ли случаи, когда лица, не относящихся к числу сотрудников организации, пребывают в пределах контролируемой зоны ИС, применяемых Вашей организацией?

10. Если ответ на предыдущий вопрос положительный, то выполняется ли сопровождение этих лиц сотрудниками Вашей организации и документируется ли информация о времени и цели пребывания этих лиц в пределах контролируемой зоны ИС?

11. Осведомляется ли сотрудник Вашей организации, который сопровождает лиц, пребывающих в пределах контролируемой зоны ИС, о том, какие сведения об этой системе не подлежат разглашению?

12. Ситуативно ли назначается сотрудник, который сопровождает лиц, пребывающих в пределах контролируемой зоны ИС?

13. Проводится ли регулярное тестирование работоспособности систем охранной и пожарной сигнализации (в том числе при имитации критических условий эксплуатации)?

Перечень вопросов для анкетирования старших производителей работ или начальников строительных участков организаций электросвязи категории 1

1. Выполняете ли Вы проверку средств и линий электросвязи на предмет отсутствия производственных дефектов перед их монтажом?
2. Если ответ на предыдущий вопрос положительный, то каким документом регламентируется процесс выполнения названной проверки?
3. Выполняете ли Вы измерение амплитуды побочных электромагнитных излучений средств и линий электросвязи в процессе их пуско-наладки?
4. Выполняется ли оценка защищенности от воздействия внешних факторов (неблагоприятные погодные условия) построенных объектов электросвязи?
5. Если ответ на предыдущий вопрос положительный, то каким документом регламентируется процесс выполнения такой оценки?
6. Всегда ли выполняется силами сотрудников Вашей организации монтаж инженерно-технических средств защиты объектов электросвязи?
7. Если ответ на предыдущий вопрос отрицательный, то реализуется ли контроль пребывания сотрудников сторонних организаций, выполняющих монтаж инженерно-технических средств защиты объектов электросвязи, в пределах контролируемой зоны этих объектов?
8. Выполняется ли оценка состояния инженерно-технических средств защиты объектов электросвязи?
9. Если ответ на предыдущий вопрос положительный, то как часто выполняется такая оценка? Какие критерии используются для выполнения такой оценки?
10. Проводите ли Вы с подчиненными Вам сотрудниками теоретическое и практическое обучение по вопросам устранения повреждений средств и линий электросвязи?
11. Имеют ли подчиненные Вам сотрудники постоянные пропуска в пределы контролируемой зоны объектов электросвязи, работы по строительству и пуско-наладке которых уже выполнены силами Вашей организации?
12. Если ответ на предыдущий вопрос отрицательный, то каким образом и как быстро Вы и подчиненные Вам сотрудники получаете доступ в пределы контролируемой зоны объекта электросвязи после возникновения необходимости устранения повреждений его элементов?

ПРИЛОЖЕНИЕ Б
Содержание модулей для формирования контрольных листов

Содержание модуля 3.1 для формирования контрольного листа № 3

Выберите реализуемые на Вашем предприятии мероприятия из представленного ниже перечня.

Определение состава информации о событиях информационной безопасности, подлежащих регистрации.

Обеспечение сбора и хранения информации о событиях информационной безопасности в течение установленного срока хранения, но не менее одного года.

Определение способа и периодичности мониторинга (просмотра, анализа) событий информационной безопасности уполномоченными на это пользователями информационной системы.

Обеспечение сбора и хранения информации о функционировании средств вычислительной техники, сетевого оборудования и средств защиты информации в течение установленного срока хранения, но не менее одного года.

Регламентация порядка использования в информационной системе съемных носителей информации, мобильных технических средств и контроля за таким использованием.

Обеспечение контроля за работоспособностью, параметрами настройки и правильностью функционирования средств вычислительной техники, сетевого оборудования, системного программного обеспечения и средств защиты информации.

Обеспечение защиты от несанкционированного доступа к резервным копиям, параметрам настройки сетевого оборудования, системного программного обеспечения, средств защиты информации и событиям безопасности.

Обеспечение контроля за соблюдением правил генерации и смены паролей пользователей информационной системы.

Обеспечение блокировки доступа к объектам информационной системы после истечения установленного времени бездействия (неактивности) пользователя информационной системы или по его запросу.

Обеспечение разграничения доступа пользователей к средствам вычислительной техники, сетевому оборудованию, системному программному обеспечению и средствам защиты информации.

Обеспечение контроля за соблюдением правил генерации и смены паролей пользователей информационной системы.

Определение перечня разрешенного программного обеспечения и регламентация порядка его установки.

Обеспечение контроля за составом объектов информационной системы.

