Министерство образования и науки Российской Федерации

Государственное образовательное учреждение
высшего профессионального образования
«Алтайский государственный технический университет
им. И.И.Ползунова»

НАУКА И МОЛОДЕЖЬ – 2007

IV Всероссийская научно-техническая конференция студентов, аспирантов и молодых ученых

СЕКЦИЯ

ИНФОРМАЦИОННЫЕ И ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

подсекция

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И ЗАЩИТА ИНФОРМАЦИИ

Барнаул – 2007

ББК 784.584(2 Рос 537)638.1

IV Всероссийская научно-техническая конференция студентов, аспирантов и молодых ученых "Наука и молодежь – 2007". Секция «Информационные и образовательные технологии». Подсекция «Безопасность информационных технологий и защита информации». / Алт. гос. техн. ун-т им. И.И.Ползунова. – Барнаул: изд-во АлтГТУ, 2007. – 22 с.

В сборнике представлены работы научно-технической конференции студентов, аспирантов и молодых ученых, проходившей в апреле 2007 г.

Организационный комитет конференции:
Максименко А.А., проректор по НИР – председатель, Марков А.М., зам. проректора по НИР – зам. председателя, Арзамарсова А.А. инженер Центра НИРС и молодых учёных – секретарь оргкомитета, Кантор С.А., заведующий кафедрой «Прикладная математика» АлтГТУ – руководитель секции.

Научный руководитель подсекции: зав. каф. ЗИРС, проф., д.т.н., Белов В.М.
Секретарь подсекции: доцент, к.в.н., Загинайлов Ю.Н.

СОДЕРЖАНИЕ

ПОСТРОЕНИЕ МОДЕЛИ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ РЕГИОНАЛЬНЫХ НАЛОГОВЫХ ОРГАНОВ С ИСПОЛЬЗОВАНИЕМ АППАРАТА НЕЧЕТКИХ МНОЖЕСТВ

Белов В.М. – к.ф.-м.н., д.т.н., профессор, Пивкин Е.Н. – аспирант
Алтайский государственный технический университет (г. Барнаул)

История развития региональных налоговых органов является результатом сложного многоуровневого процесса взаимодействия нормативно-правовой сферы, налоговой базы и непосредственно самой налоговой службы в единстве ее организационной структуры, кадрового состава, форм, принципов и методов работы и их конкретных результатов. Наиболее важной в деле повышения эффективности работы региональных налоговых органов является борьба с коррупцией в рядах налоговиков, прогнозирование угроз, внедрение схем, средств и систем защиты информации и проведение аудита информационной безопасности.

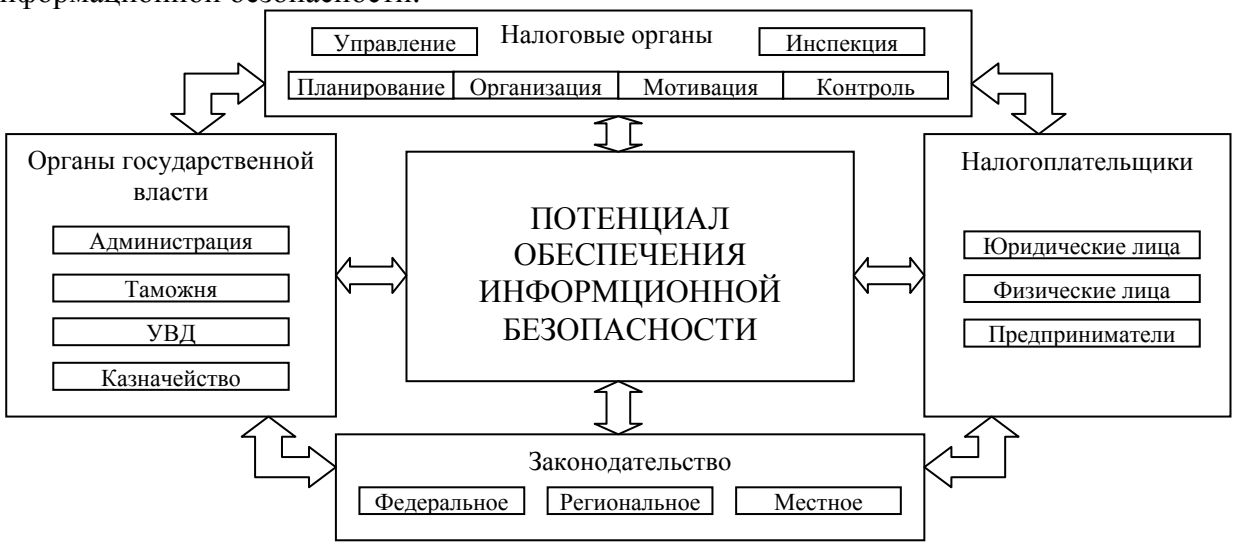

Рисунок 1 – Схема информационных связей в регионе

Информационные связи и потоки, представленные на рисунке 1 показывают взаимодействие региональных налоговых органов с различными государственными и негосударственными организациями. Зачастую для обмена информацией между органами применяют разнообразный состав средств и систем защиты информации. Данные средства устанавливают и оговаривают на региональном, местном уровне, а не доводят и не регулируют на федеральном. В связи с чем возникают сложности выполнения: требований нормативно-правовых документов, сопряжения различных подходов к построению и использованию телекоммуникационных средств и систем, обеспечения информационной безопасности, конфиденциальности и защиты информации.

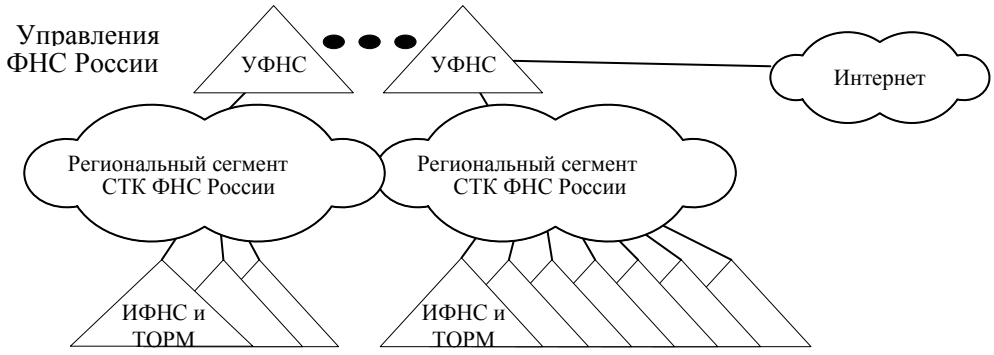

Рисунок 2 – Структура региональных налоговых органов

На рисунке 2 приведена общая структура региональных налоговых органов. Трудность исследования вопросов обеспечения информационной безопасности в региональных налоговых органах усугубляет большая неопределенность условий функционирования информационных систем в различных регионах. Можно, выделить как минимум три звена построения телекоммуникационных узлов (далее – ТКУ) системы телекоммуникаций ФНС России на региональном уровне: ТКУ 1 типа – Управления ФНС России по субъектам РФ и Межрегиональные инспекции, ТКУ 2 типа – инспекции ФНС России, ТКУ 3 типа – территориально обособленные рабочие места (далее – ТОРМ). Зачастую угрозы, присущие налоговым органам одного региона, являются несущественными и маловероятными для другого. Следовательно, довольно затруднительно определить оптимальную структуру комплексной системы защиты информации (далее – КСЗИ), реализация которой будет актуальной, универсальной для всех регионов с возможностью быстрой реорганизации для отражения или минимизации потерь от воздействия возможных угроз.

