УДК 004.728

ВОПРОСЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ОБЕСПЕЧЕНИИ ИНТЕРОПЕРАБЕЛЬНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Черницкая Т.Е.

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), 197376, Россия, Санкт-Петербург, ул. Профессора Попова, дом 5, email: drukarsu@mail.ru

Рассмотрены вопросы информационной безопасности при обеспечении интероперабельности информационных систем. Предложен теоретической подход к оценке параметров информационной безопасности интероперабельности информационных систем.

Ключевые слова: SCOPE-модель, интероперабельность, информационная безопасность, информационная система.

INFORMATION SECURITY ISSUES WHILE ENSURING THE INTEROPERABILITY OF INFORMATION SYSTEMS

Chernitskaya T.E.

St. Petersburg State Electrotechnical University "LETI" named after V.I. Ulyanov (Lenin), 197376, Russia, St. Petersburg, Professor Popov street, 5, email: drukarsu@mail.ru

The issues of information security in ensuring interoperability of information systems were considered. A theoretical approach to assessing information security parameters of information systems interoperability is proposed.

Keywords: SCOPE-model, interoperability, information security, information system.

Повсеместное внедрение сетевой архитектуры, привело к актуализации проблемы интероперабельности информационных систем (ИС). На сегодняшний день это понятие применимо к любой прикладной области, которая использует достоинства человеко-машинного взаимодействия.

Консорциумом по сетецентрическим операциям NCOIC (Network-Centric Operations Industry Consortium) [1] разработана модель оценки интероперабельности систем, возможностей, действий, программ и организаций (SCOPE – модель), которая предназначена для качественно – количественной характеристики аспектов интероперабельности систем в соответствии с набором определенных параметров.

Параметры модели организованы в иерархическом виде. На нижнем уровне каждый параметр соответствует определенному аспекту интероперабельности системы и определяет этот аспект в виде количественных или качественных показателей.

На верхнем уровне иерархии SCOPE – модель состоит из 4-х групп параметров интероперабельности:

1) параметры сетевого взаимодействия – характеризуют способность системы формировать и управлять сетевыми структурами;

2) внутренние параметры системы – характеризуют внутренние параметры системы, которые определяют уровень ее интероперабельности;

3) внешние параметры системы – характеризуют внешние факторы, которые влияют уровень интероперабельности систем;

4) технико-экономические параметры – описывают технологические решения, на основе которых достигается свойство интероперабельности, а также экономические аспекты целесообразности или риска от их внедрения.

Анализ Доктрины информационной безопасности [2] показывает, что одной из первостепенных задач в рамках обеспечения интероперабельности информационных систем является, решение проблемы информационной безопасности (ИБ). При решении проблемы интероперабельности необходимо учитывать угрозы ИБ. Анализ этих угроз должен привести к формированию стандартов обеспечения ИБ в модели интероперабельности ИС [3].

Параметры ИБ в SCOPE-модели описывают способы разрешения проблем ИБ, характерные для сетевого

взаимодействия, когда все данные и сервисы доступны каждому пользователю в сети. Для обеспечения интероперабельности систем необходимо убедиться в доступности сервисов и данных, корректности отображения отчетов о состоянии систем.

Параметры ИБ могут быть использованы как для классификации существующих мероприятий по защите информации, так и для проектирования новых, в соответствии с требуемым классом защищенности. При этом требования к безопасности обусловлены свойствами системы и установленными уровнями доверия между пользователями.

В сетецентрических системах требования к ИБ распространяются на интерфейсы, сервисы, информационные ресурсы внутри сети, а не только по ее «периметру». Особенное внимание уделяется управлению данными для аутентификации, пользовательскими разрешениями, шифрованию потоков данных и электронному подписанию документов.

Степень защищенности информации зависит от уровня доверия к внешней сетевой платформе. Для обеспечения ИБ необходимо удостовериться в защищенности внешнего подключения по сети. При этом способы решения задач ИБ внутри внешней платформы не имеют значения.

