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

На правах рукописи

УДК 004.056.5

Руденя
Виктор Юрьевич

МЕТОДЫ И АЛГОРИТМЫ ОБЕСПЕЧЕНИЯ ТЕХНОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

АВТОРЕФЕРАТ
диссертации на соискание степени
магистра технических наук

по специальности 1-38 80 04 – Технология приборостроения

Минск 2019

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 кафедры проектирования информационно-компьютерных систем Белорусского государственного университета информатики и радиоэлектроники

Рецензент: **БОНДАРИК Василий Михайлович,**
кандидат технических наук, доцент, декан факультета доуниверситетской подготовки и профессиональной ориентации Белорусского государственного университета информатики и радиоэлектроники

Защита диссертации состоится «5» февраля 2019 года в 9^{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, корп. 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

В современном мире информация и персональные данные стали стратегическим ресурсом. Обеспечение безопасности персональных данных является одним из достоинств развитого государства. Стремительное совершенствование информатизации в Республике Беларусь, проникновение ее во все сферы общества и государства вызвали помимо внушительных преимуществ и некоторые недостатки. Одним из недостатков является необходимость обеспечения защиты информации и информационных систем. Нужно понимать, что с увеличением и усовершенствованием сферы информатизации, пропорционально растет потенциальная её уязвимость.

Информационные технологии развиваются очень стремительно, необходимо постоянно отслеживать изменение и релиз новых программ, технических и технологических средств по обеспечению защиты информации. Необходимо применять только те защитные меры и технологии, правильность работы которых может быть проверена. При этом требуется ответственно и своевременно проводить анализ защитных мер и эффективность применяемых технологий. Только придерживаясь этих принципов можно говорить о том, что обеспечение защиты данных в информационной системе соблюдается.

В процессе эксплуатации информационных систем наблюдаются попытки несанкционированного доступа к информации или личным данным для ее раскрытия, изменения, уничтожения или иных неправомерных действий. Решение задач, связанных с предотвращением воздействия непосредственно на информацию, осуществляется в рамках комплексного обеспечения безопасности информации и имеет хорошо развитую научно-методическую базу. Данный вариант обеспечения безопасности информационных систем и средств ее обработки именуется технологической безопасностью, так как применяются технические средства в информационной системе.

Информационные системы технологической безопасности являются сложными иерархически организованными автоматизированными системами, которые можно рассматривать как совокупность комбинированных подходов, методов и алгоритмов по обеспечению безопасности данных. Главной целью таких систем является своевременное обнаружение внешних или внутренних угроз для информационной системы.

Темп усовершенствования процессов информатизации общества, возникновение новейших технологий для информационных систем, подталкивает на повышенное внимание к обеспечению безопасности и защите персональных данных. Поэтому Республика Беларусь, как и зарубежные страны, совершенствует законодательную базу, модернизирует регламентирующие документы в сфере обеспечения безопасности информации и персональных данных в информационных системах.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования

Необходимость и актуальность исследования методов и алгоритмов обеспечения технологической безопасности информационных систем основывается на том факте, что данные, которые хранят современные информационные системы, представляют собой очень важную информацию, потеря которых влечет за собой серьёзные проблемы. Темп усовершенствования процессов информатизации общества, возникновение новейших технологий для информационных систем, подталкивает на повышенное внимание к обеспечению технологической безопасности и защите персональных данных. Именно поэтому важно использовать актуальные методы и алгоритмы обеспечения технологической безопасности в информационных системах.

В связи с вышесказанным, исследование методов и алгоритмов обеспечения технологической безопасности в информационных системах является актуальным.

Степень разработанности проблемы

Исследование методов и алгоритмов обеспечения технологической безопасности информационных систем осуществлялось на основе построения теоретических моделей с использованием работ российских, белорусских, а так же зарубежных ученых: Пугин В.В., Пулко Т.А., Баранова Е.К., Бабаш А.В., Борботько Т.В., Урбанович П.П., Харин Ю.С., Томчик Л.С., Куракин А.С., Шередин Р.В., Баскаков Е.А., Саксонов Е.А., Романенко Д.М., *McCallister Er., Grance T., Scarfone K., Babak B.R., Boneh D.*

Одним из недостатков исследований в представленной литературе является недостаточно современная информация об обеспечении технологической защиты, с помощью которой можно было бы максимально эффективно защитить информационные системы.

