На правах рукописи

Алферов Игорь Леонидович

МЕТОДИКА ОБРАБОТКИ РИСКОВ НАРУШЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ОБЪЕКТНО-ОРИЕНТИРОВАННЫХ СЕТЯХ ХРАНЕНИЯ ДАННЫХ

Специальность: 05.13.19 – «Методы и системы защиты информации, информационная безопасность»

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Автор: _____

Москва – 2010

Работа выполнена в Национальном исследовательском ядерном университете «МИФИ» (НИЯУ МИФИ)

Научный руководитель: кандидат технических наук, доцент
Запечников Сергей Владимирович

Официальные оппоненты: доктор технических наук, профессор,
заслуженный деятель науки РФ
Ловцов Дмитрий Анатольевич

кандидат физико-математических наук, доцент
Варфоломеев Александр Алексеевич

Ведущая организация: Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН)

Защита состоится «26» мая 2010 г. в 15 часов 00 минут на заседании диссертационного совета ДМ 212.130.08 при Национальном исследовательском ядерном университете «МИФИ» по адресу: 123557, г. Москва, ул. Пресненский вал, д. 19, Центр информационных технологий и систем органов исполнительной власти (ЦИТиС), тел. для справок: +7 (495) 323-95-26, 324-84-98.

С диссертацией можно ознакомиться в библиотеке Национального исследовательского ядерного университета «МИФИ».

Отзывы в двух экземплярах, заверенные печатью организации, просьба направлять по адресу: 115409, г. Москва, Каширское ш., д. 31, диссертационные советы МИФИ, тел.: +7 (495) 323-95-26.

Автореферат разослан «____» _____ 2010 г.

Ученый секретарь
диссертационного совета:
кандидат технических наук, доцент Горбатов В.С.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы. Информационные технологии к настоящему времени стали фундаментальным средством автоматизации и повышения эффективности труда, проникшим во все сферы человеческой деятельности. Развитие современных коммерческих и общественных организаций происходит параллельно с развитием используемых ими информационных систем (ИС), в которых все большие требования предъявляются к объему, оперативности доступа, надежности и безопасности долговременного хранения массивов данных.

Для удовлетворения растущих требований до последнего времени применялись две наиболее популярные архитектуры – сети хранения данных (СХД, англ. Storage Area Network, SAN) и сетевые хранилища данных (англ. Network Attached Storage, NAS). Обе архитектуры предназначены для обеспечения эффективного доступа к данным со стороны клиентских узлов сети, но каждая обладает своими недостатками. В частности, в СХД организация совместного доступа к данным возможна только с помощью вспомогательных внешних механизмов синхронизации доступа между клиентами, требующих дополнительного сетевого взаимодействия, в то время как в сетевых хранилищах данных все передаваемые данные проходят через централизованный сервер, что ограничивает производительность и масштабируемость сети. Кроме того, в обеих архитектурах используется традиционный блочный интерфейс доступа к устройствам хранения данных (УХД), предполагающий выполнение функций оптимизации, связанных с физическим распределением данных и их кэшированием, клиентским программным обеспечением. В большинстве случаев в качестве клиентского программного обеспечения выступает реализация какой-либо файловой системы общего назначения, которая выполняет лишь поверхностную оптимизацию независимо от специфики отдельных массивов хранимых данных. Также блочный интерфейс не позволяет реализовать эффективную модель безопасности, так как управление доступом включает в себя решение сложной задачи отображения правил доступа на блочный уровень и требует высоких затрат ресурсов, а имеющаяся возможность управления доступом на уровне логических разделов УХД не обладает достаточной гибкостью.

Все эти сложности традиционных подходов привели к возникновению новой технологии, соединяющей их достоинства и устраняющей недостатки – архитектуре объектного хранения данных (англ. Object Storage Architecture, OSA). Исследования таких ученых, как G. Gibson, D. Nagle, H. Gobioff, J. Zelenka, P. Braam, и других специалистов в 90-х годах заложили основы концепции объектного хранения данных, как способа повышения масштабируемости и производительности систем хранения данных посредством расширения функций обработки информации, выполняемых УХД. В последние несколько лет концепция объектного хранения данных получила существенное развитие совместными усилиями представителей различных фирм-производителей (HP, IBM, Intel, Lingua Data, Panasas, Seagate, Veritas, Xyratex) в рабочей группе OSD Technical Workgroup ассоциации SNIA (Storage Networking Industry Association). Данная архитектура продолжает стремительно развиваться и ее промышленные реализации (например, PanFS, Lustre) уже применяются для практического решения задач хранения данных.

Одним из важных движущих факторов при разработке архитектуры объектного хранения данных являлось обеспечение безопасности информации (ОБИ) в построенных на основе этой архитектуры сетях. Вопросы ОБИ в системах хранения данных, использующих концепцию объектного хранения данных, исследовали H. Gobioff, B. Reed, A. Azagury, M. Factor, S. Halevi, D. Naor, V. Kher, C. Olson, E. Miller, D. Nagle, A. Leung и другие известные зарубежные специалисты. Среди отечественных трудов можно отметить работы С. В. Запечникова, посвященные решению задач ОБИ в СХД, а также научные и практические положения в области ОБИ в распределенных компьютерных системах, разработанные А. Ю. Щербаковым, Д. П. Зегждой, Д.А. Ловцовым и др.

Принятый в 2004 г. стандарт ANSI INCITS 400-2004, определяющий расширения интерфейса SCSI для взаимодействия с объектно-ориентированными УХД (ООУХД, англ. Object Storage Device, OSD), задает протокол безопасности, который выполняется при осуществлении доступа к ООУХД. Рабочая группа NFSv4 Workgroup в составе Internet Engineering Task Force (IETF) в настоящее время завершает разработку протокола NFSv4.1, включающего в себя механизмы взаимодействия клиентов с сервером метаданных и параллельного доступа к ООУХД в составе ООСХД на основе архитектуры pNFS (parallel NFS). При этом в имеющихся стандартах и проектах уровень разработанности вопросов ОБИ в ООСХД остается недостаточным. В частности, недостаточно разработанными являются методы безопасного обмена с серверами метаданных, защиты конфиденциальности данных в процессе их передачи по каналам связи, защиты данных при хранении на физических носителях.

Также следует отметить, что в современных организациях основным движущим фактором, определяющим используемые методы ОБИ, становится их экономическая эффективность. В этих условиях внедрение и использование ООСХД в современных организациях сопряжено с построением системы защиты от существующих в среде сетей хранения данных угроз, требующей комплексного экономически обоснованного подхода, применения различных стандартов и технологий и их интеграции. В связи с этим **актуальной** является научно-техническая задача разработки и применения методики обработки рисков нарушения безопасности информации (БИ) в ООСХД, позволяющей оптимизировать применение средств защиты информации в ООСХД с учетом связанных с ними затрат и ожидаемого ущерба от возможных нарушений БИ.

Целью диссертационной работы является повышение информационной безопасности предприятий, использующих ООСХД в составе корпоративных ИС, путем разработки и применения методики обработки рисков нарушения БИ в ООСХД, моделей и протоколов ОБИ в ООСХД.

Объектом исследования являются ООСХД.

Предметом исследования являются риски нарушения БИ в ООСХД.

