МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 629.4.067

ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ПОДСИСТЕМАХ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ ОПЕРАТИВНОГО УПРАВЛЕНИЯ ПЕРЕВОЗКАМИ НА ЖЕЛЕЗНОДОРОЖНОМ ТРАНСПОРТЕ

Клепцов М.Я.[*], **Любимова Л.В.**[**]
[*]Московский государственный университет путей сообщения, г. Москва
[**]ОАО «НИИАС», г. Москва

Поступила в редакцию 06.03.2013, после переработки 25.11.2014.

В статье рассматриваются вопросы защиты персональных данных в автоматизированных системах на железнодорожном транспорте.

Ключевые слова: персональные данные, информационная система персональных данных, система защиты персональных данных, локальная вычислительная сеть, сеть передачи данных, защита информации.

Вестник ТвГУ. Серия: Прикладная математика. 2015. № 2. С. 147–161.

Введение

Железнодорожный транспорт, являясь одной из ключевых отраслей Российской Федерации, играет важную роль в экономике страны и в жизни ее граждан. Компьютерные системы предприятий и компаний данной отрасли имеют многоуровневую распределенную архитектуру, которая характеризуется тем, что в них производится обработка и хранение персональных данных. Поэтому важной составляющей компьютерной системы является обеспечение защиты персональных данных (ПДн).

Необходимость защиты персональных данных российскими предприятиями и организациями определена требованиями федерального закона №152 «О персональных данных», который был принят и вступил в силу в конце февраля 2007 года. Для обеспечения требуемого уровня защиты информации и минимизации возможных потерь информации от различных угроз, для обеспечения гарантий выполнения требований безопасности и условий для эффективного выполнения основных задач системы необходимо создать систему защиты персональных данных.

Для решения этой задачи предлагается следующий подход к решению проблемы защиты персональных данных для автоматизированной системы оперативного управления перевозками (АСОУП), которая предназначена для автоматизации функций учета и контроля, а также автоматизации задач анализа, прогнозирования и планирования перевозочного процесса по сети дорог ОАО «РЖД».

Суть данного подхода заключается в том, что в первую очередь, необходимо:

– Произвести анализ программно-технической среды обработки ПДн;

– Разработать модель угроз персональных данных при их обработке в АСОУП;

– Сформулировать требования к структуре и функциям подсистем системы защиты персональных данных (СЗПДн).

Так как в АСОУП требуется обеспечение не только конфиденциальности ПДн, но и их целостности и доступности, необходимо произвести построение модели угроз безопасности персональных данных, выявить перечень актуальных угроз и оценить возможный ущерб от их реализации.

1. Описание системы

Автоматизированная система оперативного управления перевозками является распределенной, включает в свой состав ряд локальных вычислительных сетей (ЛВС), работающих в режиме реального времени.

Компоненты АСОУП, серверы и автоматизированные рабочие места (АРМ) пользователей размещены в пределах контролируемых зон (КЗ), в которых предусмотрен контроль доступа и средства физической охраны.

Пользователями компьютерной системы АСОУП являются сотрудники линейных предприятий, работа которых поддерживается соответствующими АРМ или терминальными станциями.

Алгоритм работы системы состоит в том, что пользователям, в режиме реального времени, предоставляется информация из единой дорожной базы, состоящей из следующих моделей управления движением поездов:

– Поездной модели;

– Вагонной модели;

– Контейнерной модели;

– Модели погрузки-выгрузки;

– Отправочной модели;

– Локомотивной модели;

– Бригадной модели.

Бригадная модель дороги (БМД) и Оперативный контроль дислокации и состояния локомотивных бригад (ОКДБ) являются подсистемами (функциональными подзадачами) АСОУП. Они предназначены для организации оперативного контроля за наличием, состоянием и дислокацией локомотивных бригад (машинистов, помощников машинистов, машинистов-инструкторов) дороги на основе создания бригадной модели дороги (БМД) при поступлении информационных сообщений о движении поезда, локомотива и бригады, об операциях с бригадой в депо и поездке бригады пассажиром.