Для минимизации потерь или снижения риска проявления возможных угроз применяют: точечные продукты, комплексные интегрированные средства и системы защиты информации. В будущем предпочтение будут отдавать адаптивным, самоуправляющимся и самовосстанавливающимся безопасным сетям [1].

Для перехода к таким средствам и системам необходимо иметь полную математическую модель КСЗИ. Получение и использование информации необходимо осуществлять непосредственно в процессе функционирования системы путем постепенного накопления необходимых данных, анализа и использования её для эффективного выполнения системой заданной целевой функции в изменяющихся условиях внутренней и внешней среды.

Указанные факторы считают существенными препятствиями для построения точных моделей, основой которых служат классические математические теории и методы. Известные математические модели, используемые для описания структуры, поведения и управления КСЗИ в условиях некорректной постановки задач не дают желаемого результата. Поэтому необходимо применять иные, ориентированные на специфику процессов защиты информации, методы и средства моделирования [2].

Проблема выбора альтернатив (принятия решений) – одна из наиболее распространенных классов задач с практическим приложением, в которой решения принимают в таких условиях, когда поставленные цели, имеющие ограничения и следствия, порождаются возможными, точно не известными действиями. Применение методов теории вероятности, принятия решений, управления не применимы к неточно известным величинам, поскольку понятие неточности отождествляют со случайностью. Расхождения между случайностью и расплывчатостью состоит в том, что случайность связана с неопределенностью относительно принадлежности или непринадлежности определенного объекта к классическому методу, тогда как в системах защиты информации, используемых для решения указанных задач, большую роль играют не полностью определенные (размытые) факторы.

Задача построения КСЗИ не поддается строгой формализации, поэтому её необходимо решать с использованием субъективных и расплывчатых представлений нечеткой логики, которая устраняет разногласия между строгостью математики и неопределенностью реального мира.

Для реализации поставленных задач требуется применять логико-лингвистический подход в задачах оценки состояния безопасности. Определение уровня безопасности информации в компьютерных системах является тяжелоструктурированным и формулируемым. Решение данной задачи связано с высокой трудоемкостью процедур анализа и зависимостью конечного результата от субъективных факторов. Во время решения данной задачи возникает потребность в анализе и обработке исходных данных, представленных в качественной форме. При этом возникает необходимость поиска зависимостей, которые связывают нечетко заданные входные и выходные данные.

Методологический базис, состоящий из совокупности методов и моделей, необходимых и достаточных для исследования проблемы защиты информации, является важнейшим компонентом теории защиты [3].

Методология синтеза систем оценки уровня безопасности информационных ресурсов содержит следующие этапы:

– определение характеристик безопасности информации;

– анализ угроз, служащих входной информацией для формирования экспертных запросов;

– определение базового экспертного запроса;

– ранжирования исходных данных, позволяющих обнаружить наиболее опасные угрозы для того, чтобы потом расставить необходимые акценты во время оценивания;

– формирование лингвистических термов;

– выбор метода обработки нечетких чисел;

– выбор нечеткой модели;

– вычисление и интерпретацию уровня безопасности информации.

На основании предложенной методологии синтеза можно строить как программные, так и программно-аппаратные системы реального времени, предназначенные для эффективной оценки уровня безопасности информации в компьютерных системах региональных налоговых органов.

Недостаточное методологическое обоснование, а также слабая практическая проработка положений по моделированию систем и процессов обеспечения защиты информации, что особенно остро прослеживают в региональных налоговых органах, а также выбор оптимальных средств защиты предопределили цель, структуру и содержание настоящей работы. Целью исследования является построение математической модели КСЗИ, методологических положений и методических подходов, позволяющих оптимизировать процессы моделирования и эксплуатации средств защиты информации на примере региональных налоговых органов.

В соответствие с поставленной целью в работе сформулированы и решены следующие основные задачи:

– проведен анализ современного состояния систем информационной безопасности компьютерных систем, их особенностей и перспектив развития;

– рассмотрены объекты и элементы защиты современных автоматизированных систем (АС);

– исследованы подходы к проектированию систем защиты информации, методы организации и управления;

– рассмотрено математическое обеспечение и подробно проанализированы математические методы в проектировании систем защиты информации;

– дана оценка угроз безопасности информации;

– определены основные направления организации работы по защите информации.

Литература

1. Г.А. Бузов, С.В. Калинин, А.В. Кондратьев. Защита от утечки информации по техническим каналам. – М.: Горячая линия – Телеком, 2005. – 416 с., ил.
2. В.В. Домарев. Безопасность информационных технологий. Методология создания систем защиты. – К.: ООО «ТИД ДС», 2001. – 688 с.
3. А.Г. Корченко. Построение систем защиты информации на нечетких множествах. Теория и практические решения. – К.: «МК-Пресс», 2006. – 320 с., ил.

РАЗРАБОТКА РУКОВОДСТВА ПО ЗАЩИТЕ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА ОТ ТЕХНИЧЕСКИХ РАЗВЕДОК И ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ В АЛТГТУ

Викулов Ю.А. – студент, Трухачев А.В. – студент
Загинайлов Ю.Н. – к.в.н., доцент
Алтайский государственный технический университет (г. Барнаул)

Одной из актуальных задач обеспечения безопасности вуза, является защита информации ограниченного доступа. Системный подход к решению этой задачи дает возможность укрепления экономической безопасности университета, что способствует созданию условий для долгосрочного, устойчивого функционирования университета.

Система защиты информации ограниченного доступа в современных условиях должна обеспечивать защиту сведений, которые циркулирует в вузе и содержат государственную тайну, коммерческую информацию, служебную информацию органов управления и подразделений, персональные данные преподавателей, сотрудников, студентов и абитуриентов [1,2,3].

Прежде чем строить комплексную систему защиты информации нужно определить, какие задачи она будет решать, чем будут регламентированы ее функции на различных этапах обработки информации ограниченного доступа при применении для этого автоматизированных систем и средств телекоммуникаций.