В соответствии с поставленной целью в диссертационной работе решаются следующие **задачи**:

- анализ и систематизация существующих организационно-управленческих подходов к ОБИ предприятий, включая методы управления рисками наруше-

ния БИ и методы ОБИ в ООСХД в рамках данных подходов, постановка задачи разработки методики обработки рисков нарушения БИ в ООСХД;

- обоснование и разработка согласованной с организационно-управленческими подходами к управлению рисками методики обработки рисков нарушения БИ в ООСХД, позволяющей учитывать требования, предъявляемые к экономическому обоснованию деятельности по ОБИ;
- разработка схемы применения механизмов защиты (МЗ) в ООСХД для комплексного снижения и устранения рисков нарушения БИ в рамках разработанной методики обработки рисков нарушения БИ в ООСХД;
- разработка комплекса протоколов аутентификации клиентских приложений при доступе к информации, размещенной на ООУХД и серверах метаданных в составе ООСХД;
- разработка модели обеспечения целостности и конфиденциальности информации, хранимой на ООУХД в составе ООСХД;
- разработка математической модели функционирования системы предотвращения вторжений уровня ООУХД;
- разработка информационного и программного обеспечения для применения методики обработки рисков нарушения БИ в ООСХД, включая примерный состав базового каталога МЗ для ООСХД и программное инструментальное средство для автоматизации выполнения методики;
- экспериментальный анализ эффективности разработанной методики обработки рисков нарушения БИ в ООСХД в промышленных предприятиях и определение практических рекомендаций по ее использованию.

Основными **методами исследований**, используемыми в работе, являются методы системного анализа, исследования операций, дискретной оптимизации, теории вероятностей и теории множеств.

На защиту выносятся следующие основные результаты работы:

- методика обработки рисков нарушения БИ в ООСХД;
- комплекс протоколов аутентификации клиентских приложений при доступе к информации, размещенной на ООУХД и серверах метаданных в составе ООСХД;
- модель обеспечения целостности и конфиденциальности информации, хранимой на ООУХД.

Научная новизна результатов, полученных лично автором, заключается в следующем:

- обоснована и разработана методика обработки рисков нарушения БИ в ООСХД, основанная на математической модели учета влияния БИ в ООСХД на процессы деловой деятельности (ПДД) и применении методов дискретной оптимизации для поиска экономически обоснованного набора средств защиты информации;
- разработан комплекс протоколов аутентификации узлов ООСХД при доступе к информации, размещенной на ООУХД и серверах метаданных в составе сети, на основе применения ролевой модели контроля доступа, ролевых ключей и распределенного хранения информации о политике безопасности;

- построена модель обеспечения целостности и конфиденциальности информационных объектов, хранимых на ООУХД в составе ООСХД, в том числе на устройствах, не являющихся доверенными, и реализующие ее протоколы сопровождения политики безопасности и доступа к информационным объектам, основанные на использовании алгоритмов шифрования и электронной цифровой подписи (ЭЦП), ролевой модели контроля доступа, распределенного хранения информации о политике безопасности и группового распределения ключей.

Теоретическую значимость представляет осуществленное в работе развитие математического аппарата для анализа и обработки рисков нарушения БИ, разработанная математическая модель учета влияния БИ в ООСХД на процессы деловой деятельности, разработанные модели и протоколы ОБИ в ООСХД.

Практическую значимость представляет разработанная методика обработки рисков нарушения БИ в ООСХД и реализованное программное инструментальное средство для ее автоматизации ИСКР 1.0 (подтверждается актом о внедрении результатов диссертационной работы в компании ООО “Одноклассники”, актом об использовании результатов диссертационной работы в Небанковской Кредитной Организации “Международная Расчетная Палата” (ООО)). В работе сформулированы практические рекомендации по выполнению разработанной методики обработки рисков в рамках общего управления рисками нарушения БИ предприятий, организации рабочей группы для выполнения методики, определению организационного порядка ее выполнения, формированию каталога МЗ с учетом разработанной схемы применения МЗ в ООСХД, а также применению разработанного программного инструментального средства ИСКР 1.0 для уменьшения трудоемкости выполняемых процессов.

Достоверность полученных результатов подтверждается математическими доказательствами и формальными выводами основных утверждений, сформулированных в работе, использованием известных проверенных на практике методов, протоколов и алгоритмов, а также практикой применения результатов работы в крупных промышленных предприятиях.

Реализация результатов исследования. Результаты диссертационной работы использованы для обеспечения безопасности информации в системах хранения данных компании ООО “Одноклассники” и Небанковской Кредитной Организации “Международная Расчетная Палата” (ООО), а также внедрены в учебный процесс на факультете “Информационная безопасность” Национального исследовательского ядерного университета «МИФИ». Результаты исследования представляют практическую ценность для обеспечения безопасности информации в системах хранения данных российских и зарубежных корпоративных структур различного масштаба.

Публикации и апробация работы. По теме диссертации опубликованы 10 печатных работ, в том числе 4 научных статьи в журналах Перечня ВАК и 6 тезисов научных докладов. Результаты диссертационной работы докладывались на Общероссийской научно-технической конференции “Методы и технические средства обеспечения безопасности информации” (С.-Петербург, 2006-2007 гг.), Всероссийской научной конференции “Проблемы информационной безопасности в системе высшей школы” (Москва, 2007-2008 гг.), Всероссийской научно-технической кон-

ференции студентов, аспирантов и молодых ученых “Научная сессия ТУСУР-2007” (Томск, 2007 г.), а также на семинарах кафедры “Информационная безопасность банковских систем” МИФИ (Москва, 2007-2009 гг.).

Структура и объем работы. Работа состоит из введения, четырех глав, заключения, списка использованных источников, включающего 188 наименований, и шести приложений. Текст диссертации изложен на 219 страницах, включая 12 рисунков и 7 таблиц.

СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обоснована актуальность темы диссертации, выделены и сформулированы цель и задачи исследования, описана структурно-логическая схема диссертационного исследования.

В первой главе – **"Анализ задач обеспечения безопасности информации в объектно-ориентированных сетях хранения данных"** – проведены анализ и постановка задачи разработки методики обработки рисков нарушения БИ в ООСХД.

В работе исследована общая задача ОБИ в корпоративных системах хранения данных и ООСХД в частности, определены пути ее решения в рамках сложившихся к настоящему времени организационно-управленческих подходов к ОБИ, научно-методической и нормативно-технической базы в области ОБИ предприятия, а также системы стандартов и документов в области обеспечения безопасности хранения данных. На основе выявленной научно-методической и информационной базы исследования задач ОБИ в ООСХД (рис. 1) проведена постановка задачи разработки методики обработки рисков нарушения БИ в ООСХД.

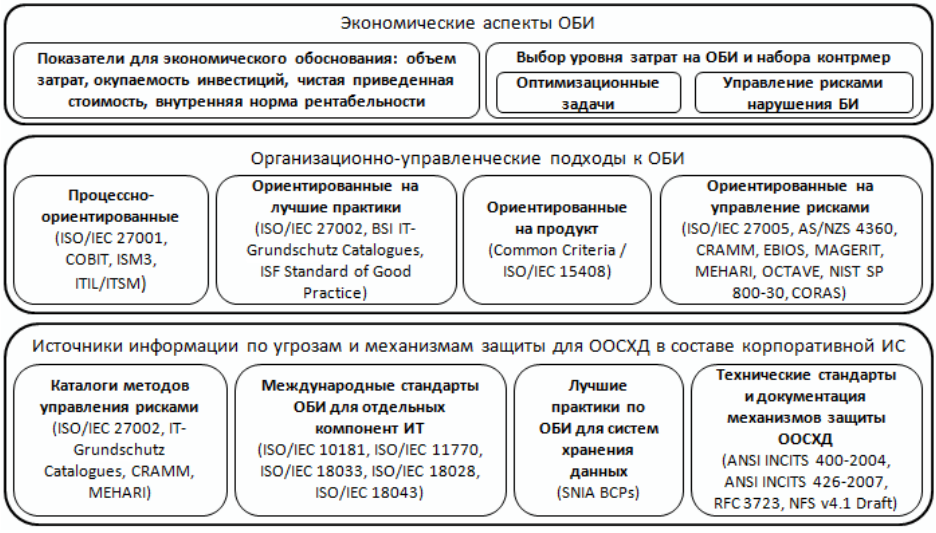

Рис. 1. Научно-методическая и информационная база исследования задач ОБИ в ООСХД

Проведенное автором исследование факторов, обуславливающих потребность предприятий в ОБИ, и применяемых подходов к обоснованию затрат на ОБИ показало, что современная мировая практика требует решения как организационных, так и технических вопросов ОБИ в рамках единого экономически обоснован-

