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

На правах рукописи

УДК 004.056.53

БОНДАРУК
Андрей Александрович

МЕТОДЫ И АЛГОРИТМЫ ПОСТРОЕНИЯ ЗАЩИЩЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

АВТОРЕФЕРАТ
диссертации на соискание степени
магистра техники и технологий

по специальности 1-39 81 01 – Компьютерные технологии
проектирования электронных систем

Минск 2017

Работа выполнена на кафедре проектирования информационно-компьютерных систем учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

Научный руководитель: **АЛЕКСЕЕВ Виктор Федорович,** кандидат технических наук, доцент, заместитель заведующего кафедры проектирования информационно-компьютерных систем учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

Рецензент: **ПОЛУБОК Владислав Анатольевич,** кандидат технических наук, доцент, заведующий кафедрой микропроцессорных систем и сетей учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

Защита диссертации состоится «22» июня 2017 г. года в 10 00 часов на заседании Государственной комиссии по защите магистерских диссертаций в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники» по адресу: 220013, Минск, ул. П.Бровки, 6, копр. 1, ауд. 415, тел. 293-20-80, e-mail: kafpiks@bsuir.by

С диссертацией можно ознакомиться в библиотеке учреждения образования «Белорусский государственный университет информатики и радиоэлектроники».

ВВЕДЕНИЕ

Информационные системы используются практически во всех сферах деятельности человека. В процессе их функционирования могут возникать недопустимые последствия, обусловленные несанкционированным доступом к информационной системе.

В информационной системе могут хранится и обрабатываться персональные данные сотрудников компании, а также разработки, представляющие коммерческую тайну. Одной из основных угроз безопасности информационных систем являются преднамеренные действия злоумышленника, в качестве которого может быть, как преступник, так и сотрудник компании. Получив доступ к информационной системе, преступник может нарушить работоспособность организации и нанести значительный экономический ущерб.

Существует большое количество средств, обеспечивающих защиту информационных систем, например, разграничение доступа пользователей к информационным ресурсам. Однако, этот подход не решает всей проблемы защиты информационный систем от злоумышленников. В тоже время следует учитывать, что применяемые меры защиты должны соответствовать вероятности осуществления атаки на информационную систему и возможному ущербу с учетом затрат на обеспечение защиты.

На сегодняшний день существует большое число работ в области защиты информационных систем. Наиболее значимые результаты были получены российскими учеными, которые проводили исследования по обеспечению безопасности информационных систем (Цирлов В.Л., Гайкович В.Ю., Ершов Д.В., Шаньгин В.Ф. Запечников С.В. и др.).

Формирование новых методов и алгоритмов защиты информации и их использование приводит к повышению качества обеспечения защиты, обосновывают актуальность темы.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования

В информационной системе могут хранится и обрабатываться персональные данные сотрудников компании, а также разработки, представляющие коммерческую тайну, повреждение которых может нанести значительный ущерб работоспособности организации. В связи с этим актуальной является разработка методов и алгоритмов защиты информации и их использование для повышения качества обеспечения защиты.

Степень разработанности проблемы

Исследование защиты информационных систем от воздействия различных угроз, осуществлялось на основе построения теоретических моделей с использованием работ российских ученых: Запечников С.В., Гайкович В.Ю., Ершов Д.В., Цирлов В.Л., Шаньгин В.Ф.

Цель и задачи исследования

Целью диссертации является разработка методики и алгоритма защиты информационной системы от несанкционированного доступа.

Поставленная цель работы определяет следующие основные задачи:

1) Провести анализ существующих методов и алгоритмов обеспечения безопасности информационных систем.

2) Разработать методику и алгоритм обеспечения защиты информационной системы, на основе результатов анализа исходной защищенности.

3) Обосновать эффективность разработанной методики посредствам моделирования защиты информационной системы предприятия.

Область исследования

Содержание диссертации соответствует образовательному стандарту высшего образования второй ступени (магистратуры) специальности 1-39 81 01 «Компьютерные технологии проектирования электронных систем».