В БМД, ОКДБ обрабатываются следующие персональные данные:

- Код дороги приписки;
- Код депо приписки;
- Табельный номер работника;
- Фамилия, имя, отчество работника;
- Дата рождения работника;
- Код станции местожительства;
- Профессия (код должности) (классификатор);
- Дата вступления работника в должность;
- Остальные сведения представлены в виде специфических кодов и не относятся к персональным данным работников.

Рассматриваемая система является информационной системой, обрабатывающей персональные данные сотрудников оператора.

Для рассматриваемой системы актуальны угрозы 3-го типа, так как для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

В рассматриваемой системе обрабатываются персональные данные менее чем 1000 субъектов персональных данных.

Устанавливается необходимость обеспечения 3-го уровня защищенности персональных данных при их обработке в данной системе.

Характеристики безопасности обрабатываемых персональных данных типовые.

По структуре рассматриваемая система является распределенной информационной системой – комплексом автоматизированных рабочих мест и (или) локальных информационных систем, объединенных в единую информационную систему средствами связи с использованием технологии удаленного доступа без подключения к сетям общего пользования.

Режим обработки ПДн многопользовательский с разграничением прав доступа.

Все технические средства рассматриваемой информационной системы находятся в пределах Российской Федерации.

2. Модель угроз

В документе «Базовая модель угроз персональных данных при их обработке в информационных системах персональных данных» (далее «Базовая модель угроз»), утвержденном Федеральной службой по техническому и экспортному контролю (ФСТЭК) России 18 февраля 2008 года содержится систематизированный перечень угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

Для того чтобы определить возможные угрозы информационной безопасности для АСОУП БМД, ОКДБ необходимо рассмотреть вероятных нарушителей и информационные активы потенциально подверженные угрозам информационной безопасности.

По признаку принадлежности к АСОУП БМД, ОКДБ все нарушители делятся на две группы:

– внешние нарушители – физические лица, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование АСОУП БМД, ОКДБ;

– внутренние нарушители – физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование АСОУП БМД, ОКДБ.

В качестве внешнего нарушителя информационной безопасности, рассматривается нарушитель, который не имеет непосредственного доступа к техническим средствам и ресурсам системы, находящимся в пределах контролируемой зоны.

Предполагается, что внешний нарушитель не может воздействовать на защищаемую информацию через каналы связи, ввиду отсутствия подключений АСОУП БМД, ОКДБ к сетям связи общего пользования, а также достаточной трудоемкости возможности необнаруженного несанкционированного подключения к сети передачи данных ОАО «РЖД».

Предполагается также, что внешний нарушитель не может воздействовать на защищаемую информацию по техническим каналам утечки, а также осуществлять съем акустической информации, вследствие реализации необходимых препятствующих организационных и режимных мер защиты информации. Объем и характер информации, хранимой и обрабатываемой на остальных объектах рассматриваемой системы, а также акустической информации, является недостаточным для возможной мотивации внешнего нарушителя к осуществлению действий, направленных на утечку информации по техническим каналам утечки.

Таким образом, возможные действия нарушителя по отношению к защищаемым активам АСОУП БМД, ОКДБ являются маловероятными и в настоящей модели не рассматриваются.

Возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны ограничительных факторов, из которых основным является реализация комплекса организационно-технических мер, в том числе по подбору, расстановке и обеспечению высокой профессиональной подготовки кадров, допуску физических лиц внутрь контролируемой зоны и контролю за порядком проведения работ, направленных на предотвращение и пресечение несанкционированных действий.

Исходя из особенностей функционирования рассматриваемой системы, допущенные к ней физические лица, имеют разные полномочия на доступ к информационным, программным, аппаратным и другим ресурсам АСОУП БМД, ОКДБ в соответствии с принятой политикой информационной безопасности (правилами).