ного подхода, опирающегося на оценку технико-экономических показателей: затрат, окупаемости инвестиций (англ. Return on Investment, ROI), чистой приведенной стоимости (ЧПС, англ. Net Present Value, NPV) и внутренней нормы рентабельности (англ. Internal Return Rate, IRR). В работе отдельно исследованы основные задачи, возникающие в ходе анализа и синтеза систем защиты информации: оценка ущерба от реализации атак нарушителей, оценка эффективности МЗ, выбор уровня затрат на ОБИ и набора применяемых мер ОБИ. Анализ известных методов и моделей для выбора уровня затрат на ОБИ и набора применяемых мер ОБИ показал, что они базируются на понятийном и алгоритмическом аппарате концепции управления рисками, а также решении оптимизационных задач с целевыми функциями, соответствующими выделенным технико-экономическим показателям.

В соответствии с концепцией управления рисками в работе введены основные теоретические понятия:

- *риск* – набор упорядоченных пар неблагоприятных событий и вероятностей их реализации за период времени:

$$Risk(\tau) = \{(O_1, P_1(\tau)), \ldots, (O_n, P_n(\tau))\},$$

где O_i, $i=1,...,n$ – неблагоприятные события, P_i, $i=1,...,n$ – вероятности их реализации, τ - рассматриваемый период времени, $n \in \boldsymbol{N}$, $\boldsymbol{N}$ – множество натуральных чисел;

- *уровень риска* – математическое ожидание ущерба, вызываемого неблагоприятными событиями риска за период времени:

$$| Risk(\tau) | = \sum_{i=1}^{n} M[i(O_i) f(O_i, \tau)],$$

где $i(O_i)$ – случайная величина ущерба, возникающего при единичном наступлении события O_i, $f(O_i, \tau)$ – случайная величина количества событий O_i, наступающих за период времени τ;

- *ожидаемый ущерб* – математическое ожидание совокупного ущерба от реализации рисков за период времени:

$$LE(\tau) = \sum_{i=1}^{m} | Risk_i(\tau) |,$$

где $Risk_i(\tau)$, $i=1,...,m$, $m \in \boldsymbol{N}$ – рассматриваемые риски, содержащие непересекающиеся множества неблагоприятных событий.

В работе проведен анализ и систематизация литературных источников, международных стандартов, нормативных и справочных документов, определяющих организационно-управленческие подходы к ОБИ. Показано, что предприятия испытывают потребность в инфраструктуре непрерывного управленческого контроля за ОБИ, реализуемой системами управления информационной безопасностью (СУИБ, англ. Information Security Management System, ISMS). Организационно-управленческие подходы к ОБИ условно классифицированы на несколько подгрупп: процессно-ориентированные (ISO/IEC 27001, COBIT, ITIL/ITSM, ISM3), ориентированные на лучшие практики (ISO/IEC 27002, BSI IT-Grundschutz Catalogues, ISF Standard of Good Practice), ориентированные на продукт (Common Criteria / ISO/IEC 15408), ориентированные на управление рисками (ISO/IEC 27005, AS/NZS 4360, CRAMM, EBIOS, MAGERIT, MEHARI, OCTAVE, NIST SP 800-30, CORAS). Подходы, ориентированные на управление рисками, предоставляют основу для реализации процессов управления рисками в СУИБ, построенных в соответ-

ствии с моделями СУИБ, определенными в процессно-ориентированных подходах. Выявлено, что большинство известных организационно-управленческих подходов к ОБИ и методов управления рисками нарушения БИ характеризуется недостаточной разработанностью вопросов управления затратами на ОБИ, что обуславливает необходимость более глубокой разработки вопросов экономически оправданного решения задач ОБИ в ООСХД.

Согласно существующим источникам информации по угрозам и МЗ для ООСХД в составе корпоративных ИС (каталоги методов управления рисками (ISO/IEC 27002, IT-Grundschutz Catalogues и др.), международные стандарты ОБИ для отдельных компонент ИТ (ISO/IEC 10181, ISO/IEC 18028, ISO/IEC 18043 и др.), лучшие практики по ОБИ для систем хранения данных SNIA BCPs, технические стандарты и документация МЗ ООСХД (ANSI INCITS 400-2004, ANSI INCITS 426-2007, RFC 3723 и др.)) в работе проведен анализ задач ОБИ в ООСХД в рамках организационно-управленческих подходов к ОБИ. На основе выявленных структурно-функциональных особенностей ООСХД и системного анализа множества МЗ для ООСХД, приведенных в существующих источниках информации, определены недостаточно разработанные технологические возможности ОБИ в ООСХД: шифрование данных в протоколах доступа клиентов к ООУХД, использование систем обнаружения и предотвращения вторжений в среде ООСХД, хранение данных на ООУХД в зашифрованном виде, хранение кодов проверки целостности и аутентичности данных на ООУХД.

На базе полученных обзорно-аналитических результатов проведена формальная постановка основной задачи для достижения цели диссертационной работы, заключающейся в разработке методики обработки рисков нарушения БИ в ООСХД, реализующей оператор $F(S,X,E,L)$, где S - система, состоящая из ООСХД предприятия, хранимой и обрабатываемой в них информации, а также ПДД предприятия, использующих ресурсы ООСХД, X – организационно-техническая среда эксплуатации ООСХД предприятия, E – набор технико-экономических показателей эффективности ПДД предприятия, использующих ресурсы ООСХД, L – функция проверки ограничений на показатели эффективности E, включающая проверку одного из возможных требований их оптимизации. Значением оператора $F(S,X,E,L)$, если оно может быть найдено, является преобразование $c(S)$ системы S, изменяющее уровни рисков нарушения БИ в ООСХД и приводящее к тому, что функция L для преобразованной системы дает положительный результат.

Для решения задачи разработки методики обработки рисков нарушения БИ в ООСХД, реализующей оператор F, автором выделены частные задачи разработки самой методики, ее информационного и программного обеспечения. В целях расширения множества функций L, для которых оператор F способен находить преобразования системы S, в работе поставлены задачи разработки информационного обеспечения методики: 1) разработать схему применения МЗ в ООСХД, позволяющую достичь более высокой по сравнению с моделью безопасности, предложенной в стандарте ANSI INCITS 400-2004, производительности операций аутентификации, контроля доступа и сопровождения политики безопасности; 2) разработать комплекс протоколов аутентификации клиентских приложений (КП) при доступе к информации, размещенной на ООУХД и серверах метаданных в составе ООСХД; 3)

разработать модель обеспечения целостности и конфиденциальности данных, хранимых на ООУХД в составе ООСХД; 4) исследовать эффективность применения систем обнаружения и предотвращения вторжений в среде ООСХД и разработать математическую модель функционирования системы предотвращения вторжений (СПВ) уровня ООУХД.

