**Информационная безопасность**

На тему:

«Исследование нормативно-правовой базы информационной безопасности предприятия отделения Юго-Западного банка Сбербанка России №»

**Структура**

1 Краткие теоретические сведения о нормативно- правовой базе и классификации угроз информационной безопасности (не более 4-5 стр.)

2 Постановка задачи исследования в соответствии с индивидуальным заданием

3 Модель угроз ИБ на заданном предприятии

4 Сравнительный анализ отдельных вопросов защиты информации в зарубежных и отечественных документах (по индивидуальному заданию)

5 Разработка документов по обеспечению информационной безопасности на предприятии

6 Выводы по результатам исследований

**1. Краткие теоретические сведения о нормативно- правовой базе и классификации угроз информационной безопасности**

Информационная безопасность – это весьма важный вопрос для любой компании. В серьезных компаниях вопросами защиты информации и безопасности данных занимаются специально обученные люди — сисадмины (системные администраторы) или обишники (инженеры по обеспечению безопасности информации). От большинства простых пользователей они отличаются тем, что, даже разбуженные ночью или в пьяном угаре, как отче наш проговорят три принципа защиты информации на компьютере.

Принцип предотвращения подразумевает, что лучше избежать проблемы, чем заполучить ее, героически с ней сражаться и с блеском решить.

Принцип обнаружения сводится к тому, что, если предотвратить неприятность не удалось, своевременное ее обнаружение в большинстве случаев способно свести неприятности к минимуму. Если вы ненароком подцепили вирус (компьютерный, хотя для болезнетворных вирусов принцип также работает), то быстро начатое лечение способно пресечь разрушительные действия паразита.

Принцип восстановления гласит, что данные, которые могут быть утеряны, обязательно должны храниться в виде резервных копий. Что подойдет лично вам — дискетки, магнитооптика, CD-RW или “брелки” с flash-карточкой, — вам же и решать. Вариантов современная компьютерная индустрия предлагает множество. Даже методы форматирования жестких дисков развиваются согласно принципам восстановления и защиты информации.

Прошли те времена, когда хакерами были специалисты, детально знающие компьютерную технику и способные творить чудеса с программным кодом. Сейчас любой усидчивый, любознательный, но особо не обремененный моральными принципами подросток способен создать рядовому пользователю массу проблем. За примерами далеко ходить не надо, достаточно почитать “Новости интернета”. По нескольку раз в месяц разгораются скандалы или целые судебные разбирательства, связанные с молодыми людьми, запустившими новый почтовый червь, взломавшими сервер банка, компьютеры министерства обороны США... Как правило, такие хулиганы попадаются из-за собственной невнимательности или желания прославиться. При соблюдении мер предосторожности мошенников в сфере высоких технологий вычислить весьма трудно. В частности, именно поэтому преступлениями в сфере информационных технологий занимается Интерпол.

Злоумышленнику, для того чтобы получить доступ к конфиденциальной информации, порой не требуется даже специальных навыков и умений. Во многих случаях срабатывает человеческий фактор, например бумажка с написанным паролем на мониторе или под стеклом возле клавиатуры. Пароли, как правило, тоже оригинальностью не отличаются. А в недрах интернета всегда можно найти программы, которые возьмут на себя рутинную работу по перебору наиболее очевидных паролей.

Сейчас любой, даже слабо разбирающийся в компьютерах, хулиган за 15 минут найдет в интернете с десяток программ для подбора пароля из 4—6 символов и предоставляющих доступ к удаленному компьютеру. А ведь помимо хакеров есть еще и фрикеры, специализирующиеся на взломе электронных устройств, в частности, на сотовых телефонах, и кардеры, взламывающие пароли и подбирающие номера к кредиткам.

Из этого следует, что к вопросу информационной безопасности следует подходить серьезно и с полной отдачей.

**2. Постановка задачи исследования**

Цель этой работы на основе оценки возможных угроз информационной безопасности и с учетом существующей отечественной и международной нормативно-правовой базы построить модель угроз, дать сравнительный анализ нормативных и правовых документов по организации защиты информации в Донецком отделении Юго-Западного банка Сбербанка России №7749 и разработать рабочую документацию по информационной безопасности банка.

**3.** **Модель угроз на \*\*\*\*\*\*\* отделении Юго-Западного банка Сбербанка России №\*\*\*\***

**Совет банка**, как правило, входят его учредители. Совет банка утверждает годовой отчет банка, организует ежегодные собрания учредителей и пайщиков, принимает или может принимать участие в решении стратегических вопросов банковской деятельности.

**Правление (Совет директоров)** банка отвечает за общее руководство банка, утверждает стратегическое направление его деятельности. В состав Правления входят высшие руководители банка: председатель (президент, управляющий) банка, его заместители, руководители важнейших подразделений банка.

