Каждая страна по уровню своего ТЭР в текущий год отображается конкретной ячейкой на карте. Ячейки с одинаковыми координатами содержат страны с подобным состоянием ТЭР. Чем дальше на карте координаты стран, тем больше отличается друг от друга их технико-экономический портрет.

Заключение

Современный этап научно-технического прогресса характеризуется зарождением нового технологического уклада, под которым, согласно С. Глазьеву понимается некоторая совокупность сопряженных производств, находящихся примерно на одном и том же уровне технического развития. Опыт макроэкономических исследований говорит не только о возможности, но и о плодотворности использования межстрановых сопоставлений для получения и качественных, и довольно точных количественных выводов, в том числе прогнозного характера.

Системное использование математико-статистических методов, приемов и показателей в комплексе с интеллектуальными подходами обеспечивает на практике всесторонний анализ экономических явлений и процессов, происходящих в современной экономике. Научно-обоснованный анализ является базовым фундаментом разработки сценариев развития экономики и стратегии государственного регулирования стихийно-рыночных процессов.

Исследование выполнено при финансовой поддержке РФФИ (грант № 16-29-12858).

Литература.

1. Количественные методы в экономических исследованиях / Под ред. М.В. Грачевой и др. – М.: ЮНИТИ-ДАНА, 2004. – 791 с.
2. Глазьев С.К. Теория долгосрочного технико-экономического развития. М., 1993. – 157 с.
3. Кондратьев Н.Д. Большие циклы конъюнктуры и теория предвидения. – М.: «Экономика», 2002, с.245-267
4. Горбачев С.В., Горбачева Н.Н. Нейросетевое измерение уровня и темпов глобального технико-экономического развития. Материалы VII Научно-практической конференции «Информационно-измерительная техника и технологии» с международным участием, г.Томск, 25-28 мая 2016 г., с. 47-63

ЗАЩИТА ИНФОРМАЦИИ В БАНКОВСКИХ СИСТЕМАХ

И.В. Грасмик, студент группы 17В41,
Юргинский технологический институт (филиал) Национального исследовательского Томского политехнического университета
652055, Кемеровская обл., г. Юрга, ул. Ленинградская, 26

Банковская деятельность всегда имела тесную связь с обработкой и хранением огромного количества конфиденциальных данных. В первую очередь это личные данные каждого клиента, их вклады и все осуществляемые операции.

Абсолютно вся коммерческая информация, которая хранится и обрабатывается в кредитных организациях, подвергается различным рискам, связанными с вирусами, поломкой аппаратного обеспечения, сбоями операционных систем и т.п. Но большинство из этих проблем не способны нанести кокой-либо серьезный ущерб. Ежедневное резервное копирование данных, без которого невозможна работа любой информационной системы предприятия, благодаря этому риск безвозвратной утери информации сводится к минимуму. Помимо того, существуют давно уже известные способы защиты от вышеперечисленных угроз. Поэтому на передний план выходят риски, которые связанны с несанкционированным доступом к конфиденциальной информации.

В настоящее время выделяют следующие проблемы:

1. Проблема уничтожения банковской информации, которая может быть вызвана, какой-либо поломкой или сбоями ПО, так и, например, специальными вирусами, способными вызывать сбои операционной системы. Потери информации из-за этих факторов сводится к минимальному значению с помощью ежедневного резервного копирования данных, постоянного обновления ОС и специального защитного ПО.
2. Проблема искажения банковской информации, которая тесно связана с человеческим фактором, причем в большинстве случаев с собственными человеческими ресурсами банка. Иногда сами сотрудники банка могут сделать какую-нибудь ошибку при копировании или транспортировки данных, притом, ошибка бывает, как намеренной, так и автоматической. Решается эта проблема с помощью тщательного отбора персонала, которые получают доступ к важной информации, авто-

матизации процессов внесения данных, шифрованию данных, а также контроль за действиями рядовых работников со стороны менеджеров.

3. Проблема получения банковской информации третьими лицами — это самая главная угроза для банковской системы, приводящая к большим финансовым потерям. На сегодняшний день могут быть применены несколько основных способов несанкционированного доступа к банковской информации:
    a) Доступ к месту обработки и хранения данных. Может быть получен, такими путями как физический взлом банка, взлом электронного хранилища информации (очень редкий случай, если учитывать степень защиты таких источников) и кража данных с помощью электронных носителей информации самих работников банка.
    b) Создание и использование резервных копий. Доступ к копиям информационных блоков не такой строгий, чем доступ к самим носителям информации, которые в случае недоброго умысла или какой-либо ошибки могут оказаться в руках мошенников. В мировой практике было большое количество случаев кражи денежных средств именно благодаря помощи резервных копий информационных блоков.
    c) Несанкционированный доступ со стороны работников банка. Это самый вероятный и наиболее частый способ потери банковской информации.

Защита банковской информации от утечки и разглашения третьим лицам производится при помощи следующих инструментов:

1. Надежное специальное ПО.
2. Программы для защиты от атак вирусами и другими вредоносными программами - антивирусное ПО.
3. Строгий отбор и контроль за персоналом, который имеет доступ к банковской информации; различные уровни доступа.
4. Системы способные распознать пользователя.
5. Программы специального шифрования информации.
6. Применение межсетевых экранов.
7. Защита от физического грабежа.