Использование объектов информационной системы под пользовательскими учетными записями (использование административных учетных записей только в случае настройки объектов информационной системы или особенностей объектов информационной системы).

Определение состава и содержания информации, подлежащей резервированию.

Обеспечение обновления программного обеспечения объектов информационной системы и контроля за своевременностью такого обновления.

Содержание модуля 3.2 для формирования контрольного листа № 3

Выберите реализуемые на Вашем предприятии мероприятия из представленного ниже перечня.

Обеспечение идентификации и аутентификации пользователей информационной системы.

Обеспечение защиты обратной связи при вводе аутентификационной информации.

Обеспечение полномочного управления (создание, активация, блокировка и уничтожение) учетными записями пользователей информационной системы.

Обеспечение блокировки доступа к объектам информационной системы после истечения установленного времени бездействия (неактивности) пользователя информационной системы или по его запросу.

Обеспечение резервирования информации, подлежащей резервированию.

Обеспечение защиты средств вычислительной техники от вредоносных программ.

Обеспечение подлинности и контроля целостности электронных документов в информационной системе (средства выработки электронной цифровой подписи, средства проверки электронной цифровой подписи, средства выработки личного ключа или открытого ключа электронной цифровой подписи).

Содержание модуля 3.3 для формирования контрольного листа № 3

Выберите реализуемые на Вашем предприятии мероприятия из представленного ниже перечня.

Обеспечение изменения атрибутов безопасности сетевого оборудования, системного программного обеспечения и средств защиты информации, установленных по умолчанию.

Обеспечение обновления объектов информационной системы.

Обеспечение контроля и управления физическим доступом в помещения, в которых постоянно размещаются объекты информационной системы.

Обеспечение синхронизации временных меток и (или) системного времени в информационной системе и системе защиты информации.

Содержание модуля 4.1 для формирования контрольного листа № 4

Выберите реализуемые на Вашем предприятии мероприятия из представленного ниже перечня.

Определение состава информации о событиях информационной безопасности, подлежащих регистрации.

Обеспечение сбора и хранения информации о событиях информационной безопасности в течение установленного срока хранения, но не менее одного года.

Определение способа и периодичности мониторинга (просмотра, анализа) событий информационной безопасности уполномоченными на это пользователями информационной системы.

Обеспечение сбора и хранения информации о функционировании средств вычислительной техники, сетевого оборудования и средств защиты информации в течение установленного срока хранения, но не менее одного года.

Регламентация порядка использования в информационной системе съемных носителей информации, мобильных технических средств и контроля за таким использованием.

Обеспечение контроля за работоспособностью, параметрами настройки и правильностью функционирования средств вычислительной техники, сетевого оборудования, системного программного обеспечения и средств защиты информации.

Обеспечение защиты от несанкционированного доступа к резервным копиям, параметрам настройки сетевого оборудования, системного программного обеспечения, средств защиты информации и событиям безопасности.

Обеспечение контроля за соблюдением правил генерации и смены паролей пользователей информационной системы.

Обеспечение блокировки доступа к объектам информационной системы после истечения установленного времени бездействия (неактивности) пользователя информационной системы или по его запросу.

Обеспечение разграничения доступа пользователей к средствам вычислительной техники, сетевому оборудованию, системному программному обеспечению и средствам защиты информации.

Обеспечение контроля за соблюдением правил генерации и смены паролей пользователей информационной системы.

Определение перечня разрешенного программного обеспечения и регламентация порядка его установки.

Обеспечение контроля за составом объектов информационной системы

Использование объектов информационной системы под пользовательскими учетными записями (использование административных учетных записей только в случае настройки объектов информационной системы или особенностей объектов информационной системы).

Определение состава и содержания информации, подлежащей резервированию.

Обеспечение обновления программного обеспечения объектов информационной системы и контроля за своевременностью такого обновления.

Содержание модуля 4.2 для формирования контрольного листа № 4

Выберите реализуемые на Вашем предприятии мероприятия из представленного ниже перечня.

Обеспечение идентификации и аутентификации пользователей информационной системы.

Обеспечение защиты обратной связи при вводе аутентификационной информации.

Обеспечение полномочного управления (создание, активация, блокировка и уничтожение) учетными записями пользователей информационной системы.

Обеспечение блокировки доступа к объектам информационной системы после истечения установленного времени бездействия (неактивности) пользователя информационной системы или по его запросу.

Обеспечение резервирования информации, подлежащей резервированию.

Обеспечение защиты средств вычислительной техники от вредоносных программ.

Обеспечение подлинности и контроля целостности электронных документов в информационной системе (средства выработки электронной цифровой подписи, средства проверки электронной цифровой подписи, средства выработки личного ключа или открытого ключа электронной цифровой подписи).