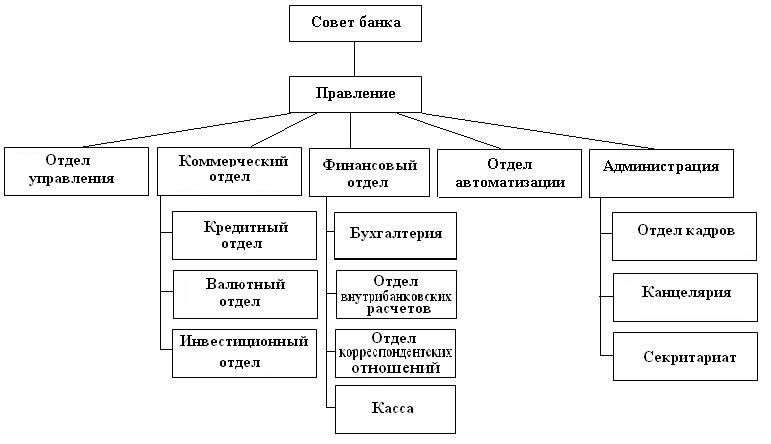
**Отдел управления** входит организацияпланирования, прогнозирования деятельности банка, подготовка методологии, безопасность и юридическая служба.

**Коммерческий отдел** охватывает организацию различных банковских услуг (кредитование, инвестирование, валютные, трастовые и другие операции). Сюда входит все, что связано с обслуживанием клиентов на коммерческих началах.

**Финансовый отдел** обеспечивает учет внутрибанковских расходов, учет собственной деятельности банка как коммерческого предприятия. В финансовый блок входят такие отделы как бухгалтерия, отдел внутрибанковских расчетов и корреспондентских отношений, касса.

**Отдел автоматизации** также является обязательным элементом структуры банка. Денежные потоки, которые проходят через современный банк, невозможно обработать вручную, нужен комплекс средств, электронных машин.

**Администрация**. В его состав входит отдел кадров банка, секретариат, канцелярия, хозяйственные подразделения.



**Угрозы**

***1. Случайные угрозы*** (стихийные бедствия, сбои и отказы, ошибки пользователей) – Этим угрозам подвержены все отделы, т.к от стихийных бедствий, сбоев, ошибок никто не застрахован.

***2. Преднамеренные угрозы***

***2.1*** ***Традиционный шпионаж и диверсии*** – Здесь угрозам подвержены такие отделы как: Финансовый отдел, Отдел автоматизации, Коммерческий отдел. Шпионаж поможет злоумышленнику узнать как устроен банк для того чтобы организовать ограбление.

***2.2.*** ***Несанкционированный доступ к информации –*** Тут в основном угрожает Отделу автоматизации. Злоумышленник, взломав КС банка, может получить много ему полезной информации. Узнав, эту информация под угрозой могут быть и все остальные отделы.

***2.3 Электромагнитные излучения и наводки*** – Также угроза для Отдела автоматизации.

***2.4 Несанкционированная модификация структур*** - Также угроза для Отдела автоматизации.

***2.5 Вредительские программы -*** Также угроза для Отдела автоматизации. И из этого вытекает угроза для всех остальных отделов.

**Модели злоумышленников.**

1. Хакер – Это опытный пользователь ПК, который взломав КС банка может использовать юту информацию в своих целях либо продать ее иному лицу. Он представляет большую угрозу Отделу автоматизации. Он также может, взломав КС перевести деньги на свой счет.
2. Сотрудник банка – Он тоже может предоставлять большую угрозу банку т.к он вращается в этой сфере и как никто другой знает как что устроено. Также это может быть бывший сотрудник потому что он тоже знает устройство банка, особенно если это бывший сотрудник Отдела автоматизации т.к он знает как устроена КС банка.
3. Разработчик КС – т.к он знает как устроена КС которую он разрабатывал.

**4. Сравнительный анализ отдельных вопросов защиты информации в зарубежных и отечественных документах**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | «Оранжевая книга» (TCSEC) | ***Защита информации***Специальные защитные знаки. Классификация и общие требования | Требования к процессу квалификационного анализа ИТ-продукта | Требования гарантии безопасности |
| **Совет банка** | Д | С1 | Контроль процесса сопровождения | УГО 1 |
| **Правление** | Д | С1 | Контроль процесса сопровождения | УГО 1 |
| **Отдел управления** | С1 | С1 | Независимое тестирование | УГО 2 |
| **Коммерческий отдел** | | | | |
| Кредитный отдел | В3 | В1 | Независимое тестирование | УГО 5 |
| Валютный отдел | В1 | А1 | Независимое тестирование | УГО 4 |
| Инвестиционный отдел | В1 | В2 | Независимое тестирование | УГО 4 |
| **Финансовый отдел** | | | | |
| Бухгалтерия | В3 | В2 | Независимое тестирование | УГО 4 |
| Отдел внутрибанковских расчетов | В2 | С1 | Независимое тестирование | УГО 3 |
| Отдел корреспондентских отношений | В2 | С1 | Независимое тестирование | УГО 3 |
| Касса | С2 | С2 | Независимое тестирование | УГО 3 |
| **Отдел автоматизации** | А1 | С1 | Анализ, контроль, тестирование | УГО 7 |
| **Администрация** | | | | |
| Отдел кадров | С1 | В2 | Независимое тестирование | УГО 2 |
| Канцелярия | Д | С2 | Независимое тестирование | УГО 1 |
| Секритариат | Д | С2 | Независимое тестирование | УГО 1 |

УТВЕРЖДАЮ

Руководитель предприятия

Журавлев А.А.

