УДК 681.3

Комплексный анализ уровня безопасности информации цифровой телефонной станции

Осовецкий Л. Г., Ефимов В. В.

Постановка задачи: *в настоящее время активно развиваются фиксированные и подвижные сети предоставления услуги голосовой связи. Эти сети базируются на основе цифровых автоматических телефонных станций (ЦАТС). При этом обеспечение информационной безопасности ЦАТС является актуальной прикладной задачей.* ***Цель работы*** *– анализ типовой ЦАТС, обоснование характерных угроз и обоснование организационно-технических рекомендаций по повышению уровня информационной безопасности ЦАТС.* ***Используемый метод*** *– системный многофакторный анализ.* ***Результаты:*** *на основе анализа структуры ЦАТС и угроз, характерных ее основным элементам, сформирована описательная модель угроз для типовой ЦАТС. На основе модели угроз сформированы основные уязвимости ЦАСТ, как для системы в целом, так и для отдельных ее элементов. На основе системного анализа уязвимостей ЦАТС предложены рекомендации по проведению организационно-технических мероприятий, направленных на повышение уровня информационной безопасности.* ***Практическая значимость.*** *Предложенные в работе организационно-технические мероприятия могут быть использованы операторами фиксированной и подвижной связи для повышения уровня информационной безопасности своих ЦАТС с учетом специфики используемого ими оборудования.*

Ключевые слова: *АТС, ЦАТС, угрозы безопасности, программное обеспечение.*

Актуальность и постановка задачи

В настоящее время широкое распространение получили цифровые автоматические телефонные станции (ЦАТС). При этом зачастую они являются уязвимыми объектами с точки зрения информационной безопасности. В связи с этим, в статье решается актуальная задача анализа и определения уровня информационной безопасности ЦАТС. Целью и задачами исследования являются:

- анализ информационной безопасности объекта;
- построение модели угроз безопасности информации объекта;
- комплексный анализ уровня информационной безопасности объекта;
- выдача рекомендаций по улучшению технологии эксплуатации объекта и устранению угроз.

Состав и конфигурация основных компонент программного обеспечения ЦАТС

Для последующего анализа угроз ЦАТС из полного перечня ее программных блоков и файлов коммутационной системы исключены модули, не влияющие на безопасность. Ниже приведен перечень программных блоков и файлов, влияющих на безопасность ЦАТС, с описанием выполняемых ими функций.

Сигнальная системная библиотека. Предназначена для выполнения следующих функций:

- установка и сброс сигнальных наблюдений и посылка сообщений на принтер;
- обновление счетчика ошибок;
- инициализация библиотеки и обновление информации файла.

Библиотека обслуживания дисков. Используется программными блоками в обход блока для получения прямого доступа к магнитным носителям.

Загружаемый во время начальной загрузки блок, который содержит параметры, необходимые сервисному блоку (операционная система), типы индексов, буферы памяти различных размеров, таблицу связей программных блоков.

Библиотека системных файлов. Содержит подпрограммы, используемые для создания, чтения и записи в файлы программных модулей, для чтения атрибутов файлов.

Программный блок начального загрузчика и ответственный за начальную загрузку в различных ситуациях перезагрузки системы.

Программный блок принтера. Управляет выводом сообщений на дисплей и принтер, подключённые через специальный интерфейс к модулю их обслуживания.

Блок резервного копирования. С помощью этого блока оператор может копировать файлы с диска на диск, с диска на магнитную ленту, с магнитной ленты на магнитную ленту, и с магнитной ленты на диск.

Библиотечный модуль ядра. Коммутационная система имеет ядро операционной системы, работающее в реальном масштабе времени.

Сервисный блок отладки. Блок предназначен для испытаний системы, отладки и системного контроля.

Программный блок файловой системы. Программный блок предназначен для обработки файлов в коммутационной. Типичный файловый сервис включает в себя создание файла, чтение файла, запись в файл, а также чтение и изменение атрибутов файла. Существует возможность загрузки файла с диска или памяти, обновления файла в дисковом массиве и распределения файла по различным дискам.

Список начальной загрузки. Загружаемый во время начальной загрузки файл, содержащий список модулей, которые загружаются на компьютер.

Файл управления печатью. Файл, который содержит данные управления печати тревожных сообщений, время срабатывания тревоги и время существования активных тревожных сообщений.

