МОДЕЛЬ ОБЕСПЕЧЕНИЯ КРИТЕРИЕВ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В РЕШЕНИЯХ ПОДСИСТЕМЫ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

А.Н. Вознюк, Г.В. Тумуров

Подсистема технической защиты информации (ПТЗИ) является важнейшей составляющей системы защиты информации объектов информатизации (ОИ) на предприятии. Главным целевым содержанием ПТЗИ является обеспечение безопасности информации. В свою очередь безопасность информации обеспечивается по определенным критериям. Существующие модели обеспечения критериев безопасности информации в недостаточной мере четко и ясно формируют представление о ее структуре, составе и содержании, что создает проблематику эффективного обеспечения информационной безопасности на предприятии. В связи с этим, в целях оптимизации обеспечения информационной безопасности объектов защиты, целесообразна разработка системной модели обеспечения критериев безопасности информации в решениях ПТЗИ.

Безопасность информации (данных): Состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность [1]. Исходя из этого, основными критериями безопасности информации являются конфиденциальность, доступность, целостность.

Правовое понятие конфиденциальности определено, как обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя [2]. Вместе с этим это понятие требует уточнения с точки зрения технической защиты информации. При этом необходимо принять во внимание, что конфиденциальность так же определена в [3], как состояние информации [ресурсов автоматизированной системы], при котором доступ к ней [к ним] осуществляют только субъекты, имеющие на него право. Учитывая изложенное, представляется возможным переформулировать понятие конфиденциальности следующим образом:

Конфиденциальность информации [ресурсов автоматизированной системы]: состояние защищенности информации [ресурсов автоматизированной системы], при котором несанкционированный доступ (НСД) к ней (к ним) исключен.

Целостность (информации [ресурсов автоматизированной системы]): Состояние защищенности информации [ресурсов автоматизированной системы], при котором ее [их] изменение осуществляется только преднамеренно субъектами, имеющими на него право [3].

Доступность (информации [ресурсов автоматизированной системы]): Состояние защищенности информации [ресурсов автоматизированной системы], при котором субъекты, имеющие право доступа, могут реализовать их беспрепятственно [3].

В качестве структурного базиса модели обеспечения критериев безопасности информации представляется целесообразным использовать обобщенную модель ПТЗИ ОИ [4], представленную на рисунке 1.

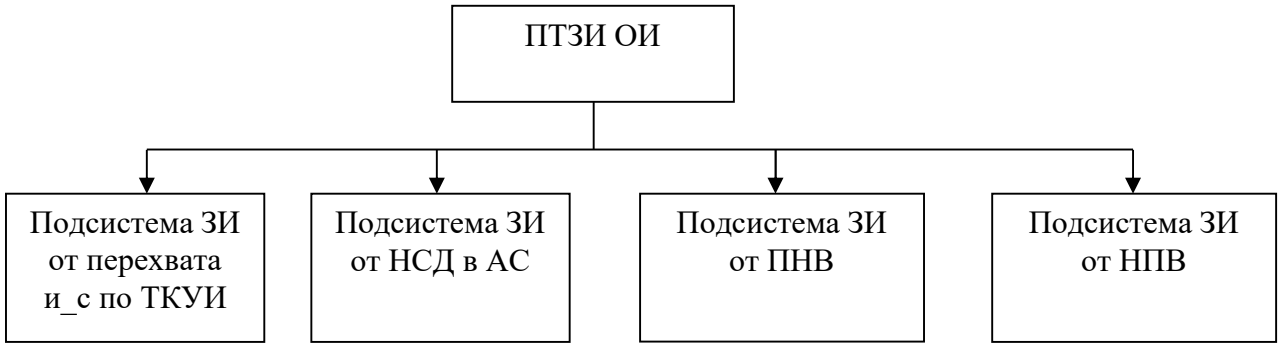

Рисунок 1 – Обобщенная модель ПТЗИ.

Под перехватом информации предполагается неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов [3], поэтому подсистема ЗИ от перехвата и_с по ТКУИ обеспечивает конфиденциальность информации.

Несанкционированный доступ к информации [ресурсам автоматизированной системы] – это доступ к информации [ресурсам автоматизированной системы], осуществляемый с нарушением установленных прав и (или) правил доступа к информации [ресурсам автоматизированной системы]. К правам доступа относятся: право на чтение, изменение, копирование, уничтожение информации, а так же право на изменение, использование, уничтожение ресурсов [3]. Исходя из этого, можно сделать вывод, что НСД приводит к нарушению конфиденциальности, доступности и целостности информации. Соответственно, подсистема ЗИ от НСД в АС обеспечивает эти свойства.

