А. Н. Бабкин, *кандидат технических наук, доцент*
С. П. Алексеенко, *кандидат физико-математических наук, доцент*

МОДЕЛЬ ЗАЩИЩЕННОЙ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ ОРГАНИЗАЦИИ

SECURE INFORMATION AND TELECOMMUNICATION MODEL ORGANIZATION NETWORKS

В статье рассматривается пример формирования модели защищенной информационно-телекоммуникационной сети организации.

Отличительной особенностью построения сети является её разделение (сегментация) на внутреннюю сеть, содержащую серверную часть с данными, относящимися к конфиденциальной информации и внешнюю сеть (демилитаризованную часть), содержащую общедоступный сервер для внешних пользователей.

Рассматриваются рубежи защиты периметров внутренней и внешней сетей.

The article considers an example of the formation of a model of a secure information and telecommunication network of an organization.

A distinctive feature of building a network is its division (segmentation) into an internal network containing a server part with data related to confidential information and an external network (demilitarized part) containing a public server for external users.

The boundaries of protection of perimeters of internal and external networks are considered.

Введение. В настоящее время трудно представить функционирование крупной организации (предприятия) без использования информационно-телекоммуникационной сети (ИТКС).

В такой сети, как правило, циркулирует информация, носящая конфиденциальный характер, например персональные данные сотрудников, или данные ограниченного распространения, например сведения, касающиеся направлений развития организации, ценовой политики и др.

В связи с ростом криминогенности в информационной сфере защита информационного ресурса организации является важнейшей задачей, направленной на обеспечение её надежного функционирования и развития.

При этом объектом информационных атак становится ИТКС организации, и проблема обеспечения её информационной безопасности, разработка модели защищенной ИТКС становятся одной из наиболее актуальных и значимых задач в информационной сфере.

Основная часть. В основе модели защищенной ИТКС организации лежат возможные угрозы, направленные на основные компоненты (как программные, так и программно-аппаратные) сети, и методы и средства их защиты.

На ИТКС организации могут действовать как внешние, так и внутренние источники угроз безопасности информации [1].

Данные источники угроз могут использоваться злоумышленниками для реализации информационных атак.

В [2] приводится классификация информационных атак на автоматизированные системы, рассматривается жизненный цикл информационной атаки, а также представлены различные модели информационных атак.

При этом рассматривается обобщенная архитектура защищенной автоматизированной системы.

В [3] рассматриваются технологии безопасности на основе фильтрации и мониторинга трафика и представлены различные архитектуры сетей с защитой периметра и разделением внутренних зон.

В [4—6] рассмотрены вопросы моделирования и прогнозирования угроз информационной безопасности, а также моделирование процессов передачи данных в телекоммуникационной сети в условиях воздействия угроз информационной безопасности.

В основе модели защищенной ИТКС организации лежат три фундаментальных понятия: объект информатизации (или объект защиты, ОИ), угроза информационной безопасности (УИБ), система защиты ОИ (СЗИ).

В качестве ОИ выступает ИТКС организации, в отношении которой действуют угрозы информационной безопасности.

Как известно [1, 3], основным принципом защиты ИТКС является подход «сверху вниз».

Данный подход означает, что на верхнем уровне (уровне руководства организации) принимаются общие решения по защите информационной среды организации, которые затем трансформируются в конкретные решения исполнителями (техническими сотрудниками, ответственными за это направление) по обеспечению информационной безопасности ИТКС.

Все это находит отражение в формировании политики безопасности организации.

Таким образом, задача обеспечения информационной безопасности ИТКС заключается в:

- определении видов информации (общедоступная или с ограниченным доступом), циркулирующей в организации;
- определении структуры организации (отделы, подразделения, группы и т. п.);
- анализе возможных угроз информационной безопасности;
- физической и логической структуризации сети (сегментации сети);
- применении программных и программно-аппаратных средств защиты информации, направленных на противодействие угрозам в каждом сегменте сети.

