МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ
БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СЕРВИСА»
(ФГБОУ ВО «ПВГУС»)

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО
ОБРАЗОВАНИЯ
МОСКОВСКОЙ ОБЛАСТИ
«ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(«МГОТУ»)

ЭВОЛЮЦИОННЫЕ ПРОЦЕССЫ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Сборник трудов по материалам
4-й международной научно-технической конференции
5 апреля 2019 г.

Тольятти
2019

УДК 681.3
ББК 32.81
Э15

Рецензенты:
Ставровский М.Е., д.т.н., профессор;
Семенов А.Б., д.т.н., профессор.

Научный редактор:
Артюшенко В.М. – д.т.н., профессор
Воловач В.И. – д.т.н.

Э15 **Эволюционные процессы информационных технологий**: сборник трудов по материалам 4-й международной научно-технической конференции 5 апреля 2019 г. / колл. авторов; под общ. науч. ред. док. техн. наук, профессора Артюшенко В.М., и док. техн. наук Воловача В.И. – М.: Издательство «Научный консультант», 2019. – 130 с

ISBN 978-5-907196-08-7

Предлагаемый сборник научных статей основан на материалах 4-й международной научно-технической конференции «Эволюционные процессы информационных технологий», прошедшей 5 апреля 2019 г. на базе кафедр «Информационный и электронный сервис» (ФГБОУ ВО «ПВГУС») и «Информационные технологии и управляющие системы» («МГОТУ»). Он стал результатом творчества ученых, профессорско-преподавательского состава, сотрудников, студентов, связанных с информационными технологиями в различных областях деятельности.

Сборник рассчитан на преподавателей, аспирантов, магистров и бакалавров, а также для широкого круга специалистов в области информационных систем.

УДК 681.3
ББК 32.81

Сборник научных статей подготовлен по материалам, представленным в электронном виде. Ответственность за содержание материалов несут авторы.

ISBN 978-5-907196-08-7

Содержание

ВВЕДЕНИЕ

В предлагаемом сборнике научных трудов рассматривается широкий круг вопросов, связанных с использованием современных средств моделирования сигналов и помех в радиотехнических системах и устройствах, применением информационных технологий при производстве ракетных двигателей, поисково-обнаружительных самоходных установок «MUS», моделированием траектории лунной орбиты, системы ограничений по использованию ресурсов, учитываемых при распределении средств управления космическими аппаратами, расчетом частотно-территориальных разносов для земных станций и радиоэлектронных средств беспроводного доступа и т.д.

Проанализированы вопросы, связанные с использование средств для интеллектуального анализа данных СУБД MICROSOFT SQL SERVER, топографической классификацией плотности распределения вероятностей, обзором программных средств реализации методов DATA MINING.

Рассмотрены технические и организационные рекомендации по повышению помехоустойчивости оборудования систем автоматизации жизнеобеспечения зданий, вопросы функциональных особенностей безопасности проектов «Умный город», комплексные решения проблем электромагнитной совместимости структурированных кабельных систем.

Проведен сравнительный анализ применения структурных и объектно-ориентированных методов проектирования баз данных, различных видов и программных систем разработки современных веб-приложений, методов передачи видеосигнала. Рассмотрены вопросы, связанные с особенностями современных информационных систем, с точки зрения безопасности

Материалы данного сборника будут интересны не только бакалаврам и магистрам таких специальностей как: «Информационные системы и технологии», «Прикладная информатика», «Управление в технических системах», но и аспирантам специальностей «Системный анализ, управление и обработка информации», «Теоретические основы информатики», а также для широкого круга специалистов в области информационных технологий.

ОСОБЕННОСТИ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ, СУЩЕСТВЕННЫЕ С ТОЧКИ ЗРЕНИЯ БЕЗОПАСНОСТИ

Ковалева О.В.,
специалист по УМР 1 кат., аспирант кафедры ИТУС
Технологический университет («МГОТУ»)
Россия, г. Королев

В статье рассмотрены особенности современных информационных систем, существенные с точки зрения безопасности. Структура информационной системы.

Ключевые слова: информационные технологии, информационные системы, безопасность информационных систем.

Каждая современная организация – от малого предприятия до крупного холдинга нуждается в информационных системах и технологиях. Любая информационная система имеет структуру, которая достаточно хорошо описывается четырехуровневой моделью [1-3]:

Внешний уровень, определяющий взаимодействие информационной системы организации с глобальными ресурсами и системами других организаций. Функционально он характеризуется как сетевыми сервисами, предоставляемыми данной организацией, так и, аналогичными сервисами, запрашиваемыми из глобальной сети. На этом уровне должны ограничиваться как попытки внешних пользователей несанкционированно получить от организации дополнительный сервис, так и попытки собственных пользователей осуществить подобные операции по отношению к внешним сервисам или не санкционированно переслать информацию в глобальную сеть.

Сетевой уровень связан с доступом к информационным ресурсам внутри интрасети организации. Безопасность информации на этом уровне обеспечивается средствами проверки подлинности пользователей и разграничением доступа к ресурсам интрасети (аутентификация и авторизация). *Авторизация* – это полномочия, устанавливаемые администратором системы для конкретных лиц, позволяющие последним использовать транзакции, процедуры или всю систему в целом.

Защита информации и выявление атак злоумышленников на сетевом уровне имеет определенную специфику. Если на системном уровне проникнуть в систему можно лишь в результате раскрытия пароля пользователя, то в случае распределенной конфигурации сети становится возможен перехват пользовательских имени и пароля техническими средствами. Кроме аутентификации пользователей, в интрасети должна производиться также аутентификация машин-клиентов. Высокая степень защиты достигается заменой стандартных открытых сервисов на сервисы, шифрующие параметры пользователя/машины-клиента, чтобы даже перехват пакетов не позволял раскрыть эти данные. Наконец, немаловажное значение имеет аудит событий, происходящих в распределенной информационной среде, поскольку в этих условиях злоумышленник не столь заметен и имеет достаточно времени и ресурсов для выполнения своих задач, если в системе отсутствуют автоматическое оповещение и реакция на возможные нарушения.

