**ТРЕБОВАНИЯ К СИСТЕМЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МЕЖВИДОВОЙ СИСТЕМЫ ИНФОРМАЦИОННОГО ОБМЕНА ВООРУЖЕННЫХ СИЛ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**Шибин Андрей Сергеевич**

Слушатель магистратуры

Научный руководитель: **Обозовский Александр Анатольевич**

Краснодарское высшее военное училище имени генерала армии С.М.Штеменко

**Аннотация:** В статье рассматривается синтез модели формирования требований к системе обеспечения информационной безопасности межвидовой системы информационного обмена Вооруженных Сил Российской Федерации с учетом уровня значимости обрабатываемой информации и анализом требований руководящих документов в данной области.

**Ключевые слова:** система информационной безопасности, межвидовая система информационного обмена, объект информатизации, автоматизированная система.

**REQUIREMENTS FOR THE INFORMATION SECURITY SYSTEM OF THE INTERSPECIFIC INFORMATION EXCHANGE SYSTEM OF THE ARMED FORCES OF THE RUSSIAN FEDERATION**

**Shibin Andrey Sergeevich**

Scientific adviser: **Obozovsky Alexander Anatolyevich**

**Abstract:** The article considers the synthesis of a model for the formation of requirements for the information security system of the interspecific information exchange system of the Armed Forces of the Russian Federation, taking into account the level of importance of the information being processed and the analysis of the requirements of the governing documents in this area.

**Keywords:** information security system, interspecific information exchange system, informatization object, automated system.

Модель формирования требования к системе обеспечения безопасности информации (далее – СОИБ) межвидовой системы информационного обмена Вооруженных Сил Российской Федерации (далее – МСИО) предназначена для формирования перечня требований по правовым, организационным и техническим мерам защиты информации и к СОИБ в целом.

Постановка задачи синтеза модели формирования требования.

Необходимо с учетом угроз безопасности информации (далее – ИБ), нормативных правовых актов и нормативных документов сформировать перечень требований к СОИБ, обеспечивающих нейтрализацию угроз безопасности информации, обрабатываемой на объекте информатизации (далее – ОИ) военной организации.

В качестве исходных данных для синтеза модели используются:

система нормативной правовой базы в области ИБ, множество требований РП;

виды обрабатываемой информации, множество видов, обрабатываемой информации НИ;

множество угроз безопасности информации WМ

Результаты, проведенных исследований показали, что в состав модели формирования требований должны входить:

процедуры формирования требований к правовым мерам ЗИ (состав и содержание организационно-распорядительных документов);

процедуры формирования требований к организационным мерам (структура органа по обеспечению безопасности информации (ИБ), укомплектованность и уровень подготовленности сотрудников);

классификация ОИ военной организации;

процедуры формирования технических требований к системе защиты информации (далее – СЗИ).

Структура модели формирования требований представлена   
на рисунке 1.

Процедуры формирования требований к ОРД и структуре службы (подразделений), обеспечивающих ИБ, заключаются: в анализе нормативных правовых актов и нормативных документов в области ИБ; формировании перечня организационно-распорядительных документов необходимых для создания и функционирования СОИБ; требований к структуре службы (подразделений) обеспечивающих ИБ; требований к квалификации специалистов (должностных лиц по защите информации) службы (подразделений).

Руководящий документ [1] определяет порядок классификации автоматизированных систем, подлежащих защите от несанкционированного доступа к информации, и требования по защите информации в АС различных классов.

Исходными данными для определения класса защищенности автоматизированной системе (далее – АС) являются:

множество уровней значимости информации UЗ, UЗ = {uЗj}, j = 1 ÷ J - количество уровней значимости служебной информации, J = 4, где uЗ1, uЗ2, uЗ3, uЗ4 — 1 категория, 2 категория, 3 категория и объекты, которым отсутствует необходимость присвоения категории значимости соответственно;

масштаб АС (ОИ) MИС, MИС = {mИС1,mИС2, mИС3}, где mИС1,mИС2, mИС3 ‒ распределенная, локальная сеть либо отдельный ОВТ соответственно;

множество видов информации HИ, HИ = {hИi}, где i = 1, 2, ... , I - количество видов информации;

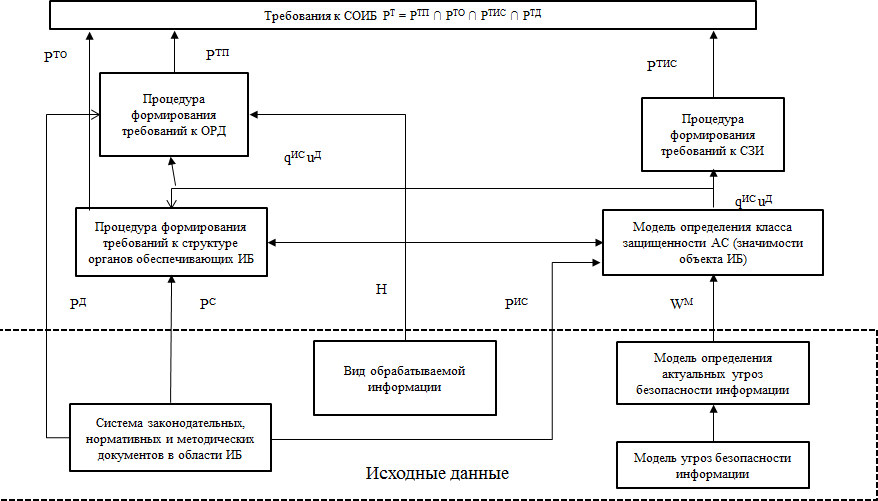
множество свойств безопасности информации С, С = {сп}, где  
n = 1 ÷ N - количество свойств безопасности информации;

множество областей деятельности D, D = {dg}, g = 1 ÷ G - количество областей деятельности;

WA - множество актуальных угроз безопасности информации  
WA = {wAr}, г = 1 ÷ R - количество актуальных угроз безопасности;

Ув - множество видов ущерба, Ув = {уВк}, k =1 ÷ K - количество видов ущерба;

Ус - множество степеней возможного ущерба, Ус = {усm}, m =1 ÷ М - количество степеней ущерба М = 3, где ус1, ус2, ус3 - высокий, средний, низкий уровни возможного ущерба соответственно;



**Рисунок 1. Модель технологии формирования требований к системе обеспечения информационной безопасности**

QИС- множество режимов обработки данных и прав доступа пользователей, QИС = {qИСz}, z = 1 ÷ Z - количество возможных вариантов совмещения.