С помощью программных средств можно реализовать следующие способы защиты:

1. Криптографическое преобразование или просто шифрование информации. наиболее распространенными методами считаются DES и RSA. DES — DATA ENCRIPTION STANDART — этот стандарт шифрования данных разработанный фирмой IBM для собственных нужд, но позднее ставший основным стандартом США. Алгоритм DES очень часто используется во всем мире так как является открытым. Он довольно-таки простой для понимания и использует метод защиты, основанный на ключе и при этом не зависит от степени «секретности» алгоритма. RSA — считается самым перспективным методом на данный момент, т.к. он не требует передачи ключа для шифрования другим пользователем. Криптографическое преобразование данных осуществляется с помощью первого открытого ключа, а восстановление данных происходит вторым уже секретным ключом. Основным применением RSA на данный момент является защита электронного документооборота. В качестве примера можно привести протокол SSL (Secure Sockets Layer), который гарантирует безопасную передачу информации по сети. SSL комбинирует криптографическое шифрование с открытым ключом и блочным шифрованием данных. Единственный недостаток алгоритма RSA это то, что он не полностью изучен и нельзя давать100% гарантию его надежности.
2. Аутентификация пользователей или проверка на правильность введенных пользователем регистрационных данных при входе в систему. В основном используется для принудительного применения избирательных прав доступа к информационным ресурсам и получении прав на выполнение каких-либо операций в системе.
3. Разграничение прав и привилегий пользователей на доступ к банковским информационным ресурсам.
4. Контроль целостности данных, антивирусная защита, аудит или. просмотр деятельности пользователей и ПО, работающих в системе путем регистрирования определенных событий в системном журнале безопасности, а также выполнение определенных ответных действий или запрещение выполнения.
5. Наблюдение за работоспособностью комплексов защиты данных, как программных, так и аппаратных или реализация средств контроля и управления механизмами защиты системы, обеспечивающей безопасность.
6. Резервное копирование информации и в последствии ее восстановление.

7. Брандмауэр (firewall) - система или комбинация систем, которая создает защищающий барьер между двумя или большим количеством сетей и предотвращающий вторжение в частную сеть. Firewall'ы используются как виртуальные барьеры для передачи пакетов данных из одной сети в другую.

Самым большим недостатком систем защиты, сконструированных на основе только программных комплексов, считается возможность их анализа при несанкционированном доступе. Исходя из этого нельзя исключить возможность разработки способов, которые могут преодолеть комплексы программных средств обеспечения безопасности или его модификации.

Несмотря на возросший уровень информационных технологий, которые позволяют не санкционированно получать доступ к банковской информации, современный рынок может предложить наиболее эффективные и надежные способы защиты банковских данных, совершенствующиеся с большой скоростью не уступающей инструментам взлома. Обеспечение информационной безопасности — это одна из самых актуальных проблем, касающаяся каждого банка, в которое вкладывается огромное количество ресурсов.

Литература.

1. Абрамцева Т.М. «Информатика для экономистов»: Понятийно-терминологический словарь. - М.: Мысль, 2008. - 421С.
2. Бухарин П.Р. «Информационные технологии в экономике и управлении». - М.: Центр, 2007. - 450С.
3. Чистов Г.В. «Информационные технологии в экономике». - М.: Флора, 2003. - 570С.

АНАЛИЗ СТАТИСТИЧЕСКИХ ДАННЫХ ИННОВАЦИОННОЙ ДЕЯТЕЛЬНОСТИ В ОБЛАСТИ АВТОМОБИЛЕСТРОЕНИЯ РОССИИ

К.О. Ефимова, студ.
Научный руководитель: Темпель Ю.А.
Тюменский индустриальный университет
625000, г. Тюмень, ул. Володарского, 38
E-mail: efimova-k@mail.ru

Машиностроительный комплекс Российской Федерации является главной отраслью промышленного производства. Поскольку машиностроение не только охватывает различные отрасли промышленности (см. рис. 1 [1]), но и влияет на развитие других сфер хозяйственной деятельности, а продукция машиностроения играет главную роль в процессе реализации инновационных достижений современного научно-технического прогресса страны.

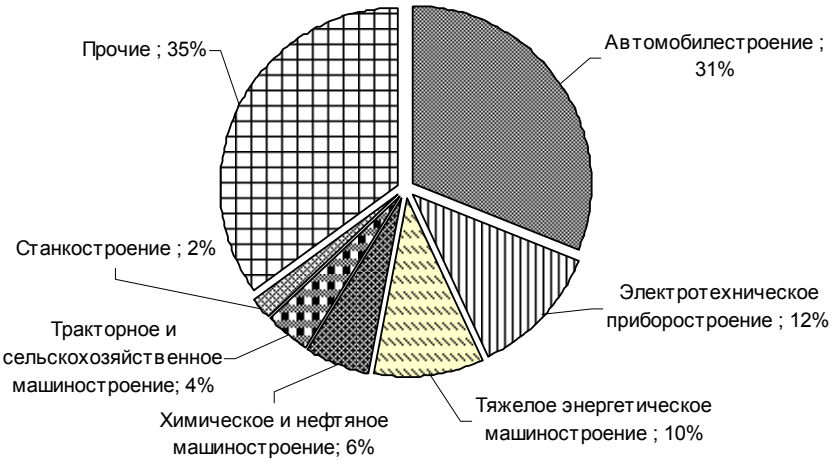

Рис. 1. Структура продукции машиностроительного комплекса России

Согласно диаграмме, представленной на рисунке 1, главенствующее положение среди отраслей промышленности занимает автомобилестроение (31%). Данная группа в настоящий момент составляет порядка 1% ВВП и обеспечивает около 400 тыс. рабочих мест на предприятиях.

Кроме того, наибольший вклад в прирост производства машиностроительного сектора внесло транспортное машиностроение (58,8% от общего объема прироста), и, прежде всего, автомобиле-