Предложенное исследование направлено на устранение данного недостатка, основывается на проведении исследования современных методов и алгоритмов обеспечения технологической безопасности информационных систем, а также критическому анализу каждому из рассмотренных методов.

Цель и задачи исследования

Целью диссертации является исследование методов и алгоритмов обеспечения технологической безопасности информационных систем путем сравнения современных подходов, принципов и методов обеспечения безопасности, делая критический анализ рассматриваемых методов.

Поставленная цель работы определяет следующие основные задачи:

1. Провести обзор и анализ нормативно-правового обеспечения информационной безопасности в Республике Беларусь, рассмотреть основные фак-

торы, определяющие ее технологическую безопасность и оценить проблему защиты данных в информационных системах.

2. Исследовать подходы и принципы обеспечения технологической безопасности информационных систем, методы и средства информационной безопасности предприятия, а также способы защиты информационных систем.

3. Исследовать методы и алгоритмы обеспечения технологической безопасности информационных систем.

Область исследования

Содержание диссертации соответствует образовательному стандарту высшего образования второй ступени (магистратуры) специальности 1-38 80 04 «Технология приборостроения».

Теоретическая и методологическая основа исследования

В основу диссертации легли работы белорусских, российских и зарубежных ученых в области исследования методов и алгоритмов обеспечения безопасности информационных систем, а также анализ технических нормативных правовых актов по рассматриваемой тематике.

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 полученных результатов работы заключается в исследовании методов и алгоритмов обеспечения технологической безопасности информационных систем, путем сравнения современных подходов и принципов, делая критический анализ рассматриваемых методов.

Теоретическая значимость работы заключается в детальном анализе методов и алгоритмов обеспечения технологической безопасности информационных систем с учетом их особенностей.

Практическая значимость диссертации состоит в том, что на основании исследования методов и алгоритмов обеспечения технологической безопасности информационных систем можно построить такую информационную систему, которая будет удовлетворять современным стандартам технологической безопасности.

Основные положения, выносимые на защиту

1. Обоснование обеспечения безопасности персональных данных методом обезличивания, основанного на подходах перемешивания, декомпозиции, изменения состава или семантики и введения идентифика-

торов, а также методология выбора подхода обезличивания и выбор подхода обезличивания в зависимости от класса решаемых задач.

2. Критическая оценка современных видов вредоносного программного обеспечения, позволяющих сделать вывод о современных методах обеспечения безопасности информационных систем от вредоносного программного обеспечения.

3. Критический анализ обеспечения технологической безопасности криптографическими методами и алгоритмами, используя особенности безопасности на протоколах транспортного и прикладного уровня.

Апробация диссертации и информация об использовании ее результатов

Результаты исследований, вошедшие в диссертацию, докладывались и обсуждались на 53-й научной конференции аспирантов, магистрантов и студентов БГУИР (Беларусь, 2017) и 54-й научной конференции аспирантов, магистрантов и студентов БГУИР (Беларусь, 2018).

Публикации

Изложенные в диссертации основные положения и выводы опубликованы в 4 печатных работах. Эти статьи опубликованы в репозитории БГУИР.

Общий объем публикаций по теме диссертационной работы составляет 12 авторских листов.

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 приведен обзор нормативно-правового обеспечения информационной безопасности в Республике Беларусь, где описано на чем основывается Государственная политика обеспечения информационной безопасности Республики Беларусь, основные национальные интересами в информационной сфере Беларуси, а также проект закона о персональных данных для Республики Беларусь. Рассмотрены основные факторы, определяющие технологическую безопасность информационных систем, а также сделаны выводы о проблемах защиты данных в информационных системах. **Во второй главе** исследованы подходы и принципы обеспечения технологической безопасности информационных систем, методы и средства информационной безопасности предприятия, включая механизмы защиты, а также сделаны выводы о способах защиты информационных систем. **В третьей главе** представлено исследование обеспечения технологической безопасности методом обезличивания