Перечень файлов базы данных. Содержит физическое описание файлов в базе данных.

Файл параметров базы данных. Содержит информацию о параметрах баз данных.

Операционный файл защиты. Содержит детальную информацию относительно событий, связанных с защитой.

Файл контроля работы оператора. Используется для регистрации статистики работы оператора и индекса обслуживающего оператора.

Информация может сохраняться с периодичностью 15 минут, полчаса, день, неделя, месяц.

Анализ возможных каналов НСД, разработка модели угроз ЦАТС

Коммутационная система ЦАТС использует следующие каналы связи:

- с центром управления 1-го уровня (ЦУЦС);
- с центром управления 2-го уровня (районный узел);
- с системой биллинга;
- с системой удаленного управления и технического обслуживания фирмы разработчика;
- с локальными терминалами;
- с абонентами.

Помимо использования каналов связи несанкционированные действия в отношении ЦАТС могут быть произведены при физическом доступе к коммутационной системе:

- физический доступ к коммутационной системе;
- несанкционированный доступ к каналу удаленного управления и технического обслуживания фирмы;
- действия операторов терминального оборудования по уровням: локальные терминалы, терминалы 2-го уровня управления, терминалы 1-го уровня управления;
- несанкционированное подключение дополнительного оборудования для использования в качестве терминалов коммутационной системы по уровням: в локальной сети; в локальной сети, подключенной к блоку MSW; в локальной сети подключенной к блоку OMC;
- несанкционированные действия с использованием системы биллинга;
- несанкционированные действия с магнитными накопителями информации по уровням:
  - магнитные носители информации терминалов коммутационной системы;
  - магнитные носители информации системы биллинга,
  - магнитные носители информации блока MSW,
  - магнитные носители информации блока OMC;
- несанкционированный доступ к съемным носителям информации;
- несанкционированное подключение к каналам управления, соединяющим абонентов коммутационную систему с центрами 1-го и 2-го уровня управления;
- несанкционированные действия со стороны абонентов коммутационной системы несанкционированные действия на уровне абонентских линий коммутационной системы.

Рассмотрим более подробно угрозы НСД, ориентированные на уязвимости канала связи с центром управления 1-го уровня. Данный канал связи позволяет получать от станции сигналы системы аварийной сигнализации и осуществлять удаленное управление. На данном уровне (центр управления 1-

го уровня) производится работа администраторов коммутационной системы, обладающих максимальными привилегиями.

Угрозы канала связи с центром управления 1-го уровня:

- при НСД к каналу связи – несанкционированное получение, удаление, изменение (модификация) информации, используемой при функционировании коммутационной системы (ЦУЦС имеет выделенный канал связи с коммутационной системой, при этом в канале связи используются сертифицированные средства криптографической защиты, поэтому вероятность угроз в данном случае определяется качеством реализации средств криптографической защиты);
- при НСД к базе данных – несанкционированное получение и модификация информации, хранимой в базе данных;
- при НСД к терминальному оборудованию – несанкционированное получение (в том числе копирование на отчуждаемый носитель) информации от коммутационной системы, получение идентификационных и аутентификационных данных пользователей (администратора, диспетчера, оператора) различными способами, выведение из строя терминального оборудования, несанкционированное управление коммутационной системой, несанкционированное создание новых учетных записей и (или) несанкционированное присвоение полномочий.

Рассмотрим более подробно угрозы НСД ориентированные на уязвимости канала связи с центром управления 2-го уровня.

По способу соединения и управляющему воздействию этот канал аналогичен каналу связи с центром управления 1-го уровня. Он позволяет осуществлять удаленное управление коммутационной системой, прием и передачу служебной информации. Оконечное оборудование подключено к коммутационной системе. В качестве оконечного оборудования могут быть использованы терминалы (ПК), подключенные по локальной сети, устройства вывода текущей информации, получаемой по линиям аварийной сигнализации (принтер аварийной сигнализации, дисплей аварийной сигнализации).

Персонал центра управления 2-го уровня осуществляет удаленное управление коммутационной системой (получение и обработка служебной информации, настройка конфигурации, отслеживание сообщений аварийной сигнализации) и обладает более низким уровнем полномочий, чем персонал 1-го уровня управления.