На основании вышесказанного можно представить следующий алгоритм формирования модели защищенной ИТКС (рис. 1).

Одним из важных этапов формирования модели защищенной ИТКС является оценка защищенности сети от информационных атак. Основной угрозой информационной безопасности ИТКС является утечка информации за счет несанкционированного доступа (НСД) в информационную среду организации.

В [1, 2] анализируются основные методы обнаружения информационных атак, моделируя которые можно проводить анализ защищенности ИТКС.

К таким методам относятся:

- метод сигнатурного (контекстного) поиска;
- метод анализа состояний сети (сети Петри);
- метод экспертных оценок;
- метод, основанный на генетических алгоритмах;
- нейросетевой метод.

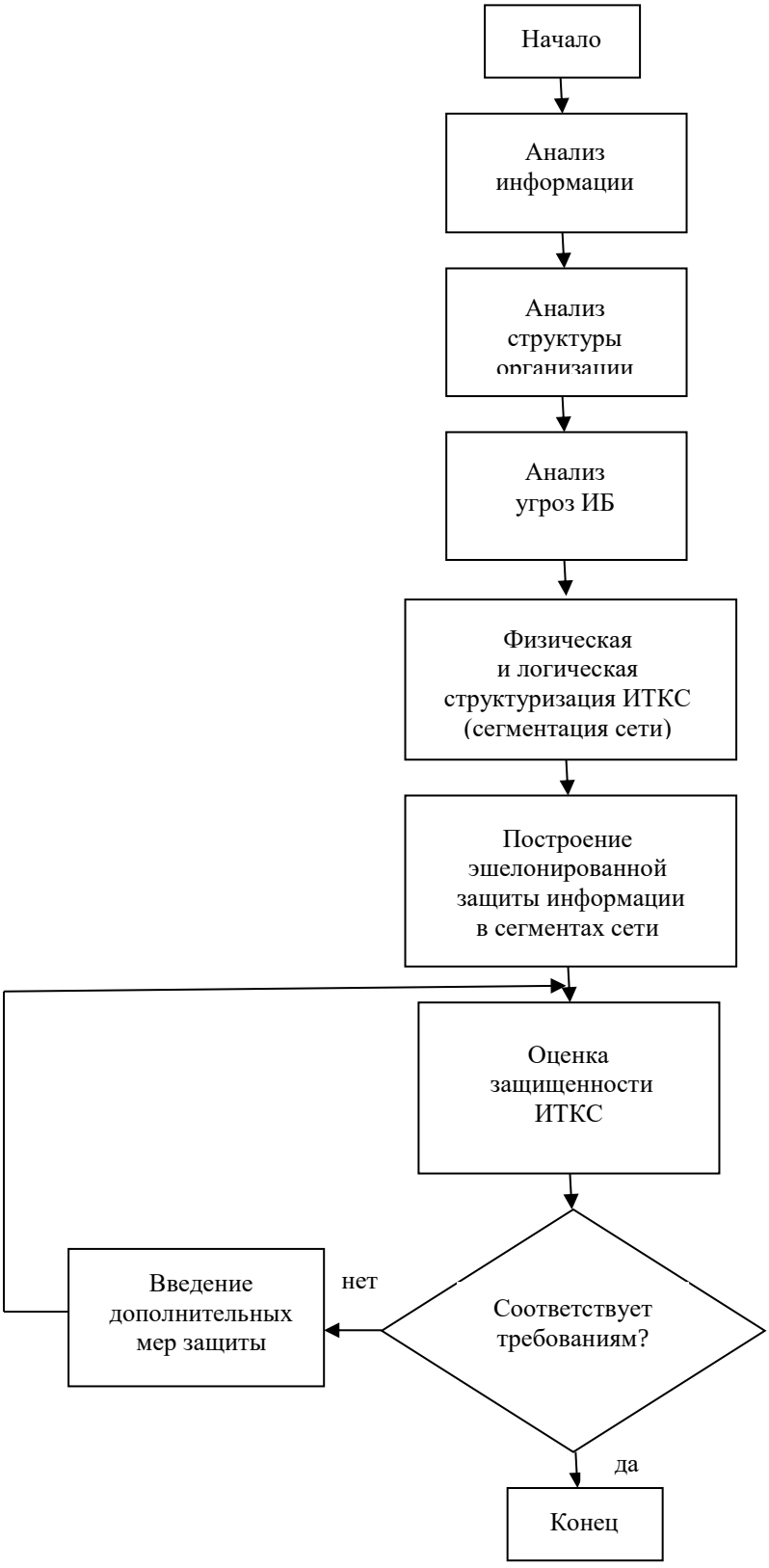

Рис. 1. Алгоритм формирования модели защищенной ИТКС

В [4—6] рассматривается моделирование процессов передачи данных в телекоммуникационной сети в условиях воздействия угроз информационной безопасности на основе сетей Маркова и сетей Петри.

Одним из эффективных инструментов оценки защищенности ИТКС, от информационных атак являются сети Петри.

Моделирование с помощью сетей Петри основано на формировании маркировки информационно-телекоммуникационной сети последовательно при срабатывании переходов информационного пакета между хостом пользователя, хостом нарушителя и сервером.

На основе алгоритма формирования модели защищенной ИТКС на рис. 2 представлена структурная схема сети.

На этом рисунке обозначены: К — коммутатор; М — маршрутизатор; ФРВ — файервол; СОВ — система обнаружения вторжений.

Сеть имеет две зоны: внутреннюю и демилитаризованную (DMZ).

ИТКС организации содержит два общедоступных сервера, расположенных в демилитаризованной зоне DMZ: внешние DNS и WWW серверы.

Во внутренней сети расположены внутренние DNS и WWW серверы организации.