Содержание модуля 4.3 для формирования контрольного листа № 4

Выберите реализуемые на Вашем предприятии мероприятия из представленного ниже перечня.

Физическая изоляция сегмента виртуальной инфраструктуры (системы хранения и обработки данных), предназначенного для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам.

Содержание модуля 4.4 для формирования контрольного листа № 4

Выберите реализуемые на Вашем предприятии мероприятия из представленного ниже перечня.

Обеспечение изменения атрибутов безопасности сетевого оборудования, системного программного обеспечения и средств защиты информации, установленных по умолчанию.

Обеспечение обновления объектов информационной системы.

Обеспечение контроля и управления физическим доступом в помещения, в которых постоянно размещаются объекты информационной системы.

Обеспечение синхронизации временных меток и (или) системного времени в информационной системе и системе защиты информации.

Содержание модуля 5.1 для формирования контрольного листа № 5

Выберите реализуемые на Вашем предприятии мероприятия из представленного ниже перечня.

Определение состава информации о событиях информационной безопасности, подлежащих регистрации.

Обеспечение сбора и хранения информации о событиях информационной безопасности в течение установленного срока хранения, но не менее одного года.

Определение способа и периодичности мониторинга (просмотра, анализа) событий информационной безопасности уполномоченными на это пользователями информационной системы.

Обеспечение сбора и хранения информации о функционировании средств вычислительной техники, сетевого оборудования и средств защиты информации в течение установленного срока хранения, но не менее одного года.

Регламентация порядка использования в информационной системе съемных носителей информации, мобильных технических средств и контроля за таким использованием.

Обеспечение контроля за работоспособностью, параметрами настройки и правильностью функционирования средств вычислительной техники,

сетевого оборудования, системного программного обеспечения и средств защиты информации.

Обеспечение защиты от несанкционированного доступа к резервным копиям, параметрам настройки сетевого оборудования, системного программного обеспечения, средств защиты информации и событиям безопасности.

Обеспечение контроля за соблюдением правил генерации и смены паролей пользователей информационной системы.

Обеспечение блокировки доступа к объектам информационной системы после истечения установленного времени бездействия (неактивности) пользователя информационной системы или по его запросу.

Обеспечение разграничения доступа пользователей к средствам вычислительной техники, сетевому оборудованию, системному программному обеспечению и средствам защиты информации.

Обеспечение контроля за соблюдением правил генерации и смены паролей пользователей информационной системы.

Определение перечня разрешенного программного обеспечения и регламентация порядка его установки.

Обеспечение контроля за составом объектов информационной системы

Использование объектов информационной системы под пользовательскими учетными записями (использование административных учетных записей только в случае настройки объектов информационной системы или особенностей объектов информационной системы).

Определение состава и содержания информации, подлежащей резервированию.

Обеспечение обновления программного обеспечения объектов информационной системы и контроля за своевременностью такого обновления.

Содержание модуля 5.2 для формирования контрольного листа № 5

Выберите реализуемые на Вашем предприятии мероприятия из представленного ниже перечня.

Обеспечение идентификации и аутентификации пользователей информационной системы.

Обеспечение защиты обратной связи при вводе аутентификационной информации.

Обеспечение полномочного управления (создание, активация, блокировка и уничтожение) учетными записями пользователей информационной системы.

Обеспечение блокировки доступа к объектам информационной системы после истечения установленного времени бездействия (неактивности) пользователя информационной системы или по его запросу.

Обеспечение резервирования информации, подлежащей резервированию.

Обеспечение защиты средств вычислительной техники от вредоносных программ.

Обеспечение подлинности и контроля целостности электронных документов в информационной системе (средства выработки электронной цифровой подписи, средства проверки электронной цифровой подписи, средства выработки личного ключа или открытого ключа электронной цифровой подписи).

Обеспечение конфиденциальности и контроля целостности личных ключей, используемых при выработке электронной цифровой подписи (криптографические токены).

Содержание модуля 5.3 для формирования контрольного листа № 5

Выберите реализуемые на Вашем предприятии мероприятия из представленного ниже перечня.

Обеспечение защиты от агрессивного использования ресурсов виртуальной инфраструктуры потребителями услуг.

Обеспечение защиты виртуальной инфраструктуры от несанкционированного доступа и сетевых атак из виртуальной и физической сети, а также виртуальных машин.

Обеспечение резервного копирования пользовательских виртуальных машин.

Физическая изоляция сегмента виртуальной инфраструктуры (системы хранения и обработки данных), предназначенного для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам.

Содержание модуля 5.4 для формирования контрольного листа № 5

Выберите реализуемые на Вашем предприятии мероприятия из представленного ниже перечня.

Обеспечение изменения атрибутов безопасности сетевого оборудования, системного программного обеспечения и средств защиты информации, установленных по умолчанию.