Угрозы канала связи с центром управления 2-го уровня:

- несанкционированное получение (в том числе копирование на отчуждаемый носитель) информации от коммутационной системы;
- получение идентификационных и аутентификационных данных пользователей (диспетчера, оператора);
- выведение из строя терминального оборудования;
- несанкционированное управление коммутационной системой;

- несанкционированное создание новых учетных записей;
- несанкционированное чтение, создание, изменение, удаление информации об абонентах;
- несанкционированное воздействие на систему биллинга с целью вывода её из строя (для сокрытия информации о попытках НСД);
- изменение первичной информации, формирующейся в коммутационной системе и передаваемой для дальнейшей обработки в биллинговую систему (снижение тарифа, занижение времени разговора, замена типа услуги и пр.);
- несанкционированное получение информации о трафике абонентов;
- получение исходной информации для последующей организации НСД (в частности анализ информации, поступающей на аварийный дисплей и выводящейся на принтер аварийной сигнализации);
- внесение изменений в настройки системы аварийной сигнализации для блокирования вывода (частичного блокирования вывода) аварийной информации с целью осуществления НСД или уничтожения регистрационной информации о попытках НСД;
- контроль и анализ изменений, производимых персоналом 1-го уровня управления с целью осуществления НСД, в том числе:
  - поиск и использование незаблокированных старых учетных записей;
  - поиск и использование учетных записей, предназначенных для тестирования;
  - поиск и использование новых учетных записей, находящихся в процессе создания;
- анализ компонент новых версий программного обеспечения с целью обнаружения уязвимых мест в системе защиты;
- запуск и выполнение программ, предназначенных для контроля действий других пользователей коммутационной системы;
- запуск потенциально опасных команд или программ с целью несанкционированного изменения привилегий пользователя, обхода системы защиты или обращения напрямую к блокам и устройствам коммутационной системы;
- вывод из строя оборудования коммутационной системы или системы аварийной сигнализации;
- установка и запуск программ, предназначенных для:
  - взлома или перехвата паролей, используемых персоналом,
  - изменение системного времени терминала с целью досрочного завершения пользователем работы с коммутационной системой,
  - перехвата информации, получаемой пользователем и последующего несанкционированного её копирования, в том числе на отчуждаемые носители информации;
- чтение остаточной информации из оперативной памяти или магнитных носителей;

– поиск паролей пользователей коммутационной системы, хранящихся в явном виде (на различных носителях информации, в том числе на бумажных и магнитных носителях информации).

Рассмотрим более подробно угрозы НСД ориентированные на уязвимости канала связи с системой биллинга.

Коммутационная система связана, с локальным оборудованием системы биллинга (терминал, ПК) и далее, через локальное оборудование системы биллинга, по каналу передачи информации с удаленной системой биллинга. Удаленная система биллинга представляет собой сервер (группу серверов) с установленной базой данных и локальной (возможно подключение по модему или через каналы передачи данных общего пользования) вычислительной сетью.

Для передачи данных между коммутационной системой и системой биллинга используется специальный протокол. В дальнейшем под системой биллинга понимается канал удаленного получения и обработки информации, все угрозы, действующие с удаленных терминалов системы биллинга, приравниваются к угрозам локального терминала системы биллинга.

Угрозы канала связи с системой биллинга:

– несанкционированное изменение, создание и удаление информации, несанкционированное повышение прав учетных записей, предназначенных для системы биллинга;
– перехват информации с использованием оборудования, подключаемого к каналу связи между коммутационной системой и системой биллинга.

Рассмотрим угрозы НСД ориентированные на уязвимости канала связи с удаленной системой управления и технического обслуживания. Канал не является защищенным выделенным каналом. Данный канал имеет физическую связь только с центром управления 1-го уровня и не имеет непосредственной физической связи с коммутационной системой, однако это не исключает перечисленные ниже угрозы.

Угрозы канала связи с удаленной системой управления и технического обслуживания:

– внедрение программных закладок, а также активизация программных закладок с целью реализации любых управляющих воздействий на коммутационную систему;
– удаленный вывод из строя, путем воздействия на управляющее оборудование ЦУЦС;
– несанкционированное получение информации через промежуточный носитель (т.е. первичным местом сбора информации является коммутационное оборудование ЦУЦС).

