УДК 004.56

***БЕДЕРДИНОВА Оксана Ивановна**, кандидат технических наук, доцент кафедры информатики института судостроения и морской арктической техники (Севмашвтуза) филиала САФУ в г. Северодвинске. Автор 49 научных публикаций*

***КОРЯКОВСКАЯ Наталья Владимировна**, кандидат технических наук, доцент кафедры автоматизации технологических процессов и производств института энергетики и транспорта Северного (Арктического) федерального университета имени М.В. Ломоносова. Автор 57 научных публикаций*

# *АЛГОРИТМ РАЗРАБОТКИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ*

Алгоритм разработки системы защиты информации на предприятии создан на основе анализа требований стандартов и нормативных документов РФ с учетом системного подхода. Предложенный алгоритм возможно использовать для создания политики информационной безопасности, обеспечивающей необходимый уровень надежной защиты объектов информатизации на предприятиях.

***Ключевые слова:** информация ограниченного доступа, информационные ресурсы, объекты информатизации, политика информационной безопасности, система защиты информации.*

В связи с интенсивным внедрением в деятельность предприятий автоматизированных систем организационно-финансового управления, в которых обрабатывается, хранится и передается третьим лицам информация ограниченного доступа, задача обеспечения безопасности информации, обрабатываемой и передаваемой средствами и системами вычислительной техники и связи, является актуальной.

Под информационной безопасностью предприятия понимается защищенность интересов владельцев, руководства, клиентов, поставщиков и информационных ресурсов от внутренних и внешних угроз.

Основными целями политики информационной безопасности является обеспечение устойчивого функционирования предприятия и предотвращение угроз безопасности информации ограниченного доступа. Другими целями политики безопасности являются:

– формирование комплексного представления о системе безопасности предприятия и всех ее элементов, обеспечивающей необходимый уровень надежной защищенности информационных ресурсов;

– повышение конкурентноспособности предприятия и роста прибыли за счет обеспечения безопасности имущественных прав и интересов клиентов и поставщиков.

Для достижения необходимого уровня безопасности информации ограниченного доступа требуется системное согласование всех используемых мер, методов и средств защиты. Поэтому, только комплексное применение организационных и технических мероприятий способно решить задачи информационной безопасности объектов информатизации с необходимым уровнем надежности.

Целью работы является разработка алгоритма создания системы защиты информации ограниченного доступа на предприятиях с учетом системного подхода.

В результате проведенного анализа требований ГОСТ Р 51583-2000, национальных стандартов РФ ИСО/МЭК 17799 -2005, ИСО/МЭК 27001-2006 и других нормативных документов создан алгоритм разработки системы защиты конфиденциальной информации на предприятии, приведенный на *рисунке*.

Предпроектная стадия включает следующие этапы:

1. Предпроектное обследование защищаемых объектов информатизации:

1.1. Формирование комиссии обследования и назначение руководителя.

1.2. Определение перечня сведений конфиденциального характера, подлежащих защите от несанкционированного доступа (НСД) и от утечки по техническим каналам.

1.3. Проведение анализа внутриобъектового режима защиты объектов информатизации:

– проведение анализа территориального расположения и режима функционирования объекта защиты;

– проведение анализа организации физической охраны, пропускного и внутриобъектового режимов объекта защиты;

– определение перечня выделенных помещений, подлежащих защите;

– определение условий расположения объектов информатизации относительно границ контролируемой зоны;

– проведение анализа конструктивных элементов защищаемых помещений на соответствие требованиям к необходимым классам защиты в зависимости от подгруппы защищаемого объекта.

1.4. Проведение обследования (специального обследования) защищаемых объектов на выявление каналов несанкционированного доступа к конфиденциальной информации:

– проведение анализа организационной структуры объекта защиты;

– проведение анализа установленной системы допуска персонала к конфиденциальной информации и конфиденциальным документам;

– проведение анализа установленной ответственности персонала за обеспечение безопасности конфиденциальной информации;

– определение конфигурации и топологии автоматизированных систем обработки конфиденциальной информации и систем связи;

– определение технических средств и систем, предполагаемых к использованию в автоматизированных системах обработки конфиденциальной информации и системах связи, условий их расположения;

– определение общесистемных и прикладных программных средств обработки конфиденциальной информации;