По отношению к защищаемым активам в БДМ, ОКДБ выделим семь категории лиц:

– администраторы (категория I);

- технический персонал (сотрудники эксплуатационных подразделений, осуществляющие техническое сопровождение оборудования, программного обеспечения и средств защиты информации) (категория II);
- пользователи (категория III);
- пользователи других систем ОАО «РЖД», являющихся внешними по отношению к АСОУП БМД, ОКДБ (категория IV);
- сотрудники ОАО «РЖД», имеющие санкционированный доступ в служебных целях в помещения, в которых размещаются активы АСОУП БМД, ОКДБ, но не имеющие права доступа к этим активам (категория V);
- обслуживающий персонал подразделений ОАО «РЖД» (охрана, работники инженерно–технических служб и т.д.) (категория VI);
- уполномоченный персонал разработчиков АСОУП БМД, ОКДБ, который имеет право на техническое обслуживание и модификацию компонентов программного обеспечения АСОУП БМД, ОКДБ (категория VII).

К лицам категории I относятся:

- администраторы АСОУП БМД, ОКДБ – группа пользователей системы, сопровождающая АСОУП БМД, ОКДБ и обеспечивающая функционирование системы;
- сетевые администраторы – обеспечивающие управление сетевым оборудованием АСОУП БМД, ОКДБ;
- администраторы информационной безопасности – обеспечивающие функционирование, управление и мониторинг внешних средств защиты информации; осуществляющие координацию взаимодействия с администраторами АСОУП БМД, ОКДБ и сетевыми администраторами по вопросам обеспечения защиты информации.

Согласно «Базовой модели угроз» эти лица соответствуют потенциальным нарушителям пятой категории (зарегистрированные пользователи с полномочиями системного администратора ИСПДн) и шестой категории (зарегистрированные пользователи с полномочиями администратора безопасности ИСПДн).

К лицам категории II в АСОУП БМД, ОКДБ относятся сотрудники эксплуатационных подразделений, осуществляющие техническое сопровождение оборудования, программного обеспечения и средств защиты информации.

На лиц категории I и II возложены задачи по администрированию и техническому сопровождению программно-аппаратных средств АСОУП БМД, ОКДБ, обслуживанию и настройки средств защиты информации, а так же сетевого и телекоммуникационного оборудования.

Предполагается, что к лицам категорий I и II ввиду их исключительной роли в АСОУП БМД, ОКДБ должен применяться комплекс особых организационно-режимных мер по их подбору, принятию на работу, назначению на должность и контролю выполнения функциональных обязанностей. Предполагается, что в

число лиц категории I и II будут включаться только доверенные лица и поэтому указанные лица исключаются из числа вероятных нарушителей.

К лицам категории III в АСОУП БМД, ОКДБ относятся пользователи линейных предприятий (локомотивных депо), непосредственно осуществляющие ввод, корректировку и удаление персональных данных работников локомотивных депо (машинистов, помощников машинистов, машинистов-инструкторов). К таким пользователям относятся сотрудники отделов кадров и нарядчики локомотивных депо.

Согласно «Базовой модели угроз» эти лица соответствуют потенциальным нарушителям второй категории (зарегистрированные пользователи ИСПДн, осуществляющие ограниченный доступ к ресурсам ИСПДн с рабочего места) и третьей категории (зарегистрированные пользователи ИСПДн, осуществляющие удаленный доступ к ПДн по распределенной информационной системе).

Лица категорий IV, V и VI согласно «Базовой модели угроз» соответствуют потенциальными нарушителями первой категории (лица, имеющие санкционированный доступ к ИСПДн, но не имеющие доступа к ПДн).

Лица категории VII согласно «Базовой модели угроз» соответствуют потенциальными нарушителями седьмой категории (программисты-разработчики (поставщики) прикладного программного обеспечения и лица, обеспечивающие его сопровождение на защищаемом объекте) и восьмой категории (разработчики и лица, обеспечивающие поставку, сопровождение и ремонт технических средств на ИСПДн).