Обеспечение обновления объектов информационной системы.

Обеспечение контроля и управления физическим доступом в помещения, в которых постоянно размещаются объекты информационной системы.

Обеспечение синхронизации временных меток и (или) системного времени в информационной системе и системе защиты информации.

Содержание модуля 6.1 для формирования контрольного листа № 6

Выберите реализуемые на Вашем предприятии мероприятия из представленного ниже перечня.

Определение состава информации о событиях информационной безопасности, подлежащих регистрации.

Обеспечение сбора и хранения информации о событиях информационной безопасности в течение установленного срока хранения, но не менее одного года.

Определение способа и периодичности мониторинга (просмотра, анализа) событий информационной безопасности уполномоченными на это пользователями информационной системы.

Обеспечение сбора и хранения информации о функционировании средств вычислительной техники, сетевого оборудования и средств защиты информации в течение установленного срока хранения, но не менее одного года.

Регламентация порядка использования в информационной системе съемных носителей информации, мобильных технических средств и контроля за таким использованием.

Обеспечение контроля за работоспособностью, параметрами настройки и правильностью функционирования средств вычислительной техники, сетевого оборудования, системного программного обеспечения и средств защиты информации.

Обеспечение защиты от несанкционированного доступа к резервным копиям, параметрам настройки сетевого оборудования, системного программного обеспечения, средств защиты информации и событиям безопасности.

Обеспечение контроля за соблюдением правил генерации и смены паролей пользователей информационной системы.

Обеспечение блокировки доступа к объектам информационной системы после истечения установленного времени бездействия (неактивности) пользователя информационной системы или по его запросу.

Обеспечение разграничения доступа пользователей к средствам вычислительной техники, сетевому оборудованию, системному программному обеспечению и средствам защиты информации.

Обеспечение контроля за соблюдением правил генерации и смены паролей пользователей информационной системы.

Определение перечня разрешенного программного обеспечения и регламентация порядка его установки.

Обеспечение контроля за составом объектов информационной системы.

Использование объектов информационной системы под пользовательскими учетными записями (использование административных

учетных записей только в случае настройки объектов информационной системы или особенностей объектов информационной системы).

Определение состава и содержания информации, подлежащей резервированию.

Обеспечение обновления программного обеспечения объектов информационной системы и контроля за своевременностью такого обновления.

Определение перечня внешних подключений к информационной системе и порядка такого подключения.

Содержание модуля 6.2 для формирования контрольного листа № 6

Выберите реализуемые на Вашем предприятии мероприятия из представленного ниже перечня.

Обеспечение идентификации и аутентификации пользователей информационной системы.

Обеспечение защиты обратной связи при вводе аутентификационной информации.

Обеспечение полномочного управления (создание, активация, блокировка и уничтожение) учетными записями пользователей информационной системы.

Обеспечение блокировки доступа к объектам информационной системы после истечения установленного времени бездействия (неактивности) пользователя информационной системы или по его запросу.

Обеспечение резервирования информации, подлежащей резервированию.

Обеспечение защиты средств вычислительной техники от вредоносных программ.

Обеспечение подлинности и контроля целостности электронных документов в информационной системе (средства выработки электронной цифровой подписи, средства проверки электронной цифровой подписи, средства выработки личного ключа или открытого ключа электронной цифровой подписи).

Обеспечение обнаружения и предотвращения вторжений в информационной системе. Использование сетевых, и (или) поведенческих, и (или) узловых систем обнаружения и предотвращения вторжений.

Обеспечение обнаружения и предотвращения вторжений в информационной системе при использовании в ней беспроводных каналов передачи данных (Wi-Fi и тому подобное). Использование беспроводных систем обнаружения и предотвращения вторжений.

Обеспечение контроля за внешними подключениями к информационной системе.

Содержание модуля 6.3 для формирования контрольного листа № 6

Выберите реализуемые на Вашем предприятии мероприятия из представленного ниже перечня.

Обеспечение защиты от агрессивного использования ресурсов виртуальной инфраструктуры потребителями услуг.

Обеспечение защиты виртуальной инфраструктуры от несанкционированного доступа и сетевых атак из виртуальной и физической сети, а также виртуальных машин.

Обеспечение резервного копирования пользовательских виртуальных машин.

Содержание модуля 6.4 для формирования контрольного листа № 6

Выберите реализуемые на Вашем предприятии мероприятия из представленного ниже перечня.

Обеспечение конфиденциальности и контроля целостности информации при ее передаче посредством сетей электросвязи общего пользования (средства линейного или предварительного шифрования).

Обеспечение резервирования конфигурационных файлов сетевого оборудования.