Теоретическая и методологическая основа исследования

В основу диссертации легли работы российских ученых в области информационной безопасности.

Информационная база исследования сформирована на основе литературы, открытой информации, технических нормативно-правовых актов, сведений из электронных ресурсов, а также материалов научных конференций и семинаров.

Научная новизна

Научная новизна и значимость заключается в формировании и исследовании методов и алгоритмов обеспечения информационной безопасности.

Теоретическая значимость работы заключается в анализе методов и алгоритмов построения защиты информационных систем.

Практическая значимость диссертации состоит в снижение расходов на обеспечение защиты информационных систем, повышение защищенности и снижения вероятности возникновения ущерба от неправомерных действий в ИС.

Основные положения, выносимые на защиту

1. Специфика формирования требований к защищенности информационной системы, заключающийся в последовательном сокращении формального перечня требований к системе защиты, на основе анализа следующих параметров: вид угроз информационной безопасности, категории информационных систем и исходной оценки их защищенности.

2. Алгоритм оценки общей защищенности информационной системы, заключающийся в вычислении коэффициента защищенности, на основе данных об актуальности рассматриваемых угроз, коэффициентах опасности этих угроз и выбранных средств защиты информации для их нейтрализации.

3. Методика построения защиты информационной системы, заключающаяся в последовательном применении методов и алгоритмов защиты, с целью повышения коэффициента общей защищенности.

Апробация диссертации и информация об использовании ее результатов

Результаты исследований, вошедшие в диссертацию, докладывались и обсуждались на XXI Всероссийской научно-технической конференции студентов, молодых ученых и специалистов, Рязань, Российская Федерация (2016г.) и 12-й Международной молодежной научно-технической конференции, Севастополь, Российская Федерация (2016г.).

Публикации

Изложенные в диссертации основные положения и выводы опубликованы в 4 печатных работах.

Общий объем публикаций по теме диссертационной работы составляет 0,5 авторских листа.

Структура и объем работы

Диссертация состоит из введения, общей характеристики работы, трех глав с краткими выводами по каждой главе, заключения, библиографического списка и приложений.

В первой главе проведен анализ существующих проблем обеспечения безопасности информационных систем, угроз, методов и алгоритмов обеспечения защиты информационных систем. **Во второй главе** представлена методика защиты информационной системы, на основе оценки исходной защищенности. **В третьей главе** представлен эксперимент по подтверждению адекватности методики, посредствам моделирования защиты на основе информационной системы предприятия. **В приложении** представлены публикации соискателя, акт внедрения и графический материал.

Общий объем диссертационной работы составляет 94 страницы. Из них 43 страницы основного текста, 14 иллюстраций на 6 страницах, 9 таблиц на 8 страницах, библиографический список из 35 наименований на 3 страницах, список собственных публикаций соискателя из 4 наименований на 1 странице, 3 приложений на 24 страницах.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** рассмотрено современное состояние проблемы защиты информации и информационных систем, а также описано обоснование актуальности темы.

В **общей характеристике работы** показана актуальность проводимых исследований, степень разработанности проблемы, сформулированы цель и задачи диссертации, обозначена область исследований, научная (теоретическая и практическая) значимость исследований, а также апробация работы.

В первой главе приведен анализ современного состояния проблемы обеспечения безопасности информационных систем (ИС).

Современные методы обработки, передачи и накопления информации способствовали появлению угроз, связанных с возможностью потери, искажения и раскрытия данных, адресованных или принадлежащих конечным пользователям. Поэтому обеспечение информационной безопасности компьютерных систем и сетей является одним из ведущих направлений развития информационных технологий.

Существует несколько видов классификаций информационных систем:

1) классификация по масштабу: одиночные, групповые, корпоративные.

2) классификация по сфере применения: системы обработки транзакций, системы принятия решений, информационно-справочные системы, офисные информационные системы.

3) классификации информационных систем представляет собой разделение информационных систем по способу организации. В соответствии этому способу, информационные системы подразделяются: системы на основе архитектуры файл-сервер, системы на основе архитектуры клиент-сервер, системы на основе многоуровневой архитектуры, системы на основе интернет-технологий.