Для рассматриваемой системы лица категорий III-VII относятся к вероятным нарушителям.

Информационными активами АСОУП БМД, ОКДБ, потенциально подверженными угрозам информационной безопасности являются следующие:

- Целевая информация (персональные данные):
  - Код дороги приписки;
  - Код депо приписки;
  - Табельный номер работника;
  - Фамилия, имя, отчество работника;
  - Дата рождения работника;
  - Код станции местожительства;
  - Профессия (код должности) (классификатор);
  - Дата вступления работника в должность;
- Технологическая информация:
  - защищаемая управляющая информация (конфигурационные файлы, настройки средств защиты информации и пр.);
  - защищаемая технологическая информация средств доступа к системе управления АСОУП БМД, ОКДБ (аутентификационная информация и др.);

  - информация о системе защиты информации, ее структуре, принципах и технических решениях защиты.

- Программное обеспечение:

  - программные информационные ресурсы АСОУП БМД, ОКДБ, содержащие общее и специальное программное обеспечение, резервные копии программного обеспечения, инструментальные средства и утилиты систем управления ресурсами АСОУП БМД, ОКДБ, чувствительные по отношению к случайным и несанкционированным воздействиям, программное обеспечение средств ЗИ.

Хранимая и обрабатываемая в АСОУП БМД, ОКДБ информация в соответствии с «Положением об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденным Постановлением Правительства РФ от 17 ноября 2007 г. № 781, относится к персональным данным.

Согласно «Базовой модели угроз» целью реализации угроз является нарушение определенных для объекта угрозы характеристик безопасности (конфиденциальность, целостность, доступность) или создание условий для нарушения характеристик безопасности объекта угрозы.

Учитывая условия функционирования АСОУП БМД, ОКДБ, возможными каналами реализации угроз информационной безопасности являются:

- каналы непосредственного доступа к защищаемым активам (визуальный просмотр, физический доступ, использование съемных носителей информации и т.п.);

- каналы доступа, образованные с использованием штатных средств АСОУП БМД, ОКДБ;

- каналы доступа, образованные с использованием доступных нарушителю (не являющихся штатными) технических средств и программного обеспечения.

Так образом можем сделать вывод, что возможными угрозами информационной безопасности для АСОУП БМД, ОКДБ являются:

Угроза 1 – осуществление несанкционированного доступа к целевой информации (персональные данные), хранимой и обрабатываемой в АСОУП БМД, ОКДБ.

Угроза 2 – осуществление несанкционированной модификации и блокировки целевой информации, хранимой и обрабатываемой в АСОУП БМД, ОКДБ.

Угроза 3 – осуществление несанкционированного ознакомления с конфигурационными файлами и настройками средств защиты информации.

Угроза 4 – осуществление несанкционированной модификации конфигурационных файлов, настроек средств защиты информации и программного обеспечения.

Угроза 5 – нарушение режимов функционирования программно-технических средств АСОУП БМД, ОКДБ.

Угроза 6 – осуществление несанкционированного доступа к передаваемой защищаемой информации.

Угроза 7 – осуществление перехвата акустической (речевой) информации.

Угроза 8 – несанкционированные действия, связанные с поиском и использованием уязвимостей элементов АСОУП БМД, ОКДБ.

Для того чтобы выбрать из возможных угроз те, которые являются актуальными для рассматриваемой системы, воспользуемся документом «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденным Федеральной службой по техническому и экспортному контролю (ФСТЭК) России 14 февраля 2008 года.

Исследования автоматизированной системы оперативного управления перевозками по определению показателей, применяемых для оценки возможности реализации угрозы, проводились авторами статьи в рамках работ по Защите информационных систем персональных данных ОАО «РЖД». В ходе проведения данных работ авторами были определены актуальные угрозы безопасности ПДн. Актуальными являются угрозы 1 – 5, неактуальными – 6 – 8.