Несанкционированное воздействие на информацию определяется, как воздействие на защищаемую информацию с нарушением установленных прав и (или) правил доступа, приводящее к утечке, искажению, подделке, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации [1]. Поэтому ЗИ от преднамеренного и непреднамеренного воздействий предполагает обеспечение конфиденциальности, доступности и целостности.

Результаты исследования позволяют сформировать модель обеспечения критериев безопасности информации в решениях ПТЗИ по составляющим структурного базиса следующим образом:

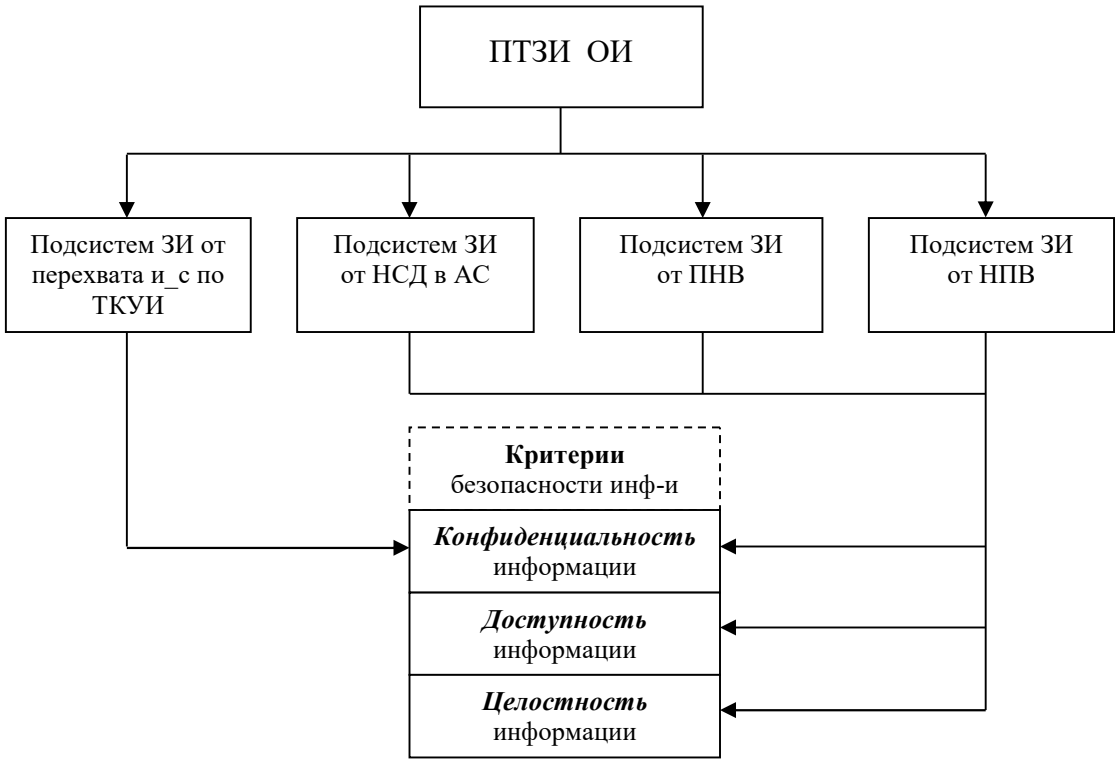

Рисунок 2 – Модель обеспечения критериев безопасности информации в решениях ПТЗИ.

Заключение

1. Разработанная модель обеспечения критериев безопасности информации ПТЗИ решает поставленную в исследовании задачу, является универсальной и позволяет системно решать задачи технической защиты информации.

2. Модель будет способствовать повышению эффективности информационной безопасности объекта защиты.

Используемые сокращения:
АС – автоматизированная система;
ЗИ – зашита информации;
и_с – информативный сигнал;
ТКУИ – технический канал утечки информации;
НПВ – непреднамеренное воздействие;
ПНВ – преднамеренное воздействие.

Литература

1. ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения» [Электронный ресурс] – Режим доступа: http://protect.gost.ru/default.aspx, (дата обращения 20.11.16).

2. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ [Электронный ресурс] – Режим доступа: http://docs.cntd.ru/document/1200039555, (дата обращения 20.11.16).

3. Р 50.1.053-2005 «Информационные технологии. Основные термины и определения в области технической защиты информации» [Электронный ресурс] – Режим доступа: http://docs.cntd.ru/document/1200039555, (дата обращения 20.11.16).

4. Загородников А.А., Козлов С.В. Модель подсистемы технической защиты информации объекта информатизации // Всероссийская научно-техническая конференция «Научная сессия ТУСУР — 2015» [Электронный ресурс] - Режим доступа: http://www.tusur.ru/export/sites/ru.tusur.new/ru/science/events/session/2015-4.pdf (дата обращения 20.11.16).