Вторая глава – **"Обоснование и разработка методики обработки рисков нарушения безопасности информации в объектно-ориентированных сетях хранения данных"** – посвящена решению задачи разработки методики обработки рисков нарушения БИ в ООСХД.

В рамках исследования решена задача обоснования и разработки согласованной с международным стандартом управления рисками нарушения БИ ISO/IEC 27005 методики обработки рисков нарушения БИ в ООСХД, устанавливающей практическую последовательность действий по реализации процессов определения контекста управления рисками, идентификации рисков, анализа рисков и обработки рисков в ООСХД. Основные результаты этого этапа исследования представлены автором диссертации в работах [1,5,6].

Разработка методики выполнена в соответствии со следующими основными требованиями: 1) определение процедур идентификации рисков, анализа рисков и обработки рисков нарушения БИ для ООСХД предприятия; 2) выбор *контрмер* (мер по модификации рисков нарушения БИ, включая снижение уровней рисков, передачу рисков, отказ от рисков и принятие рисков) в условиях комбинированных ограничений и требований оптимизации для технико-экономических показателей: уровень затрат, окупаемость инвестиций, ЧПС, внутренняя норма рентабельности; 3) наличие структурированной информации по возможным угрозам и *МЗ* (практическим реализациям контрмер снижения уровней рисков нарушения БИ) для ООСХД, позволяющей находить удовлетворяющие ограничениям и требованиям решения по обработке рисков; 4) соответствие всех процедур международному стандарту ISO/IEC 27005 и возможность их интеграции в более общие методы обработки рисков, согласованные с данным стандартом.

В целях создания математического аппарата для поиска контрмер в условиях заданных ограничений и требований оптимизации для технико-экономических показателей в работе построена математическая модель учета влияния БИ в ООСХД на ПДД, учитывающая структурно-функциональные особенности ООСХД. Основными ее компонентами являются: $A=\{Conf, Int, Avail, TempAvail\}$ – множество *измерений безопасности* (*Conf* – конфиденциальность, *Int* – целостность, *Avail* – постоянная доступность, *TempAvail* - доступность с допустимыми ограниченными временными интервалами недоступности), B – множество ПДД организации, D' – множество информационных объектов ООСХД, D – множество *доменов данных* (ДД) (соответствуют элементам разбиения множества D' по принципу зависимости от нарушений измерений безопасности его элементов фиксированных подмножеств множества B), W – множество *доменов клиентских приложений* ООСХД (домены структурных компонентов ООСХД определяются посредством группирования компонентов по принципу совпадения множеств используемых в них МЗ), N – множество *доменов сетевых соединений* ООСХД, O – множество *доменов ООУХД* сети, M – множество *доменов серверов метаданных* ООСХД, $\alpha(b)\ \forall b \in B$ – функции сниже-

ния эффективности ПДД в связи с нарушениями измерений безопасности ДД, $\gamma(b)$ $\forall b \in B$ – функции периодов нарушения работы ПДД в связи с нарушениями измерений безопасности ДД, $c(b)$ $\forall b \in B$ – функции ущерба для организации от нарушений ПДД, S – множество возможных контрмер для ООСХД, $S' \subseteq S$ – множество возможных МЗ для ООСХД, I – функция уровня затрат на реализацию контрмер в отчетные периоды времени, e_L $\forall L \in \{W,N,O,M\}$ – функции снижения *уровней уязвимости* доменов структурных компонентов ООСХД.

В рамках данной модели нарушение безопасности информационного объекта (ДД) ООСХД характеризуется нарушениями функционирования ПДД организации в соответствии с функциями α и γ. Для вычисления случайной величины ущерба для организации от наступления события нарушения измерения безопасности информационного объекта (или ДД) используется формула:

$$i(a,d) = \sum_{b \in B} c(b, \gamma(b,a,d), \alpha(b,a,d)),$$

где a – измерение безопасности информационного объекта (ДД), d – информационный объект (ДД), $\gamma(b,a,d)$ – показатель снижения эффективности ПДД b вследствие нарушения измерения безопасности a информационного объекта (ДД) d, $\alpha(b,a,d)$ – показатель периода воздействия на ПДД b нарушения измерения безопасности a информационного объекта (ДД) d, $c(b,x,y)$ – ущерб для организации от снижения эффективности ПДД b, характеризуемого показателем x, в течение периода времени, характеризуемого показателем y.

Предложенная математическая модель учета влияния БИ в ООСХД на ПДД также включает в себя другие соотношения, позволяющие вычислять уровни рисков нарушения измерений безопасности информационных объектов (ДД) и на их основе технико-экономические показатели:

$$|\, Risk^{\bar{s}}_{a,d}(\tau) \,| = \begin{cases} i(a,d) P^{\bar{s}}_{a,d}(\tau), \textit{если} (i(a,d) < I_C) \vee (P^{\bar{s}}_{a,d}(\tau) < P_C), \\ i(a,d), \textit{если} (i(a,d) \geq I_C) \wedge (P^{\bar{s}}_{a,d}(\tau) \geq P_C), \end{cases}$$

$$LE(\bar{s},\tau) = \sum_{a \in A, d \in D} |\, Risk^{\bar{s}}_{a,d}(\tau) \,|,$$

$$ROI(\bar{s},\tau) = (LE(\varnothing,\tau) - LE(\bar{s},\tau) - I(\bar{s},\tau)) / I(\bar{s},\tau), ROI(\varnothing,\tau) = 0,$$

$$NPV(\bar{s},d,\Delta\tau,N) = \sum_{p=1}^{N} \frac{LE(\varnothing,\tau_p) - LE(\bar{s},\tau_p)}{(1+d)^p} - \sum_{p=1}^{N} \frac{I(\bar{s},\tau_p)}{(1+d)^p},$$

$$IRR(\bar{s},\Delta\tau,N) = d \,|_{NPV(\bar{s},d,\Delta\tau,N)=0}.$$

Здесь $\bar{s}$ – некоторый набор применяемых контрмер, $P^{\bar{s}}_{a,d}(\tau)$ – вероятность нарушения измерения безопасности a ДД d в течение периода времени τ при наличии контрмер $\bar{s}$ (предполагается, что значения $P^{\bar{s}}_{a,d}(\tau)$ близки к нулю), I_C – минимальное значение ущерба, являющегося катастрофическим для организации, P_C – максимально допустимая вероятность катастрофического ущерба, $LE(\bar{s},\tau)$ – ожидаемый ущерб для организации за период времени τ при наличии контрмер $\bar{s}$, $ROI(\bar{s},\tau)$ – окупаемость инвестиций на реализацию контрмер $\bar{s}$ за период времени τ, $I(\bar{s},\tau)$ – уровень затрат на реализацию контрмер $\bar{s}$ за период времени τ, $NPV(\bar{s},d,\Delta\tau,N)$ – ЧПС контрмер $\bar{s}$ для N отчетных периодов τ_p, $p=1,\ldots,N$ равной длительности $\Delta\tau$, $IRR(\bar{s},\Delta\tau,N)$ – внутренняя норма рентабельности контрмер $\bar{s}$ для N отчетных перио-

дов τ_p, $p=1,\ldots,N$ равной длительности $\Delta\tau$, d – *ставка дисконтирования* для вычисления ЧПС (отражает стоимость инвестируемого капитала).