Решением этих вопросов на первом и последующих этапах проектирования такой системы является разработка нормативных документов. Одним из основных нормативных документов является Руководство по защите информации ограниченного доступа от технических разведок и от утечки по техническим каналам в АлтГТУ. Для разработки других нормативных документов (Руководство по защите информации ограниченного доступа, циркулирующей в АС, должностные инструкции ответственных лиц по защите информации ограниченного доступа, перечни сведений ограниченного доступа и т.д.) данное Руководство будет являться руководящим документом [4].

Разработка нормативных документов до настоящего времени носит теоретический характер, а их состав и структура, определенные ещё в конце 90-х годов прошлого века, не учитывают новые реалии, возникшие в связи с изменением Законодательства РФ в последние годы, стандартизацию систем управления качеством образовательных учреждений и развитием средств телекоммуникаций и информационных систем.

Целью дипломной работы является: изучение структуры вуза, функций научных и учебных подразделений, работающих с информацией ограниченного доступа, определение требований к правовому, организационному и техническому обеспечению защиты данной информации, определение критериев формирования состава и структуры Руководства по защите информации ограниченного доступа от технических разведок и от утечки по техническим каналам в АлтГТУ.

В соответствии с поставленной целью решению подлежат следующие задачи:

- изучение существующей нормативно-правовой базы;
- определение состава и структуры Руководства;
- определение перечня руководящих документов;
- разработка конкретных разделов Руководства.

Для анализа был использован Алтайский государственный технический университет, так как он имеет разветвленную структуру, в которой присутствуют все виды возможных подразделений. Руководство по защите информации разрабатывается подразделением по защите информации от технических разведок и от ее утечки по техническим каналам совместно с основными подразделениями объекта.

При отсутствии подразделения или отдельных специалистов по защите информации разработку Руководства организует Руководитель объекта по договору с предприятиями, организациями, имеющими лицензию, на данный вид деятельности.

Руководство подписывается должностным лицом, ответственным за защиту информации на объекте и утверждается Руководителем объекта по согласованию с представителем заказчика, головным подразделением отрасли по защите информации (для предприятий, входящих в состав ведомств) и соответствующим территориальным органом государственной безопасности.

Согласованное Руководство утверждается Руководителем органа государственной власти или предприятия (учреждения, организации).

Изменения в Руководство вносятся, согласовываются и утверждаются в том же порядке и на том же уровне, что и основной документ.

К ознакомлению с Руководством в полном объеме допускается строго ограниченный круг лиц по решению Руководителя объекта. Исполнители мероприятий по защите информации на объекте должны быть ознакомлены с Руководством в части, их касающейся.

В Руководстве предусмотрены подразделы, в которых определены:

- цель защиты информации, которая должна быть поставлена при построении комплексной системе защиты;
- замысел достижения цели защиты информации, в чем он заключается и какими способами он должен достигаться;
- пути реализации замысла, проведением каких основных мероприятий по защите информации воплощается реализация замысла;
- состав охраняемых сведений, какие сведения входят в состав защищаемых информационных ресурсов АлтГТУ;
- перечень сведений, которые не могут быть включены в информационные ресурсы, подлежащие защите, обусловленные законами;
- перечень подразделений (отделов) АлтГТУ, в которых циркулирует информация ограниченного доступа, для каждого вида защищаемой информации.

Данные подразделы определяют цель создания комплексной системы защиты информации способы её достижения. Также эти пункты определяют объекты, подлежащие защите, степень необходимой защищенности.

Разработанное Руководство прошло экспертизу и согласование и принято в качестве нормативно-методического документа в АлтГТУ.

Литература

1. Концепция защиты информации от иностранной технической разведки (ИТР);
2. Федеральный закон РФ от 21 июля 1993 г. N 5485-1 «О государственной тайне»;
3. Федеральный закон РФ от 29.07.2004 №98-ФЗ «О коммерческой тайне»;
4. Гостехкомиссия России Решение № 42 от 03.10.1995 «О типовых требованиях к содержанию и порядку разработки руководства по защите информации от технических разведок и от ее утечки по техническим каналам на объекте»;

СПОСОБЫ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ РАЗЛИЧНЫХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

Ступкина А.А. – аспирант, Загинайлов Ю.Н. – к.в.н., доцент
Алтайский государственный технический университет (г. Барнаул)

Любая угроза безопасности информации реализуется применением определённого способа воздействия, предусматривающего использование соответствующего этому способу средства. В случае с конфиденциальной информацией (информацией ограниченного доступа) необходимо создание специального канала для передачи этой информации. Путь от источника конфиденциальной информации к её незаконному получателю (злоумышленнику) называют каналом утечки информации. Каналы утечки информации существуют всегда, когда отсутствуют меры и средства защиты этих каналов на объекте информатизации.

Исходя из существующих норм защиты информации, определённых в нормативных документах Правительства РФ, Федеральной службы по техническому и экспортному контролю РФ, теории и практики защиты информации, компьютерных систем, можно выделить следующие группы каналов утечки информации и НСД:

- организационные каналы утечки информации [1];
- технические каналы утечки информации [2];
- инфокоммуникационные каналы утечки информации;
- системно - программные каналы утечки информации;
- комбинированные каналы утечки информации [1].

Способы несанкционированного доступа к конфиденциальной информации при использовании каждого канала имеют свои особенности, основанные на определённых принципах работы используемых для этого средств доступа.

Способы НСД с использованием организационного канала. Для этого канала наиболее характерным является несанкционированный физический доступ на объект информатизации и к защищаемой информации. Несанкционированный физический доступ может быть реализован одним из следующих способов:

- преодоление рубежей территориальной защиты обманным путём и доступ к незащищенным информационным ресурсам;
- хищение документов и носителей информации;
- визуальный перехват информации, выводимой на экраны мониторов и принтеры, а также подслушивание.

Способы НСД с использованием технических каналов утечки. Технические каналы утечки информации образуются в результате высокочастотного излучения при организации радиоканала на объекте информатизации (функциональный канал), побочных и паразитных электромагнитных излучений, наводок на цепи электропитания, заземления, линии связи и другие токопроводящие элементы, акустоэлектрических преобразований и акустических волн. Технические каналы по диапазону частот и по физической природе носителя подразделяют на [2]:

- радиоэлектронные (электромагнитный и электрический);
- оптические (визуально - оптический, фотографический, оптико - электронный);
- акустические (акустический, гидроакустический);
- материально – вещественный канал.

Способы доступа с использованием технических каналов утечки информации зависят от применяемых средств разведки. Доступ с использованием технических средств разведки является противоправным, он осуществляется разведывательными органами конкурентов или разведками иностранных государств.