Архитектура параметров ИБ в SCOPE – модели представлена в виде четырех ключевых областей:

- безопасность передачи информации;
- доступность сервисов;
- информационно – ситуационная осведомленность и Защита сети;
- безопасность процессов управления и контроля.

На основании перечисленных областей может быть проведена дальнейшая декомпозиция параметра ИБ на качественные/количественные показатели. Практические средства обеспечения ИБ включают элементы, необходимые для защищенного взаимодействия приложений. Базовым требованием к ИБ является обеспечение контроля доступа пользователей к сетевой машине. Контроль доступа состоит в предварительной аутентификации и авторизации пользователя. Одновременно с получением доступа к сети, приложение получает права на использование ресурсов, файлов, баз данных и др. Обеспечение доступа к ряду ресурсов может потребовать организации защищенного канала и безопасного хранения сведений о пользовательских разрешениях. Спецификация практических средств обеспечения ИБ может быть следующей:

Тип значения Уровень доступа

Набор значений

- Реализация контроля доступа, включая аутентификацию и авторизацию на сервисах;
- Предоставление отдельного типа разрешений для использования ресурсов;
- Защищенное взаимодействие;
- Безопасное хранение сведений о пользовательских разрешениях и ресурсах.

Сетецентрические системы должны взаимодействовать со средствами обеспечения ИБ Для обеспечения доступа пользователя к машине, конфигурация системы должна содержать набор разрешений, соответствующих пользовательскому уровню доступа. Для обеспечения доступа к ресурсу, система запрашивает дополнительное разрешение, соответствующее данному серверу, базе данных и др. В качестве примера можно привести пользовательские роли, пароли, шифрование и другие методы обеспечения ИБ.

Также для обеспечения ИБ широко применяется внедрение защитных политик ИБ. Реальные задачи интероперабельности систем подразумевают организацию взаимодействий вне защищенного домена, к примеру, с бизнес – партнерами. В сетецентрических системах необходимо найти компромисс между мероприятиями по защите информации и обеспечением доступа к данным и сервисам в сети. Внедрение политик безопасности способствует установлению контроля над потоками данных для эффективного управления информацией.

Заключение: проведен анализ SCOPE – модели интероперабельности информационных систем с точки зрения вопросов информационной безопасности. Рассмотрена спецификация практических средств обеспечение информационной безопасности интероперабельности систем. В рамках существующей SCOPE-модели предложен теоретический подход к оценке параметров ИБ при обеспечении интероперабельности информационных систем.

Список литературы

1. Systems, Capabilities, Operations, Programs, and Enterprises (SCOPE) Model for Interoperability Assessment. Version 1.0. – NCOIC, 2008. – 37 с., 80 – 83 с.

2. Доктрина информационной безопасности Российской Федерации (Указ президента РФ №646 от 5 декабря) // Электронный фонд правовой и нормативно – технической документации [Электронный ресуср]. 06.12.2016. – URL: http://docs.cntd.ru/document/420384668 (дата обращения 30.10.2019).

3. Башлыкова А.А., Олейников А.Я. Интероперабельность и информационное противоборство в военной сфере // Журнал радиоэлектроники. 2016. № 11. С. 16.

References

1. Systems, Capabilities, Operations, Programs, and Enterprises (SCOPE) Model for Interoperability Assessment. Version 1.0. - NCOIC, 2008. - 37 p., 80 - 83 p.

2. Information Security Doctrine of the Russian Federation (Presidential Decree No. 666 of December 5) // Electronic Fund for Legal and Regulatory Technical Documentation [Electronic Resource]. 06.12.2016. - URL: http://docs.cntd.ru/document/420384668 (circulation date 30.10.2019).

3. Bashlykova, A.A.; Oleinikov, A.Ya. Interoperability and information confrontation in the military field (in Russian) // Journal of Radioelectronics. 2016. № 11. - p. 16.