персональных данных, где описаны свойства и правила обезличивания данных, сделана методология выбора подхода обезличивания, а также определен выбор подхода обезличивания в зависимости от класса решаемых задач. Исследовано современное вредоносное программное обеспечение, к каждому типу вирусов представлены примеры, а также сделан вывод о методах борьбы с ними. Выполнен критический анализ симметричного и асимметричного криптографических методов шифрования, выявлены особенности обеспечения безопасности на протоколах прикладного и транспортного уровня. Сделан вывод о проблемах и перспективах развития криптографических методов и алгоритмов защиты данных в информационных системах. **В приложениях** представлены публикации автора, акт внедрения в учебный процесс и презентация.

Общий объем диссертационной работы составляет 88 страниц. Из них 58 страниц основного текста, 2 иллюстрации на 2 страницах, библиографический список из 88 наименований на 7 страницах, список собственных публикаций соискателя из 2 наименований на 1 странице, 3 приложения на 16 страницах.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** рассмотрено современное состояние проблемы обеспечения безопасности данных в информационных системах, указаны основные направления исследований, проводимых по данной тематике, 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 обзор текущего нормативно-правового обеспечения информационной безопасности в Республике Беларусь. Так закон об информации налагает обязательство на любое лицо, собирающее персональные данные (далее – ПД), принимать меры по их надлежащей защите до момента, когда лицо, к которому относятся персональные данные, дает согласие на их разглашение либо до момента обезличивания персональных данных.

Трактовка Концепции национальной безопасности Республики Беларусь, утвержденной Указом Президента Республики Беларусь от 09.11.2010 №575 гласит, что под **информационной безопасностью** понимается состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере. Данное понятие является первичным и основным для определения компетенции государственных органов по обеспечению информационной безопасно-

сти, а также установлению государственной политики в информационной сфере.

В работе отмечено, что правовое обеспечение информационной безопасности и защиты информации в Республике Беларусь базируется на:

— Международных договорах в области информационной безопасности.

— Конституции Республики Беларусь от 15.03.1994.

— Кодифицированных нормативных правовых актах.

— Законах Республики Беларусь.

— Приказах и постановлениях Оперативно-аналитического цента при Президенте Республики Беларусь.

— Указах Президента Республики Беларусь и постановлениях Совета Министров Республики Беларусь.

— Государственных программах, утвержденных с целью формирования современных подходов к проектированию и созданию защищенных компьютерных систем, новых технологий и средств технической защиты информации.

Рассмотрен Проект закона о персональных данных для Республики Беларусь, который планируется принять в середине 2019 года. Так, в Республике Беларусь существует необходимость принятия Концепции информационной безопасности, которая бы **комплексно** урегулировала данную сферу отношений и отразила государственную политику в сфере обеспечения информационной безопасности, меры защиты информации, виды и источники угроз в сфере информационной безопасности, первоочередные мероприятия по обеспечению информационной безопасности. Концепция информационной безопасности Республики Беларусь должна развивать и дополнять Конституцию и Концепцию национальной безопасности Беларуси.

Также в первой главе рассмотрены основные факторы, определяющие технологическую безопасность информационных систем (далее – ИС), а также сделаны выводы о проблемах защиты данных в ИС.

Показано, что требования по обеспечению безопасности в различных ИС могут существенно отличаться, однако они всегда направлены на достижение трех основных свойств:

– **Целостность.** Информация, на основе которой принимаются решения, должна быть достоверной и точной, защищенной от возможных непреднамеренных и злоумышленных искажений.

– **Доступность.** Информация и соответствующие автоматизированные службы должны быть доступны, готовы к работе всегда, когда в них возникает необходимость.

– **Конфиденциальность.** Информация должна быть доступна только тому, кому она предназначена.

Для решения проблем информационной безопасности необходимо сочетание законодательных, организационных, технологических и стандартизационных мероприятий.

Во второй главе исследованы подходы и принципы обеспечения технологической безопасности ИС.

Показано, что существует два принципиальных подхода к обеспечению компьютерной безопасности для предприятий:

1. Фрагментарный. Данный подход ориентируется на противодействие строго определенным угрозам при определенных условиях (например, специализированные антивирусные средства, отдельные средства регистрации и управления, автономные средства шифрования и т.д.).