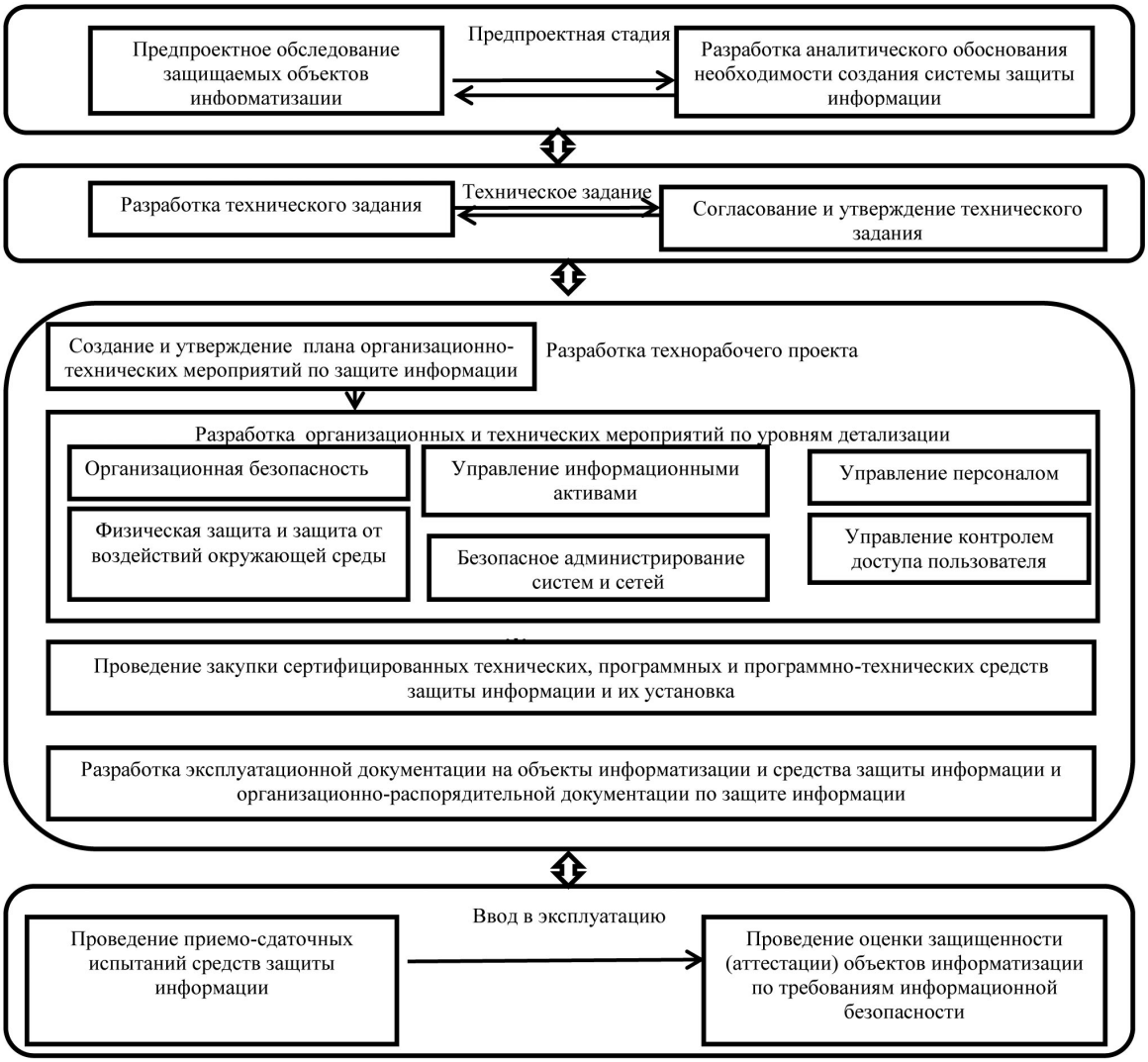
– определение режимов обработки информации, характеристик и класса защищенности автоматизированных систем обработки информации ограниченного доступа.

1.5. Проведение обследования (специального обследования) защищаемых объектов на выявление технических каналов утечки конфиденциальной информации:

За пределами контролируемой зоны (КЗ):

1.5.1. установление месторасположения трансформаторной подстанции, электрощитовой, распределительных щитов;

1.5.2. определение соединительных линий вспомогательных технических средств и систем (линий телефонной связи, оповещения, систем охранной и пожарной сигнализации, часофикации и т.п.), выходящие за пределы контролируемой зоны;




Алгоритм разработки системы защиты объектов информатизации

1.5.3. определение смежных помещений с защищаемыми и находящимися за пределами контролируемой зоны;

1.5.4. проведение оценки возможности ведения из близлежащих зданий разведки с использованием направленных микрофонов и лазерных акустических систем разведки, а также средств визуального наблюдения и съемки;

1.5.5. проведение оценки возможности приема информации, передаваемой сетевыми закладками (при их установке в защищаемых помещениях), за пределами контролируемой зоны.