Несанкционированный доступ возможен по специально организованным техническим каналам утечки информации. При этом основными способами являются [3]:

- подключение к техническим средствам и системам объекта информатизации;
- использование закладочных устройств;
- использование дистанционных средств разведки.

В свою очередь способы доступа с использованием закладочных устройств могут выполняться в зависимости от средств:

- с использованием средств радиоэлектронной разведки;
- с использованием средств оптико – электронной разведки;
- с использованием средств фотографической разведки;
- с использованием средств визуально-оптической разведки;
- с использованием средств акустической разведки;
- с использованием средств гидроакустической разведки.

Способы НСД с использованием инфокоммуникационного канала. НСД с использованием инфокоммуникационного канала предусматривает подключение типовых аппаратных или программных средств или специальных технических к каналам коммутируемых линий связи, каналам выделенных линий связи, каналу локальной вычислительной сети, которые используются для организации инфокоммуникационных сетей, каналу машинных носителей информации, каналу терминальных и периферийных устройств и получение «трафика» с конфиденциальной информацией в обход средств защиты. Это может быть подключённый к линии связи ПК, другие средства съёма информации в т.ч. и специальные средства компьютерной разведки вычислительных сетей - снифферы, сканеры и др. Данный способ предусматривает перехват передаваемых по сети сообщений («пакетов») и может быть выполнен:

- непосредственным подключением к линии связи;
- доступом к компьютеру сети, принимающему сообщения или выполняющему функции маршрутизации;
- внедрением в сеть несанкционированного маршрутизатора с перенаправлением через него потока сообщений на компьютер злоумышленника.

Выделение из перехватываемых пакетов сообщений необходимой информации выполняется с помощью специализированных программ-анализаторов. Подобные программы могут использоваться и для модификации перехваченных пакетов.

Для переадресации пакетов сообщений выполняется модификация адресной информации в их заголовках.

В последние годы для передачи «пакетов» по сети используются защищённые протоколы, например IPsec. В этом случае перехваченные или перенаправленные пакеты «вскрываются» с использованием криптоанализа.

Способы НСД с использованием системно – программного канала. Основными способами НСД с использованием программного обеспечения являются:

- «маскировка под зарегистрированного пользователя»;
- использование дефектов программного обеспечения ОИ («люков» и др.)
- использование программных закладок;
- применение программных вирусов.

Маскировка под зарегистрированного пользователя. Маскировка под зарегистрированного пользователя осуществляется путем похищения паролей и других реквизитов разграничения доступа к информации, используемой в системах обработки (АС). В этом случае пользователь присваивает себе каким - либо образом полномочия другого пользователя выдавая себя за него.

Данный способ в теории компьютерной безопасности получил название «маскарад».

Ключи и пароли могут быть получены следующими способами [4]:

- перехват ключей и паролей;
- подбор ключей и паролей;
- прогнозирование генерируемых ключей и паролей;

- подмена ключей и паролей.

Кроме этого маскировка под зарегистрированного пользователя может быть осуществлена:

- путём изменения параметров настройки систем защиты;
- назначением дополнительных полномочий.

В качестве дефектов или недостатков ПО, которые могут быть использованы для несанкционированного доступа к конфиденциальной информации рассматриваются:

- наличие средств отладки и тестирования в конечных продуктах;
- «чёрные ходы», « люки», скрытые возможности проникновения в компьютерную сеть.

Использование программных закладок. Внедрение закладки в компьютерную систему может выполняться:

- с помощью аппаратных средств;
- через электронные документы;
- с помощью обычных программ;
- с помощью мобильных программ;
- по вирусной технологии.

При внедрении закладки по вирусной технологии закладка обязательно должна обладать свойством саморазмножения, присущим обычному вирусу.

Литература

1. Герасименко В.А., Малюк А.А. Основы защиты информации. М.: 000 "Инком-бук", 1997.
2. Торокин А.А. Основы инженерно-технической защиты информации. М.: Ось-89, 1998.
3. ГОСТ Р 51275-99. Объект информатизации. Факторы воздействующие на информацию.
4. Анин Б.Ю. Защита компьютерной информации. - СПб.:БХВ-Санкт Петербург, 2000 - 384с.:ил.

ОСОБЕННОСТИ ЗАЩИТЫ ИНФОРМАТИЗАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Петров М.А., Александров Н.Н. – студенты, Шарлаев Е.В. – к.т.н., доцент
Алтайский государственный технический университет (г. Барнаул)

В настоящее время все больше компьютеров объединяются в сети для самых различных целей. Если во время расцвета информационных технологий компьютерные сети использовались только Министерствами обороны и университетами для обмена информацией, носящей скорее научный характер, то на сегодняшний день сети используются в самых различных сферах человеческой деятельности. Начиная с простого обмена музыкой и фильмами в самой малой сети, состоящей всего лишь из двух компьютеров, и заканчивая видеоконференциями и работой огромных корпораций, в самой большой в мире сети – Интернет, человек должен оставаться уверенным, что его информация будет доступна только определенному кругу лиц. Основная проблема защиты информации от несанкционированного доступа заключается в недостаточной компетенции руководителя организации или лиц, ответственных за ее безопасность, в вопросе предотвращения и противодействия угрозам, направленных на незаконное получение сведений конфиденциального характера. Эти сведения могут содержать как персональные данные какого-то отдельного человека, так и нести в себе информацию, составляющую коммерческую или другие виды тайн, в том числе и государственную. Пренебрежение элементарными средствами сетевой защиты, такими как межсетевые экраны или антивирусы могут привести компанию к банкротству, причем сама компания может и не узнать причину того, что с ней случилось. Мероприятия по защите от несанкционированного доступа должны быть четко сформулированы и обоснованы. Вероятность проникновения в систему уменьшается, если эти мероприятия представляют собой комплекс по защите информационных ресурсов, когда этим занимаются высококвалифицированные специалисты, способные реально представить масштабы угроз, оценить возможные потери и принять необходимые меры для их предотвращения.

Сегодня невозможно организовать работу предприятия без доступа в сеть Интернет. Но чем больше клиентов локальной сети имеют такой доступ, тем больше вероятность попадания в нее вирусов, вредоносных программ, бесполезной информации. Таким образом, задача в защите собственной локальной сети как от атак извне, так и от вредоносных программ и даже утечки информации остается быть актуальной и имеет тенденцию к росту интереса к ней.

Типичный пример организации доступа в сеть Интернет таков: один персональный компьютер выступает в роли псевдо-сервера, который предоставляет неограниченный доступ в глобальную сеть всем или нескольким компьютерам локальной сети.