На основе построенной математической модели учета влияния БИ в ООСХД на ПДД в работе выявлен набор данных, необходимых для определения контекста управления рисками, который включает в себя значения: I_{max} – максимальный уровень затрат на реализацию контрмер, LE_{max} – максимальный ожидаемый ущерб, ROI_{min} – минимальная окупаемость инвестиций, NPV_{min} – минимальная ЧПС, IRR_{min} – минимальная внутренняя норма рентабельности, $r \in R=\{optCost,optROI,optNPV\}$ – решаемая в рамках процесса обработки рисков нарушения БИ оптимизационная задача для технико-экономических показателей (*optCost* – минимизация суммарных затрат организации, связанных с реализацией рисков и их обработкой, *optROI* - максимизация окупаемости инвестиций, *optNPV* – максимизация ЧПС).

С использованием построенной математической модели, положений международного стандарта ISO/IEC 27005 и метода дерева атак в диссертации выполнен анализ процессов идентификации, анализа и обработки рисков нарушения БИ в ООСХД, позволивший установить практические действия для реализации данных процессов, включая сбор информации, вычисление на ее основе уровней рисков и технико-экономических показателей, а также решение поставленной оптимизационной задачи. Полученная в результате методическая основа оформлена в работе в виде методики обработки рисков нарушения БИ в ООСХД, удовлетворяющей поставленным требованиям. В работе показано, что разработанная методика обладает рациональной трудоемкостью за счет применения дискретных шкал для отдельных измеряемых величин, группирования рассматриваемых сущностей в множества малой мощности, применения многократно используемого каталога МЗ для ООСХД и использования методов дискретной оптимизации для решения оптимизационных задач с помощью вычислительной техники.

Разработанная методика обработки рисков нарушения БИ в ООСХД имеет следующую структуру.

1. *Общие положения*. В этом разделе даются основные понятия, определяются условия применения методики и цель ее выполнения.

2. *Номенклатура используемых данных и структура методики*. Задается номенклатура для исходных и результирующих данных методики. Определяется, что выполнение методики осуществляется в виде двух последовательных процедур – *определения контекста* и *обработки рисков*.

3. Определение контекста. Определяется практическая последовательность действий для получения всех необходимых параметров методики с использованием доступных внешних источников информации, в которые входят: мнения лиц, принимающих решения, результаты экспертных оценок, исторические статистические данные, релевантная открытая информация, например, научные публикации, отчеты профильных организаций, публикации в средствах массовой информации.

4. Обработка рисков. Определяются формулы для вычисления на основе полученной в ходе определения контекста информации уровней рисков и технико-экономических показателей, постановка оптимизационной задачи поиска набора контрмер для ООСХД в условиях заданных параметров и возможные методы ее решения. Для решения оптимизационной задачи рекомендуется использование

метода ветвей и границ или метода перебора с возвратом. Результатом выполнения методики является определение набора контрмер, внедрение которых оптимизирует технико-экономические показатели деятельности предприятия по ОБИ в ООСХД.

Основными отличительными особенностями разработанной методики являются: 1) применение цикла обработки рисков нарушения БИ, соответствующего международному стандарту ISO/IEC 27005; 2) оценка уровней рисков на основе математической модели учета влияния БИ в ООСХД на ПДД; 3) снижение трудоемкости за счет группирования сущностей и их взаимосвязей в домены на основе структурных особенностей объектно-ориентированного хранения информации и логической организации ООСХД; 4) снижение трудоемкости за счет каталогизации информации о МЗ для ООСХД; 5) поиск набора контрмер для ООСХД в качестве решения оптимизационной задачи, сформулированной для целевой функции одного из технико-экономических показателей: суммарных затрат организации, связанных с реализацией рисков и их обработкой, окупаемости инвестиций, ЧПС; 6) возможность расширенного применения при использовании адаптированных каталогов МЗ для систем хранения данных, не являющихся объектно-ориентированными, но обладающих логической организацией соответствующей логической организации ООСХД.

В третьей главе – **"Разработка моделей и протоколов обеспечения безопасности информации в объектно-ориентированных сетях хранения данных"** – решены задачи разработки информационного обеспечения методики обработки рисков нарушения БИ в ООСХД: разработана схема применения МЗ в ООСХД, комплекс протоколов аутентификации КП при доступе к информации в ООСХД, модель обеспечения целостности и конфиденциальности данных, хранимых на ООУХД, математическая модель функционирования СПВ уровня ООУХД.

Для того чтобы предоставить основу для формирования каталога МЗ для ООСХД, применимого в рамках разработанной методики обработки рисков, в работе исследованы недостаточно разработанные в существующих научно-технических публикациях технологические возможности ОБИ в ООСХД. На основе анализа схемы и сценариев доступа КП к информации в ООСХД, соответствующих стандарту ANSI INCITS 400-2004 и архитектуре pNFS, определен общий перечень МЗ, необходимых для снижения вероятностей нарушения измерений безопасности хранимых в сети данных. Для отдельных видов МЗ исследованы возможности по улучшению производительности операций аутентификации, контроля доступа и сопровождения политики безопасности по сравнению с моделью безопасности ООСХД, приведенной в стандарте ANSI INCITS 400-2004. На основе полученных результатов в работе предложена схема применения МЗ в ООСХД, представляющая собой совокупность МЗ, реализующих их протоколов и алгоритмов, которые применяются в каждом из сценариев выполнения операций над хранимыми в сети данными с целью снижения вероятностей нарушения измерений безопасности этих данных.

Предложенная схема применения МЗ в ООСХД содержит: 1) предположения относительно доверия к узлам ООСХД; 2) перечень протоколов прикладного уровня для выполнения операций над данными в ООСХД; 3) перечень применяемых МЗ; 4) описание сценариев доступа КП к информации в ООСХД и соответствующе-

го им применения протоколов прикладного уровня и МЗ для ОБИ. На рис. 2 приведена иллюстрация предложенной схемы и сценария доступа КП к информационному объекту, размещенному в ООСХД.

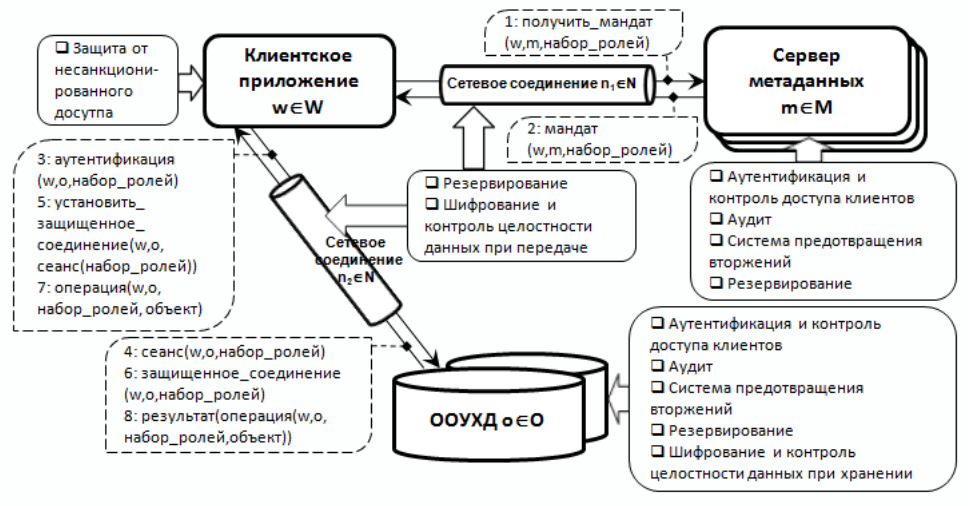

Рис. 2. Схема применения МЗ в ООСХД

В рамках предложенной схемы применения МЗ в ООСХД в работе проведена разработка комплекса протоколов аутентификации КП, модели обеспечения целостности и конфиденциальности данных, хранимых на ООУХД, и математической модели функционирования СПВ уровня ООУХД. Основные результаты этого этапа исследования представлены автором диссертации в работах [2-4,7-10].