На основании анализа актуальности выявленных угроз безопасности, для достижения требуемого уровня защиты следует осуществить следующие мероприятия:

- организационные;
- технические;
- контролирующие.

3. Требования к системе

Требования к структуре и функционированию системы защиты персональных данных АСОУП БМД, ОКДБ:

В состав СЗПДн АСОУП БМД, ОКДБ должны входить следующие основные подсистемы:

- подсистема управления доступом;
- подсистема регистрации и учета;
- подсистема обеспечения целостности;
- подсистема антивирусной защиты;
- подсистема межсетевого экранирования.

В состав СЗПДн АСОУП БМД, ОКДБ должны входить следующие типы программно-технических средств:

- межсетевые экраны для организации единой защищенной точки доступа к хранилищам информации АСОУП БМД, ОКДБ;
- сертифицированные по требованиям ФСТЭК России серверные и клиентские операционные системы;

- сертифицированное антивирусное программное обеспечение;
- средства гарантированного уничтожения информации;
- программное обеспечение для резервного копирования конфигурационных данных средств защиты информации.

СЗПДн АСОУП БМД, ОКДБ должна обеспечивать следующие базовые сервисы:

1. управление информационной безопасностью;
2. идентификацию пользователей;
3. аутентификацию пользователей;
4. разграничение и контроль доступа пользователей к ресурсам и объектам инфраструктуры системы;
5. регистрацию пользователей и управление учетными записями;
6. межсетевое экранирование;
7. очистку памяти;
8. регистрацию событий, связанных с подключением пользователей, доступом к объектам системы, отключением пользователей.

На основании этого можно разработать комплекс требований к системе защиты персональных данных АСОУП БМД, ОКДБ:

1. Требования к подсистеме управления доступом:
   (a) Каждый администратор и пользователь должен иметь уникальные идентификатор и пароль.
   (b) Должна осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов.
   (c) Допуск к защищаемой информации лиц, работающих в АСОУП БМД, ОКДБ (пользователей, обслуживающего персонала), должен производиться в соответствии с порядком, установленным разрешительной системой допуска.
   (d) Необходимо разграничивать доступ пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации.
2. Требования к подсистеме регистрации и учёта:
   (a) Необходимо регистрировать действия пользователей АСОУП БМД, ОКДБ и обслуживающего персонала, контролировать несанкционированный доступ и действия пользователей, обслуживающего персонала и посторонних лиц.

(b) Должна осуществляться регистрация входа (выхода) субъекта доступа в систему (из системы), либо регистрация загрузки и инициализации ОС и её программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АСОУП БМД, ОКДБ. В параметрах регистрации указываются:

- дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
- результат попытки входа (успешная или неуспешная – несанкционированная);
- идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа.

(c) Должна осуществляться регистрация выдачи печатных (графических) документов на "твердую"копию. В параметрах регистрации указываются:

- дата и время выдачи (обращения к подсистеме вывода);
- спецификация устройства выдачи (логическое имя (номер) внешнего устройства);
- краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа;
- идентификатор субъекта доступа, запросившего документ.

(d) Должна осуществляться регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов. В параметрах регистрации указываются:

- дата и время запуска;
- имя (идентификатор) программы (процесса, задания);
- идентификатор субъекта доступа, запросившего программу (процесс, задание);
- результат запуска (успешный, неуспешный - несанкционированный).

(e) Должен проводиться учёт всех защищаемых носителей информации с помощью их маркировки и с занесением учётных данных в журнал (учётную карточку).

(f) Должен проводиться учёт защищаемых носителей информации в журнале (картотеке) с регистрацией их выдачи (приёма).

(g) Должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти устройства и внешних накопителей. Очистка осуществляется однократной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов).