Достоинством фрагментарного подхода является его высокая избирательность относительно конкретной угрозы. Недостатком – локальность действия, т.е. фрагментарные меры защиты обеспечивают эффективную защиту конкретных объектов от конкретной угрозы.

2. Комплексный. Данный подход получил широкое распространение вследствие недостатков, присущих фрагментарному. Он объединяет разнородные меры противодействия угрозам и традиционно рассматривается в виде трех дополняющих друг друга направлений. Организация защищенной среды обработки информации позволяет в рамках существующей политики безопасности обеспечить соответствующий уровень безопасности ИС. Недостатком данного подхода является высокая чувствительность к ошибкам установки и настройки средств защиты, а также сложность управления.

Также в главе рассмотрены **методы обеспечения защиты информации на предприятии:**

1. Препятствие – метод физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т.п.).

2. Управление доступом – метод защиты информации регулированием использования всех ресурсов автоматизированной информационной системы предприятия.

3. Маскировка – метод защиты информации в автоматизированной информационной системе предприятия путем ее криптографического закрытия.

4. Регламентация – метод защиты информации, создающий такие условия автоматизированной обработки, хранения и передачи информации, при которых возможность несанкционированного доступа к ней сводилась бы к минимуму.

5. Принуждение – метод защиты информации, при котором пользователи и персонал системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной и уголовной ответственности.

6. Побуждение – метод защиты информации, который побуждает пользователей и персонал системы не нарушать установленные правила за счет соблюдения сложившихся моральных и этических норм.

В работе описано, что указанные выше методы обеспечения информационной безопасности реализуются с помощью одного или комплекса следующих средств: физических, аппаратных, программных, аппаратно-программных, криптографических, организационных, законодательных и морально-этических.

Рассмотрены способы защиты информационных систем:

1. Защита конфиденциальной информации от несанкционированного доступа и модификации, которая призвана обеспечить решение одной из наиболее важных задач – защиту хранимой и обрабатываемой в вычислительной технике информации от всевозможных злоумышленных покушений, которые могут нанести существенный экономический и другой материальный и нематериальный ущерб.

2. Защита информации в каналах связи, которая направлена на предотвращение возможности несанкционированного доступа к конфиденциальной информации, циркулирующей по каналам связи различных видов между различными уровнями управления экономическим объектом или внешними органами.

3. Защита юридической значимости электронных документов оказывается необходимой при использовании систем и сетей для обработки, хранения и передачи информационных объектов, содержащих в себе приказы и другие распорядительные, договорные, финансовые документы.

4. Защита информации от утечки по каналам побочных электромагнитных излучений и наводок является важным аспектом защиты конфиденциальной и секретной информации в вычислительной технике от несанкционированного доступа со стороны посторонних лиц.

5. Защита от несанкционированного копирования и распространения программ и ценной компьютерной информации является самостоятельным видом защиты прав, ориентированных на проблему охраны интеллектуальной собственности, воплощенной в виде программ и ценных баз данных.

В третьей главе представлено исследование обеспечения технологической безопасности методом обезличивания персональных данных. **Обезличивание персональных данных** – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Описаны **свойства обезличенных данных:**

1. ***Полнота*** – сохранение всей информации о персональных данных конкретных субъектов или группах субъектов, которая имелась до обезличивания.

2. ***Структурированность*** – сохранение структурных связей между обезличенными данными конкретного субъекта или группы субъектов, соответствующих связям, имеющимся до обезличивания.

3. ***Релевантность*** – возможность обработки запросов по обработке персональных данных и получения ответов в одинаковой семантической форме.

4. ***Семантическая целостность*** – соответствие семантики атрибутов обезличенных данных семантике соответствующих атрибутов персональных данных при их обезличивании.

5. ***Применимость*** – возможность обработки персональных данных с целью решения задач, стоящих перед Оператором, без предварительного деобезличивания всего объема записей о субъектах.

6. ***Анонимность*** – невозможность однозначной идентификации субъектов данных, полученных в результате обезличивания, без применения дополнительной информации.