В контролируемой зоне (КЗ):

1.5.6. определение мест установки на объектах информатизации технических средств обработки информации и прокладки их соединительных линий;

1.5.7. проведение оценки возможности перехвата информации, обрабатываемой тех-

ническими средствами, специальными техническими средствами по электромагнитным и электрическим каналам утечки информации;

1.5.8. проведение оценки возможности утечки речевой информации из защищаемых помещений по виброакустическим каналам;

1.5.9. проведение технического контроля по оценке реальных экранирующих свойств конструкций здания звуко- и виброизоляции помещений.

1.6. Определение мероприятий по обеспечению конфиденциальности информации в процессе проектирования объекта информатизации.

Предпроектное обследование защищаемого объекта проводится комиссией, назначенной руководителем предприятия (организации, фирмы) или специализированной сторонней организацией, имеющей соответствующую лицензию с заключением соответствующих договоров на проведение работ по обследованию защищаемых объектов.

Результатами проведения этапа предпроектного обследования является документация, включающая отчеты о результатах обследования объектов информатизации на выявление технических каналов утечки конфиденциальной информации и на выявление каналов несанкционированного доступа к конфиденциальной информации.

2. Разработка аналитического обоснования необходимости создания системы защиты конфиденциальной информации (СЗИ).

Процесс разработки аналитического обоснования включает этапы:

2.1. Определение перечня сведений, подлежащих защите (перечень сведений конфиденциального характера утверждается руководителем организации).

2.2. Определение системы допуска персонала к конфиденциальной информации и конфиденциальным документам.

2.3. Разработка матрицы доступа персонала к сведениям конфиденциального характера, подлежащих защите.

2.4. Определение модели вероятного нарушителя.

2.5. Проведение классификации и категорирования объектов информатизации и выделенных помещений.

2.6. Обоснование необходимости привлечения специализированных организаций, имеющих необходимые лицензии на право проведения работ по защите информации, для проектирования и внедрения СЗИ;

2.7. Проведения оценки материальных, трудовых и финансовых затрат на разработку и внедрение СЗИ;

2.8. Определение сроков разработки и внедрения СЗИ.

Результаты аналитического обоснования необходимости создания СЗИ оформляются в виде пояснительной записки, которая включает:

2.8.1. Перечень сведений конфиденциального характера с указанием их уровня конфиденциальности;

2.8.2. Перечень сотрудников предприятия, допущенных до конфиденциальной информации, с указанием их режима доступа;

2.8.3. Матрица доступа к конфиденциальной информации;

2.8.4. Информационную характеристику и организационную структуру объектов защиты;

2.8.5. Перечень объектов информатизации, подлежащих защите;

2.8.6. Перечень выделенных помещений, подлежащих защите;

2.8.7. Перечень и характеристики технических средств обработки конфиденциальной информации с указанием их места установки;

2.8.8. Перечень и характеристики вспомогательных технических средств и систем с указанием их места установки;

2.8.9. Предполагаемый уровень оснащения вероятного нарушителя;

2.8.10. Перечень технических каналов утечки информации, подлежащие закрытию (устранению);

2.8.11. План организационных мероприятий по закрытию технических каналов утечки информации;

2.8.12. Перечень и характеристики предлагаемых к использованию технических средств

защиты информации с указанием их места установки;

2.8.13. Методы и порядок контроля эффективности защиты информации;

2.8.14. Обоснование необходимости привлечения специализированных организаций, имеющих необходимые лицензии на право проведения работ по защите информации, для проектирования;

2.8.15. Оценку материальных, трудовых и финансовых затрат на разработку и внедрение СЗИ;

2.8.16. Ориентировочные сроки разработки и внедрения СЗИ;

2.8.17. Перечень мероприятий по обеспечению конфиденциальности информации на стадии проектирования СЗИ.

Пояснительная записка подписывается руководителем комиссии, проводившей аналитическое обоснование, согласовывается с руководителем службы безопасности и утверждается руководителем предприятия.

3. Техническое (частное техническое) задание на создание СЗИ.

Техническое задание включает этапы:

3.1. Разработка технического задания на создание СЗИ.

3.2. Согласование и утверждение ТЗ.

