6. *Abramov E.S., Andreev A.V., Mordvin D.V., Makarevich O.B.* Corporate networks security evaluation based on attack graphs // Proceedings of the 4th international conference on Security of information and networks (SIN '11)-ACM, New York, NY, USA, 2011. – P. 29-36.
7. *Aleksandar Kuzmanovic, Edward W. Knightly*. Low-rate TCP-targeted denial of service attacks and counter strategies // IEEE/ACM Trans. Netw. – 2006. – № 14 (4). – С. 683-696.
8. *Paxson V., Allman M., Chu H.K., and Sargent M.* Computing TCP's Retransmission Timer, RFC 6298, Proposed Standard, June 2011.

Статью рекомендовал к опубликованию д.т.н., профессор Н.И. Витиска.

Тарасов Ярослав Викторович – ЗАО «Инфосистемы Джет»; e-mail: info@jet.msk.su; 127015, Москва, ул. Большая Новодмитровская, 14-1; тел.: +74954117601; директор по развитию.

Макаревич Олег Борисович – Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Южный федеральный университет»; e-mail: mak@tsure.ru; 347928, г. Таганрог, ул. Чехова, 2; тел.: 88634371905; кафедра безопасности информационных технологий; зав. кафедрой.

Tarasov Yaroslav Viktorovich – Jet Infosystems; e-mail: info@jet.msk.su; 14-1, Large Novodmitrovskaya street, Moscow, 127015, Russia; phone: +74954117601; director of development.

Makarevich Oleg Borisovich – Federal State-Owned Autonomy Educational Establishment of Higher Vocational Education “Southern Federal University”; e-mail: mak@tsure.ru; 2, Chekhova street, Taganrog, 347928, Russia; phone: +78634371905; the department of security in data processing technologies; head the department.

УДК 004.056.5

В.Г. Миронова, А.А. Шелупанов

АНАЛИЗ РЕЖИМОВ РАЗГРАНИЧЕНИЯ И РАСПРОСТРАНЕНИЯ ПРАВ ДОСТУПОВ НА ОСНОВЕ ДИСКРЕЦИОННОЙ МОДЕЛИ РАЗГРАНИЧЕНИЯ ПРАВ ДОСТУПОВ TAKE-GRANT

В функционирующих информационных системах обработки конфиденциальной информации используются два режима обработки данных – однопользовательский и многопользовательский. При многопользовательском режиме обработки данных целесообразно использование разграничения прав доступа пользователей к информации, поскольку это увеличивает уровень безопасности информации. Обеспечение безопасности информации, обрабатываемой как в электронном, так и бумажном виде начинается с режима разграничения прав доступов пользователей. Но не стоит забывать о том, что между пользователей и злоумышленником существует возможность передачи или распространения прав доступа к конфиденциальной информации. Существует несколько политик разграничения прав доступа к информации – дискреционная и мандатная. Анализ возможностей распространения прав доступов зависит от выбранной политики безопасности и позволяет выявлять каналы утечки конфиденциальной информации и способы ее распространения. Данные о каналах утечки информации и способах ее распространения позволяют проектировать и создавать надежную систему защиты информации.

Информационная безопасность; политика безопасности; модель; разграничение прав доступа.

V.G. Mironova, A.A. Shelupanov

ANALYSIS AND DISSEMINATION SUPPORT DIFFERENT ACCESS RIGHTS BASED MODEL DISCRETIONARY ACCESS RIGHTS TAKE-GRANT

In the functioning of information systems for handling confidential information are two modes of data processing – a single-user and multi-user. With the multiplayer mode data using appropriate access rights to information for users, as it increases the level of information security. Ensuring security of information processed in both electronic and paper form begins with a mode of access rights of users. But do not forget that between the user and the attacker can also transfer or distribution of access rights to sensitive information. There are several policy distinction between the rights of access to information – discretionary and credentials. Analysis of the possibilities for extending the right of access depends on the security policy, and to identify channels of leakage of confidential information and the means of its dissemination. Channel data leaks and how to spread it possible to design and build a reliable system of information protection.