Трафик локализован в сегментах 1 и i.

Внешний файервол вместе с СОВ осуществляет фильтрацию трафика из внешней сети для защиты периметра и внутренней сети ИТКС и работает на сетевом и транспортном уровнях.

Внутренний файервол совместно с СОВ защищает внутреннюю сеть от угроз безопасности информации, исходящих от внешней сети и от сети периметра, и функционирует на сетевом, транспортном и прикладном уровнях.

Таким образом, сеть имеет два рубежа (эшелона) защиты: первый рубеж реализован на основе внешнего файервола и СОВ, второй рубеж — на основе внутреннего файервола и СОВ.

Кроме того, каждый хост внутренней и внешней сети имеет индивидуальные средства защиты, к которым относятся средства антивирусной защиты, разграничения доступа, аудита, средства контроля подключений к узлу, средства защиты от НСД к каталогам и файлам и др.

Во внутренней сети расположен сервер, на котором хранятся сведения, относящиеся к конфиденциальной информации (в частности, персональные данные сотрудников организации), а также информация ограниченного распространения, например, направления развития организации, информация о финансовой деятельности и др.

Данная информация должна обладать свойствами конфиденциальности, целостности и доступности.

В демилитаризованной зоне расположен сервер, на котором хранится информация о направлениях деятельности организации: товарах, услугах и др. Данная информация должна обладать свойствами целостности и доступности. К серверу демилитаризованной зоны должны иметь доступ внешние пользователи (пользователи сети Интернет).

Основные угрозы информационной безопасности ИТКС возникают на сетевом уровне и связаны с перехватом злоумышленником трафика, нарушением функционирования компонентов ИТКС, приводящих к отказу в обслуживании. Такие угрозы реализуются с использованием протоколов межсетевого взаимодействия стека TCP/IP.