Рассмотрим угрозы НСД ориентированные на уязвимости канала связи с локальными терминалами.

Связь коммутационной системы может осуществляться с персональным компьютером с установленным программным обеспечением и выполняющим функции терминала.

Угрозы для канала связи с локальными терминалами:

- осуществление попыток соединения с коммутационной системой с целью подбора пароля;
- подключение к каналу передачи информации между коммутационной системой и терминалом;
- выполнение пользователем, подключившимся с терминала действий, направленных на нарушение нормального режима функционирования с коммутационной системы или с целью модификации первичной информации, поступающей в систему биллинга;
- несанкционированное получение информации (в том числе считывание информации с экрана монитора терминала);
- несанкционированное повышение уровня полномочий пользователя;
- подключение вместо штатного терминала другого устройства, выполняющего функции терминала (например, переносного компьютера) с установленным программным обеспечением, предназначенным для взлома системы защиты с коммутационной системы;

Угрозы для канала связи с локальными терминалами в случае использования персонального компьютера:

- несанкционированное получение информации, несанкционированное удаление, изменение, запись информации;
- повышение полномочий пользователя коммутационной системы;
- несанкционированное копирование информации (или вывод информации), в том числе на отчуждаемый носитель;
- установка и запуск программ, способствующих осуществлению НСД (взлом паролей, перехват паролей, перехват информации, идущей от пользователей коммутационной системы, восстановление остаточной информации из памяти и магнитных носителей информации, уничтожение информации хранимой на терминале, и пр.);
- запись на магнитные носители терминала с внешних носителей информации файлов, содержащих вирусы, запуск с внешних носителей информации инфицированных вирусами файлов и программ;
- подключение терминала помимо коммутационной системы к другим каналам связи (удаленные соединения с использованием модема и других устройств, соединение в локальную или распределенную сеть с другими персональными компьютерами (рабочими станциями, ноутбуками и пр.), не являющимися терминалами станции);
- соединение с использованием COM, LPT, USB разъемов;
- подключение дополнительных устройств ввода-вывода информации (в частности, дополнительных мониторов);

– соединение по инфракрасному каналу передачи данных;
– установка в терминальное оборудование дополнительных устройств (плат, блоков, схем) способствующих осуществлению НСД;
– хищение носителей информации (в том числе магнитных носителей терминального оборудования);
– некорректная работа оператора терминала (пользователя коммутационной системы), в том числе некорректное завершение сеанса связи, при котором злоумышленник может проникнуть в систему, используя учетную запись оператора;
– сообщение (разглашение) служебной информации лицам, по долгу службы не связанным с обработкой данной информации (в том числе раскрытие и(или) передача пароля (идентификатора учетной записи) другим лицам, сообщение сведений касающихся абонентов, абонентских линий связи, трафике абонентов, сведений о текущих настройках системы безопасности и системы аварийной сигнализации);

Угрозами для каналов связи с абонентами являются:

– осуществление удаленного управления коммутационной системой по цифровым каналам;
– незаконное подключение к линии связи, соединяющей абонента с коммутационной системой с последующей организацией перехвата абонентского трафика;
– анализ сигналов, выдаваемых коммутационной системой с целью незаконного подключения или несанкционированного использования служебных сервисов (встроенных разработчиком станции функций);
– использование абонентских линий связи с предварительно настроенным каналом НСД (предварительная настройка канала НСД выполняется либо в коммутационной системе, либо с помощью каналов удаленного управления);
– нарушение нормального функционирования абонентской линии связи и абонентского комплекта для изменения стоимости услуг, объема услуг (времени разговора) или нарушения работы системы тарификации;
– незаконное подключение к абонентской линии коммутационной системы с целью пользования абонентскими услугами без их оплаты.