3. Требования к подсистеме обеспечения целостности:

(a) Должна быть обеспечена целостность программных средств защиты в составе системы защиты информации, а также неизменность программной среды. При этом:

- целостность средств защиты проверяется при загрузке системы по контрольным суммам компонент средств защиты информации;
- целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации.

(b) Должно проводиться периодическое тестирование функций системы защиты информации при изменении программной среды и персонала АСОУП БМД, ОКДБ с помощью тест-программ.

(c) Должны быть в наличии средства восстановления системы защиты информации, предусматривающие ведение двух копий программных средств защиты информации и их периодическое обновление и контроль работоспособности.

4. Требования к подсистеме антивирусной защиты:

(a) Должна проводиться автоматическая проверка на наличие вредоносных программ (ВП) или последствий программно-математических воздействий (ПМВ) при импорте в АСОУП БМД, ОКДБ всех программных модулей (прикладных программ), которые могут содержать ВП, по их типовым шаблонам и с помощью эвристического анализа.

(b) Должны быть реализованы механизмы автоматического блокирования обнаруженных ВП путём их удаления из программных модулей или уничтожения.

(c) Должна регулярно выполняться проверка на предмет наличия ВП в средствах защиты от ПМВ (при первом запуске средства защиты от ПМВ и с установленной периодичностью).

(d) Факт выявления ПМВ должен инициировать автоматическую проверку на наличие ВП.

(e) Должен быть реализован механизм отката для установленного числа операций удаления ВП из оперативной или постоянной памяти, из программных модулей и прикладных программных средств, содержащих ВП.

(f) Должно предотвращаться внедрение в АСОУП БМД, ОКДБ программ-вирусов, программных закладок.

5. Требования к подсистеме межсетевого экранирования:

(a) Должно проводиться межсетевое экранирование, при этом межсетевой экран (МЭ) должен выполнять следующие функции:

- фильтрация для каждого сетевого пакета независимо;
- идентификация и аутентификация администратора МЭ при его локальных запросах на доступ;
- возможность для идентификации и аутентификации по идентификатору (коду) и паролю условно-постоянного действия;

- регистрация входа (выхода) администратора МЭ в систему (из системы) либо загрузки и инициализации системы и её программного останова;
- контроль целостности своей программной и информационной части;
- фильтрация пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;
- фильтрация с учётом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов;
- фильтрация с учётом любых значимых полей сетевых пакетов;
- восстановление после сбоев и отказов оборудования;
- возможность регламентного тестирования реализации правил фильтрации, процесса идентификации, аутентификации и регистрации действий администратора МЭ, контроля целостности программной и информационной части МЭ, восстановления после сбоев и отказов.

6. Требования к техническим средствам:
   (a) В АСОУП БМД, ОКДБ должно осуществляться резервирование технических средств и дублирование массивов информации.
7. Требования к средствам защиты информации
   (a) Подключение АСОУП БМД, ОКДБ к другой автоматизированной системе (локальной или распределенной вычислительной сети) должно осуществляться с использованием МЭ, требования к которым определяются руководящие документы ФСТЭК России.

Основываясь на сделанных выше выводах, ввиду неактуальности ряда угроз информационной безопасности, при создании СЗПДн АСОУП БМД, ОКДБ допускается не реализовывать:

- требования по защите информации от утечек по ПЭМИН (побочные электромагнитные излучения и наводки);
- требования по защите информации от перехвата при ее передаче;
- требования по анализу защищенности элементов АСОУП БМД, ОКДБ;
- требования защиты информации по управлению потоками информации на основе меток конфиденциальности.

Заключение

Общей целью создания системы защиты персональных данных АСОУП БМД, ОКДБ является обеспечение требуемого уровня защиты информации ограниченного распространения и минимизация возможных потерь информации от различных угроз, обеспечение гарантий выполнения требований безопасности и условий для эффективного выполнения основных задач системы.