“6” октября 2008

**Должностная инструкция**

**сотруднику, ответственному за защиту информации**

***Общая часть***

1. Ответственный за защиту информации (штатный специалист) назначается и освобождается от должности руководителем предприятия по согласованию с Управлением Гостехкомиссии России по Южному федеральному округу.
2. Ответственный за защиту информации назначается из числа ИТР, имеющих опыт работы по основной деятельности предприятия или в области защиты информации.
3. В своей производственной деятельности ответственный за защиту информации подчиняется руководителю предприятия или его заместителю, ответственному за организацию защиты информации.
4. Работа ответственного за защиту информации проводится в соответствии с планами работ по защите информации. На ответственного по защите информации запрещается возлагать задачи, не связанные с его деятельностью.
5. Ответственный за защиту информации свою работу проводит в тесном взаимодействии с научными, производственными, режимно-секретными подразделениями предприятиями, представителями территориальных органов ФСБ, ФАПСИ, Гостехкомиссии.
6. Ответственный за защиту информации в своей деятельности руководствуется:
   * положением о государственной системе защиты информации в РФ;
   * нормативно-техническими документами по противодействию иностранным техническим разведкам;
   * приказами, указаниями вышестоящих органов по защите информации;
   * ведомственными организационно-распорядительными и нормативно-методическими документами.

***Основные функциональные задачи и обязанности:***

* 1. Планирование работ по защите информации на предприятии, предусматривающее решение конкретных вопросов по защите информации, организацию их выполнения, а также контроль за их эффективностью.
  2. Участие в подготовке предприятия к аттестованию на право проведения работ с использованием сведений, отнесенных к гостайна.
  3. Организация разработки нормативно-методических документов по защите информации на предприятии.
  4. Согласование мероприятий по защите информации для рабочих мест, на которых проводятся работы с использованием сведений, отнесенных к гостайне.
  5. Организация и проведение работ по выявлению:

- демаскирующих признаков предприятия и выпускаемой продукции;

- видов и средств технической разведки, которые позволяют получить сведения о деятельности предприятия;

- технических каналов утечки информации;

- возможности несанкционированного доступа к информации, ее разрушения (уничтожения) или искажения и разработка соответствующих мер по защите информации.

* 1. Разработка (самостоятельно или совместно с режимными органами и другими подразделениями) проектов распорядительных документов по вопросам организации защиты информации.
  2. Организация, в соответствии с нормативно-техническими документами, специальных проверок и проведение аттестования рабочих мест, ПЭВМ и т.д. с выдачей предписания на право проведения на них работ с секретной информацией.
  3. Разработка предложений по совершенствованию системы защиты информации на предприятии.
  4. Разработка совместно с другими подразделениями предприятия Руководства по защите информации на предприятии.
  5. частие в разработке комплекса мероприятий по защите гостайны при установлении и осуществлении научно-технических и торгово-экономических связей с зарубежными фирмами, а также при посещении предприятия иностранными специалистами.
  6. частие в разработке требований по защите информации при проведении работ, связанных с движением и хранением продукции, а также при проектировании, строительстве (реконструкции) и эксплуатации объектов предприятия.
  7. Участие в согласовании ТЗ на проведение работ, связанных со сведениями, содержащими гостайну.
  8. Организация и проведение периодического контроля эффективности мер защиты информации на предприятии. Учет и анализ результатов контроля.
  9. Участие в расследовании нарушений в области защиты информации на предприятии и разработка предложений по устранению недостатков и предупреждению подобного рода нарушений.
  10. Подготовка отчетов о состоянии работ по защите информации на предприятии.
  11. Организация проведения занятий с руководителями и специалистами предприятия по вопросам защиты информации.

***Ответственный за защиту информации имеет право:***

* + 1. Допуска к работам и документам подразделений предприятия, для оценки принимаемых мер по защите информации и подготовки предложений по их дальнейшему совершенствованию.
    2. Готовить предложения о привлечении к проведению работ по защите информации предприятия, имеющего лицензию на соответствующий вид деятельности.
    3. Контролировать деятельность любого структурного подразделения предприятия по выполнению требований по защите информации.
    4. Участвовать в работе технической комиссии предприятия при рассмотрении вопросов защиты информации.
    5. Вносить предложения руководителю предприятия о **приостановке** работ в случае обнаружения утечки (или предпосылок к утечке) информации.
    6. Получать лицензии на право выполнения работ по защите информации и при ее получении оказывать услуги в этой области другим предприятиям.
    7. Быть соисполнителем при проведении на договорной основе работ, связанных с защитой информации по темам НИОКР, а также производственным заказам или программам испытаний.