Information security; security policy; the model of access rights.

Развитие современного информационного общества немыслимо без применения информационных технологий. В настоящее время компьютерные системы и телекоммуникации определяют надежность систем обороны и безопасности страны, реализуют современные информационные технологии, обеспечивая обработку и хранение информации, автоматизируют технологические процессы. Массовое использование компьютерных систем, которое позволило решить проблему автоматизации процессов производства, обработки и хранения информации, сделало уязвимым эти процессы, в результате чего появилась новая проблема – проблема информационной безопасности [1].

Обеспечение информационной безопасности (ИБ) достигается путем внедрения систем защиты информации (СЗИ), которые включают в себя: системы разграничения прав доступа, системы антивирусной защиты, системы безопасного межсетевого взаимодействия и др.

Существует два типа политик разграничения прав доступа: мандатная и дискреционная политики безопасности.

Целью мандатной политики безопасности является предотвращение утечки информации от объектов с высоким уровнем доступа к объектам с низким уровнем доступа.

Основу мандатной политики безопасности составляет мандатное управление доступом, которое подразумевает, что:

- все субъекты и объекты системы должны быть однозначно идентифицированы;
- задан линейно упорядоченный набор меток секретности;
- каждому объекту системы присвоена метка секретности, определяющая ценность содержащейся в нем информации;
- каждому субъекту системы присвоена метка секретности, определяющая уровень доверия к нему в информационной системе (ИС) [2].

В настоящее время широко используется дискреционная политика безопасности, к достоинствам которой можно отнести относительно простую реализацию механизмов защиты информации в информационных системах (ИС).

Основой дискреционной политики безопасности является дискреционное управление доступом, которое определяется двумя свойствами:

- все субъекты и объекты должны быть идентифицированы;
- права доступа субъектов к объекту ИС определяются на основании некоторого внешнего по отношению к системе правила.

В случае использования дискреционной политики безопасности возникает необходимость определения правил распространения прав доступа и анализ их влияния на безопасность ИС.

Модель распространения прав доступа Take-Grant используется для анализа систем дискреционного разграничения доступа, в первую очередь для анализа путей распространения прав доступа в таких системах. Обычно данную модель описывают в терминах графов доступа.

Формально описание модели Take-Grant выглядит следующим образом:

1. Множество объектов – $\boldsymbol{O}$, где $o_j \in \boldsymbol{O}$, $\boldsymbol{O} = \{o_1, o_2, \ldots, o_j\}$, $j \in \boldsymbol{N}$;
2. Множество субъектов – $\boldsymbol{S}$, где $s_n \in \boldsymbol{S}$, $\boldsymbol{S} = \{s_1, s_2, \ldots, s_n\}$, $n \in \boldsymbol{N}$;
3. Множество активных субъектов – $\boldsymbol{S} \subseteq \boldsymbol{O}$;
4. Множество прав доступа $\boldsymbol{R}$, где $r_i \in \boldsymbol{R}$, $\boldsymbol{R} = \{r_1, r_2, \ldots, r_j\} \cup \{t, g\}$, где *t (take)* – право брать права доступа, g(grant) – права давать права доступа;
5. Конечный помеченный ориентированный граф без петель, представляющий текущие доступы в системе $G = (\boldsymbol{S}, \boldsymbol{O}, \boldsymbol{E})$, где элементы множества $E \subseteq O \times O \times R$ представляют дуги графа, помеченные непустыми подмножествами из множества прав доступа $\boldsymbol{R}$ [3, 4].

Модель нарушителя ИБ, описанная в [5] формирует в себе комплекс знаний об имеющихся нарушителей ИБ, поэтому большое значение приобретает оценка путей распространения и разграничения прав доступа к КИ. Провести анализ возможных пути реализации действий злоумышленника для систем с дискреционным разграничением прав доступа, можно используя модели, построенные на основе модели Take-Grant.