Системный уровень связан прежде всего с управлением доступа к ресурсам ОС. Именно на этом уровне происходит непосредственное взаимодействие с пользователями и, самое главное, определяются правила общения между информационной системой и пользователем - задается либо изменяется конфигурация системы. В этой связи естественно понимать защиту информации на данном уровне, как четкое разделение, к каким ресурсам ОС, какой пользователь и когда может быть допущен. Защите системных ресурсов и информации, определяющей конфигурацию системы, должно уделяться особое внимание, поскольку несанкционированный доступ к ним может сделать бессмысленными прочие меры безопасности, в том числе и защиту пользовательских данных.

Уровень приложений связан с использованием прикладных ресурсов информационной системы. Поскольку именно приложения на содержательном уровне работают с пользовательскими данными, для них нужны собственные механизмы обеспечения информационной безопасности. Особого внимания требуют приложения, обслуживающие удаленных пользователей. Для каждого приложения определяются требования к безопасности и соответствующие необходимые средства обеспечения безопасности (протоколы и необходимая инфраструктура), которые смогут удовлетворять этим требованиям.

Типичными приложениями для интрасети являются: электронная почта; электронные публикации; информационный поиск; конференции; передача файлов; распределенные вычисления (ActiveX, Java); телефония (Интернет-телефония); электронная коммерция.

Протоколы прикладного уровня ориентированы на конкретные прикладные задачи, решаемые в интрасети. Они определяют, как процедуры по организации взаимодействия определенного типа между прикладными процессами, так и форму представления информации при таком взаимодействии.

Вопросы авторизации, делегирования полномочий с ограничениями также решаются на прикладном уровне. Например, чтобы передать серверу печати право на доступ только к определенным файлам и только на чтение или защитить строки своих таблиц в базе данных от удаления сервером приложений, оставив за ним возможность добавления информации, нужно перестроить систему авторизации на основе архитектуры клиент-сервер. В нынешней ситуации, когда каждое приложение (операционная система, СУБД, почтовая служба, Web-браузеры клиентов интрасети и т.п.) использует специфические методы контроля доступа, универсальное, стандартное решение получить невозможно. Например, браузеры - основные, но не единственные пункты защиты клиента в интрасети. Они могут оказаться не более защищенными, чем операционные системы и рабочие станции, на которых запускаются эти браузеры. Если исходить из традиционных критериев, предъявляемых к информационным системам, то современные Web-браузеры - очень уязвимые клиентские приложения. Браузеры, предлагаемые для массового рынка, не имеют функций защиты, необходимых для поддержки критически важных приложений интрасети. Среди самых уязвимых мест современных коммерческих браузеров - отсутствие защиты паролем, неограниченный доступ к локальным ресурсам компьютера и возможность раскрытия критически важных данных при помощи кнопок «вперед/назад», закладок и выделенных цветом ссылок.

Информационная система типичной современной организации является весьма сложным образованием, построенным в многоуровневой архитектуре клиент/сервер, которая пользуется многочисленными внешними сервисами и, в свою очередь, предоставляет собственные сервисы. Даже сравнительно небольшие магазины, обеспечивающие расчет с покупателями по пластиковым картам, зависят от своих информационных систем и в частности, от защищенности всех компонентов систем и коммуникаций между ними.

Разрушение важной информации, кража конфиденциальных данных, перерыв в работе вследствие отказа - все это выливается в крупные материальные потери, наносит ущерб репутации организа-

ции. Современные информационные системы сложны и, значит, опасны уже сами по себе, даже без учета активности злоумышленников. Постоянно обнаруживаются новые уязвимые места в программном обеспечении. Приходится принимать во внимание чрезвычайно широкий спектр аппаратного и программного обеспечения, многочисленные связи между компонентами.

Меняются принципы построения корпоративных информационных систем. Используются многочисленные внешние информационные сервисы; предоставляются собственные: получило широкое распространение явление, обозначаемое словом «аутсорсинг», когда часть функций корпоративной информационно системы передается внешним организациям. Развивается программирование с активными агентами. Подтверждением сложности проблематики информационной безопасности является параллельный рост затрат на защитные мероприятия и количества нарушений информационной безопасности в сочетании с ростом среднего ущерба от каждого нарушения.

Успех в области информационной безопасности может принести только комплексный подход, сочетающий меры четырех уровней: законодательного; административного; процедурного; программно-технического. Проблема информационной безопасности - не только техническая; без законодательной базы, без постоянного внимания руководства организации и выделения необходимых ресурсов, без мер управления персоналом и физической защиты решить ее невозможно. Комплексность усложняет проблематику информационно безопасности, требуется взаимодействие специалистов из разных областей.

Список используемых источников

1. Артюшенко В.М., Корчагин В.А. Анализ беспроводных технологий обмена данными в системах автоматизации жизнеобеспечения производственных и офисных помещений // Электротехнические и информационные комплексы и системы. 2010. Т.6. № 2. С. 18-24.

2. Аббасова Т. С., Артюшенко В.М. Сервис информационных систем при аварийном планировании // Вестник Ассоциации ВУЗов туризма и сервиса. 2010. №4. С. 68 – 74.

3. Артюшенко В.М., Белянина Н. В. Цифровые сети доступа технологии. М.: Изд-во СГУ, 2010. 210 с.