Комплекс протоколов аутентификации разработан на основе следующих основных требований: 1) обеспечение взаимной аутентификации между КП и ООУХД или серверами метаданных; 2) работа через открытые сетевые соединения без дополнительных протоколов защиты; 3) поддержка ролевой модели контроля доступа (англ. Role-Based Access Control, RBAC); 4) устойчивость к активным и пассивным сетевым атакам; 5) повышение производительности. Предложенный комплекс протоколов включает в себя два протокола: *GetCap* – протокол получения КП от сервера метаданных мандата на использование назначенных ему ролей, *Auth* – протокол аутентификации КП на ООУХД или сервере метаданных с использованием мандата для установления защищенного соединения. Каждый из протоколов представлен в двух вариантах – для ООСХД с защищенной синхронизацией системного времени узлов сети и без нее. В основу разработанных протоколов положено использование *ролевых ключей* и распределенное хранение информации о политике безопасности, при котором соответствие ролей и привилегий сопровождается децентрализованно на ООУХД, а соответствие пользователей (КП) и ролей – централизованно на серверах метаданных. При этом повышение производительности протоколов достигается за счет отсутствия избыточных операций, снижения количества используемых ключей доступа, снижения интенсивности обменов между КП и серверами метаданных. Объединение протоколов *GetCap* и *Auth* при отсутствии синхронизации

системного времени узлов сети имеет следующий вид.

$$(1) A \rightarrow M : I_A, I_B, N_{A_1}, \qquad idKey_{AB} \equiv MAC_{K_{BM}}(I_A, H(roleList), L),$$

$$(2) A \leftarrow M : E_{K_{AM}}(N_{A_1}, idKey_{AB}, roleList, L, I_B), \qquad roleKey_{AB} \equiv MAC_{idKey_{AB}}(activeRoleList),$$

$$(3) A \leftarrow B : N_B, \qquad k \equiv f(k_A, k_B),$$

$$(4) A \rightarrow B : I_A, roleList, L, activeRoleList, E_{roleKey_{AB}}(I_A, N_B, N_{A_2}, k_A),$$

$$(5) A \leftarrow B : E_{roleKey_{AB}}(N_{A_2}, k_B).$$

Здесь *A* – КП, *B* – ООУХД или сервер метаданных, *M* – сервер метаданных, $idKey_{AB}$ – личный ключ *A* для взаимодействия с *B*, $roleKey_{AB}$ – ролевой ключ *A* для взаимодействия с *B*, *roleList* – полный набор ролей *A*, *activeRoleList* – набор ролей *A*, активируемых в сеансе, *L* – срок действия и/или номер версии личного ключа $idKey_{AB}$, K_{AM} – общий секретный ключ *A* и *M*, K_{BM} – общий секретный ключ *B* и *M*, *N* – случайные числа, *E* – симметричный алгоритм шифрования, *MAC* – код аутентификации сообщений (например, HMAC), *H* – хэш-функция с трудно обнаруживаемыми коллизиями, *f* – функция комбинирования сеансовых подключей, *k* – сеансовый ключ защищенного соединения *A* и *B*.

Для разработанных протоколов в работе проведен анализ их корректности с использованием формального метода верификации протоколов защиты – BAN-логики. Доказано, что в условиях заданных предположений о доверии к участникам протокола они достигают требуемых результатов и являются корректными.

В качестве основы для создания МЗ в диссертации предложена модель обеспечения целостности и конфиденциальности информации, размещенной на ООУХД, удовлетворяющая следующим основным требованиям: 1) защита конфиденциальных объектов с помощью симметричного шифрования; 2) защита целостности и аутентичности информационных объектов с помощью ЭЦП; 3) возможность использования в сети ООУХД, не являющихся доверенными; 4) отсутствие возможности раскрытия ключей доступа любыми КП; 5) поддержка ролевой модели контроля доступа; 6) повышение производительности. Данная модель включает в себя ряд технических решений, позволяющих обеспечивать целостность и конфиденциальность информации на ООУХД в соответствии со следующими требованиями: 1) использование доверенных посредников между КП и ООУХД - *криптографических адаптеров* (КА), осуществляющих обработку и передачу трафика между КП и ООУХД при доступе к защищенным информационным объектам; 2) шифрование и подпись информационных объектов ООУХД на независимых ключах, помещаемых в специальные информационные объекты – *ключевые блоки*, размещаемые на том же ООУХД и шифруемые на *ролевых мастер-ключах* (РМК), ставящихся в соответствие каждой роли; 3) распределение РМК на основе протокола группового распределения ключей TGDH (Tree-Based Group Diffie-Hellman) между КП и КА в соответствии с назначенными КП ролями; 4) распределенное хранение информации о политике безопасности, при котором соответствие ролей и привилегий сопровождается децентрализованно на ООУХД, а соответствие пользователей (КП) и ролей – централизованно на серверах метаданных. При этом распределение РМК на основе протокола TGDH обеспечивает возможность вычисления РМК только парой, состоящей из КП и КА, что исключает раскрытие ключей доступа для КП. Необходимые для работы протокола данные, включающие в себя деревья затемненных долей РМК КП и КА, сохраняются на серверах метаданных.

Операции назначения и отзыва ролей КП в рамках данного протокола с учетом установленного распределенного хранения информации о политике безопасности осуществляются посредством малого количества действий и с участием минимального количества участников.

Описание модели обеспечения целостности и конфиденциальности информации, размещенной на ООУХД, в работе представлено в виде спецификации, включающей в себя предположения относительно доверия к узлам ООСХД и используемой политики безопасности, а также реализующие модель протоколы выполнения основных операций сопровождения политики безопасности и доступа к информационным объектам в ООСХД.

Заключительная часть главы посвящена исследованию вопросов обнаружения и предотвращения вторжений на уровне ООУХД. Показано, что СПВ, размещаемые на уровне ООУХД, обладают рядом положительных качеств: 1) высокая вероятность обнаружения любых атак на ИС, обращающихся к хранимой на ООУХД информации; 2) высокий уровень надежности вследствие сложности компрометации СПВ; 3) возможность обнаружения атак в случае компрометации других узлов ООСХД и ИС, частью которой она является; 4) возможность оперативного реагирования на инциденты нарушения БИ и предотвращения распространения вторжений в ИС; 5) облегчение расследования инцидентов нарушения БИ.

В работе выделяются четыре базовые категории признаков вторжений, которые могут обнаруживаться на уровне ООУХД: модификация редко изменяемых данных и атрибутов, шаблоны доступа, нарушение целостности содержимого информационных объектов, подозрительное содержимое информационных объектов. Исследование этих категорий и вариантов ответной реакции позволило предложить математическую модель функционирования СПВ уровня ООУХД, основанную на организации исполнения на ООУХД конфигурируемых правил обнаружения и ответной реакции на определенные виды операций над информационными объектами, форматы информационных объектов и временные характеристики шаблонов доступа. Модель определяет формулы генерации ответной реакции СПВ на основе входных данных, описывающих поступающие от КП запросы доступа к информационным объектам, хранимым на ООУХД, и может служить основой для практической реализации СПВ уровня ООУХД.