#### ИНСТРУКЦИЯ

**о порядке ввода в эксплуатацию объектов ЭВТ, допуска сотрудников к работе на ПЭВМ, и соблюдению требований собственной безопасности при обработке закрытой информации на СВТ**

К работе на ПЭВМ в Отделе автоматизации допускаются сотрудники, имеющие соответствующую квалификацию (прошедшие подготовку), после сдачи ими зачета по знанию инструкции о порядке ввода в эксплуатацию объектов ЭВТ, допуска сотрудников к работе на ПЭВМ, и соблюдению требований собственной безопасности при обработке закрытой информации на средствах вычислительной техники, инструкции по защите электронной информации от компьютерных вирусов по заявлению установленного образца.

Все приобретенные компьютеры, независимо от источника их получения в 10-дневный срок должны пройти проверку в **Отделе автоматизации**. Пуско-наладочные работы по вводу ПЭВМ в эксплуатацию и последующее техническое обслуживание СВТ осуществляются специалистами ВЦ.

На ПЭВМ устанавливается только необходимое, сертифицированное проверенное математико-программное обеспечение (МПО), утвержденное директором Журавлевым (Вн. №854796).

Узлы и блоки оборудования СВТ, к которым в процессе эксплуатации доступ не требуется, опечатываются специалистами ВЦ с целью предупреждения несанкционированного вскрытия оборудования.

**По всем фактам несанкционированного вскрытия узлов и блоков СВТ проводится служебное разбирательство.**

Замена или подключение других технических средств, не входящих в комплект объекта ЭВТ, не допускается.

***Запрещается :***

* устанавливать и использовать нештатное МПО без согласования с ВЦ;
* производить обработку секретной информации на СВТ, не прошедших соответствующую проверку в ВЦ, регистрацию, категорирование и не имеющих предписания на эксплуатацию;
* сообщать устно или письменно кому бы то ни было, если это не вызвано служебной необходимостью, любые сведения о характере выполняемой на СВТ работы; о применяемых системах защиты информации; о паролях, используемых в средствах защиты; о системе охраны и пропускном режиме;
* перевозить машинные носители, содержащие конфиденциальную информацию, и документы общественным транспортом, заходить с ними в места, не связанные с выполнением задания, и транспортировать их без соответствующей упаковки.

***Категорически запрещается :***

1. осуществлять ремонт СВТ с установленными магнитными носителями в сторонних организациях без согласования с ВЦ и Начальника отдела автоматизации.

Ответственность за обеспечение режима конфиденциальности и выполнение мероприятий по защите информации, обрабатываемой на СВТ, несет начальник подразделения.

###### Начальник Отдела Автоматизации

Кузьмин В.В.

Утверждена

приказом руководителя предприятия №77 от 3 октября 2008 г.

#### Матрица доступа субъектов автоматизированной системы объекта информатизации\*\*\*\*\*\*\* отделении Юго-Западного банка Сбербанка России №\*\*\*\*\**]* к ее защищаемым информационным ресурсам

|  |  |
| --- | --- |
| Уровень полномочий | Права по доступу к защищаемым информационным ресурсам |
| Администратор | Полные права по доступу к ресурсам по п.п. 5, 6 Перечня (инв. №856). |
| Начальник ОА | Полные права по доступу к ресурсам по п.п. 1, 2, 3, 4 Перечня (инв. №987). |
| Пользователь 2 | Полные права по доступу к ресурсам по п.п. 1, 2, 4 Перечня (инв. №254). |

Подпись

Экз. № 88

**УТВЕРЖДАЮ**

Директор Журавлев А.А.

«5» октября 2008 г.

**Описание технологического процесса обработки информации в автоматизированной системе объекта информатизации «*Сбербанка*».**

Субъектом доступа автоматизированной системы (АС) объекта информатизации (ОИ) **«*Сбербанка*»** является пользователь АС – старшая машинистка по секретной переписке Иванова Е.Е., которой присвоен идентификатор «Lena».

Объектами доступа АС ОИ **«*Сбербанка*»** являются текстовые и табличные файлы пользователя, размещаемые на накопителе на жестких магнитных дисках (НГЖД) ПЭВМ и на гибких магнитных дисках.

Штатными средствами доступа к информации в АС являются:

* + пакет программных продуктов Microsoft Office 2000 в составе MS Word и MS Ecxel, серийный номер: 12547896.;
  + программная оболочка - Windows Commander версия 4.01 (сборка 4.00.950), серийный номер: 56987236;
  + продукт для просмотра графических изображений ACDSee32, версии 2.4., серийный номер 99987412;
  + для защиты информации в АС применен программно-аппаратный комплекс защиты от НСД Secret Net , версия 4.0. в составе:
  + аппаратная плата Secret Net;
  + программное обеспечение Secret Net версия 4.0 (автономный вариант), №Б 57596621.