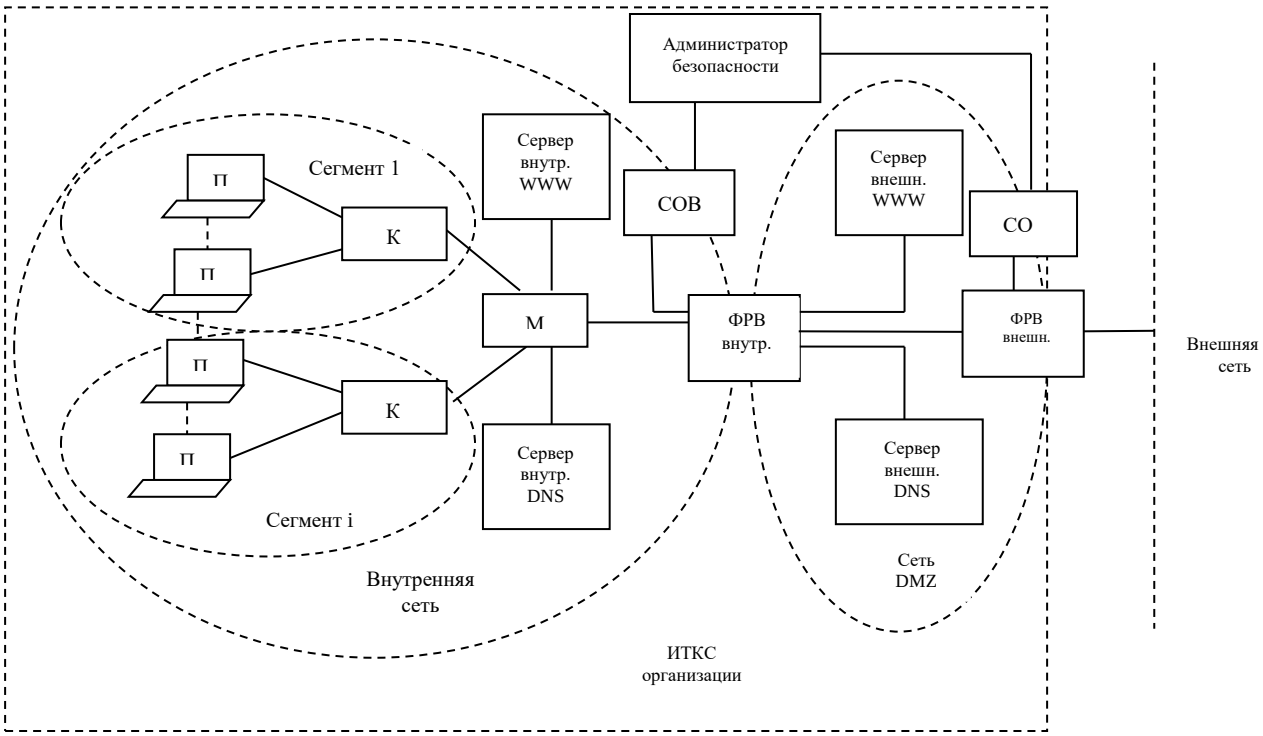

Рис. 2. Структурная схема ИТКС организации

На рис. 3 представлен граф, моделирующий проникновение злоумышленника в ИТКС организации, где S_i — состояния сети в результате действий злоумышленника.