Четвертая глава – **"Разработка и применение инструментального средства для обработки рисков нарушения безопасности информации в объектно-ориентированных сетях хранения данных"** – посвящена разработке информационного и программного обеспечения методики обработки рисков нарушения БИ в ООСХД для ее практического применения, а также экспериментальному анализу эффективности методики.

Так как применение разработанной методики обработки рисков нарушения БИ в ООСХД сопряжено с большим объемом организационной и вычислительной работы, в рамках диссертационного исследования поставлена задача разработки программного инструментального средства, позволяющего снизить трудоемкость практического выполнения шагов методики за счет автоматизации обработки необходимой информации и проведения вычислений. Для определения возможностей по упрощению спецификации в рамках инструментального средства каталога МЗ для

ООСХД в работе проведен анализ структуры и состава данного каталога. Выявлено, что значительная часть информации, содержащейся в каталоге, может многократно использоваться при применении методики обработки рисков нарушения БИ как в рамках одной, так и в рамках различных организаций. С учетом этого свойства предложена схема каталогизации информации о МЗ для ООСХД в форме актуализируемого базового каталога, позволяющая снизить трудозатраты на формирование актуальных каталогов МЗ перед применением методики обработки рисков.

В качестве источников информации о МЗ для базового каталога выделяются: 1) каталоги методов управления рисками нарушения БИ (ISO/IEC 27002, IT-Grundschutz Catalogues, CRAMM, MEHARI); 2) международные стандарты, детализирующие обеспечение сетевой безопасности и использование систем обнаружения вторжений (ISO/IEC 18028, ISO/IEC 18043); 3) лучшие практики по обеспечению безопасности систем хранения данных SNIA BCPs; 4) технические стандарты и документация МЗ, предусмотренных в протоколах, применяемых для построения ООСХД (ANSI INCITS 400-2004, ANSI INCITS 426-2007, RFC 3723, NFSv4.1 [Internet Draft] и др.); 5) научно-исследовательские работы и публикации; 6) предложенная в диссертации схема применения МЗ для ООСХД, разработанные модели и протоколы; 7) продукты мировых производителей программного и аппаратного обеспечения.

В развитие информационного обеспечения методики обработки рисков нарушения БИ в ООСХД в диссертации определен и представлен в табличной форме примерный состав базового каталога МЗ для ООСХД, содержащий множество частных реализаций МЗ, предусматриваемых разработанной схемой применения МЗ в ООСХД.

С учетом полученных результатов автором разработано программное инструментальное средство автоматизации ИСКР 1.0 для применения разработанной методики обработки рисков нарушения БИ в ООСХД, удовлетворяющее базовым требованиям совместимости, удобства в использовании, высокой производительности, переносимости и обновляемости. На основе анализа базовых требований в качестве наиболее подходящего технологического решения для реализации инструментального средства ИСКР 1.0 использована клиент-серверная архитектура доступа к Web-приложению, написанному на языке программирования Java и реализующему графический пользовательский интерфейс для редактирования каталога МЗ для ООСХД и выполнения шагов методики обработки рисков. Функциональные требования к реализации инструментального средства определены посредством последовательного рассмотрения спецификации исходных данных и отдельных шагов методики обработки рисков нарушения БИ в ООСХД с точки зрения возможности использования инструментального средства для автоматизации выполняемых действий.

Разработанное инструментальное средство ИСКР 1.0 обладает следующими особенностями: 1) представление каталога МЗ в виде XML-файла для многократного использования; 2) наличие двух отдельных Web-интерфейсов для редактирования каталога МЗ и применения методики обработки рисков нарушения БИ в ООСХД; 3) ввод информации о значениях функций, определенных над конечными множествами с помощью HTML-форм табличного вида; 4) ввод и редактирование

информации, связанной с сущностями из одного множества, с помощью визуального редактора, реализованного в виде HTML-страницы; 5) реализация алгоритма поиска решения оптимизационной задачи на основе метода перебора с возвратом в рамках выделенного потока на Web-сервере в асинхронном режиме.

Экспериментальный анализ эффективности разработанной в диссертации методики обработки рисков нарушения БИ в ООСХД был проведен в двух крупных промышленных предприятиях. В компании ООО “Одноклассники”, сопровождающей высоконагруженный Web-ресурс www.odnoklassniki.ru, задача обработки рисков была поставлена следующим образом: определить и привести в исполнение набор контрмер, использование которых в рамках ООСХД, применяемой для хранения архива переписки пользователей, позволит минимизировать ожидаемые суммарные затраты компании на применение контрмер и покрытие ущерба, связанного с нарушением безопасности данных переписки пользователей, за период 3 года. На основе такой формулировки и дополнительных исходных данных с помощью средства ИСКР 1.0 был получен результирующий набор контрмер и расчетные значения технико-экономических показателей: в течение трех лет ожидаемый предотвращенный ущерб составляет 428 тыс. долл. (оценки выполнялись в долларах США), окупаемость инвестиций 1.02033, уровень затрат на внедрение и эксплуатацию контрмер 212 тыс. долл., ЧПС применения контрмер 160 тыс. долл., внутренняя норма рентабельности 5.4604.

В Небанковской Кредитной Организации “Международная Расчетная Палата” (ООО), обслуживающей расчетные и инвестиционные операции физических и юридических лиц, задача обработки рисков была поставлена следующим образом: определить и привести в исполнение набор контрмер, ЧПС применения которых в рамках ООСХД, используемой для хранения базы данных архива расчетных операций, является максимальной за период 5 лет. С помощью средства ИСКР 1.0 был получен результирующий набор контрмер и расчетные значения технико-экономических показателей: в течение пяти лет ожидаемый предотвращенный ущерб составляет 2841 тыс. руб., окупаемость инвестиций 0.103398, уровень затрат на внедрение и эксплуатацию контрмер 2575 тыс. руб., ЧПС применения контрмер 102 тыс. руб., внутренняя норма рентабельности 0.18185.

Экспериментальный анализ показал, что разработанная методика обработки рисков нарушения БИ в ООСХД может успешно применяться на практике для повышения технико-экономических показателей деятельности предприятий по ОБИ.

В **заключении** приведены основные результаты диссертационной работы, рассмотрены пути дальнейшего развития темы исследования.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

В диссертации представлены результаты теоретических и прикладных исследований, направленных на решение научно-технической задачи разработки и применения методики обработки рисков нарушения БИ в ООСХД, позволяющей оптимизировать применение средств защиты информации в ООСХД с учетом связанных с ними затрат и ожидаемого ущерба от возможных нарушений БИ.

Основным научным результатом исследования является создание методики обработки рисков нарушения БИ в ООСХД, позволяющей повысить информацион-

ную безопасность предприятий, использующих ООСХД в составе корпоративных ИС.

В процессе выполнения работы получены следующие основные результаты:

1. На основе исследования факторов, обуславливающих потребность предприятий в ОБИ, и применяемых подходов к обоснованию затрат на ОБИ установлена потребность в решении организационных и технических вопросов ОБИ в рамках единого экономически обоснованного подхода. Проведенный анализ и систематизация литературных источников, международных стандартов, нормативных и справочных документов, определяющих организационно-управленческие подходы к ОБИ, позволил установить в качестве научно-методической базы для решения задачи выбора уровня затрат на ОБИ и набора применяемых мер защиты понятийный и алгоритмический аппарат концепции управления рисками. На основе анализа литературных источников и документов, связанных с задачами ОБИ в ООСХД и их решением в рамках организационно-управленческих подходов, произведена формальная постановка задачи обработки рисков нарушения БИ в ООСХД и решаемой в диссертации задачи разработки методики обработки рисков нарушения БИ в ООСХД.