Данный вариант обладает несколькими недостатками:

1. Все или большинство компьютеров локальной сети имеют неограниченный доступ в Интернет
2. Администратор сети не имеет возможности контролировать распределение ресурсов по локальной сети
3. Каждый компьютер открыт для несанкционированного доступа извне
4. Высока вероятность утечки конфиденциальной информации

Методы решения поставленной проблемы:

Первой задачей является составление концептуальной модели построения локальной сети. Если требуется обеспечить доступ в сеть Интернет всем входящим в нее компьютерам, то это один вариант. Если доступ в глобальную сеть должны иметь только несколько компьютеров, то это второй вариант.

Оба варианта имеют однотипную схему построения локальной сети, а именно – все компьютеры находятся в одноранговой сети вместе с сервером, который имеет доступ в Интернет. (Рис. 1)

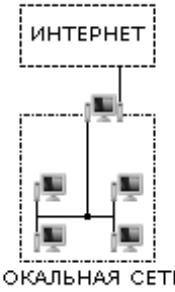

Рис. 1. Структура локальной сети

Оптимальный вариант конфигурации сервера следующий:

1. Сервер должен иметь как минимум два физических сетевых интерфейса, первый - в Интернет, второй - в локальную сеть. Оба эти интерфейса не должны контактировать друг с другом напрямую, как это обычно делается путём создания моста между ними.
2. На сервере должна быть установлена программа маршрутизации трафика между сетевыми интерфейсами. Она настраивается, исходя из нужд предприятия.
3. Также сервер должен иметь виртуальный сетевой интерфейс, с которого клиенты будут получать доступ в сеть Интернет.
4. Сервер должен иметь прозрачный кэширующий прокси - сервер, посредствам которого будет осуществляться непосредственный доступ на web - ресурсы. Данный прокси - сервер будет фильтровать весь поступающий трафик, а именно – проверять на вирусы, предотвращать доступ на нежелательные сайты, блокировать, по возможности, поступающую рекламу, распределять пропускную полосу на всех клиентов локальной сети, которые в данный момент находятся в сети Интернет, резервировать минимум 10% от общего канала на нужды сервера.

Принцип работы данной схемы (Рис. 2):

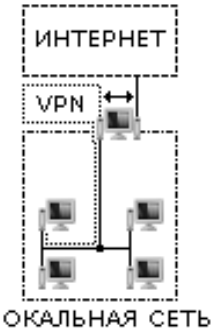

Рис. 2. Принцип организации доступа в Интернет

1. Клиентская машина инициирует соединение по шифрованному каналу передачи данных с созданным виртуальным сетевым интерфейсом сервера через физический сетевой интерфейс, который подключён в локальную сеть.
2. Программа маршрутизации, которая также выступает в роли брандмауэра, включает перенаправление сетевого потока с созданного клиентом виртуального интерфейса на прозрачный прокси-сервер.
3. Прокси-сервер активирует соединение с Интернетом и передаёт полученные данные программе маршрутизации, которая в свою очередь отдаёт полученные данные на созданный клиентом виртуальный интерфейс.

Преимущества оптимального варианта конфигурирования сервера при распределении доступа локальной сети в сеть Интернет:

1. Клиентский компьютер не имеет прямого доступа в сеть Интернет.
2. Клиент соединяется с сервером, имеющим доступ в Интернет, по шифрованному каналу передачи данных, что повышает безопасность данных, передаваемых между клиентом, сервером и сетью Интернет.
3. Сетевой поток, поступающий на виртуальный интерфейс от клиентов, транслируется на физический интерфейс сервера, подключённый в Интернет через брандмауэр и прокси-сервер.
4. Брандмауэр может быть отдельно сконфигурирован администратором сети на фильтрацию трафика по протоколам, портам или пунктам назначения для каждого клиента в отдельности или для общей сети в целом.
5. Прокси-сервер выступает в роли дополнительного фильтра трафика, который будет отсеивать ненужную информацию, будь то реклама или что-нибудь иное.

6. Прокси-сервер будет выступать также в роли распределителя пропускной способности сетевого интерфейса, подключенного в сеть Интернет.
7. Прокси-сервер может быть сконфигурирован на проверку поступающего трафика на вирусы, трояны или иные вредоносные программы.
8. Прокси-сервер может кэшировать весь поступающий трафик, тем самым снижая общее потребление ресурсов из сети Интернет.
9. Гибкость настроек позволяет администратору сети блокировать доступ в сеть Интернет к каким-либо ресурсам, будь то ICQ, FTP, почта для каждого клиента в отдельности или для всех в целом.
10. Создание ложного виртуального интерфейса для доступа в сеть Интернет предотвратит несанкционированный доступ извне к клиенту в локальной сети.
11. Правильно сконфигурированный брандмауэр для физического интерфейса, подключённого в сеть Интернет, не позволит злоумышленнику получить доступ к самому серверу.
12. Администратор, анализируя записи прокси-сервера об использовании Интернета, может выяснить, кто и в какое время использовал ресурсы сети Интернет и какие именно ресурсы были использованы.

В большинстве случаях на предприятии не требуется предоставление доступа в сеть Интернет всем компьютерам, поэтому рассмотрим более надёжный вариант организации локальной сети предприятия с доступом в глобальную сеть.

Так как несколько компьютеров не должны иметь никакого контакта с сервером, то целесообразно выделить эти компьютеры в отдельный периметр. (Рис.3)

При использовании варианта с двумя периметрами мы добиваемся поставленных целей, а именно:

1. Гарантированно запрещаем доступ в сеть Интернет компьютерам, которых находятся во внутреннем периметре.
2. Преимущества оптимального варианта также действительны.

Технически это реализуется созданием псевдо- сервера с двумя физическими сетевыми интерфейсами, каждый из которых подключён к разным периметрам.

Так как контакта между двумя этими интерфейсами нет, следовательно, второй периметр гарантированно не получит доступ в сеть Интернет.

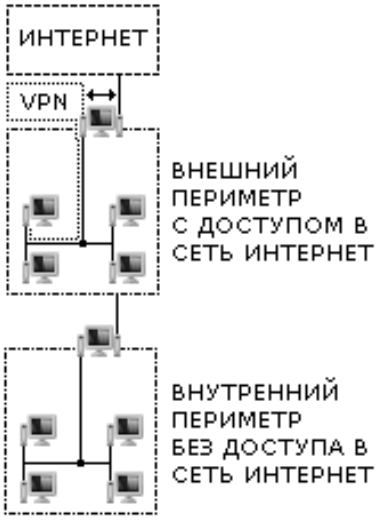

Рис. 3. Организации сети с двумя периметрами

Использование методов, изложенных выше при создании локальной сети с доступом в Интернет на предприятии, позволяет:

1. Защитить компьютеры в локальной сети от несанкционированного доступа извне.
2. Избежать попадания вирусов, троянов и иных вредоносных программ из сети Интернет.
3. Блокировать доступ к нежелательным сервисам в сети Интернет.
4. Следить за потреблением ресурсов каждым из клиентов.
5. Контролировать пропускную способность канала с доступом в сеть Интернет.
6. Частично или полностью запретить доступ некоторым клиентам локальной сети предприятия.