Обеспечение в реальном масштабе времени автоматической проверки файлов данных, передаваемых по почтовым протоколам, и обезвреживание обнаруженных вредоносных программ.

Обеспечение управления внешними информационными потоками (маршрутизация) между информационными системами. Использование маршрутизатора (коммутатора маршрутизирующего).

Обеспечение ограничений входящего и исходящего трафика (фильтрация) информационной системы только необходимыми соединениями. Использование межсетевого экрана, функционирующего на канальном, и (или) сетевом, и (или) транспортном, и (или) сеансовом, и (или) прикладном уровнях.

Содержание модуля 6.5 для формирования контрольного листа № 6

Выберите реализуемые на Вашем предприятии мероприятия из представленного ниже перечня.

Обеспечение изменения атрибутов безопасности сетевого оборудования, системного программного обеспечения и средств защиты информации, установленных по умолчанию.

Обеспечение обновления объектов информационной системы.

Обеспечение контроля и управления физическим доступом в помещения, в которых постоянно размещаются объекты информационной системы.

Обеспечение синхронизации временных меток и (или) системного времени в информационной системе и системе защиты информации.

Содержание модуля 7.1 для формирования контрольного листа № 7

Выберите реализуемые на Вашем предприятии мероприятия из представленного ниже перечня.

Определение состава информации о событиях информационной безопасности, подлежащих регистрации.

Обеспечение сбора и хранения информации о событиях информационной безопасности в течение установленного срока хранения, но не менее одного года.

Определение способа и периодичности мониторинга (просмотра, анализа) событий информационной безопасности уполномоченными на это пользователями информационной системы.

Обеспечение сбора и хранения информации о функционировании средств вычислительной техники, сетевого оборудования и средств защиты информации в течение установленного срока хранения, но не менее одного года.

Регламентация порядка использования в информационной системе съемных носителей информации, мобильных технических средств и контроля за таким использованием.

Обеспечение контроля за работоспособностью, параметрами настройки и правильностью функционирования средств вычислительной техники, сетевого оборудования, системного программного обеспечения и средств защиты информации.

Обеспечение защиты от несанкционированного доступа к резервным копиям, параметрам настройки сетевого оборудования, системного программного обеспечения, средств защиты информации и событиям безопасности.

Обеспечение контроля за соблюдением правил генерации и смены паролей пользователей информационной системы.

Обеспечение блокировки доступа к объектам информационной системы после истечения установленного времени бездействия (неактивности) пользователя информационной системы или по его запросу.

Обеспечение разграничения доступа пользователей к средствам вычислительной техники, сетевому оборудованию, системному программному обеспечению и средствам защиты информации.

Обеспечение контроля за соблюдением правил генерации и смены паролей пользователей информационной системы.

Определение перечня разрешенного программного обеспечения и регламентация порядка его установки.

Обеспечение контроля за составом объектов информационной системы.

Использование объектов информационной системы под пользовательскими учетными записями (использование административных учетных записей только в случае настройки объектов информационной системы или особенностей объектов информационной системы).

Определение состава и содержания информации, подлежащей резервированию.

Обеспечение обновления программного обеспечения объектов информационной системы и контроля за своевременностью такого обновления.

Определение перечня внешних подключений к информационной системе и порядка такого подключения.

Обеспечение централизованного управления учетными записями пользователей информационной системы и контроль за соблюдением правил генерации и смены паролей пользователей информационной системы.

Обеспечение сегментирования (изоляции) сети управления объектами информационной системы от сети передачи данных.

Содержание модуля 7.2 для формирования контрольного листа № 7

Выберите реализуемые на Вашем предприятии мероприятия из представленного ниже перечня.

Обеспечение идентификации и аутентификации пользователей информационной системы.

Обеспечение защиты обратной связи при вводе аутентификационной информации.

Обеспечение полномочного управления (создание, активация, блокировка и уничтожение) учетными записями пользователей информационной системы.

Обеспечение блокировки доступа к объектам информационной системы после истечения установленного времени бездействия (неактивности) пользователя информационной системы или по его запросу.

Обеспечение резервирования информации, подлежащей резервированию.

Обеспечение защиты средств вычислительной техники от вредоносных программ.

Обеспечение подлинности и контроля целостности электронных документов в информационной системе (средства выработки электронной цифровой подписи, средства проверки электронной цифровой подписи, средства выработки личного ключа или открытого ключа электронной цифровой подписи).

Обеспечение конфиденциальности и контроля целостности личных ключей, используемых при выработке электронной цифровой подписи (криптографические токены).

Обеспечение обнаружения и предотвращения вторжений в информационной системе. Использование сетевых, и (или) поведенческих, и (или) узловых систем обнаружения и предотвращения вторжений.