Единственный пользователь Lena имеет полный доступ ко всем ресурсам АС.

Схема информационных потоков приведена в приложении.

Начальник ОА

**Приложение**

к Описанию технологического процесса обработки информации в автоматизированной системе объекта информатизации **«*Сбербанка*»**

Схема информационных потоков автоматизированной системы объекта информатизации **«*Сбербанка*»**.

|  |
| --- |
| Файлы с информацией на жестком магнитном диске |

|  |
| --- |
| Файлы с информацией на гибком магнитном диске |

|  |
| --- |
| Пакет программных продуктов Microsoft Word, Microsoft Exel. |

|  |
| --- |
| Пользователь |

|  |
| --- |
| Программа архивации ARJ |

|  |
| --- |
| Печать документов |

|  |
| --- |
| Программная оболочка Windows Commander |

Начальник ОА подпись

**Схема построения антивирусной защиты**

(на основе пакета Antiviral Toolkit Pro)

**Общие положения**

Настоящая технология (далее – Технологическая схема) разработана во исполнение пунктов об антивирусной защите Концепции информационной безопасности **«*Сбербанка*»**.

Целью разработки Технологической схемы является совершенствование нормативно-правовой и методической базы **«*Сбербанка*»** в области обеспечения информационной безопасности.

Технологическая схема отражает технические решения по следующим вопросам организации антивирусной защиты информации в **«*Сбербанка*»** :

* внедрение средств антивирусной защиты информации Antiviral Toolkit Pro;
* применение средств антивирусной защиты информации Antiviral Toolkit Pro;
* порядок обновления баз данных средств антивирусной защиты информации Antiviral Toolkit Pro;
* действия должностных лиц при обнаружении заражения информационно-вычислительных ресурсов **«*Сбербанка*»** программными вирусами.

Технологическая схема разрабатывалась на основе следующих нормативно-методических документов:

* 1. Федеральный закон от 20.02.95 № 24-ФЗ «Об информации, информатизации и защите информации»;
  2. Положение о государственной системе защиты информации в Российской Федерации от иностранной технической разведки и от ее утечки по техническим каналам, утвержденное постановлением Совета Министров - Правительства Российской Федерации от 15.09.93 г. № 912-51;
  3. Постановление Правительства Российской Федерации «О сертификации средств защиты информации» от 26.06.95 г. № 608,
  4. Указ Президента Российской Федерации от 09.09.2000 № 1895 «Об утверждении Доктрины информационной безопасности Российской Федерации»;

Основными путями проникновения вирусов в информационно-вычислительную сеть таможенного органа являются:

гибкие магнитные диски, компакт-диски, почта сети Интернет, файлы, получаемые из сети Интернет, ранее зараженные рабочие станции.

Внедрение системы антивирусной защиты информации осуществляется в рамках работ по созданию и развитию **«*Сбербанка*»**. Оснащение **«*Сбербанка*»** средствами антивирусной защиты информации, необходимых для реализации Технологической схемы планируется по договору между сторонами на основании Федеральных критериев безопасности информационных технологий.

 **Организация антивирусной защиты информации в «*Сбербанке*»**

**Цель и задачи организации антивирусной защиты информации**

 Организация антивирусной защиты информации в **«*Сбербанке*»** направлена на предотвращение заражения информационно-вычислительных ресурсов автоматизированных систем банка программными вирусами.

Защита информации от воздействия программных вирусов на объектах информатизации **«*Сбербанка*»** осуществляется посредством применения средств антивирусной защиты. Порядок применения средств антивирусной защиты устанавливается с учетом следующих требований:

обязательный входной контроль на отсутствие программных вирусов всех поступающих на объект информатизации машинных носителей информации, информационных массивов, программных средств общего и специального назначения;

периодическая проверка пользователями жестких магнитных дисков (не реже одного раза в неделю) и обязательная проверка используемых в работе гибких магнитных дисков перед началом работы с ними на отсутствие программных вирусов;

внеплановая проверка магнитных носителей информации на отсутствие программных вирусов в случае подозрения на наличие программного вируса;

восстановление работоспособности программных средств и информационных массивов в случае их повреждения программными вирусами.

Порядок применения средств антивирусной защиты, учитывающий особенности объекта информатизации **«*Сбербанка*»** и выполняемых на данном объекте работ, определяется инструкцией по антивирусной защите информации. В разделе должны быть определены:

должностные лица, ответственные за получение, рассылку, установку, поддержание в работоспособном состоянии и использование средств антивирусной защиты;

должностные лица, осуществляющие контроль за организацией антивирусной защиты;

порядок установки и применения средств антивирусной защиты

порядок ликвидации последствий воздействий программных вирусов.

Состояние вопросов антивирусной защиты отражается в отчете о состоянии обеспечения информационной безопасности в **«*Сбербанке*»** с обязательным указанием выявленных нарушений, вызванных заражением программными вирусами, описанием причин появления вирусов, характера и последствий их воздействия и принятых мерах.