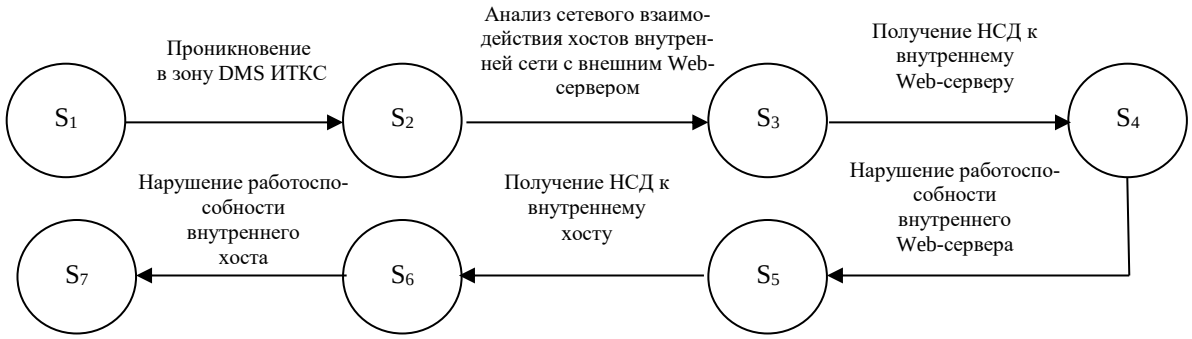

Рис. 3. Граф, моделирующий проникновение злоумышленника в ИТКС организации

Как отмечалось выше, одной из основных угроз информационной безопасности является утечка информации за счет несанкционированного доступа злоумышленника к информационным ресурсам организации.

При этом состояние ИТКС может описываться при помощи трех основных параметров ИТКС: множества объектов (сущностей), множества субъектов и множества прав доступа субъектов к объектам.

Переход ИТКС из одного состояния в другое происходит в результате изменения состава любого из этих множеств.

Одним из эффективных способов анализа состояний сети является применение сетей Петри [5, 6], позволяющих учитывать различные параметры атаки [7, 8].

Сеть Петри представляет собой ориентированный граф, состоящий из состояний и переходов, соединенных между собой дугами.

Анализируя ИТКС на основе сетей Петри, можно представить сеть организации как множество состояний С:

$$C = \{S, T, F_{вх}, F_{вых}\},$$

где $S = \{S_i\}$ — множество состояний сети, $T = \{T_j\}$ — множество переходов сети, $F_{вх}$ — входная функция, соответствующая начальному состоянию сети, $F_{вых}$ — выходная функция, соответствующая конечному состоянию сети.

Учитывая информацию, циркулирующую в ИТКС организации, можно сделать вывод о том, что во внутренней сети основными угрозами информационной безопасности будут потеря конфиденциальности, целостности и доступности, в демилитаризованной сети — потеря целостности и конфиденциальности.

Заключение. Информационно-телекоммуникационная сеть предназначена для эффективной организации финансовой деятельности организации.

Наряду с общедоступной информацией о направлениях деятельности организации, товарах и услугах для внешних пользователей (пользователей сети Интернет) в организации присутствует и конфиденциальная информация, в частности персональные данные сотрудников, а также информация ограниченного распространения, касающаяся, например, направлений развития.

Данные обстоятельства предъявляют повышенные требования к структуризации ИТКС, обеспечению её информационной безопасности.

Представленная в статье модель защищенной ИТКС позволяет решить вопрос о защите информации конфиденциального характера с обеспечением её конфиденциальности, целостности и доступности и общедоступной информации с обеспечением её доступности и целостности.

Решение состоит в разделении ИТКС на внутреннюю и внешнюю (демилитаризованную) сети с защитой в каждой сети периметра с применением программно-аппаратных средств в виде файерволов и систем обнаружения вторжений.

ЛИТЕРАТУРА

1. Язов Ю. К., Соловьев С. В. Организация защиты информации в информационных системах от несанкционированного доступа : монография. — Воронеж : Кварта, 2018. — 588 с.

2. Сердюк В. А. Новое в защите от взлома корпоративных систем. — М. : Техносфера, 2007. — 360 с.

3. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы : учебник для вузов. — 5-е изд. — СПб. : Питер, 2016. — 992 с.

4. Бабкин А. Н., Алексеенко С. П., Куличенко А. Ю. Модель информационной безопасности сегмента телекоммуникационной сети ОВД // Вестник Воронежского института ФСИН России. — 2020. — № 2. — С. 34—40.

5. Бабкин А. Н., Куличенко А. Ю., Широкий А. А. Моделирование и прогнозирование угроз информационной безопасности регионального сегмента ИСОД МВД России // Вестник Воронежского института МВД России. — 2020. — № 2. — С. 79—88.

6. Бабкин А. Н., Акчурина Л. В. Моделирование процессов передачи данных в телекоммуникационной сети в условиях воздействия угроз информационной безопасности // Вестник Воронежского института ФСИН России. — 2021. — № 3. — С. 50—57.