Обеспечение обнаружения и предотвращения вторжений в информационной системе при использовании в ней беспроводных каналов передачи данных (Wi-Fi и тому подобное). Использование беспроводных систем обнаружения и предотвращения вторжений.

Обеспечение контроля за внешними подключениями к информационной системе.

Автоматизированный контроль за составом средств вычислительной техники и сетевого оборудования.

Содержание модуля 7.3 для формирования контрольного листа № 7

Выберите реализуемые на Вашем предприятии мероприятия из представленного ниже перечня.

Обеспечение защиты от агрессивного использования ресурсов виртуальной инфраструктуры потребителями услуг.

Обеспечение защиты виртуальной инфраструктуры от несанкционированного доступа и сетевых атак из виртуальной и физической сети, а также виртуальных машин.

Обеспечение резервного копирования пользовательских виртуальных машин.

Физическая изоляция сегмента виртуальной инфраструктуры (системы хранения и обработки данных), предназначенного для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам.

Содержание модуля 7.4 для формирования контрольного листа № 7

Выберите реализуемые на Вашем предприятии мероприятия из представленного ниже перечня.

Обеспечение конфиденциальности и контроля целостности информации при ее передаче посредством сетей электросвязи общего пользования (средства линейного или предварительного шифрования).

Обеспечение резервирования конфигурационных файлов сетевого оборудования.

Обеспечение в реальном масштабе времени автоматической проверки файлов данных, передаваемых по почтовым протоколам, и обезвреживание обнаруженных вредоносных программ.

Обеспечение управления внешними информационными потоками (маршрутизация) между информационными системами. Использование маршрутизатора (коммутатора маршрутизирующего).

Обеспечение ограничений входящего и исходящего трафика (фильтрация) информационной системы только необходимыми соединениями. Использование межсетевого экрана, функционирующего на канальном, и (или) сетевом, и (или) транспортном, и (или) сеансовом, и (или) прикладном уровнях.

Обеспечение в реальном масштабе времени автоматической проверки пакетов сетевого трафика и файлов данных, передаваемых по сети, и обезвреживание обнаруженных вредоносных программ.

Содержание модуля 7.5 для формирования контрольного листа № 7

Выберите реализуемые на Вашем предприятии мероприятия из представленного ниже перечня.

Обеспечение изменения атрибутов безопасности сетевого оборудования, системного программного обеспечения и средств защиты информации, установленных по умолчанию.

Обеспечение обновления объектов информационной системы.

Обеспечение контроля и управления физическим доступом в помещения, в которых постоянно размещаются объекты информационной системы.

Обеспечение синхронизации временных меток и (или) системного времени в информационной системе и системе защиты информации.

Содержание модуля 8.1 для формирования контрольного листа № 8

Выберите реализуемые на Вашем предприятии мероприятия из представленного ниже перечня.

Определение состава информации о событиях информационной безопасности, подлежащих регистрации.

Обеспечение сбора и хранения информации о событиях информационной безопасности в течение установленного срока хранения, но не менее одного года.

Определение способа и периодичности мониторинга (просмотра, анализа) событий информационной безопасности уполномоченными на это пользователями информационной системы.

Обеспечение сбора и хранения информации о функционировании средств вычислительной техники, сетевого оборудования и средств защиты информации в течение установленного срока хранения, но не менее одного года.

Регламентация порядка использования в информационной системе съемных носителей информации, мобильных технических средств и контроля за таким использованием.

Обеспечение контроля за работоспособностью, параметрами настройки и правильностью функционирования средств вычислительной техники,

сетевого оборудования, системного программного обеспечения и средств защиты информации.

Обеспечение защиты от несанкционированного доступа к резервным копиям, параметрам настройки сетевого оборудования, системного программного обеспечения, средств защиты информации и событиям безопасности.

Обеспечение контроля за соблюдением правил генерации и смены паролей пользователей информационной системы.

Обеспечение блокировки доступа к объектам информационной системы после истечения установленного времени бездействия (неактивности) пользователя информационной системы или по его запросу.

Обеспечение разграничения доступа пользователей к средствам вычислительной техники, сетевому оборудованию, системному программному обеспечению и средствам защиты информации.

Обеспечение контроля за соблюдением правил генерации и смены паролей пользователей информационной системы.

Определение перечня разрешенного программного обеспечения и регламентация порядка его установки.

Обеспечение контроля за составом объектов информационной системы

Использование объектов информационной системы под пользовательскими учетными записями (использование административных учетных записей только в случае настройки объектов информационной системы или особенностей объектов информационной системы).

Определение состава и содержания информации, подлежащей резервированию.

Обеспечение обновления программного обеспечения объектов информационной системы и контроля за своевременностью такого обновления.