**Организационная структура системы антивирусной защиты информации в «*Сбербанке*»**

Общее руководство и контроль за организацией и обеспечением антивирусной защиты информации в **«*Сбербанке*»** осуществляет **Администратор**.

**Разграничение полномочий и ответственность за организацию антивирусной защиты информации**

На **Администратора** возлагается:

* разработка проектов нормативных документов по организации антивирусной защиты информации;
* обобщение заявок от **Начальника ОА** на средства антивирусной защиты, организация заказа и закупки средств антивирусной защиты информации;
* контроль состояния антивирусной защиты информации в **«*Сбербанке*»**;
* анализ состояния работы по антивирусной защите информации и выработка предложений по ее совершенствованию;
* участие в проведении расследований по фактам заражения компьютерными вирусами в автоматизированных системах **«*Сбербанке*»** .

На **Администратора** возлагается:

* участие в разработке проектов нормативных документов по организации антивирусной защиты информации;
* закупка средств антивирусной защиты информации на основании решений **Руководства** ;
* обеспечение внедрения средств антивирусной защиты информации в локальных вычислительных сетях подразделений **банка**;
* доведение до **работоспособности** средств антивирусной защиты информации;
* организация обновления баз данных средств антивирусной защиты информации;
* участие в проведении расследований по фактам заражения компьютерными вирусами в автоматизированных системах **«*Сбербанке*»**.

Непосредственное руководство проведением работ по антивирусной защите информации в **«*Сбербанке*»** осуществляет **Начальник ОА**.

**Начальник ОА** обеспечивают практическое выполнение мероприятий по организации антивирусной защите информации.

Ответственность за своевременную инсталляцию антивирусных средств защиты и обновление их баз данных возлагается на администратора АВЗ.

**Начальник ОА** несут ответственность за организацию антивирусной защиты на эксплуатируемых средствах вычислительной техники.

Сотрудники **«*Сбербанка*»** обязаны строго соблюдать установленные правила применения средств антивирусной защиты при работе на средствах вычислительной техники. На них возлагается непосредственная ответственность за защиту информации от заражения программными вирусами.

**Установка средств антивирусной защиты информации**

**Структура средств антивирусной защиты информации**

**Рабочие станции** оснащаются антивирусным пакетом **Dr.Web**. Комплект средств \_ **Dr.Web** позволяет построить многослойную схему антивирусной защиты и обеспечить максимальную защищенность информационно-вычислительных ресурсов **«*Сбербанка*»** от заражения программными вирусами.

Пакет **Dr.Web** включает следующие средства:

1. Средства антивирусной защиты для почтовых серверов:
2. Средства антивирусной защиты информации для серверов баз данных и файловых серверов:

AVP for Windows NT Server; AVP for Novell Netware; AVP for Linux; AVP for FreeBSD; AVP for BSDi UNIX.

1. Средства антивирусной защиты информации для автономных, мобильных и сетевых рабочих станций:AVP for OS/2; AVP for Firewall;
2. Средства администрирования и управления антивирусной защитой информации:

AVP Центр Управления; AVP Сетевой Центр Управления.

Полученные средства антивирусной защиты устанавливаются на всех эксплуатируемых в **«*Сбербанке*»** на объекте информатизации, независимо от категорий объектов информатизации, на которых они используются, в максимально короткий срок.

В первую очередь, установка антивирусных средств осуществляется на Intranet и Internet серверах, серверах баз данных, почтовых серверах, рабочих станциях, задействованных в **«*Сбербанке*»**, и рабочих станциях, подключенных к информационно-вычислительным сетям общего пользования.

**Схема типового функционирования средств антивирусной защиты информации**

 Инсталляция комплекта средств AntiViral Toolkit Pro осуществляется на трех основных уровнях

1 Уровень автономных рабочих станций, мобильных компьютеров и рабочих станций ЛВС.

2 Уровень серверов локальной вычислительной сети таможенных органов.

3 Уровень рабочей станции администратора АВЗ.

Инсталляция комплекта средств AntiViral Toolkit Pro на автономных и сетевых рабочих станциях и мобильных компьютерах

На рабочих станциях устанавливается комплект антивирусных программ. На рабочих станциях использующих ОС MS-DOS должен быть установлен антивирусный сканер и дисковый ревизор, который автоматически проверят компьютер при его включении и создает список – отчет об изменившихся и новых файлах, которые необходимо проверить антивирусным сканером.

 Использование совместно сканера и ревизора позволит усилить степень проверки и значительно уменьшит время работы комплекта средств **Dr.Web**.

Комплект средств **Dr.Web** устанавливаемый на компьютерах с многозадачными операционными системами (Windows NT Server) должен иметь в своем составе антивирусный монитор, который запускается при включении компьютера и работает постоянно, в фоновом режиме без существенного замедления работы системы в целом или отдельных ее приложений, а так же антивирусный сканер, который осуществляет проверку по запросу.