Угрозы информационной безопасности подразделяются на: угрозы нарушения конфиденциальности информации, в результате реализации которых информация становится доступной субъекту, не располагающему полномочиями для ознакомления с ней, угрозы нарушения целостности информации, к которым относится любое злонамеренное искажение информации, об-

рабатываемой с использованием информационной системы, угрозы нарушения доступности информации, возникающие в тех случаях, когда доступ к некоторому ресурсу информационной системы для легальных пользователей блокируется.

Средства защиты информации подразделяться на следующие группы:

– технические и аппаратные средства включают в себя устройства различного принципа действия, обеспечивающие на техническом (внешнем) и аппаратном (внутреннем) уровне решение задач защиты информации;

– программные средства включают в себя специальное программное обеспечение, предназначенное для идентификации пользователей, контроля доступа, шифрования информации, удаления временных файлов, тестового контроля (в основном контроль целости) системы защиты и мониторинга средств защиты;

– смешанные аппаратно-программные средства реализуют те же функции, что аппаратные и программные средства в отдельности, и имеют промежуточные свойства;

– организационные средства являются наиболее универсальными средствами защиты информации, способными закрыть все уязвимости и недостатки при применении всех вышеуказанных средств. Организационные средства состоят из организационно-технических и организационно-правовых средств.

Среди методов защиты ИС одним из наиболее распространенных является аудит информационной безопасности, проводимый для получения независимой и объективной оценки текущего уровня защищённости предприятия от угроз информационной безопасности. Аудит позволяет выявить недостатки в системе защиты информации на основе имеющегося опыта экспертов, участвующих в процедуре обследования, найти и устранить уязвимости программно-аппаратного обеспечения системы, а также оценить соответствие системы защиты ИС предъявляемым требованиям.

Одним из наиболее часто применяемых методов для защиты персональных данных от несанкционированного доступа является управление рисками информационной безопасности. Суть управления рисками состоит в оценке их размера, выработке эффективных и экономичных мер их снижения, а также в установлении приемлемых рамок для них.

Во второй главе представлена сформированная методика сбора и анализа информации в ИС, включающая классификацию ИС, оценку текущего уровня защищенности ИС, и построение множества актуальных угроз безопасности.

Классификация ИС осуществляется с учетом категорий и объема накапливаемых, обрабатываемых и распределяемых с их использованием персональных данных с целью установления методов и способов защиты, необходимых для обеспечения безопасности персональных данных.

В целях снижения вероятности проявления угроз на всех стадиях жизненного цикла информационной системы необходимо использовать комплекс мер и средств защиты:

1) технические и аппаратные средства;
2) программные средства;
3) программно-технические средства;
4) организационные средства.

Таблица 1 – Возможности нарушителя

Тип нарушителя	Информация об объекте атаки	Средства атаки	
		Чем располагают	Как использовать
H_1		доступные в свободной продаже аппаратными компонентами и криптосредствами	могут использовать штатные криптосредствами только за пределами КЗ
H_2		=	используют штатные средства в зависимости от орг. мер
H_3	известны все сети связи, работающие на еди- ном ключе	= + дополнительные средства в зависимости от орг. мер.	=
H_4	=	=	= + проводят лаб. анализ криптосредств
H_5	= + имеют исходные тексты прикладного программного обеспечения	=	=
H_6	=	безграничный доступ	=
Примечание: знаком «=» в таблице обозначены условия информационной атаки, соответствующие предыдущему типу нарушителя, а знаком «+» – вновь появляющиеся условия.			

Актуальной считается угроза, которая может быть реализована в информационной системе и представляет опасность для хранящейся в ней информации.

При оценке опасности на основе опроса экспертов (специалистов в области защиты информации) определяется вербальный показатель опасности для рассматриваемой ИС. Этот показатель имеет три значения:

1) низкая опасность – если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;

2) средняя опасность – если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;

3) высокая опасность – если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

Так же производится вероятностная оценка нарушителя

Для вероятностной оценки действий нарушителя необходимо определить шесть основных типов: $H_1, H_2, \ldots, H_6$. При этом возможности нарушителя типа H_{i+1} включают в себя возможности нарушителя типа H_i, где $1 \leq i \leq 5$, а для отдельных типов нарушителей можно выделить отличительные признаки, приведенные в таблице 1.