Коммутационная система ЦАТС позволяет производить как локальное, так и удаленное управление с помощью команд специального языка. В связи с этим для нее характерны следующие типы угроз:

1) угрозы, действующие со стороны локальных терминалов и системы биллинга (угрозы оператора, перехват информации, несанкционированное управление, снятие информации и пр.);
2) угрозы, действующие на линии аварийной сигнализации (выведение из строя, подмена и выдача ложной информации, блокирование работы, косвенное управление блоками коммутационной системы);

3) угрозы с удаленных терминалов управления и угрозы организации каналов НСД (угрозы удаленных операторов управления, угрозы распределенного хранения информации, угрозы подключения к каналам связи, угрозы установки (подключения) дополнительного оборудования с целью несанкционированного доступа и пр.);
4) угрозы, действующие со стороны локальных терминалов (угрозы действий оператора, угрозы подключения дополнительных устройств с целью осуществления НСД и организации каналов НСД);
5) угрозы подключения терминалов и перехвата (управления) информации, передаваемой на магнитные носители;
6) угрозы подключения дополнительных устройств, блоков с целью перехвата информации (управления);
7) угрозы чтения остаточной информации и областей памяти, загрузка в память не декларированного кода;
8) угрозы подключения локальных терминалов и устройств вывода информации (принтеры), угрозы загрузки в процессор и выполнения недекларированного кода;
9) угрозы несанкционированного снятия информации, доступа к файлам, хищения и вывода из строя носителей информации;
10) угрозы хищения носителей, несанкционированного копирования на носители информации, угрозы внедрения в коммутационную систему недекларированного кода;
11) загрузка и выполнение недекларированного кода, перехват информации;
12) несанкционированное получение доступа к абонентским линиям связи, организация каналов прослушивания и перехвата абонентской информации;
13) угрозы нарушения работы, вывода из строя коммутационной системы, изменение тактовых импульсов с целью сокрытия информации о попытках НСД;
14) несанкционированное подключение с целью перехвата информации и организации каналов НСД;
15) организация каналов НСД, использование встроенных коммутационную систему функций для организации НСД;

Угрозы, действующие на блоки питания коммутационной системы (вывод из строя) в статье не рассматриваются.

Результаты анализа угроз информационной безопасности ЦАТС

Основными факторами, влияющими на уровень безопасности информации коммутационной системы ЦАТС, являются:

– наличие каналов удалённого управления 1-го и 2-го уровня, при этом учтен факт передачи информации по выделенным каналам с использованием сертифицированных криптографических средств защиты;

– наличие канала удалённого управления и технического обслуживания фирмы разработчика, имеющего подключение к ЦУЦС;
– наличие внешней системы биллинга;
– возможность подключения дополнительных удаленных терминалов;
– наличие открытых каналов связи;
– наличие распределенных хранилищ информации.

Наличие каналов удалённого управления 1-го и 2-го уровня позволяет реализовывать такие виды угроз, как:

– перехват, блокировка и подмена передаваемых данных; чтение, удаление и модификация циркулирующей информации;
– получения НСД к функциям и модулям коммутационной системы.

Оконечным оборудованием при реализации удаленного управления являются терминалы (ПК) операторов 1-го и 2-го уровней, подключенные соответственно к блокам OMC и MSW. С помощью средств локального терминала оператора возможна реализация таких видов угроз, как:

– несанкционированная модификация данных, хранимых на магнитных носителях,
– перехват информации, циркулирующей в коммутационной системе,
– перехват паролей пользователей,
– сокрытие факта несанкционированного доступа,
– блокирование вывода сигнальных сообщений операторам узлов OMC и MSW.

Фактором, способствующим возможности реализации этих угроз, является отсутствие технической и эксплуатационной документации по регламенту эксплуатации терминала оператора.

Наличие системы биллинга, управляемой по выделенному каналу с использованием протокола FTAM описывающего взаимодействие коммутационной системы с системой биллинга, снижает общий уровень безопасности, поскольку канал связи может быть использован для осуществления НСД. Существует возможность несанкционированного получения и копирования информации, в том числе на отчуждаемые носители информации, несанкционированного изменения как первичной (получаемой от коммутационной системы), так и непосредственно обрабатываемой в системе биллинга информации, связанной с тарифами и стоимостью абонентских услуг (время разговора, категория вызова, и пр.).

Предложения по построению комплексной системы безопасности информации в ЦАТС

Рекомендации, направленные на повышение уровня безопасности коммутационной системы разделены на группы:

1) организационно-технические мероприятия;
2) перечень действий, запрещенных лицам, имеющим физический доступ к оборудованию коммутационной системы.