Литература

1. Блэк У. Интернет: протоколы безопасности. Учебный курс. – СПб.: Питер, 2001.
2. Колисниченко Д.Н. Linux-сервер своими руками. – СПб: Наука и Техника, 2002.

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Гридасов С.В. – студент, Загинайлов Ю.Н. – к.в.н., доцент
Алтайский государственный технический университет (г. Барнаул)

В связи с появлением федерального закона «О персональных данных» в 2006 году одной из актуальных проблем обеспечения безопасности, является проблема защиты персональных данных. Система защиты персональных данных дает возможность укрепления экономической безопасности организации, что способствует созданию условий для долгосрочного, устойчивого функционирования организации.

Мы оставляем соответствующие “информационные следы” в паспортном столе, в отделах кадров, в социальных службах, органах исполнительной власти, в общественных организациях, в сфере услуг и других сферах общественной жизни. Часто сообщение подобной информации находится в рамках наших интересов или является необходимым условием получения определенного социального статуса либо определенных услуг (например, хотим получить престижную работу, максимальную пенсию, оперативную медицинскую помощь и т.п.). В ряде случаев сообщение такой информации нежелательно (интимная жизнь) или не оправдано серьезными причинами (для получения гостиничных услуг и др.).

Распространение такой информации без согласия человека может способствовать формированию его положительного имиджа (например, информация о наградах или иных заслугах), а может нанести непоправимый урон, моральный вред, особенно если такая информация недостоверна. Поэтому информация персонального характера, относится к так называемой чувствительной информации и обращение с ней требует особой регламентации.

Устанавливается шесть принципов обработки персональных данных, защищающих персональную информацию человека.

1. Персональные данные должны собираться и использоваться законно и добросовестно. Эта норма говорит о том, что персональные данные должны быть собраны и использованы в соответствии с законодательством РФ и только с согласия субъекта персональных данных, но за исключением случаев, когда такое согласие не требуется. Согласие на обработку своих персональных данных субъект персональных данных должен дать в письменной форме. Письменное согласие должно содержать:

- фамилию, имя, отчество, адрес субъекта, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- наименование (фамилию, имя, отчество) и адрес оператора, получающего согласие субъекта;
- цель обработки персональных данных;
- перечень персональных данных, на обработку которых дается согласие субъекта;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
- срок, в течение которого действует согласие, а также порядок его отзыва.

2. Заранее четко определенные цели использования персональных данных не должны изменяться. Персональные данные не могут собираться и использоваться для иных целей, о которых субъект, давший письменное согласие на обработку своих данных, не был заранее информирован.

3. Объем, характер и способы обрабатываемых персональных данных должны соответствовать целям обработки персональных данных.

4. Персональные данные должны быть достоверными, а объем собираемой персональной информации должен быть оправдан целями ее сбора. Объем собираемых персональных данных не должен быть избыточным, если это не соответствует определенным и законным

целям. При этом, если обнаружено, что были допущены ошибки и персональные данные неточны, субъекту персональных данных принадлежит право внести необходимые изменения.

5. Закон запрещает объединение персональных данных в единую информационную систему персональных данных, которые были собраны операторами персональных данных для разных целей.

6. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

Оператор и третьи лица, получившие доступ к персональным данным, должны обеспечивать их конфиденциальность, за исключением случая обезличивания персональных данных, когда невозможно по ним идентифицировать конкретного человека и относительно общедоступных персональных данных, которые могут содержаться в адресных книгах, справочниках и иных общедоступных источниках персональных данных с согласия их субъекта.

За некоторыми исключениями, закон не допускает автоматизированную обработку так называемых специальных категорий персональных данных граждан, т.е. «чувствительной информации», к которой относится информация, касающаяся расовой, национальной принадлежности человека, его политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни. Что касается сведений о судимости, они также относятся к специальной категории персональных данных человека и могут обрабатываться государственными и муниципальными органами только в пределах полномочий, предоставленными им в соответствии с законодательством РФ.

Субъект персональных данных обладает следующими правами:

- право на доступ к своим персональным данным;
- право требовать от оператора уточнения своих персональных данных, а также их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;
- имеет право принимать предусмотренные Законом меры по защите вышеуказанных прав;
- а также запретительные права относительно использования персональных данных в целях продвижения товаров, работ, услуг на рынке, а также в целях политической агитации;
- права, защищающие от принятия решений на основании автоматизированной обработки персональных данных, порождающих юридические последствия в отношении субъекта персональных данных.

Чтобы получить доступ к своим персональным данным, субъект персональных данных или должен направить письменный запрос оператору, в котором должен быть указан номер основного документа, удостоверяющего личность гражданина. Оператор обязан в течение десяти рабочих дней со дня получения запроса, направленного субъектом персональных данных или его представителем, предоставить возможность ознакомления с персональными данными.

При обработке персональных данных оператор должен выполнять следующие действия.

1. Уведомить по форме, уполномоченный орган по защите прав субъектов персональных данных о намерении осуществлять обработку данных. Такое уведомление не требуется при обработке персональных данных собственных работников, общедоступных сведений, содержащих только фамилию, имя и отчество, а также в некоторых других случаях.

2. Убедиться, что персональные данные получены с соблюдением требований действующего законодательства и соответствуют заявленным целям обработки, т.е. либо данные получены из открытого источника, либо во исполнение федерального закона, либо с

соответствующим согласием субъекта. Если эти условия не соблюдаются, оператор до начала обработки таких данных обязан предоставить субъекту информацию о себе и предполагаемой обработке.

3. Предпринять предусмотренные Законом и подзаконными актами меры для защиты конфиденциальности полученных персональных данных.

4. Предоставлять соответствующую информацию по требованию субъекта или его законного представителя, а также уполномоченного органа по защите прав субъектов персональных данных.

На основе рассмотренных требований по защите информации определён состав и структура нормативных правовых актов организации для работы с персональными данными и режим их защиты.

Режим конфиденциальности персональных данных включает и считается установленным после принятия оператором (держателем) персональных данных следующих мер:

1) определение перечня персональных данных (в соответствии с письменным согласием субъектов персональных данных);

2) ограничение доступа к персональным данным путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;

3) учет лиц, получивших доступ к персональным данным, которым такая информация была предоставлена или передана;

4) регулирование отношений по использованию персональных данных лицами, получившими доступ к персональным данным;

5) получения (наличия) лицензии предусматривающей право на обработку персональных данных;

6) наличия сертифицированных информационной системы и средств защиты;

7) регистрации в уполномоченном органе по защите прав субъектов персональных данных.