Обеспечение безопасности персональных данных осуществляется путем выполнения комплекса организационных и технических мероприятий, реализуемых в рамках создаваемой системы защиты персональных данных.

Создание системы защиты, в том числе, направлено на обеспечение условий, исключающих возможность несанкционированного доступа к защищаемой информации, результатом которого могут стать модификация, уничтожение, блокирование, копирование, распространение данных, а также иные несанкционированных действия.

Система защиты включает организационные меры и технические средства защиты информации, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных, а также используемые в информационной системе информационные технологии.

При обработке персональных данных в информационной системе должно быть обеспечено:

- проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;
- своевременное обнаружение фактов несанкционированного доступа к персональным данным;
- недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
- возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- постоянный контроль за обеспечением уровня защищенности персональных данных.

Список литературы

[1] «Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденное Постановлением Правительства Российской Федерации № 781 от 17 ноября 2007 г.

[2] «Требования к защите персональных данных при их обработке в информационных системах персональных данных», утвержденные Постановлением Правительства Российской Федерации N 1119 от 1 ноября 2012 г.

[3] «Базовая модель угроз персональных данных при их обработке в информационных системах персональных данных», утвержденная Федеральной службой по техническому и экспортному контролю (ФСТЭК) России от 18 февраля 2008 г.

[4] «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденная Федеральной службой по техническому и экспортному контролю (ФСТЭК) России 14 февраля 2008 г.

[5] Федеральный закон №152 «О персональных данных» от 27 июля 2006 г.

[6] Материалы по обследованию ИСПДн: «Автоматизированная система оперативного управления перевозками Бригадная модель дороги, Оперативный контроль дислокации и состояния локомотивных бригад».

Библиографическая ссылка

Клепцов М.Я., Любимова Л.В. Обеспечение защиты персональных данных в подсистемах автоматизированной системы оперативного управления перевозками на железнодорожном транспорте // Вестник ТвГУ. Серия: Прикладная математика. 2015. № 2. С. 147–161.

Сведения об авторах

1. **Клепцов Михаил Яковлевич**
   профессор кафедры управления и защиты информации Московского государственного университета путей сообщения (МИИТ).

   Россия, 127994, г. Москва, ул Образцова, д 9, стр. 9. E-mail: mkleptsov@mail.ru.

2. **Любимова Лариса Владимировна**
   сотрудник научно-исследовательского и проектно-конструкторского института информатизации, автоматизации и связи на железнодорожном транспорте.

   Россия, 109029, г. Москва, Нижегородская ул., д. 27, стр. 1, ОАО «НИИАС». E-mail: lv.lyubimova@gmail.com.

SECURITY OF PERSONALLY IDENTIFIABLE INFORMATION IN THE SUBSYSTEMS OF AUTOMATED SYSTEM OF OPERATIONAL MANAGEMENT OF TRANSPORTATION IN THE RAILWAY TRANSPORT

Kleptsov Mikhail Yakovlevich
Professor of Management and Information Protection department,
Moscow State University of Railway Engineering (MIIT)
Russia, 127994, Moscow, 9 Obraztsova str, building 9. E-mail: mkleptsov@mail.ru

Lyubimova Larisa Vladimirovna
Institute of Information Systems, Automation and Communication
in Railway Transport
Russia, 109029, Moscow, 27 Nizhegorodskaya str, building 1.
E-mail: lv.lyubimova@gmail.com

Received 06.03.2013, revised 25.11.2014.

The article deals with the protection of personal data in automated systems for rail transport.

Keywords: personal data, information systems of personal data, protection system of personal data, local area network, data network, information protection.

Bibliographic citation

Kleptsov M.Ya., Lyubimova L.V. Security of personally identifiable information in the subsystems of automated system of operational management of transportation in the railway transport. *Vestnik TvGU. Seriya: Prikladnaya matematika* [Herald of Tver State University. Series: Applied Mathematics], 2015, no. 2, pp. 147–161. (in Russian)