Организационно-технические мероприятия. Основным каналом внешних угроз НСД является канал управления между коммутационной системы и узлами управления 1-го и 2-го уровня. Снижение вероятности возникновения угроз, действующих на центры управления 1-го и 2-го уровня, повышает общий уровень безопасности коммутационной системы. Необходимо отметить, что канал связи между коммутационной системой и узлами управления 1-го и 2-го уровня обычно имеет сертифицированную криптографическую защиту, что способствует блокированию несанкционированного подключения и перехвата информации; передача информации между коммутационной системой и узлами управления 1-го и 2-го уровня осуществляется по защищенному каналу связи. Кроме того, на объекте действует система ограничения физического доступа персонала в помещение с оборудованием коммутационной системы.

При использовании в качестве терминалов коммутационной системы персональных компьютеров и рабочих станций для предотвращения возможности несанкционированного изменения программной среды с использованием внешних устройств необходимо:

- демонтировать или опечатать устройства, позволяющие работать со сменными носителями информации (в качестве сменных носителей могут выступать: дискеты, CD, DVD - диски, кассеты (диски) стримеров, магнитные карты, переносные винчестеры и пр.);
- демонтировать или опечатать разъемы (блоки) подключения внешних устройств, в качестве которых могут выступать COM, LPT, USB, ИК порты, дополнительные видеокарты, дополнительные сетевые карты и пр.);
- запретить выполнение на персональных компьютерах и рабочих станциях, используемых в качестве терминалов коммутационной системы работ, не входящих в список регламентных.

Перечень действий, запрещенных лицам, имеющим физический доступ к оборудованию коммутационной системы.

Необходимо опечатать все терминальные устройства с целью исключения возможности установки в них дополнительных компонентов (устройств, печатных плат, и пр.)

Необходимо блокировать возможность подключения дополнительных устройств, не входящих в список штатного оборудования, для чего все коммутационные линии, соединяющие терминалы с коммутационной системой , блоками MSW и OMC, должны быть физически недоступны, должны отсутствовать дополнительные точки подключения на линиях связи от устройства коммутации до терминалов.

Поскольку для хранения и обработки информации коммутационной системой используется система распределенного хранения информации, необходимо обеспечить защиту информации на всех местах её обработки и хранения. В частности, НСД к информации может осуществляться в системе биллинга, поэтому необходимо ограничить доступ операторов системы биллинга к информации, хранимой в базе данных системы биллинга,

использовать вычислительную технику и программное обеспечение, соответствующее требованиям по защите информации.

Необходимо исключить удаленный доступ к информации по модемным соединениям и с использованием переносной вычислительной техники (ноутбуков), для этого все возможные точки подключения такой техники должны быть опечатаны.

Необходимо в документальной форме установить регламент работы и права доступа операторов коммутационной системы. Необходимо вести регистрацию и учет действий операторов коммутационной системы с помощью журналов регистрации и учета, в которых отражаются такие изменения, как:

- регистрация и учет новых операторов,
- создание и удаление учетных записей операторов,
- повышение и ограничение прав операторов,
- изменение конфигурации и настроек программно-аппаратного обеспечения коммутационной системы, терминалов операторов, локальных сетей терминалов, узлов управления, баз данных и хранилищ информации.

Вывод

В статье проведен анализ угроз информационной безопасности типовой ЦАТС. На основе проведенного анализа сформулированы ппредложения по построению комплексной системы безопасности информации в ЦАТС. Данные предложения носят прикладной характер и могут быть использованы операторами фиксированной и подвижной связи для повышения уровня информационной безопасности своих объектов.

Литература

1. РД АС – Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Руководящий документ. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. – М.: ФСТЭК России, 1992.

2. ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования/ – М.: Издательство стандартов, 1995.

3. РД МЭ – Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Руководящий документ. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 25 июля 1997 г. – М.: ФСТЭК России, 1997.

4. Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также

объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды. Утвержден приказом ФСТЭК России № 31 от 14 марта 2014 г. – М.: ФСТЭК России, 2014.

References

1. *Avtomatizirovannye sistemy. Zashchita ot nesanktsionirovannogo dostupa k informatsii. Klassifikatsiia avtomatizirovannykh sistem i trebovaniia po zashchite informatsii. Rukovodiashchii dokument* [Automated systems. Protection against unauthorized access to information. Automated systems classification and requirements for protection of information. Guidance document]. Approved by the decision of the Chairman of the State technical Commission under the President of the Russian Federation dated 30 March 1992. Moscow, FSTEC of Russian, 1992.

