D.S. Chernyavskiy

A Task of Multi-objective Selection of Network Security Systems in Accordance with Information Security Policies

Key words:information security policy, network security system

A selection task of network security systems in accordance with information security policies is a topical network security concern due to increasing number of information security policies in computer networks and increasing complexity of network security system, which are designed to enforce the policies. The paper discusses methods for selection of network security systems and presents a multi-objective selection model.

Д.С. Чернявский

ЗАДАЧА МНОГОКРИТЕРИАЛЬНОГО ВЫБОРА СЕТЕВЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В СООТВЕТСТВИИ С ПОЛИТИКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Введение

Выбор средств защиты информации, необходимых для реализации политик информационной безопасности (ИБ) (далее – политик), является одним из этапов процесса управления политиками [1]. В силу большого числа политик для информационно-телекоммуникационных сетей (далее – сетей) в организациях [2], а также сложностью сетевых средств защиты информации (ССЗИ) и ограниченностью ресурсов [3], актуальна проблема выбора ССЗИ, в конфигурации которых предполагается реализации политик. В статье рассмотрены существующие методы выбора ССЗИ, а также представлена модель многокритериальной задачи выбора ССЗИ и описан метод решения данной задачи.

Существующие методы нахождения оптимального сетевого средства защиты

Методы, описанные в [4, 5] применяются для решения задачи нахождения оптимального ССЗИ, соответствующего политике, и размещения его в сети. Одним из недостатковданных методов является использование не всех возможных классов ССЗИ. В рамках метода работы [4] используется понятие «почти эквивалентных» функций, однако формального критерия их определения не приводится, что не позволяет классифицировать ССЗИ. В [5] используется четыре класса ССЗИ (межсетевые экраны (МЭ), системы обнаружения вторжений (СОВ), виртуальные частные сети и прокси-серверы), что не позволяет, например, различить пакетный фильтр и МЭ с учетом состояния соединения, так как данные ССЗИ в [4] относятся к одному классу – «МЭ».

Оптимизационная задача в [4] формулируется только как нахождение «почти эквивалентных» ССЗИ, обладающих минимальной стоимостью, где под стоимостью подразумевается значение риска, связанного с неполной реализацией политики. Иными словами, минимизация риска равносильна максимизации защищенности сети, при этом стоимость ССЗИ и ограничения на бюджет не учитываются. Случай, когда несколько различных ССЗИ (не «почти эквивалентных», а эквивалентных) подходят для реализации политики, не рассматривается в [4].

Метод работы [5] позволяет находить оптимальное ССЗИ с учетом его стоимости и ограничений на бюджет, при этом целевая функция задается как максимум защищенности. В данном методе не рассматривается случай, если несколько ССЗИ одного класса подходят для реализации политики, например, МЭ различных платформ не различаются.

Задача выбора ССЗИ может быть сформулирована как многокритериальная, однако оба данных метода решают однокритериальные задачи.

Модель сети и размещение сетевых средств защиты информации

Пусть ССЗИ представлено как одно или совокупность нескольких простых ССЗИ. Простое ССЗИ в свою очередь является абстрактным вычислительным устройством (автоматом), преобразующим входной сетевой трафик в выходной сетевой трафик и вспомогательную информацию (записи журналов регистрации событий, сообщения о нарушениях политик в сети) с учетом заданных политик. Пусть множество простых ССЗИ разбито на классы эквивалентности таким образом, что все простые ССЗИ в рамках класса производят одинаковые выходы при одинаковых входах в соответствии с некоторыми политиками (формальное описание модели ССЗИ и классификации выходит за рамки данной статьи). Простые ССЗИ по сути определяют функциональные возможности ССЗИ (далее простые ССЗИ называются функциями). Таким образом, каждое ССЗИ включает в себя одну или несколько функций, каждая из которых принадлежит некоему классу эквивалентности. Политики задаются с учетом того, в конфигурации функций каких классов предполагается их реализация, при этом политики не зависят от особенностей платформ ССЗИ.