Таким образом, модель определения класса защищенности АС должна включать в себя:

определение вида информации H = {hψ};

масштаб объекта защиты MИС = {mИС1};

определения степени ущерба Ус (множество свойств безопасности информации С, С = {сп}; области деятельности D = {dg}; виды ущерба, Ув = {уВк};степени возможного ущерба, Ус = {усm});

определение уровня значимости информации UЗ = F6(C, Ус);

определение режима обработки данных и прав доступа пользователей QИС =F7(UЗ, MИС).

Для каждого свойства безопасности информации (с1, с2, с3) устанавливаются следующие степени возможного ущерба:

высокой, если в результате нарушения одного из свойств безопасности информации возможны существенные негативные последствия и (или) АС перестала выполнять возложенные на неё функции;

средней, если в результате нарушения одного из свойств безопасности информации возможны умеренные негативные последствия и (или) АС не могут выполняет хотя бы одну из возложенных на неё функций;

низкой, если в результате нарушения одного из свойств безопасности информации возможны незначительные негативные последствия и (или) АС выполняет возложенные функции с кратковременным снижением эффективности с привлечением дополнительных сил и средств.

Определяем следующие уровни значимости информации:

информация имеет высокий уровень значимости (uЗ1), если хотя бы для одного из свойств безопасности информации определена высокая степень возможного ущерба;

информация имеет средний уровень значимости (uЗ2), если хотя бы для одного из свойств безопасности информации определена средняя степень ущерба и нет ни одного свойства, для которого определена высокая степень ущерба;

информация имеет низкий уровень значимости (uЗ3), если для всех свойств безопасности информации определены низкие степени ущерба;

информация имеет минимальный уровень значимости (uЗ4), если обладателем информации и (или) оператором степень ущерба от нарушения свойств безопасности информации не может быть определена, но при этом информация подлежит защите в соответствии с законодательством Российской Федерации.

В случае обработки в информационных системах двух и более видов значимой информации (конфиденциальные данные и иные установленные законодательством Российской Федерации виды информации ограниченного доступа) уровень значимости информации определятся отдельно для каждого вида информации.

Итоговый уровень значимости информации, обрабатываемой в ИС, устанавливается по наивысшим значениям степени возможного ущерба, определенным для конфиденциальности, целостности, доступности информации каждого вида информации.

Множество требований к СОИБ (PT), в общем случае, включает в себя:

‒ множество требований, предъявляемых к правовым мерам ОИБ (PТП);

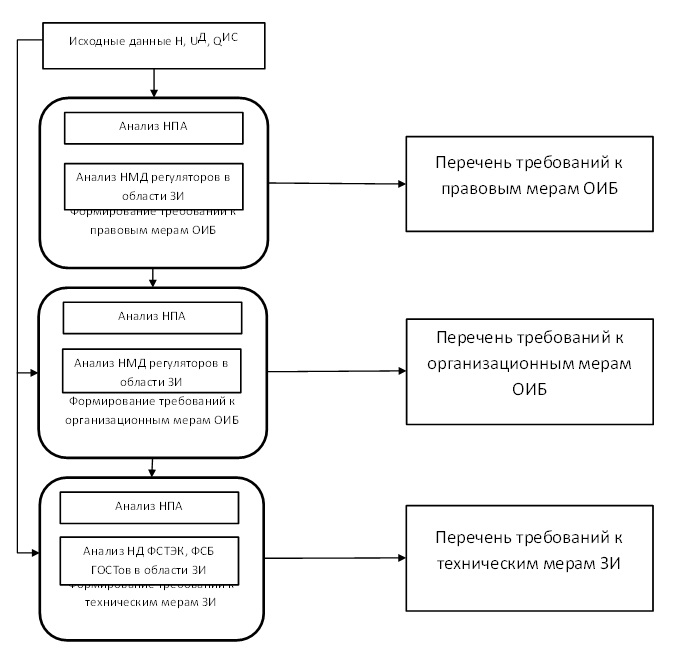
‒ множество требований, предъявляемых к организационным мерам ОИБ (РТО);

‒ множество требований, предъявляемых к техническим мерам ОИБ (РТИС).

Данные процедуры целесообразно реализовывать с использованием логических операций алгебры логики.

Требования к СОИБ определяются с учетом: вида обрабатываемой информации (Н); используемых АС и систем передачи данных (QИС) и уровня значимости информации (UПД).

Процесс реализации процедур определения требований к ОИБ военной организации может быть представлен в виде, как показано на рисунке 2.



**Рисунок 2. Порядок реализации процедур определения требований к обеспечению информационной безопасности организации**

Таким образом, сформированная модель перечней требований позволяет осуществить создание СОИБ в межвидовой системе информационного обмена Вооруженных Сил Российской Федерации. Для определения уровня ИБ военной организации потребуется провести синтез математической модели оценки состояния СОИБ.

**Список литературы**

1. Руководящий документ от 30.03 1992 г. «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».