Отличительной особенностью организаций, в которых производится обработка и хранение КИ, является наличие рубежей защиты.

Типовыми зонами организации, указанными на рис. 1, являются:

- территория, занимаемая организацией и ограничиваемая забором или условной внешней границей;
- здание на территории;
- коридор или его часть;
- помещение (служебное, кабинет, комната, зал, техническое помещение, склад и др.);
- шкаф, сейф, хранилище.

Соответственно, рубежи защиты:

- забор;
- стены, двери, окна здания;
- двери, окна (если они имеются), стены, пол и потолок (перекрытия) коридора;
- двери, окна, стены, пол и потолок (перекрытия) помещения;
- стены и двери шкафов, сейфов, хранилищ.

Проведем анализ реализации злоумышленных действий – проникновение на территорию здания. Проникновение на территорию здания сопровождается нарушением первого рубежа защиты, в связи с этим построим модель типа «Первый рубеж защиты в организации».

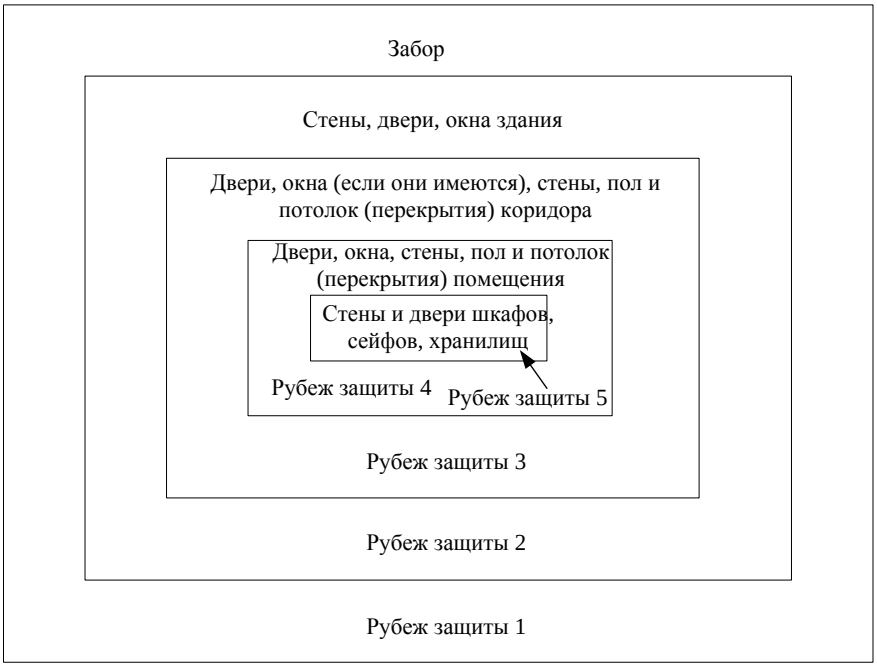

Рис. 1. Рубежи защиты организации

Модель «Первый рубеж защиты в организации» состоит из следующих компонент:

1. Субъекты доступа в здание организации s_n, $s_n \in \mathbf{S}$, $\mathbf{S} = \{s_1, s_2, \ldots, s_n\}$, $n \in N$ [6]. Под субъектами будем понимать:
   - персонал организации, являющийся как штатными сотрудниками подразделений организации;
   - персонал, обеспечивающий физическую защиту помещений организации;
   - персонал сторонних организаций, осуществляющий техническое обслуживание и ремонт СВТ, коммуникационного оборудования и линий связи;
   - бюро пропусков.
2. Объект доступа o_{p1}, $o_{p1} \in \mathbf{O}$, $\mathbf{O} = \{o_{p1}, o_{p2}, o_{p3}, o_{p4}, o_{p5}\}$. Рубеж защиты 1.
3. Право доступа каждого субъекта из множества **S** в здание организации $r_i \in \mathbf{R}$, $\mathbf{R} = \{r_1, r_2, \ldots, r_j\} \cup \{t, g\}$. Право доступа в здание организации.
4. Монитор обращения (МО) $s_i \in \mathbf{SM}$, $\mathbf{SM} = \{s_{мо}, s_{мбо}, s_{мпс}, s_{мбс}\}$, i=1,4. Система контроля и управления доступом (СКУД) в здание организации (программная реализация СКУД, турникеты, двери и т.д.) и(или) часовым (контролером), рис. 2.
5. Поток информации между субъектом и объектом Stream ($\mathbf{S}$,$o_{зз}$). Доступом субъектов **S**, $s_n \in \mathbf{S}$, $\mathbf{S} = \{s_1, s_2, \ldots, s_n\}$, $n \in N$ к объекту o_{p1} будем называть порождение потока информации между объектом o_{p1} и **S**.
6. Монитор безопасности объектов (МБО) $s_i \in \mathbf{SM}$, $\mathbf{SM} = \{s_{мо}, s_{мбо}, s_{мпс}, s_{мбс}\}$, i=1,4. СКУД в здание организации и(или) часовой (контролер), который отвечает за предоставление доступа субъектам в здание.

7. Монитором порождения субъектов (МПС) $s_i \in \mathbf{SM}$, $\mathbf{SM} = \{s_{мо}, s_{мбо}, s_{мпс}, s_{мбс}\}$, i=1,4. Бюро пропусков.
8. Монитор безопасности субъектов (МБС) $s_i \in \mathbf{SM}$, $\mathbf{SM} = \{s_{мо}, s_{мбо}, s_{мпс}, s_{мбс}\}$, i=1,4. Руководители подразделений, которые оформляют заявки на оформление пропусков для сотрудников, командировочных и т.д., и отправляют заявки в бюро пропусков.

Согласно аксиомам в [2], активными субъектами в модели типа «Первый рубеж защиты в организации», выполняющими контроль операций субъектов над объектом o_{p1}, будет являться СКУД в здание, которая реализована посредствам специальной программы, турникетов, дверей и т.д. и(или) часовой (контролер). При предъявлении пропуска субъектом из множества **S** формируется запрос на доступ от субъекта из множества **S** к объекту o_{p1}. Затем МО анализирует базу правил (базу данных субъектов, имеющих право доступа в здание организации), соответствующую установленной в системе политике безопасности и либо разрешает проход, либо запрещает.

Пропуск может быть представлен в виде пластиковой карты, бумажного носителя, биометрических данных и т.д.

МО удовлетворяет следующим свойствам:

1. Ни один запрос на доступ субъекта из множества **S** к объекту o_{p1} не должен выполняться в обход МБО.

2. Работа МБО должна быть защищена от постороннего вмешательства.

3. Представление МБО должно быть достаточно простым для возможности верификации корректности его работы.

На рис. 2 представлена схема реализации МО в модели типа «Первый рубеж защиты в организации».

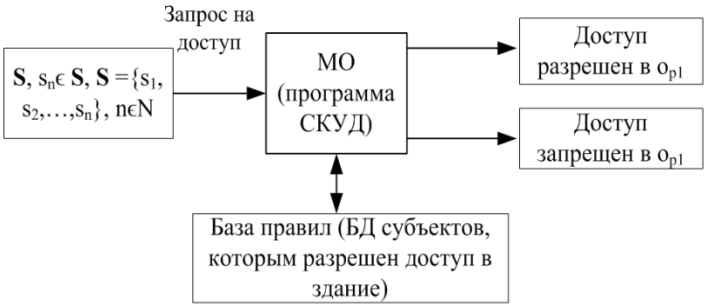

Рис. 2. МО в модели типа «Первый рубеж защиты в организации»

В случае использования дискреционной политики безопасности основной функцией МБО является предоставление доступа к объекту только для санкционированных относительно данного объекта субъектов. Перед МБО стоит задача – проверить приведут ли его действия к нарушению безопасности объекта o_{p1} или нет. Модель Take-Grant предоставляет способ проверки безопасности ИС.