Вычисление коэффициента защищенности *W* предусматривает ряд подготовительных действий таких как: определение класса ИС, определение полного множества угроз и коэффициента опасности угрозы. Данные сведения получаются на этапе сбора данных о рассматриваемой ИС. Полное множество угроз определяется путем анализа возможных уязвимостей средств защиты и нарушений со стороны исполнителей.

Разработанный таким образом метод оценки общей защищенности ИС является комплексным и включает в себя алгоритм, показанный на рисунке 1.

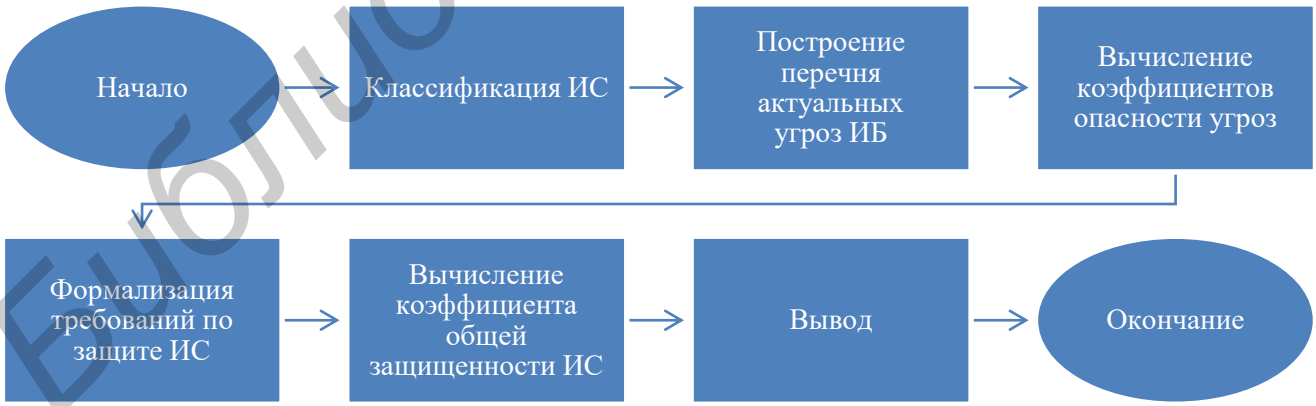

Рисунок 1 – Алгоритм построения защиты информационной системы

Построение защиты информационной системы с использованием данного алгоритма позволяет сократить затраты времени и средств для достижения необходимого уровня защиты.

В третьей главе описывается применение разработанной методики построения ИС в защищенном исполнении на примере частной организации.

В рассматриваемой информационной системе хранятся и обрабатываются данные 50 сотрудников предприятия.

По завершению первой стадии предлагаемой методики были получены следующие результаты: по специфике обрабатываемых данных и по структуре рассматриваемая информационная система была определена по классу Б2; построена модель вероятного нарушителя безопасности информационной системы; сформировано поле угроз информационной безопасности. Для защищаемой информационной системы, были рассмотрены следующие группы угроз: угрозы утечки защищаемой информации по техническим каналам, угрозы физического воздействия на компоненты информационной системы, угрозы использования специально разработанных средств реализации атак, угрозы воздействия вредоносного программного обеспечения, угрозы не технического характера, угрозы межсетевого взаимодействия.

В результате анализа применяемых в организации средств защиты информации было установлено, что в организации осуществляется разграничение доступа в контролируемую зону по средствам установленной системы контроля и управления доступом с использование электронных ключей (меток). Исходный уровень защищенности рассматриваемой информационной системы был определен как низкий. Согласно построенной модели угроз в рассматриваемой ИС выявлено 16 видов угроз с коэффициентом опасности равным 1 и 3 вида угроз с коэффициентом опасности равным 0,5. Вычисленный на основе этих данных исходный коэффициент защищенности составляет 0,0487.