7. Бабкин А. Н., Акчурина Л. В., Алексеенко С. П. Пример применения сетей Петри для анализа защищенности информационных процессов // Вестник Воронежского института МВД России. — 2022. — № 4. — С. 65—71.

8. Бабкин А. Н., Акчурина Л. В., Алексеенко С. П. Моделирование угроз информационных атак в сети Internet на основе сетей Петри // Вестник Воронежского института МВД России. — 2023. — № 2. — С. 105—110.

REFERENCES

1. Yazov Yu. K., Solov`ev S. V. Organizaciya zashhity` informacii v informacionny`x sistemax ot nesankcionirovannogo dostupa : monografiya. — Voronezh : Kvarta, 2018. — 588 s.

2. Serdyuk V. A. Novoe v zashhite ot vzloma korporativny`x sistem. — M. : Texnosfera, 2007. — 360 s.

3. Olifer V., Olifer N. Komp`yuterny`e seti. Principy`, texnologii, protokoly` : uchebnik dlya vuzov. — 5-e izd. — SPb. : Piter, 2016. — 992 s.

4. Babkin A. N., Alekseenko S. P., Kulichenko A. Yu. Model` informacionnoj bezopasnosti segmenta telekommunikacionnoj seti OVD // Vestnik Voronezhskogo instituta FSIN Rossii. — 2020. — № 2. — S. 34—40.

5. Babkin A. N., Kulichenko A. Yu., Shirokij A. A. Modelirovanie i prognozirovanie ugroz informacionnoj bezopasnosti regional`nogo segmenta ISOD MVD Rossii // Vestnik Voronezhskogo instituta MVD Rossii. — 2020. — № 2. — S. 79—88.

6. Babkin A. N., Akchurina L. V. Modelirovanie processov peredachi danny`x v telekommunikacionnoj seti v usloviyax vozdejstviya ugroz informacionnoj bezopasnosti // Vestnik Voronezhskogo instituta FSIN Rossii. — 2021. — № 3. — S. 50—57.

7. Babkin A. N., Akchurina L. V., Alekseenko S. P. Primer primeneniya setej Petri dlya analiza zashhishhennosti informacionny`x processov // Vestnik Voronezhskogo instituta MVD Rossii. — 2022. — № 4. — S. 65—71.

8. Babkin A. N., Akchurina L. V., Alekseenko S. P. Modelirovanie ugroz informacionny`x atak v seti Internet na osnove setej Petri // Vestnik Voronezhskogo instituta MVD Rossii. — 2023. — № 2. — S. 105—110.

СВЕДЕНИЯ ОБ АВТОРАХ

Бабкин Александр Николаевич. Доцент кафедры информатики и вычислительной техники. Кандидат технических наук, доцент.

Международный институт компьютерных технологий.

E-mail: alex_babk@mail.ru

Россия, 394026, Воронеж, ул. Солнечная, 29б.

Алексеенко Сергей Павлович. Доцент кафедры информационной безопасности. Кандидат физико-математических наук, доцент.
Воронежский институт МВД России.
E-mail: aleks_serg@mail.ru
Россия, 394065, Воронеж, проспект Патриотов, 53.

Babkin Alexander Nikolaevich. Associate Professor of the chair of Computer Science and Applied Technology. Candidate of Technical Sciences, Associate Professor.
International Institute of Computer Technology.
Email: alex_babk@mail.ru
Work address: Russia, 394026, Voronezh, Solnechnaya Str., 29b.

Alekseenko Sergey Pavlovich. Assistant Professor of the chair of Information Security. Candidate of Sciences (Physics and Mathematics), Associate Professor.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: aleks_serg@mail.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: информация; модель; информационная безопасность; угроза информационной безопасности; информационно-телекоммуникационная сеть; моделирование; сеть Петри.

Key words: information; model; information security; information security threat; information and telecommunication network; modeling; Petri network.

УДК 621.396.62