Определение перечня внешних подключений к информационной системе и порядка такого подключения.

Обеспечение централизованного управления учетными записями пользователей информационной системы и контроль за соблюдением правил генерации и смены паролей пользователей информационной системы.

Обеспечение сегментирования (изоляции) сети управления объектами информационной системы от сети передачи данных.

Обеспечение централизованного сбора и хранения информации о событиях информационной безопасности в течение установленного срока хранения, но не менее одного года.

Ежегодное проведение внешней и внутренней проверки отсутствия либо невозможности использования нарушителем свойств программных, программно-аппаратных и аппаратных средств, которые могут быть случайно инициированы (активированы) или умышленно использованы для нарушения информационной безопасности системы и сведения о которых

подтверждены изготовителями (разработчиками) этих объектов информационной системы.

Содержание модуля 8.2 для формирования контрольного листа № 8

Выберите реализуемые на Вашем предприятии мероприятия из представленного ниже перечня.

Обеспечение идентификации и аутентификации пользователей информационной системы.

Обеспечение защиты обратной связи при вводе аутентификационной информации.

Обеспечение полномочного управления (создание, активация, блокировка и уничтожение) учетными записями пользователей информационной системы.

Обеспечение блокировки доступа к объектам информационной системы после истечения установленного времени бездействия (неактивности) пользователя информационной системы или по его запросу.

Обеспечение резервирования информации, подлежащей резервированию.

Обеспечение защиты средств вычислительной техники от вредоносных программ.

Обеспечение подлинности и контроля целостности электронных документов в информационной системе (средства выработки электронной цифровой подписи, средства проверки электронной цифровой подписи, средства выработки личного ключа или открытого ключа электронной цифровой подписи).

Обеспечение обнаружения и предотвращения вторжений в информационной системе. Использование сетевых, и (или) поведенческих, и (или) узловых систем обнаружения и предотвращения вторжений.

Обеспечение обнаружения и предотвращения вторжений в информационной системе при использовании в ней беспроводных каналов передачи данных (Wi-Fi и тому подобное). Использование беспроводных систем обнаружения и предотвращения вторжений.

Обеспечение контроля за внешними подключениями к информационной системе.

Автоматизированный контроль за составом средств вычислительной техники и сетевого оборудования.

Обеспечение конфиденциальности и контроля целостности личных ключей, используемых при выработке электронной цифровой подписи (криптографические токены).

Обеспечение обнаружения и предотвращения утечек информации из информационной системы. Использование системы обнаружения и предотвращения утечек информации из информационной системы.

Содержание модуля 8.3 для формирования контрольного листа № 8

Выберите реализуемые на Вашем предприятии мероприятия из представленного ниже перечня.

Обеспечение защиты от агрессивного использования ресурсов виртуальной инфраструктуры потребителями услуг.

Обеспечение защиты виртуальной инфраструктуры от несанкционированного доступа и сетевых атак из виртуальной и физической сети, а также виртуальных машин.

Обеспечение резервного копирования пользовательских виртуальных машин.

Физическая изоляция сегмента виртуальной инфраструктуры (системы хранения и обработки данных), предназначенного для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам.

Содержание модуля 8.4 для формирования контрольного листа № 8

Выберите реализуемые на Вашем предприятии мероприятия из представленного ниже перечня.

Обеспечение конфиденциальности и контроля целостности информации при ее передаче посредством сетей электросвязи общего пользования (средства линейного или предварительного шифрования).

Обеспечение резервирования конфигурационных файлов сетевого оборудования.

Обеспечение в реальном масштабе времени автоматической проверки файлов данных, передаваемых по почтовым протоколам, и обезвреживание обнаруженных вредоносных программ.

Обеспечение управления внешними информационными потоками (маршрутизация) между информационными системами. Использование маршрутизатора (коммутатора маршрутизирующего).

Обеспечение ограничений входящего и исходящего трафика (фильтрация) информационной системы только необходимыми соединениями. Использование межсетевого экрана, функционирующего на канальном, сетевом и прикладном уровнях.

Обеспечение в реальном масштабе времени автоматической проверки пакетов сетевого трафика и файлов данных, передаваемых по сети, и обезвреживание обнаруженных вредоносных программ.

Содержание модуля 8.5 для формирования контрольного листа № 8

Выберите реализуемые на Вашем предприятии мероприятия из представленного ниже перечня.

Обеспечение изменения атрибутов безопасности сетевого оборудования, системного программного обеспечения и средств защиты информации, установленных по умолчанию.

Обеспечение обновления объектов информационной системы.

Обеспечение контроля и управления физическим доступом в помещения, в которых постоянно размещаются объекты информационной системы.