В главе 3 также приведен пример использования и дан критический анализ современным подходам к обезличиванию:

1. Методу введения идентификаторов (замена части сведений идентификаторами с созданием таблицы соответствия идентификаторов исходным данным).

2. Методу изменения состава или семантики (изменение состава или семантики персональных данных путем замены результатами статистической обработки, обобщения или удаления части сведений).

3. Методу декомпозиции (разбиение массива персональных данных на несколько частей с их последующим раздельным хранением).

4. Методу перемешивания (перестановка отдельных записей, а также групп записей в массиве персональных данных).

Исследовано современное вредоносное программное обеспечение, приведены примеры каждых из типов вредоносного ПО с примерами. **Вредоносное программное обеспечение** – это программный код, который обладает обширной способностью заражать информационную систему. Он может выполнять вредоносные действия в системе, а также в информационных сетях системы. В ходе исследования также сделан вывод о методах борьбы с ними.

В главе 3 исследованы криптографические методы и алгоритмы обеспечения безопасности. **Криптография** – незаменимый инструмент, используемый для защиты информации в информационных системах. **Криптографическое преобразование** – это преобразование информации, основанное на некотором алгоритме, зависящем от изменяемого параметра (ключа), и обладающее свойством невозможности восстановления исходной информации по преобразованной, без знания ключа, с трудоемкостью меньше заранее заданной.

В работе выполнен критический анализ симметричного и асимметричного криптографических методов шифрования. В ***симметричных криптосистемах*** для шифрования и для дешифрования используют один ключ, такие криптосистемы часто называют системами с секретным закрытым ключом. Потому что ключ должен быть доступен и храниться только у того, кто занимается шифровкой/расшифровкой сообщений. Можно сказать, что обеспечение конфиденциальности равно пропорционально защите симметричного шифрования

В **асимметричном шифровании** используется два ключа: один для шифрования, а другой для дешифрования. Ключ шифрования называется открытым ключом, он общедоступен для всех, кто хочет отправлять вам зашифрованные сообщения. А ключ дешифрования должен оставаться секретным и называется закрытым ключом. Открытый ключ может быть вычислен из закрытого ключа, но очевидно, что закрытый ключ не может быть вычислен из открытого ключа.

Выявлены особенности обеспечения безопасности на протоколах прикладного и транспортного уровня. Сделан вывод о проблемах и перспективах развития криптографических методов и алгоритмов защиты данных в ИС.

ЗАКЛЮЧЕНИЕ

Основные научные результаты диссертации

1. Выполнен анализ белорусских и зарубежных источников по тематике обеспечение безопасности ИС, который показал, что на настоящий момент в Беларуси вопрос комплексного урегулирования сферы безопасности является актуальным. Обеспечение информационной безопасности Республики Беларусь должно развиваться и дополнять Конституцию и Концепцию национальной безопасности Беларуси. Была обоснована необходимость обеспечения технологической безопасности информационных технологий и систем от злоумышленного воздействия на программные средства или базы данных. Было отмечено, что с развитием информационных технологий наблюдается увеличение способов и методов хищения данных, а также появление новых уязвимостей в ИС.

2. Проведено исследование подходов и принципов для обеспечения технологической безопасности информационных систем, методов и средств информационной безопасности предприятия, а также способов защиты информационных систем, которое показало важность правильного выбора технологических средств для обеспечения наиболее полной безопасности ИС предприятия. Рассмотрены и систематизированы современные принципы обеспечения безопасности. В ходе исследования было выявлено, что актуальными являются вопрос универсального подхода для защиты ИС, а также метод защиты ИС, который будет актуален на протяжении длительного промежутка времени.

3. Выполнено исследование по обеспечению технологической безопасности персональных данных методом обезличивания, в ходе которого был дан критический анализ каждому из подходов деперсонализации данных, а также выявлен принцип к выбору подхода обезличивания в зависимости от класса решаемых задач. Исследование вредоносного ПО и методов борьбы с ним выявило наилучшие методы для предотвращения ИС от заражения вредоносным ПО, а также сделан вывод о проблемах и перспективах развития вредоносного ПО в современном мире. Исследование криптографических методов и алгоритмов обеспечения технологической безопасности показало разницу криптографических методов симметричного и асимметричного шифрования, был дан критический анализ особенностям криптографического обеспечения безопасности на протоколах транспортного и прикладного уровня, а также были выявлены проблемы и перспективы для развития криптографических систем.