Документ Техническое задание (ТЗ) на разработку СЗИ должно содержать:

3.2.1. Обоснование разработки;

3.2.2. Исходные данные объекта защиты в техническом, программном, информационном и организационном аспектах;

3.2.3. Источники разработки СЗИ;

3.2.4. Требования к СЗИ;

3.2.5. Перечень предполагаемых к использованию технических средств защиты информации;

3.2.6. Состав, содержание и сроки проведения работ по этапам разработки и внедрения;

3.2.7. Перечень подрядных организаций - исполнителей различных видов работ;

3.2.8. Перечень предъявляемой заказчику научно-технической продукции и документации.

Результатом выполнения стадии является документ Техническое задание на проектирование СЗИ защищаемого объекта, согласованный с проектной организацией, службой (специалистом) безопасности предприятия - заказчика и утвержденный руководителем предприятия - заказчика.

4. Разработка технорабочего проекта.

Технорабочий проект включает этапы:

4.1. Создание и утверждение плана организационно-технических мероприятий по защите информации.

4.2. Разработка организационных и технических мероприятий по уровням детализации политики информационной безопасности:

4.2.1.Уровень «Организационная безопасность»:

Управление политикой информационной безопасности;

– Распределение обязанностей по обеспечению информационной безопасности;

– Регламентация процесса использования средств обработки конфиденциальной информации;

– Аудит информационной безопасности;

– Регламентация работы со сторонними организациями.

4.2.2. Уровень «Управление информационными активами»:

– Учет активов;

– Классификация информации ограниченного доступа.

4.2.3. Уровень «Управление персоналом»:

– Подбор персонала;

– Включение вопросов информационной безопасности в должностные обязанности;

– Обучение персонала;

– Реагирование на инциденты нарушения информационной безопасности и сбои программного обеспечения.

4.2.4. Уровень «Физическая защита и защита от воздействий окружающей среды»:

– Обеспечение безопасности охраняемых зон.

– Контроль за доступом в охраняемые зоны.

– Расположение и защита оборудования.

– Обеспечение защиты электропитания и безопасности кабельной сети от повреждения и перехвата информации.

– Организация технического обслуживания оборудования

4.2.5. Уровень «Безопасное администрирование систем и сетей»:

– Операционные процедуры и обязанности персонала, допущенного к обработке и хранению информации ограниченного доступа.

– Защита от вредоносного программного обеспечения.

– Резервирование информации.

– Управление безопасностью сети.

– Обмен информацией и программным обеспечением со сторонними организациями.

4.2.6. Уровень «Управление контролем доступа пользователя»:

– Управление контролем доступа пользователя.

– Контроль сетевого доступа.

– Контроль доступа к операционной системе.

– Контроль доступа к приложениям.

– Мониторинг доступа и использования системы обработки и хранения конфиденциальной информации.

– Работа с переносными устройствами и работа в дистанционном режиме.

– Безопасность в процессах разработки и поддержки прикладных систем и информации.

4.3. Проведение закупки сертифицированных образцов и серийно выпускаемых в защищенном исполнении технических средств обработки, передачи и хранения информации и их установка.

4.4. Проведение закупки сертифицированных технических, программных и программно-технических (в т. ч. криптографических) средств защиты информации и их установка.

4.5. Разработка эксплуатационной документации на объекты информатизации и средства защиты информации, а также организационно-распорядительной документации по защите информации (приказов, инструкций и других документов).

Результатом выполнения стадии является Политика информационной безопасности предприятия и система защиты конфиденциальной информации.

5. Ввод в эксплуатацию системы защиты информации.

Стадия включает этапы:

5.1. Проведение опытной эксплуатации средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе объекта информатизации и отработки технологического процесса обработки (передачи) информации.

5.2. Проведение приемо-сдаточных испытаний средств защиты информации по результатам опытной эксплуатации.

5.3. Проведение оценки защищенности объектов информатизации по требованиям информационной безопасности.

В результате выполнения стадии создаются и утверждаются акты внедрения средств защиты информации по результатам их приемо-сдаточных испытаний и акты аттестации (соответствия) объектов информатизации требованиям информационной безопасности.

Разработанный алгоритм основан на системном подходе и обеспечивает выполнение требований законодательных и нормативных документов.