**Инсталляция комплекта средств Dr.Web на серверах**

Антивирусные средства, используемые на этом уровне, предоставляют возможность проверки в реальном режиме времени (фоновом режиме) и проверку по запросу пользователя, что защищает данные при передаче с серверов Novell Netware, Windows NT Server, Lotus Notes, Unix и обратно. При работе на сервере антивирус должен работать устойчиво, надежно и эффективно. Настройка антивирусной программы должна быть проведена с возможностью блокировать попытки записи зараженных, подозрительных файлов на сервер. Каждая такая попытка должна фиксироваться в протоколах, отчетах антивирусной программы с указанием имени зараженного файла и пути к нему. Информация о таких попытках должна немедленно отсылаться администратору сети и на рабочую станцию, с которой производилась попытка записи зараженных, подозрительных файлов. Ведение отчетов, должно осуществляться централизовано, с наличием возможности посылать предупреждения администраторам сети о вирусных атаках.

**Инсталляция комплекта средств Dr.Web** **на рабочем месте администратора антивирусной защиты информации**

 Рабочим местом администратора АВЗ является сетевая рабочая станция, с которой администратор:

управляет конфигурацией всего программного обеспечения AVP, установленного на сетевых рабочих станциях Администратор;

управляет рассылкой обновлений антивирусных баз данных;

ограничивает доступ пользователей к установленным локально средствам пакета AVP;

проводит настройку рассылки сообщений об обнаружении вируса и сбое в работе антивирусных программ и т.п., конфигурирует логическую структуру пакета антивирусных программных средств.

При этом одна ПЭВМ, по усмотрению администратора АВЗ может быть и рабочей станцией, и сервером, и рабочим местом администратора в зависимости от установленных на неё программных компонент.

Программный комплекс AVP Сетевой Центр Управления предназначен для организации защиты локальной сети (не только локальная сеть как таковая, но и несколько локальных сетей, объединенных с помощью протокола TCP/IP) и дает возможность администратору АВЗ управлять компонентами Антивируса Касперского, установленными на подключенных к сети рабочих станциях, со своего рабочего места.

Администратор АВЗ должен иметь возможность управлять потоками передаваемых данных при помощи почтовых серверов на базе SMTP, где вся информация также проверяется на вирусы. Немаловажный факт заключается в том, что средства антивирусной защиты для почтовых систем на базе SMTP являются первой линей обороны: перехватывают и уничтожают «приходящие» вирусы в режиме реального времени прежде, чем они попадут в локальную сеть и начнут свое разрушающее действие.

Первый уровень защиты представляет собой **"Межсетевой экран" (firewall)**.

Развернутая схема должна удовлетворять следующим условиям:

* администратором АВЗ должны регламентироваться права доступа как папкам-хранилищам антивирусных баз, и дистрибутивов антивирусных средств;
* своевременность (не реже одного раза в неделю или по факту проникновения вируса) обновления антивирусных баз;
* своевременность получения администратором АВЗ уведомлений о проникновении вируса.

**Инсталляция системы антивирусной защиты информации**

Для инсталляции системы антивирусной защиты информации необходимо:

1 Установить программу AVP сетевой центр Управления на рабочей станции администратора АВЗ.

2 Установить программу AVP сервер хотя бы на одном из компьютеров, подключенном к локальной сети.

3 Установить на компьютерах пользователей т серверах компоненты Антивируса Касперского и управляющую оболочку – программу AVP Центр Управления.

4 Сформировать и настроить логическую сеть AVP.

Инсталляция средств антивирусной защиты информации осуществляется в соответствии с руководствами пользователя, входящих в комплект средств **Dr.Web**. Порядок создания и настройки логической сети изложен в Руководстве пользователя на AVP Сетевой Центр Управления.

**Особенности организации и инсталляции системы антивирусной защиты информации в подразделениях «*Сбербанка*»**

Техническое обслуживание и сопровождение эксплуатации средств вычислительной техники и программного обеспечения, эксплуатируемых в подразделениях **«*Сбербанка*»**, возложены на **Начальника ОА**.

В связи с этим, можно выделить следующие основные Особенности организации и инсталляции системы антивирусной защиты информации в подразделениях **«*Сбербанка*»**:

* 1. Схема функционирования пакета **Dr.Web** в локальных сетях подразделений **«*Сбербанка*»** предусматривает централизованное управление с рабочего места администратора АВЗ – **Отдела автоматизации**.
  2. Все работы по установки средств антивирусной защиты информации в локальных вычислительных сетях подразделений **«*Сбербанка*»** выполняют сотрудники **Администраторской**.
  3. Ответственность за настройку средств антивирусной защиты информации и обновление их баз данных возложена на **Администратора**

**Порядок обновления баз данных антивирусных средств защиты информации**

**Общие требования**

Своевременное обновление антивирусных баз является неотъемлемой частью наиболее полноценной защищенности **информации** от заражения компьютерными вирусами.