Рекомендации по практическому использованию результатов

На основании результатов исследований возможно построение информационных систем, которые будут удовлетворять современным стандартам технологической безопасности.

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

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

1–А. Руденя, В. Ю. Нормативно-правовое обеспечение информационной безопасности в Республике Беларусь / В. Ю. Руденя. - Репозиторий БГУИР, 2019. – [Электронный ресурс]. - Режим доступа : https://libeldoc.bsuir.by/handle/123456789/34368.

2–А. Руденя, В. Ю. Проблемы защиты данных в информационных системах / В. Ю. Руденя. - Репозиторий БГУИР, 2018. – [Электронный ресурс]. - Режим доступа : https://libeldoc.bsuir.by/handle/123456789/34370.

3–А. Руденя, В. Ю. Подходы и принципы для обеспечения технологической безопасности информационных систем / В. Ю. Руденя. - Репозиторий БГУИР, 2018. – [Электронный ресурс]. - Режим доступа : https://libeldoc.bsuir.by/handle/123456789/34372.

4–А. Руденя, В. Ю. Методы и средства информационной безопасности предприятий / В. Ю. Руденя. - Репозиторий БГУИР, 2018. – [Электронный ресурс]. - Режим доступа : https://libeldoc.bsuir.by/handle/123456789/34373.

РЕЗЮМЕ
Руденя Виктор Юрьевич
Методы и алгоритмы обеспечения технологической безопасности информационных систем

Ключевые слова: методы и алгоритмы, технологическая безопасность, информационные системы.

Цель работы: исследование методов и алгоритмов обеспечения технологической безопасности информационных систем путем сравнения современных подходов, принципов и методов обеспечения безопасности ИС, делая критический анализ рассматриваемых методов.

Полученные результаты и их новизна: выполнен анализ белорусских и зарубежных источников по тематике обеспечение безопасности информационных систем, который показал, что на настоящий момент в Беларуси вопрос комплексного урегулирования сферы безопасности является актуальным. Была обоснована необходимость обеспечения технологической безопасности информационных технологий и систем от злоумышленного воздействия на программные средства или базы данных.

Проведено исследование подходов и принципов для обеспечения технологической безопасности информационных систем, методов и средств информационной безопасности предприятия, а также способов защиты информационных систем, которое показало важность правильного выбора технологических средств для обеспечения наиболее полной безопасности ИС предприятия. Рассмотрены и систематизированы современные принципы обеспечения безопасности.

Выполнено исследование по обеспечению технологической безопасности персональных данных методом обезличивания, в ходе которого был дан критический анализ каждому из подходов деперсонализации данных. Исследование вредоносного ПО и методов борьбы с ним выявило наилучшие методы для предотвращения ИС от заражения вредоносным ПО, а также сделан вывод о проблемах и перспективах развития вредоносного ПО в современном мире. Исследование криптографических методов и алгоритмов обеспечения технологической безопасности показало разницу криптографических методов симметричного и асимметричного шифрования, был дан критический анализ особенностям криптографического обеспечения безопасности на протоколах транспортного и прикладного уровня.

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

Область применения: любая организация, использующая технические средства с базами данных, компьютерная и электронная промышленность.

РЭЗЮМЭ

Рудзеня Віктар Юр'евіч

Метады і алгарытмы забеспячэння тэхналагічнай бяспекі інфармацыйных сістэм

Ключавыя словы: метады і алгарытмы, тэхналагічная бяспека, інфармацыйныя сістэмы.

Мэта працы: даследаванне метадаў і алгарытмаў забеспячэння тэхналагічнай бяспекі інфармацыйных сістэм шляхам параўнання сучасных падыходаў, прынцыпаў і метадаў забеспячэння бяспекі інфармацыйных сістэм, робячы крытычны аналіз разгляданых метадаў.