На втором этапе, на основании сформированного ранее поля угроз был построен перечень актуальных угроз, включающий непреднамеренное воздействие на компоненты информационной системы, несанкционированный доступ к информационной системе, воздействия вредоносного программного обеспечения, угрозы не технического характера, угрозы использования специально разработанных средств реализации атак.

На третьем этапе был сформирован список требований к защищенности информационной системы от несанкционированного доступа, касающийся обмена данных при их обработке, программного обеспечения средств защиты информации, применяемых в информационной системе, основных методов и способов защиты информации, обеспечивающих управление доступом, регистрацию и учет всех событий безопасности и обеспечения целостности данных в ИС.

На четвертой стадии методики осуществлялся выбор организационных мер и технических средств защиты информации для ИС. Оценка параметров,

учитываемых при разработке мер и выборе средств защиты информации (размер ущерба и значение вероятности возникновения риска), определялась экспертным путем.

По результатам применения алгоритма были выбраны следующие средства, нейтрализующие максимальное количество угроз и удовлетворяющие критериям по стоимости: *Kaspersky Endpoint Security* 10 для *Windows* (стоимость установки на 50 узлов равна 4560 *BYN*). Результат примененных действий показан в таблице 2.

Таблица 2 – Меры обеспечения защиты информационной системы

Актуальные угрозы	Меры реализации защиты	Системы защиты информации
Использование уязвимостей штатного программного обеспечения	Установка сертифицированного средства антивирусного контроля	В *Kaspersky Endpoint Security*, присутствует инструмент, позволяющий сканировать установленное программное обеспечение на наличие уязвимостей.
Использование программных закладок	Установка сертифицированного средства антивирусного контроля	*Kaspersky Endpoint Security* присутствуют средства позволяющие определить вредоносные изменения в исполняемых файлах и пресечь их
Социальная инженерия по отношению к штатным пользователям ИС	Обучение сотрудников организации, должны быть разработаны политики и процедуры обеспечения безопасности.	
Внедрение нештатного программного обеспечения	Разграничение доступа к ресурсам организации	Достигается дополнительной настройкой средств администрирования *Windows*, для журналирования и последующего анализа всех фактов установки ПО на рабочие станции
Внедрение вирусных программ	Установка сертифицированного средства антивирусного контроля	*Kaspersky Endpoint Security*
Отключение средств защиты информации	Ограничение доступа к устройствам и службам причастным к системе защиты информации	Разграничение доступа достигается стандартными средствами *Windows*

Пятая стадия применяемой методики представляет собой оценку соответствия принятых организационных мер и средств защиты информации тре-

буемым на основе вычисления коэффициента общей защищенности ИС, который составил 0,1429, что свидетельствует об успешном построении ИС в защищенном исполнении. В результате применения разработанной методики общая защищенность системы была увеличена почти в 3 раза.

ЗАКЛЮЧЕНИЕ

Основные научные результаты диссертации

1. Выполнен анализ применяемых требований к защищенности ИС, заключающийся в последовательном сокращении формального перечня требований к системе защиты ИС.

2. Разработана методика и алгоритм построения защиты информационной системы, в основе которого лежит детальный анализ требований к защите информационной системы, расчет результирующей оценки защищенности ИС.

3. В результате разработки методики и алгоритма построения защищенных информационных систем, было проведено моделирование обеспечения защиты информационной системы предприятия. Посредствам которого было обнаружено значительное повышение результирующей защищенности предприятия от воздействий нарушителя.

Рекомендации по практическому использованию результатов

Полученные результаты внедрены в учебный процесс на кафедре проектирвоания информационно−компьютерных систем учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» в учебный курс «Методы и технические средства обеспечения безопасности».

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

1 Бондарук, А.А. Защита компьютерных систем методом дублирования информации / А.А. Бондарук // Новые информационные технологии в научных исследованиях: материалы XXI Всероссийской научно-технической конференции студентов, молодых ученых и специалистов, Рязань, Российская Федерация / ФГБОУ ВО «РГРТУ». – Рязань. 2016. – С. 218−220.