2. Standart 50739-95. *Sredstva vychislitel'noi tekhniki. Zashchita ot nesanktsionirovannogo dostupa k informatsii. Obshchie tekhnicheskie trebovaniia* [Computer equipment. Protection against unauthorized access to information. General technical requirements]. Moscow, Izdatel'stvo Standartov Publ., 1995.

3. Sredstva vychislitel'noi tekhniki. Mezhsetevye ekrany. Zashchita ot nesanktsionirovannogo dostupa k informatsii. Pokazateli zashchishchennosti ot nesanktsionirovannogo dostupa k informatsii. Rukovodiashchii dokument [computing facilities. Firewalls. Protection against unauthorized access to information. Indicators of protection against unauthorized access to information. Guidance document] Approved by the decision of the Chairman of the State technical Commission under the President of the Russian Federation of 25 July 1997. Moscow, State Technical Commission of Russia, 1997.

4. *Trebovaniia k obespecheniiu zashchity informatsii v avtomatizirovannykh sistemakh upravleniia proizvodstvennymi i tekhnologicheskimi protsessami na kriticheski vazhnykh ob"ektakh, potentsial'no opasnykh ob"ektakh, a takzhe ob"ektakh, predstavliaiushchikh povyshennuiu opasnost' dlia zhizni i zdorov'ia liudei i dlia okruzhaiushchei prirodnoi sredy* [Requirements for ensuring information protection in automated control systems of production and technological processes at critically important objects, potentially hazardous objects and objects posing a danger to life and health of people and the environment]. Approved by the order of the FSTEC of Russia No. 31 of March 14, 2014. Moscow, FSTEC of Russian, 2014.

Информация об авторах

Осовецкий Леонид Георгиевич – доктор технических наук, профессор, лауреат государственной премии совета министров СССР. Советник генерального директора. Ленинградское отделение Центрального научно-исследовательского института связи (ЛО ЦНИИС). Область научных интересов: информационная безопасность, безопасность программных средств. E–mail: leoned.osovetsky@gmail.com

Ефимов Вячеслав Викторович – кандидат технических наук, доцент. Директор института. Ленинградское отделение Центрального научно-исследовательского института связи (ЛО ЦНИИС). Область научных

интересов: инновационные решения и перспективы развития транспортных сетей связи. E–mail: vve@loniis.ru

Адрес: Россия, 196128, Санкт-Петербург, ул. Варшавская, 11.

Comprehensive Analysis of the Level of Information Security for the Private Branch Exchange

L. G. Osovetskiy, V. V. Efimov

Purpose. *Network of voice communications are actively developing at the present time. These networks are based on the private branch exchange (PBX). The actual applied task is providing of information security of PBX.* ***The purpose*** *of this paper is the justification of organizational and technical recommendations to improve information security level of PBX. This justification is done by analyzing the model of PBX and the characteristics of its elements. The method used in paper is the multivariate systematic analysis.* ***Results.*** *The descriptive model of threats was formulated for the typical PBX on the basis of the analysis of the structure of PBX and threats which typical for its elements. Main vulnerabilities of PBX is formed as to the system as a whole and for its separate elements based on a threat model. Recommendations about carrying out of organizational-technical actions directed on increase of level of information security is offered on the basis of systematic analysis of vulnerabilities of the PBX.* ***Practical significance.*** *Organizational and technical measures which are proposed in the paper can be used by operators of fixed and mobile communications to improve information security level of the PBX which used by them.*

Keywords: *PBX, security threats, software PBX*.

Information about Authors

Leonid Georgievich Osovetskiy – Dr. habil. of Engineering Sciences, Professor, Advisor of CEO. Leningrad Branch of Central Science Research Telecommunication Institute (LO ZNIIS). Field of research: information security, security software. E–mail: leoned.osovetsky@gmail.com

Vyacheslav Viktorovich Efimov – Ph.D. of Engineering Sciences, Associate Professor. CEO of Institute. Leningrad Branch of Central Science Research Telecommunication Institute (LO ZNIIS). Field of research: innovations in telecommunications. E–mail: vve@loniis.ru

Address: Russia, 196128, Saint Petersburg, Varshavskaya str., 11.