Атрыманыя вынікі і іх навізна: выкананы аналіз беларускіх і замежных крыніц па тэматыцы забеспячэнне бяспекі інфармацыйных сістэм, які паказаў, што на дадзены момант у Беларусі пытанне комплекснага ўрэгулявання сферы бяспекі з'яўляецца актуальным. Была абгрунтавана неабходнасць забеспячэння тэхналагічнай бяспекі інфармацыйных тэхналогій і сістэм ад зламыснае ўздзеяння на праграмныя сродкі або базы дадзеных.

Праведзена даследаванне падыходаў і прынцыпаў для забеспячэння тэхналагічнай бяспекі інфармацыйных сістэм, метадаў і сродкаў інфармацыйнай бяспекі прадпрыемства, а таксама спосабаў абароны інфармацыйных сістэм, якое паказала важнасць правільнага выбару тэхналагічных сродкаў для забеспячэння найбольш поўнай бяспецы інфармацыйнай сістэмы прадпрыемства. Разгледжаны і сістэматызаваны сучасныя прынцыпы забеспячэння бяспекі.

Выканана даследаванне па забеспячэнні тэхналагічнай бяспекі персанальных дадзеных метадам обезличивания, падчас якога быў дадзены крытычны аналіз кожнаму з падыходаў деперсонализации дадзеных. Даследаванне шкоднаснага ПА і метадаў барацьбы з ім выявіла найлепшыя метады для прадухілення інфармацыйнай сістэмы ад заражэння шкоднасным праграмным забеспячэннем, а таксама зроблена выснова аб праблемах і перспектывах развіцця шкоднаснага праграмнага забеспячэння ў сучасным свеце. Даследаванне крыптаграфічных метадаў і алгарытмаў забеспячэння тэхналагічнай бяспекі паказала розніцу крыптаграфічных метадаў сіметрычнага і асіметрычнага шыфравання, быў дадзены крытычны аналіз асаблівасцяў крыптаграфічнага забеспячэння бяспекі на пратаколах транспартнага і прыкладнога ўзроўню.

Ступень выкарыстання: вынікі ўкаранёны ў навучальны працэс на ка-Федра праектавання інфармацыйна-камп'ютэрных сістэм ўстановы адукацыі "Беларускі дзяржаўны універсітэт інфарматыкі і радыёэлектронікі ў навучальны курс " Метады і тэхнічныя сродкі забеспячэння бяспекі ".

Вобласць ужывання: любая арганізацыя, якая выкарыстоўвае тэхнічныя сродкі з базамі дадзеных, камп'ютэрная і электронная прамысловасць.

SUMMARY

Rudzenia Viktar Yurevich

Methods and algorithms for ensuring the technological security of information systems

Keywords: methods and algorithms, technological security, information systems.

The object of study: research of methods and algorithms for ensuring the technological security of information systems by comparing modern approaches, principles and methods of ensuring the security of information systems, making a critical analysis of the methods under consideration.

The results and novelty: The analysis of Belarusian and foreign sources was carried out on the subject of ensuring security of information system, which showed that at the moment in Belarus the issue of comprehensive settlement of the security sphere is relevant. The need to ensure the technological security of information technologies and systems from malicious influence on software or databases was justified.

A study of approaches and principles to ensure the technological security of information systems, methods and means of information security of the enterprise, as well as ways to protect information systems, which showed the importance of the correct choice of technological means to ensure the most complete security of the enterprise IP. Considered and systematized modern principles of security.

A study was carried out to ensure the technological security of personal data by the method of anonymization, during which a critical analysis was given to each of the data depersonalization approaches. A study of malware and methods to combat it revealed the best methods to prevent information system from malware infection, and it also concluded that there are problems and prospects for the development of malware in the modern world. The study of cryptographic methods and algorithms for ensuring technological security showed the difference in cryptographic methods of symmetric and asymmetric encryption, and a critical analysis was given to the specifics of cryptographic security assurance on transport and application level protocols.

Degree of use: the results are implemented in the educational process on the design of information and computer systems for the establishment of education "Belarusian State University of Informatics and Radioelectronics in the lecture course "Methods and tools to ensure system security ".

Sphere of application: any organization using technical means with databases, computer and electronic industry.