2 Бондарук, А.А. Подходы к обеспечению защиты информации от несанкционированного доступа с учетом инцидентов информационной без-опасности / А.А. Бондарук // Новые информационные технологии в научных исследованиях: материалы XXI Всероссийской научно-технической конференции студентов, молодых ученых и специалистов, Рязань, Российская Федерация / ФГБОУ ВО «РГРТУ». – Рязань. 2016. – С. 220−222.

3 Бондарук, А.А. Криптографические методы защиты информации / А.А. Бондарук // Современные проблемы радиоэлектроники и телекоммуникаций, РТ-2016: материалы 12-я Международной молодежной научно-технической конференции, Севастополь, Российская Федерация / ФГБОУ ВО «СевГУ». – Севастополь. 2016. – С. 161.

4 Савостеев, Ю.И. Программные средства защиты информационных систем / Ю.И. Савостеев, А.А. Бондарук // Современные проблемы радиоэлектроники и телекоммуникаций, РТ-2016: материалы 12-я Международной молодежной научно-технической конференции, Севастополь, Российская Федерация / ФГБОУ ВО «СевГУ». – Севастополь. 2016. – С. 162.

РЭЗЮМЭ

Бандарук Андрэй Аляксандравіч

Метады і алгарытмы пабудовы абароненых інфармацыйных сістэм

Ключавыя словы: абарона, інфармацыйная сістэма..

Мэта працы: фарміраванне метаду і алгарытму, абароны інфармацыйных сістэм, з улікам памяншэння выдаткаў рэсурсаў.

Атрыманыя вынікі і іх навізна: выкананы аналіз існуючых метадаў і алгарытмаў забеспячэння бяспекі інфармацыйных сістэм; распрацавана методыка забеспячэння абароны інфармацыйнай сістэмы, эксперыментальна ўстаноўлена эфектыўнасць распрацаванай методыкі па сродках мадэлявання абароны інфармацыйнай сістэмы.

Ступень выкарыстання: вынікі ўкаранёны ў навучальным працэсе на ка-Фёдар праектаванне інфармацыйна-камп'ютэрныя сістэмы установы абра¬зовании «Беларускія дзяржаўным універсітэт інфарматыкі і радыёэлек¬тронике ў навучальным курсе «Метады і тэхнічныя сродкі забеспячэння бяспекі».

Вобласць ужывання: інфармацыйныя сістэмы персанальных дадзеных.

РЕЗЮМЕ

Бондарук Андрей Александрович

Методы и алгоритмы построения защищенных информационных систем

***Ключевые слова*:** защита, информационная система.

***Цель работы*:** Целью диссертации является формирование метода и алгоритма защиты информационных систем, с учетом уменьшения затрат ресурсов.

***Полученные результаты и их новизна*:** выполнен анализ существующих методов и алгоритмов обеспечения безопасности информационных систем; разработана методика обеспечения защиты информационной системы, экспериментально установлена эффективность разработанной методики по средствам моделирования защиты информационной системы.

***Степень использования*:** результаты внедрены в учебный процесс на кафедре проектирования информационно−компьютерных систем учреждения образования «Белорусский государственный университет информатики и радиоэлектроники в учебный курс «Методы и технические средства обеспечения безопасности».

***Область применения*:** информационные системы персональных данных.

SUMMARY

Bandaruk Andrei Aleksandrovich

Methods and algorithms for building secure information systems

***Keywords*:** protection, information system.

***The object of study*:** The aim of the thesis is to form a method and algorithm for the protection of information systems, taking into account the reduction of resource costs.

***The results and novelty*:** the analysis of existing methods and algorithms of maintenance of safety of information systems is executed; the method of ensuring the protection of the information system has been developed, and the effectiveness of the developed methodology on the means of modeling the protection of the information system has been experimentally established.

***Degree of use*:** the results are implemented in the educational process on the design of information and computer systems of the educational institution «Belarusian State University of Informatics and Radio Electronics» in the training course" «Methods and technical means of ensuring safety».

Sphere of application: information systems for personal data.