Согласно [7] субъект n_i, $n_i \in \mathbf{N}$, $\mathbf{N} = (n_1, n_2, \ldots, n_i)$, n_1 – нарушитель ИБ в модели типа «Первый рубеж защиты в организации» может получить право доступа к объекту o_{p1} (пропуск в здание), если существует субъект s_1, который обладает правом доступа в o_{p1} (пропуском в здание), такой, что субъекты n_1 и s_1 связаны произвольно ориентированной дугой, содержащей хотя бы одно из прав $t \in \mathbf{R}$ или $g \in \mathbf{R}$.

На рис. 4 изображен граф способа предоставления прав доступа в здание для модели типа «Первый рубеж защиты в организации» в правилах модели Take-Grant, где **S** – множество субъектов, n_1 – субъект-нарушитель, o_{p1} – объект доступа

(здание), **R** – множество прав доступа к объекту o_{p1} (возможность пройти на территорию здания, где располагается организация), и n_1, **S**, o_{p1} – различные вершины графа. Использовано правило классической модели Take-Grant «Давать» – grant (r_1, s_1, n_1, o_{p1}), «Брать» – take (r_1, n_1, s_1, o_{p1}). Таким образом, нарушитель n_1 получил право доступа на охраняемую территорию.

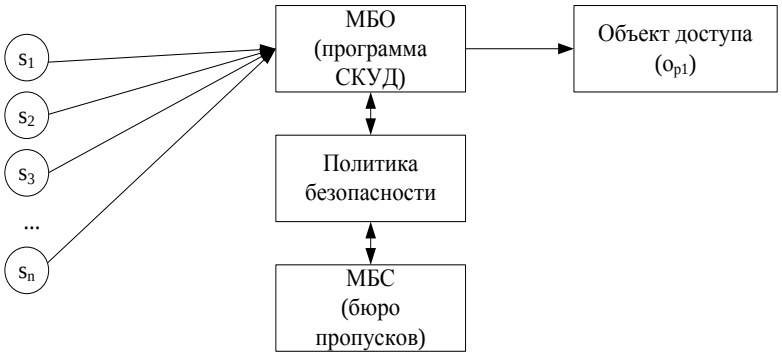

Рис. 3. Схема модели «Первый рубеж защиты в организации»

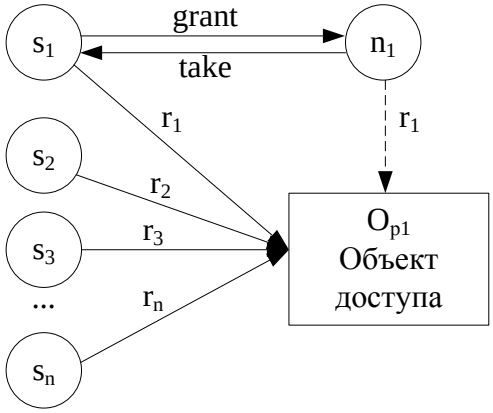

Рис. 4. Граф предоставления прав доступа в здание для модели типа «Первый рубеж защиты в организации»

Модель типа «Первый рубеж защиты в организации» позволит провести анализ реализации действий злоумышленника – проникновение на территорию здания, в ходе которого нарушается рубеж защиты 1.

Безусловно, данный подход к проведению анализа действий злоумышленника позволит выявить возможные пути проведения атак, целью которых является нарушение безопасности информации, определить перечень нарушителей.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Миронова В.Г., Шелупанов А.А., Югов Т.Н.* Реализация модели Take-Grant как представление систем разграничения прав доступа в помещениях // Доклады Том. гос. ун-та систем управления и радиоэлектроники. Ч. 3. – 2011. – № 2 (24). – С. 206-211.
2. *Девянин П.Н.* Модели безопасности компьютерных систем: учеб. пособие для студ. высш. учеб. заведений. – М.: Изд. центр «Академия», 2005. – 144 с.
3. *Грушо А.А., Тимонина Е.Е.* Теоретические основы защиты информации. – М.: Изд-во агентства «Яхтсмен», 1996. – 187 с.