На основании предложенного алгоритма и проведенной типизации автоматизированных систем обработки информации ограниченного доступа с учетом требований ФСТЭК России [5, 6] разработаны модели систем защиты коммерческой тайны и персональных данных. Модели включают:

– типовые матрицы моделей угроз, нарушителей и планов мероприятий с учетом классов защищенности используемых автоматизированных систем обработки сведений, составляющих коммерческую тайну и информационных систем обработки персональных данных;

– шаблоны организационно-нормативных и распорядительных документов.

Использование предложенного алгоритма и моделей систем защиты персональных данных и коммерческой тайны позволит разработать систему безопасности, обеспечивающую необходимый уровень надежной защиты объектов информатизации на предприятиях.

## Список литературы

1. ГОСТ Р 51583-2000. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Введ. с 01.01.2001. М., 2000.

2. ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью. Введ. с 29.12.2005. М., 2006.

3. ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. Введ. с 2006.27.12. М., 2008.

4. Порядок проведения классификации информационных систем персональных данных, утв. 13.02.2008. № 55/86/20. М., 2008.

5. РД Гостехкомиссии России. Автоматизированные системы. Защита от НСД. Классификация автоматизированных систем и требования по защите информации. М., 1992.

6. РД Гостехкомиссии России. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утв. 30.08.2002 № 282. М., 2001.

## References

1. *GOST R 51583-2000. Zashchita informatsii. Poryadok sozdaniya avtomatizirovannykh sistem v zashchishchennom ispolnenii. Obshchie polozheniya* [Russian State Standard 51583–2000. Information Security. Protective Automated Systems. General Provisions]. Moscow, 2000.

2. *ISO/IEC 17799:2005. Information Technology - Security Techniques - Code of Practice for Information Security Management.* 2005 (Russ ed.: *ISO/MEK 17799-2005 "Informatsionnaya tekhnologiya. Prakticheskie pravila upravleniya informatsionnoy bezopasnost'yu"*. Moscow, 2006.

3. *ISO/IEC 27001:2005 – Information technology – Security Techniques – Information Security Management Systems – Requirements* (Russ. ed.: *ISO/MEK 27001-2006 "Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Sistemy menedzhmenta informatsionnoy bezopasnosti. Trebovaniya"*. Moscow, 2008.

4. *The Procedure of Classification of Personal Data Information Systems, Approved by Order of FSTEC of Russia, Federal Security Service and the Ministry of Communications of Russia on 13 February 2008, no. 55/86/20.* Moscow, 2008. (in Russian).

5. *RD Gostekhkomissii Rossii. Avtomatizirovannye sistemy. Zashchita ot NSD. Klassifikatsiya avtomatizirovannykh sistem i trebovaniya po zashchite informatsii* [Guidance Document of the Russian State Technical Commission. Automated Systems. Protection from Unauthorized Access. Automated Systems Classification and Requirements for Information Security]. Moscow, 1992.

6. *RD Gostekhkomissii Rossii. Spetsial'nye trebovaniya i rekomendatsii po tekhnicheskoy zashchite konfidentsial'noy informatsii (STR-K)* [Guidance Document of the Russian State Technical Commission. Special Requirements and Recommendations for Technical Protection of Confidential Data (SRR-C)]. Moscow, 2001.

***Bederdinova Oksana Ivanovna***
Institute of Shipbuilding and Arctic Marine Engineering,
Severodvinsk Branch of Northern (Arctic) Federal University
named after M.V. Lomonosov (Severodvinsk, Russia)

***Koryakovskaya Natalya Vladimirovna***
Institute of Energy and Transport, Northern (Arctic)
Federal University named after M.V. Lomonosov (Arkhangelsk, Russia)

## ALGORITHM FOR DEVELOPMENT OF INFORMATION PROTECTION SYSTEM

An algorithm for development of corporate information protection system was created on the basis of the analysis of regulatory requirements and documents of the RF and taking into consideration the systems approach. The algorithm can be used to create information security policy providing the required level of security for corporate objects of informatization.

***Keywords:*** *confidential information, information resources, objects of informatization, information security policy, information protection system.*

*Контактная информация:*
Бедердинова Оксана Ивановна
*Адрес:* 164560, г. Северодвинск, ул. Воронина, д. 6
*e-mail:* O.Bederdinova@narfu.ru

Коряковская Наталья Владимировна
*Адрес:* 163002, г. Архангельск, наб. Северной Двины, д. 17
*e-mail:* N.Koryakovskaya@narfu.ru

Рецензент – *Кремлёва Л.В.*, доктор технических наук, профессор, заместитель директора по учебной работе института судостроения и морской арктической техники (Севмашвтуз) филиала САФУ в г. Северодвинске