Обновление баз данных осуществляется еженедельно.

**Схема обновления баз данных антивирусных средств защиты**

Схема обновления баз данных антивирусных средств защиты представляет собой многоуровневую дублируемую схему обновления антивирусных .

Первый уровень предусматривает получение обновлений баз данных антивирусных средств защиты информации с помощью настройки автоматического обновления с Интернет-сервера или Ftp-сервера «**Dr.Web**».

Второй уровень предусматривает получение обновлений баз данных антивирусных средств защиты информации с помощью принудительного обновления с Интернет-сервера **Dr.Web**.

Внутренняя структура обновления баз данных средств антивирусной защиты информации в рамках одного сегмента локальной вычислительной сети строится на основе схемы, с использованием средств управления антивирусного средства и должна также обеспечивать своевременность обновления.

***Порядок действий при обнаружении программных вирусов***

**Обнаружение программных вирусов при входном контроле**

 Вся поступающая в **«*Сбербанк*»** информация, полученная по модемной связи, а также на магнитных носителях информации (программные средства общего и специального назначения, информационные массивы), подлежат обязательной проверке на наличие программных вирусов.

О произведенной проверке и ее результатах делается отметка на сопроводительном письме (акте, аппаратном журнале и т.п.) пользователем, производившим проверку.

При обнаружении на дискетах или в полученных файлах программных вирусов пользователи докладывают об этом в подразделение **«*Сбербанка*»** по защите информации, и принимают меры по восстановлению работоспособности программных средств и данных.

О факте обнаружения программных вирусов сообщается в **Отдел автоматизации**, от которых поступили зараженные файлы, для принятия мер по локализации и устранению программных вирусов.

Перед отправкой массивов информации и программных средств, осуществляется ее проверка на наличие программных вирусов. В тексте сопроводительного письма (аппаратном журнале, техническом журнале и т.п.) указывается, что проверка на наличие программных вирусов информации произведена.

**Обнаружение программных вирусов в процессе обработки информации**

При обнаружении программных вирусов пользователь обязан немедленно прекратить все работы на ПЭВМ, поставить в известность подразделение **«*Сбербанка*»** по защите информации и принять меры к их локализации и удалению с помощью имеющихся антивирусных средств защиты.

При функционировании ПЭВМ в качестве рабочей станции вычислительной сети производится ее отключение от локальной сети, локализация и удаление программных вирусов в вычислительной сети.

Ликвидация последствий воздействия программных вирусов осуществляется **Отделом Автоматизации.**

Программные средства общего и специального назначения объекта информатизации, осуществляющие обработку информации, отнесенной к государственной или служебной тайне, подлежат обязательной переустановке с рабочих копий эталонных дискет независимо от результатов по удалению выявленных программных вирусов имеющимися средствами антивирусной защиты.

**«УТВЕРЖДАЮ»**

Начальник ОА

« 3 » октября 2008 г.

**6. Вывод**

"Оранжевая книга" являлась первым стандартом информационной безопасности, в котором компьютерную систему (продукт) в процессе оценивания, условно можно разделить на четыре типа - требования проведения последовательной политики безопасности (security policy), требования ведения учета использования продукта (accounts), требования доверия к продукту (assurance) и требования к документации на продукт.

"Федеральные критерии безопасности информационных технологий" являются по сравнению с "Оранжевой книгой" стандартом нового поколения. "Федеральные критерии" являются первым стандартом информационной безопасности, в котором определяются три независимые группы требований: функциональные требования к средствам защиты, требования к технологии разработки и к процессу квалификационного анализа (сертификации). Авторами стандарта впервые предложена концепция «Требования к процессу квалификационного анализа ИТ-продукта»- документа, призванного обеспечить надежность и корректность этого процесса. Разработчики "Федеральных критериев" также отказались от используемого в "Оранжевой книге" подхода к оценке уровня безопасности изделия ИТ на основе обобщенной универсальной шкалы классов безопасности. Вместо этого предлагается независимое ранжирование требований каждой группы, т.е. используется множество частных шкал-критериев, характеризующих обеспечиваемый уровень безопасности. Такой подход позволяет разработчикам и потребителям изделия ИТ выбрать наиболее приемлемое решение и определить необходимый и достаточный набор требований для каждого конкретного продукта ИТ и среды его эксплуатации.

"Общие критерии оценки безопасности информационных технологий" представляют собой результат обобщения всех достижений в области информационной безопасности. Они согласованы с существующими стандартами и развивают их путем введения новых концепций, соответствующих современному уровню развития информационных технологий. "Общие критерии" продолжили подход "Федеральных критериев", направленный на отказ от единой шкалы классов безопасности, и повысили гибкость и удобство применения критериев путем введения частично упорядоченных шкал. "Общие критерии" оставили далеко позади все существующие стандарты безопасности информационных технологий. "Общие критерии" разрабатываются как проект международного стандарта ИСО и должны позволить осуществлять сертификацию продуктов ИТ на глобальном уровне.