4. *Миронова В.Г., Шелупанов А.А.* Предпроектное проектирование информационных систем персональных данных как этап аудита информационной безопасности // Докл. Том. гос. ун-та систем управления и радиоэлектроники. Ч. 1. – 2010. – № 2 (22).– С. 257-259.
5. *Миронова В.Г., Шелупанов А.А.* Модель нарушителя безопасности конфиденциальной информации // Информатика и системы управления. – 2012. – № 1 (31). – С. 28-35.
6. *Миронова В.Г., Шелупанов А.А.* Сети Петри как инструмент анализа системы защиты конфиденциальной информации // Известия ЮФУ. Технические науки. – 2011. – № 12 (125). – С. 64-70.
7. *Миронова В.Г., Шелупанов А.А*. Предпроектное проектирование информационных систем персональных данных как этап аудита информационной безопасности // Доклады Том. гос. ун-та систем управления и радиоэлектроники. Ч. 1. – 2010. – № 2 (22). – С. 257-259.
8. *Шелупанов А.А., Миронова В.Г. и др.* Автоматизированная система предпроектного обследования информационной системы персональных данных «АИСТ-П» // Доклады Том. гос. ун-та систем управления и радиоэлектроники. Ч. 1. – 2010. – № 1 (21). – С. 14-22.

Статью рекомендовал к опубликованию д.т.н., профессор Л.К. Бабенко.

Миронова Валентина Григорьевна – Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Томский государственный университет систем управления и радиоэлектроники»; e-mail: mvg@security.tomsk.ru; 634050, г. Томск, пр. Ленина, 40; тел.: 89234151608; руководитель аттестационного цента института системной интеграции и безопасности ТУСУРа.

Шелупанов Александр Александрович – e-mail: saa@udcs.ru; тел.: +73822514302; д.т.н.; профессор; проректор по научной работе ТУСУРа.

Mironova Valentina Grigor'evna – Tomsk State University of Control Systems and Radio Electronics; e-mail: mvg@security.tomsk.ru; 40, Lenin avenue, Tomsk, 634050, Russia; phone: +79234151608; the head of the appraisal institute cents systems integration and security TUSUR.

Shelupanov Alexander Alexandrovich – e-mail: saa@udcs.ru; phone: +73822514302; dr. of eng. sc.; professor; vice-rector TUSUR.

УДК 004.735

И.Н. Пащенко, В.И. Васильев

РАЗРАБОТКА ТРЕБОВАНИЙ К СИСТЕМЕ ЗАЩИТЫ ИНФОРМАЦИИ В ИНТЕЛЛЕКТУАЛЬНОЙ СЕТИ SMART GRID НА ОСНОВЕ СТАНДАРТОВ ISO/IEC 27001 И 27005

Приоритетным направлением развития современной энергетики Российской Федерации является внедрение интеллектуальных энергосетей нового поколения Smart Grid. Однако как в отечественной, так и в зарубежной литературе не уделяется достаточного внимания вопросам защиты информации в подобных интеллектуальных сетях. Целью данной работы является разработка методики создания системы защиты информации в Smart Grid сетях с учетом того, что данные сети пока еще не внедрены, а их внедрение займет определенный промежуток времени. Приводится список основных угроз и уязвимостей информационной безопасности, которым подвержены Smart Grid сети. Предлагается список руководящих требований безопасности, которые необходимо выполнить при проектировании данных интеллектуальных сетей. Формируется список контрмер, которые рекомендуются для применения на Smart Grid. Рассчитывается эффективность применения контрмер путем оценки рисков информационной безопасности до и после их внедрения на примере конкретной Smart Grid сети.

Интеллектуальная сеть угрозы; уязвимости; информационные риски.