2. На основе понятийного и алгоритмического аппарата концепции управления рисками, положений международного стандарта управления рисками нарушения БИ ISO/IEC 27005, результатов анализа подходов к экономическому обоснованию деятельности по ОБИ, а также методов системного анализа и методов дискретной оптимизации построена математическая модель учета влияния БИ в ООСХД на процессы деловой деятельности. На базе этой модели обоснована и разработана методика обработки рисков нарушения БИ в ООСХД. Методика обладает рациональной трудоемкостью и позволяет решать задачи анализа и синтеза систем защиты информации в ООСХД. В частности, методика позволяет выбирать меры по ОБИ в ООСХД с учетом связанных с ними затрат и ожидаемого ущерба от возможных нарушений БИ таким образом, чтобы обеспечить оптимизацию технико-экономических показателей деятельности предприятия по ОБИ в ООСХД.

3. В рамках информационного обеспечения для методики обработки рисков нарушения БИ в ООСХД предложена схема применения механизмов защиты в ООСХД, позволяющая обеспечить пренебрежимо малую вероятность нарушения безопасности информации при осуществлении к ней доступа в рамках ООСХД, а также повысить производительность операций аутентификации, контроля доступа и сопровождения ПБ по сравнению со стандартизированной моделью безопасности ООСХД.

4. В рамках схемы применения механизмов защиты в ООСХД предложен комплекс протоколов аутентификации клиентских приложений при доступе к информации, размещенной на ООУХД и серверах метаданных в составе ООСХД. Предложенные протоколы поддерживают установление защищенных соединений между клиентами и ООУХД или серверами метаданных для обеспечения целостности и конфиденциальности передаваемых данных и обеспечивают повышенную производительность операций аутентификации. Доказано, что протоколы являются корректными.

5. Разработана модель обеспечения целостности и конфиденциальности информации, хранимой на ООУХД в составе ООСХД, основанная на использовании ролевой модели контроля доступа и протокола группового распределения ключей TGDH, а также реализующие ее протоколы для производительного выполнения основных операций сопровождения ПБ и контроля доступа. Разработанная модель предназначена для использования в рамках схемы применения механизмов защиты в ООСХД и позволяет использовать в составе сети ООУХД, не являющиеся доверенными.

6. Анализ возможности применения систем обнаружения и предотвращения вторжений для снижения уровней рисков нарушения БИ в рамках схемы применения механизмов защиты в ООСХД показал, что СПВ уровня ООУХД позволяют снижать уровни рисков нарушения БИ для всей ИС, содержащей ООСХД, в том числе в условиях частичной компрометации ИС и обхода нарушителями других механизмов защиты ООСХД. Разработана математическая модель функционирования СПВ уровня ООУХД, показывающая принципиальную возможность создания такой системы, и определены требования к практической реализации СПВ уровня ООУХД.

7. В развитие информационного обеспечения разработанной методики обработки рисков нарушения БИ в ООСХД предложена схема каталогизации информации о механизмах защиты для ООСХД в форме актуализируемого базового каталога, позволяющая существенно снизить трудозатраты на подготовительный этап перед выполнением методики, а также определен примерный состав базового каталога механизмов защиты для ООСХД.

8. Для дополнительного снижения практических трудозатрат на выполнение методики обработки рисков нарушения БИ в ООСХД разработано ее программное обеспечение в форме инструментального средства автоматизации ИСКР 1.0, упрощающего спецификацию необходимой для выполнения методики информации и автоматизирующего вычисление результата.

9. Экспериментальный анализ эффективности разработанной методики обработки рисков нарушения БИ в ООСХД, проведенный в крупных промышленных предприятиях – ООО “Одноклассники” и Небанковской Кредитной Организации “Международная Расчетная Палата” (ООО) – показал, что она может успешно применяться на практике для повышения технико-экономических показателей деятельности предприятий по ОБИ. Определены практические рекомендации по использованию методики, ее информационного и программного обеспечения в рамках общего процесса управления рисками на предприятии.

ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

Статьи в журналах, включенных ВАК в перечень ведущих рецензируемых научных журналов и изданий, в которых должны быть опубликованы основные научные результаты диссертаций

1. Алферов И.Л. Управление информационными рисками в объектно-ориентированных сетях хранения данных / И.Л. Алферов // Безопасность информационных технологий. – 2007. – № 3. – С. 23 – 30.

2. Алферов И.Л. Криптографические методы обеспечения целостности и конфиденциальности информации на объектно-ориентированных устройствах хранения данных / И.Л. Алферов // Безопасность информационных технологий. – 2007. – № 1. – С. 29 – 36.

3. Алферов И.Л. Аутентификация клиентов при доступе к информации в объектно-ориентированных сетях хранения данных / И.Л. Алферов // Безопасность информационных технологий. – 2008. – № 4. – С. 62 – 70.

4. Алферов И.Л. Предотвращение вторжений на уровне объектно-ориентированных устройств хранения данных / И.Л. Алферов // Безопасность информационных технологий. – 2008. – № 4. – С. 71 – 78.

Тезисы научных докладов

5. Алферов И.Л. Анализ информационных рисков в объектно-ориентированных сетях хранения данных / И.Л. Алферов // В сб. Методы и технические средства обеспечения безопасности информации: Материалы XVI Общероссийской научно-технической конференции. – СПб.: Изд-во Политехнического ун-та, 2007. – С. 50.

6. Алферов И.Л. Моделирование угроз для объектно-ориентированных сетей хранения данных / И.Л. Алферов // В сб. докладов Всероссийской научно-технической конференции студентов, аспирантов и молодых ученых «Научная сессия ТУСУР-2007», 3 – 7 мая 2007 г. – С. 46 – 48.

7. Алферов И.Л. Криптографическая защита информации от непосредственного считывания с носителей объектных устройств хранения данных / И.Л. Алферов // В сб. Методы и технические средства обеспечения безопасности информации: Материалы XV Общероссийской научно-технической конференции. – СПб.: Изд-во Политехнического ун-та, 2006. – С. 66.

8. Алферов И.Л. Управление доступом к информации, размещенной на недоверенных устройствах в составе объектной сети хранения данных / И.Л. Алферов // В сб. Научная сессия МИФИ – 2007. XIV Всероссийская научная конференция «Проблемы информационной безопасности в системе высшей школы». – М.: МИФИ, 2007. – С. 14 – 15.

9. Алферов И.Л. Механизмы аутентификации клиентов при доступе к информации в объектных сетях хранения данных / И.Л. Алферов // В сб. Научная сессия МИФИ – 2007. XIV Всероссийская научная конференция «Проблемы информационной безопасности в системе высшей школы». – М.: МИФИ, 2007. – С. 16 – 17.

10. Алферов И.Л. Обнаружение вторжений на уровне объектно-ориентированных устройств хранения данных / И.Л. Алферов // В сб. Научная сессия МИФИ – 2008. XV Всероссийская научная конференция «Проблемы информационной безопасности в системе высшей школы». – М.: МИФИ, 2008. – С 14 – 15.

Алферов Игорь Леонидович

МЕТОДИКА ОБРАБОТКИ РИСКОВ НАРУШЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ОБЪЕКТНО-ОРИЕНТИРОВАННЫХ СЕТЯХ ХРАНЕНИЯ ДАННЫХ

Подписано в печать 21.04.2010.
Тираж 100 экз.
ЗАО “КопиМакс”.
115054, г. Москва,
Павелецкая площадь, д.2, стр.1,
тел. +7(495)937-0770.