Литература

1. Федеральный закон Российской Федерации от 27 июля 2006 г. №152-ФЗ О персональных данных.
2. Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ Об информации, информационных технологиях и о защите информации.
3. Европейская Конвенция от 28 января 1981 г. ETS № 108 об охране личности в отношении автоматизированной обработки персональных данных,
4. Директивы Европейского парламента и Совета Европейского Союза: от 24 октября 1995 г. 95/46/ЕС о защите прав частных лиц в отношении обработки персональных данных и о свободном движении таких данных;
5. От 15 декабря 1997г. 97/66/ЕС об обработке персональных данных и защите конфиденциальности в телекоммуникационном секторе.

ЗАЩИТА ОБРАЗОВАТЕЛЬНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ АлтГТУ ОТ СЛУЧАЙНЫХ УГРОЗ

Петров А.В. – студент, Загинайлов Ю.Н. – к.в.н, доцент
Алтайский государственный технический университет (г. Барнаул)

В настоящее время сформировалось устойчивое отношение к информации всех видов, как к ценнейшему ресурсу. Объясняется это небывалым ростом объема информационных потоков в современном обществе. В первую очередь это относится к тем направлением государственной деятельности, которые являются наиболее важными в жизнеобеспечении общества, а именно: экономика; наука; образование; социальная сфера; др. Все эти направления тесно пересекаются, и развитие каждого напрямую зависит от качества используемой информации, ее достоверности и полноты, оперативности и формы представления. Поэтому особое внимание должно уделяться проблемам формирования, использования и защиты информационных ресурсов на основе применения информационных и коммуникационных технологий.

В образовательной сфере все больше проектируются и внедряются информационные системы, призванные облегчить и усовершенствовать систему образования. В связи с этим все более актуальной становится проблема защиты информационно-вычислительных ресурсов. Вопрос ставится о защите не только информации, но и информационной системы в целом. Проблема обеспечения информационной безопасности на всех уровнях может быть решена успешно только в том случае, если создана и функционирует комплексная система защиты информации, охватывающая весь жизненный цикл компьютерных систем от разработки до утилизации и всю технологическую цепочку сбора, хранения, обработки и выдачи информации.

В состав современной системы защиты информации обязательно должна входить подсистема защиты информации от случайных угроз.

Информационная система АлтГТУ является организационно – технической системой, в которой реализуются информационные технологии, и предусматривается использование аппаратного, программного и других видов обеспечения, необходимого для реализации информационных процессов сбора, обработки, накопления, хранения, поиска и распространения информации. В данной системе годами накапливается электронная база информации, необходимая для обучения студентов, исчисляемая терабайтами данных и ценность этой информации велика, и в случае потери данных ущерб будет значителен. Из этого следует, что защита информационной системы АлтГТУ необходима.

Информационная система подвержена различным видам угроз.

Источниками угроз случайного характера могут выступать:

- Обусловленные действиями субъекта (антропогенные источники) - субъекты, случайные действия которых могут привести к нарушению безопасности информации;
- Обусловленные техническими средствами (техногенные источники) – эти источники угроз менее прогнозируемы и напрямую зависят от свойств техники и поэтому требуют особого внимания;
- Стихийные источники – данная группа объединяет обстоятельства, составляющие непреодолимую силу (стихийные бедствия, или др. обстоятельства, которые невозможно предусмотреть или предотвратить или возможно предусмотреть, но невозможно предотвратить)[1].

Уязвимости ИС:

1. Объективные – зависят от особенностей построения и технических характеристик оборудования, применяемого в ИС;
2. Субъективные – зависят от действий сотрудников:

Ошибки:

- При подготовке и использовании программно обеспечения (при разработке алгоритмов и программного обеспечения, инсталляции и загрузке программного обеспечения, эксплуатации программного обеспечения, вводе данных);
- При управлении сложными системами (при использовании возможностей самообучения систем, организация управления потоками обмена информации);
- При эксплуатации технических средств (при включении /выключении технических средств, использовании технических средств охраны, использование средств обмена информацией).

3. Случайные – зависят от особенностей окружающей ИС среды и непредвиденных обстоятельств:

Сбои и отказы:

- Отказы и неисправности технических средств (обрабатывающих информацию, обеспечивающих работоспособность средств обработки информации, обеспечивающих охрану и контроль доступа);
- Старение и размагничивание носителей информации (дискет и съемных носителей, жестких дисков, микросхем, кабелей и соединительных линий);
- Сбои программного обеспечения (операционных систем и СУБД, прикладных программ, сервисных программ, антивирусных программ);
- Сбои электроснабжения (оборудования, обрабатывающего информацию; обеспечивающего и вспомогательного оборудования);

Повреждения:

- Жизнеобеспечивающих коммуникаций (электро-, водо-, газо-, теплоснабжения, канализации; кондиционирования и вентиляции);
- Ограждающих конструкций (внешних ограждений территорий, стен и перекрытий зданий; корпусов технологического оборудования)[1].

Основные угрозы информационной системе АлтГТУ: уничтожение, блокирование, искажение информации.

Основным методом защиты от случайных угроз является резервное копирование[2]. Этот метод реализован в технологии RAID(Redundant Array of Independent Disks). Эта технология реализует концепцию создания блочного устройства хранения данных с возможностями параллельного выполнения запросов и восстановления информации при отказах отдельных блоков накопителей на жестких магнитных дисках. Устройства, реализующие эту технологию, называют подсистемами RAID или дисковыми массивами RAID.

В технологии RAID выделяется 6 основных уровней: с 0-го по 5-й. С учетом различных модификаций их может быть больше. Уровни RAID определяют порядок записи на независимые диски и порядок восстановления информации. Различные уровни RAID обеспечивают различное быстродействие подсистемы и различную эффективность восстановления информации[3].

Для защиты образовательной информационной системы АлтГТУ наиболее эффективно использовать RAID 6.

Литература

1. Классификация Угроз Информационной Безопасности, Вихорев С. В. http://www2.cnews.ru/comments/security/elvis_class.shtml.
2. Завгородний В. И. Комплексная защита информации в компьютерных системах. – М.: Издательство «Логос», 2001
3. http://timcompany.ru

РЕАЛИЗАЦИЯ ТРЕБОВАНИЙ МЕЖДУНАРОДНОГО СТАНДАРТА ПО УПРАВЛЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ISO/IEC 17799-2000 НА УРОВНЕ ДОКУМЕНТИРОВАННЫХ ПРОЦЕДУР

Решетицкая А.В. – студентка, Загинайлов Ю.Н. – к.в.н., доцент
Алтайский государственный технический университет (г. Барнаул)

В последние годы всё больше российских компаний выходят на мировой рынок предоставления услуг и реализации своей продукции. При этом обязательным условием этой деятельности является наличие сертификатов, как по качеству продукции, так и по качеству управления, в том числе управления информационной безопасностью. Международный стандарт ISO/IEC 17799-2000 по управлению информационной безопасностью включает десять практических правил, выполнение которых обеспечивает определённый уровень информационной безопасности. Существует набор определенных процедур для каждого правила, документирование которых необходимо для положительных результатов оценки на соответствие требованиям международного стандарта ISO/IEC 17799-2000.

