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

УДК 004.056.53

Недосеко
Диана Юрьевна

Методика противодействия атакам на объектах информатизации средств вычислительной техники

АВТОРЕФЕРАТ
на соискание степени магистра технических наук
по специальности 1-98 80 01 Методы и системы защиты информации, информационная безопасность

_____

Научный руководитель
Утин Леонид Львович
кандидат технических наук

_____

Минск 2016

ВВЕДЕНИЕ

На сегодняшний день информатизация существует в большинстве сферах человеческой деятельности. Нормой обработки информации в корпоративных приложениях становится работа пользователя на одном и том же компьютере, как с открытой, так и с конфиденциальной информацией, требующих для обработки различной номенклатуры ресурсов. А это значит, что если не предпринять специальных мер для ее защиты, издержки, которые понесет предприятие, попытавшись восстановить утраченные данные, значительно превысят стоимость аппаратных средств, используемых для хранения этих данных. Еще более чреватой опасными последствиями является ситуация, при которой налоговая, банковская либо другая конфиденциальная информация попадет в чужие руки.

Но даже сегодня, несмотря на огромное количество разработок, программ и международных стандартов в этой области не создано единого средства защиты информации. Задача обеспечения информационной безопасности противоречива по самой своей сути. С одной стороны, средств обеспечения безопасности никогда не бывает слишком много в том смысле, что защиту всегда можно тем или иным способом преодолеть (просто каждый раз, когда повышается уровень защиты, приходится придумывать более изощренный способ ее обхода). С другой стороны, чем сильнее кого-то или что-то защищают, тем больше возникает неудобств и ограничений. Поэтому идеальной и универсальной системы защиты информации пока не существует.

В 2014 году Аналитическим центром InfoWatch зарегистрировано 13958 (3,8 в день, 116 в месяц) случаев утечки информации, из которых 72,8% произошли по вине внутреннего нарушителя. Для эффективного противодействия инсайдерским атакам необходимо разобраться от кого нужно защищаться. С одной стороны можно всех считать потенциальными вредителями и ко всем применять одинаковые меры защиты, однако такой подход слишком дорогой и может негативно сказаться не только на бюджете компании, но и на атмосфере в коллективе. С другой стороны, события, связанные с Эдвардом Сноуденом в 2013-м году, показали, что наибольшую опасность представляют люди, которые имеют доступ к управлению системой обеспечения информационной безопасности.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с приоритетными направлениями научных исследований и запросами реального сектора экономики

Тема диссертационной работы соответствует подразделу 5.5 «Методы, средства и технологии обеспечения информационной безопасности при обработке, хранении и передаче данных с использованием криптографии, квантово-криптографические системы» приоритетных направлений фундаментальных и прикладных научных исследований Республики Беларусь на 2011 – 2015 гг., утверждённых Постановлением Совета Министров Республики Беларусь 19 апреля 2010г., № 585. Работа выполнялась в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники»

Цель и задачи исследования

Цель работы – создание программного обеспечения, рассчитывающего вероятность утечки информации по вине каждого сотрудника компании.

Для достижения поставленной цели решались следующие задачи:

1. Изучить существующие подходы к системе защиты информации;
2. Рассчитать вероятности утечек информации;
3. Разработать программное обеспечение, используя объектно-ориентированный язык программирования Java и платформу для построения интегрированных сред разработки Eclipse.

Личный вклад соискателя

Все основные результаты и выводы получены соискателем самостоятельно. Аналитическое исследование современных подходов к системе защиты информации проводилось под руководством кандидата технических наук Утина Л.Л. Во время работы над диссертацией соискателем был предложен новый подход к классификации внутренних нарушителей, разработаны математическая модель и программное обеспечение, предназначенное для выявление возможного злоумышленника

Опубликованность результатов диссертации

Материалы диссертации были доложены на 51-й научной конференции студентов, магистрантов, аспирантов БГУИР, 2015; XIII Белорусско-российской научно-технической конференции «Технические средства защиты информации».

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

В первой главе приводится аналитическое исследование современных подходов к системе защиты информации, рассматриваются угрозы информационной безопасности, их источники, классификации и последствия, существующие модели разграничения доступа, подходы к построению системы защиты информации, а также существующие классификации нарушителей, предложенные компаниями Inforwatch и IDC.

Во второй главе предложен новый подход к классификации нарушителей, который был составлен с учетом достоинств и недостатков уже существующих подходов, и позволяет учитывать условия эксплуатации ОИ СВТ, потенциальные возможности пользователей совершать инсайдерскую атаку, мотивацию и цели атаки. Также была произведена оценка вероятности атаки с учетом новой классификации нарушителей.

В третьей главе была рассмотрена математическая модель для выявления потенциального злоумышленника, описана разработка программного обеспечения, а также рекомендации по его использованию.

ЗАКЛЮЧЕНИЕ

В результате проведения аналитических исследований существующих подходов к системе защиты информации, учитывая их достоинства и недостатки, был разработан новый подход к классификации инсайдеров, который позволяет учитывать условия эксплуатации ОИ СВТ, потенциальные возможности пользователей совершать инсайдерскую атаку, мотивацию и цели атаки. Предложенная классификация содержит необходимые исходные данные для решения следующих задач специалистами в области защиты информации: оптимизация финансовых расходов на создание системы защиты ОИ СВТ путем определения для конкретного типа пользователей минимального набора мер защиты необходимых и достаточных для недопущения нерегламентируемой деятельности; определение потенциального ущерба, который конкретный пользователь может нанести информационным ресурсам и инфраструктуре.

В ходе экспериментальных исследований был разработаны модематическая модель и программное обеспечение, позволяющее выявить потенциального инсайдера.

Предложенный подход может использоваться органами внутренних дел и следственным комитетом для установления мотивации и целей лиц, совершивших преступления с использованием средств вычислительной техники. А также отделом безопасности компании для преотвращения возможных утечек информации.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1–А. Д.Ю. Недосеко Методика противодействия атакам на объектах информатизации средств вычислительной техники/ 51-я научная конференция студентов, магистрантов, аспирантов. Минск: БГУИР, 2015.

2–А. Д.Ю. Недосеко Адаптивный подход к системе защиты информации / Тезисы докладов XIII Белорусско-российской научно-технической конференции «Технические средства защиты информации». Минск: БГУИР, 2015.