Обеспечение синхронизации временных меток и (или) системного времени в информационной системе и системе защиты информации.

ПРИЛОЖЕНИЕ В

Перечень вопросов для использования в целях систематизации сведений о структуре внутренних документов организации и о порядке реализации процесса работы с ИС

1. Внедрена и используется ли в организации политика ИБ?

2. Если ответ на предыдущий вопрос положительный, то соответствует ли структура политики ИБ и использованные в тексте этого документа термины требованиям актуальных ТНПА в сфере ИБ?

3. Если ответ на вопрос 1 положительный, то известно ли лицу, на которое возложены обязанности по контролю за соблюдением положений политики ИБ, о том, что на него возложены эти обязанности?

4. Если ответ на вопрос 1 положительный, то разработаны ли локальные нормативные правовые акты, направленные на реализацию политики ИБ?

5. Если ответ на предыдущий вопрос положительный, то соответствуют ли структура и содержание локальных нормативных правовых актов организации требованиям актуальных нормативных правовых актов в сфере ИБ?

6. Если ответ на вопрос 3 положительный, то доведены ли под роспись до субъектов ИС требования, изложенные в локальных нормативных правовых актах организации?

7. Выполнена ли классификация информации, хранящейся и обрабатываемой в ИС организации, в соответствии с законом Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации»?

8. Выполнена ли классификация ИС, доступ к которым имеют сотрудники организации?

9. Осведомлены ли сотрудники организации, которые имеют доступ к ИС, о том, к какому классу относятся эти системы и информация какой категории обрабатывается ими?

10. Имеются ли схемы ИС, используемых в организации для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам (далее – ИС) (с указанием объектов, внешних подключений и информационных потоков)?

11. Имеет ли ИС подключение к сетям электросвязи общего пользования (в том числе к глобальной сети Интернет)?

12. Если ответ на предыдущий вопрос положительный, то разработано ли задание по безопасности ИС?

13. Разработано ли частное техническое задание на систему защиты информации?

14. Можно ли сказать, что система защиты информации в организации представляет собой совокупность организационных, технических и правовых мер?

15. Обеспечиваются ли в организации контроль и управление физическим доступом в помещения, в которых постоянно размещаются объекты ИС?

16. Обеспечивается ли контроль за составом технических средств ИС?

17. Обеспечивается ли контроль за составом средств защиты информации в ИС?

18. Обеспечивается ли контроль за работоспособностью, параметрами настройки и правильностью функционирования средств защиты информации в ИС?

19. Обеспечивается ли разделение в ИС функций по управлению (администрированию) этой системой и функций по управлению (администрированию) ее системой защиты информации?

20. Разработан и используется ли в организации регламент для организации подключений к иным системам ИС?

21. Обеспечивается ли определение прав и обязанностей субъектов ИС?

22. Обеспечивается ли управление средствами аутентификации ИС, в том числе хранением, выдачей, инициализацией, блокированием средств аутентификации и принятием мер в случае утраты и (или) компрометации средств аутентификации?

23. Обеспечивается ли контроль за соблюдением правил генерации и смены паролей субъектов ИС?

24. Обеспечивается ли блокировка доступа к ИС после истечения установленного времени бездействия (неактивности) субъекта ИС или по его запросу?

25. Выполняется ли проверка знаний сотрудников об их обязанностях по обеспечению защиты информации, используемой ими, или безопасности ИС, доступ к которым они получают?

26. Используются ли инженерно-технические средства защиты объектов электросвязи? (отвечать в случае, если аудируемая организация относится к организациям категории 1)

27. Проводят ли начальники строительных участков или старшие производители работ для своих подчиненных теоретическое и практическое обучение по вопросам устранения повреждений средств и линий электросвязи? (отвечать в случае, если аудируемая организация относится к организациям категории 1).

Научное издание

БОЙПРАВ Владимир Андреевич
БОЙПРАВ Ольга Владимировна
УТИН Леонид Львович

АСПЕКТЫ ОБЕСПЕЧЕНИЯ АУДИТА СИСТЕМ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ ЭЛЕКТРОСВЯЗИ

Ответственный за выпуск С.Л. Бочкарева

Корректор В.П. Жукова

Подписано в печать 08.10.2025. Формат 60×84 ⅛.
Бумага офсетная. Печать офсетная.
Гарнитура «Times New Roman».
Усл. печ. л. 6,74. Уч. изд. л. 2,95.
Тираж 50 экз. Заказ 87.

Издатель и полиграфическое исполнение: УП «Бестпринт»
Свидетельство о государственной регистрации издателя, изготовителя и распространителя печатных изданий
№ 1/160 от 27.01.2014.
ул. Кальварийская, 25, каб. 116, 220073, г. Минск