1. Политика безопасности

В организации должна быть разработана, утверждена руководством, опубликована политика безопасности, с которой будут ознакомлены все сотрудники. Данный документ состоит из отдельных положений, определяющих требования к различным аспектам обеспечения информационной безопасности. Если требование выражено не конкретно и может трактоваться двояко, то допустимо вносить необходимые пояснения, либо делать ссылки на организационно-распорядительные документы, в которых объясняются и детализируются эти требования.

2. Организационные меры безопасности

В организации должна быть определена, согласована и документирована область ответственности каждого администратора информационной безопасности.

Уровни полномочий администраторов информационной безопасности также определены и документированы.

При доступе в автоматизированные системы сторонних организаций и пользователей (внешних или работающих по контракту) необходимо в рамках договорных обязательств рассмотреть и включить основные требования по информационной безопасности.

3. Учет и категорирование информационных ресурсов

В организации все ресурсы должны быть идентифицированы и документированы и каждому из них сопоставлен владелец.

Для категорированных ресурсов должны быть определены и зафиксированы процедуры маркировки информации в организационно-распорядительных документах организации.

4. Кадровые аспекты информационной безопасности

В соответствие с политикой безопасности организации в должностных инструкциях сотрудников отражены вопросы безопасности, все сотрудники ознакомлены под роспись со своими должностными инструкциями.

При приеме на работу все сотрудники подписывают обязательство о неразглашении конфиденциальных сведений. Данное соглашение подписывается до того, как сотрудник получает доступ к конфиденциальным ресурсам и пересматривается в случае изменения статуса сотрудника.

В организационно-распорядительных документах или в политике информационной безопасности организации должны быть зафиксированы процедуры информирования администраторов безопасности об обнаруженных сбоях, инцидентах, выявленных угрозах и уязвимостях. Данные процедуры должны быть доведены до сведения сотрудников.

В организации должна быть определена формальная процедура наложения дисциплинарных взысканий на сотрудников, которые нарушили принятые в организации политику информационной безопасности и соответствующие процедуры.

5. Физическая защита информационных ресурсов

В организации как одной из мер физического контроля должна проводиться регистрация даты и времени начала и окончания приема посетителей.

В организации должна быть справочная информация, определяющая расположение объектов защиты, содержащаяся в недоступном месте.

Доступ сотрудников сторонних организаций (обслуживающего персонала) строго регламентирован и находится под контролем.

В организации обязательно должна проводиться регистрация поступающего оборудования (материалов) перед установкой.

Обслуживание оборудования производится специальным персоналом в соответствии с рекомендациями поставщиков. В организации в процессе обслуживания ведется статистика всех сбоев и подозрительных ошибок в работе, четко определен порядок удаления информации, при сдаче оборудования в сервисные центры.

В организации должен быть определен порядок уничтожения информации в случае списания или передачи оборудования

Вынос оборудования, информации, программного обеспечения за пределы организации невозможен без соответствующей авторизации. Осуществляется протоколирование вынесенного и внесенного оборудования (имущества).

6.Управление технологическим процессом

На основе политики информационной безопасности определены и документированы инструкции по управлению информационной системой, регулирующие такие вопросы, как обработка и обращение (хранение, копирование, передача и т.д.) информации, расписание запуска процессов с учетом зависимости между информационными системами, порядок запуска и время работы, обработку ошибок и исключительных состояний, порядок вывода конфиденциальной информации на печать и другие носители и другие.

В организации должна вестись идентификация и запись значительных изменений в информационных системах.

При разборе инцидентов информационной безопасности должны обеспечиваться сбор и сохранения записей аудита и подобных доказательств (событий), детальное документирование и регистрация произошедших аварийных событий, формирование отчетов о произошедших аварийных событиях и их разбор.

Порядок приемки информационных систем должен включать в себя согласование и документацию приемо-сдаточные испытаний.

Регистрация действий пользователей должна осуществляться с помощью журнала событий.

В организации должен быть определен порядок обращения и хранения информации, включающий маркировку и порядок хранения всех носителей информации, запрет доступа к информации неавторизированного персонала, регистрацию получателей информации, учет всех копий информации и так далее.

В организации должны быть четко определены порядок и соглашения об обмене данными с внешними организациями.

7. Управление доступом

В организации должен быть определен порядок регистрации и удаления пользователей.

Обязательно должна осуществляется регистрация всех событий, при которых использовались привилегии, в том числе и события авторизации для использования привилегий.

В организации должны быть введены требования подписи пользователем порядка хранения паролей, обеспечивающего его конфиденциальность.

В политике информационной безопасности должны быть определены дополнительные меры защиты оборудования, работающего без участия пользователя (файл-серверов).

В политике информационной безопасности должны быть определены методы управления паролями, включающие меры ответственности при хранении индивидуальных паролей, процедуры изменения и подтверждения при смене паролей, хранение информации о предыдущих паролях (за предыдущие 12 месяцев) и другое.

При использовании системных утилит должно проводиться определение и документирование уровней авторизации системных утилит.

Политика информационной безопасности должна определять защитные меры и порядок работы с переносным оборудованием за пределами организации.

8.Разработка и сопровождение компонент ИС

Требования по информационной безопасности информационных систем определены и документированы (специфицированы).

Политика информационной безопасности должна содержать порядок использования криптографических средств защиты информации (если организация их использует).

В организации должны регистрироваться все события, связанные с изменением и обновлением системных библиотек, все действия при использовании информации во время тестирования системы, все события, связанные с доступом к исходным текстам программ.

В организации проводимые изменения в программном обеспечении должны быть оттестированы и документированы.

9. Обеспечение непрерывности работы и восстановления

Формулирование и документирование стратегии обеспечения бесперебойной работы в соответствии с целями бизнеса и его приоритетами.

Формулирование и документирование плана обеспечения бесперебойной работы в соответствии с согласованной стратегией.

10. Соответствие нормативным и руководящим документам

В организации должны быть определены и документированы для каждой системы все требования установленные законом, государственными органами и договорными обязательствами.

При проведении аудита вся ответственность, процедуры и требования документированы.

На основе данного перечня процедур можно определить состав и структуру нормативно-методических документов по управлению информационной безопасностью в организации.

Литература

1. Анализ управления рисками www.globaltrust.ru
2. Аудит информационной безопасности www.globaltrust.ru
3. BS ISO/IEC 20000 — процессный подход к управлению информационной безопасностью современной организации http://offline.cio-world.ru