Модель сети может быть задана следующим образом. Пусть $\mathcal{N} = \langle H, L \rangle$ – взвешенный ориентированный граф, где $H = \{h_1, h_2, \dots, h_n\}$ – конечное множество тов; $L = \{(h_i, \mu_{ij}, h_j)\}$ – множество взвешенных дуг, являющихся каналами связи между хостами; $\mu_{ij} \in \mathbb{R}$ – вес дуги, зависящий от пропускной способности канала. Под хостом понимается устройство с одним или более выделенным IP-адресом. Для каждой пары хостов $h_i, h_j \in H$ может существовать не более двух дуг (по одной дуге каждого направления): (h_i, μ_{ij}, h_j) и (h_j, μ_{ji}, h_i). Петли в орграфе $\mathcal{N}$ исключены. Каждой вершине графа может соответствовать один или более IP-адресов. Пусть IP – множество IP-адресов, кроме адресов диапазона 127.0.0.0- 127.255.255.255, предикат $\rho: H \times IP \rightarrow \{0,1\}$ определяет принадлежность данного IP-адреса данному хосту. Группа хостов или сеть (подсеть) также может рассматриваться как вершина графа. Пример моделируемой сети представлен на рис. 1, соответствующая ей модель представлена на рис. 2 (вершине 7 на рис. 2 соответствуют все публичные IP-адреса). ССЗИ размещаются на дугах графа.

В общем случае ССЗИ могут быть по-разному размещены в сети. Для каждого класса ССЗИ могут быть разработаны отдельные требования по его размещению и взаимному расположению относительно других ССЗИ. Так, согласно [6] не существует ограничений на местоположение МЭ в сети. МЭ могут быть размещены не только на границе между сетями, но и перед группами хостов (например, относящихся к наиболее критичным с точки зрения обеспечения ИБ структурным подразделениям организации) и отдельными хостами (серверами), тем самым формируя многоуровневую защиту (англ., defence-in-depth) [6].

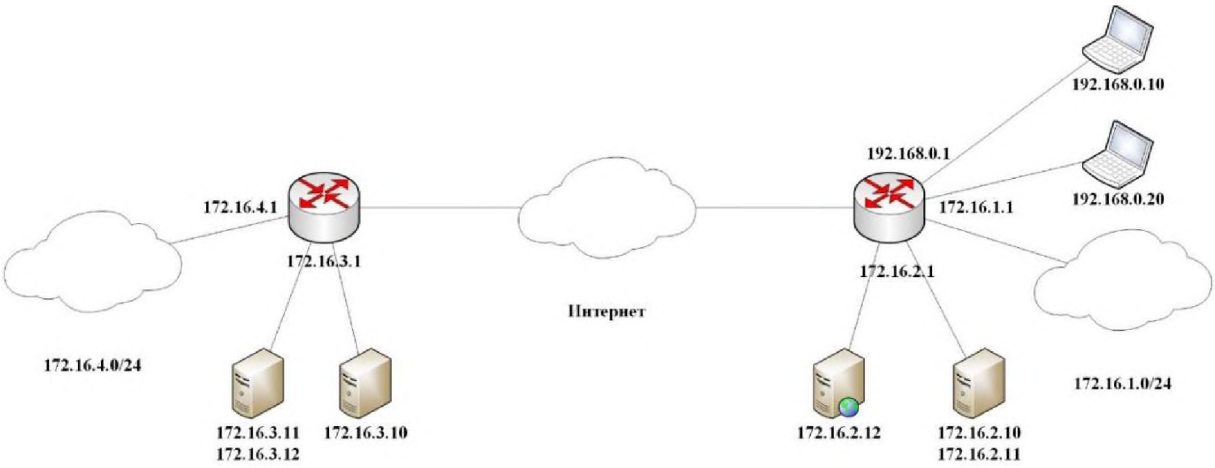

Рис. 1. Пример моделируемой сети

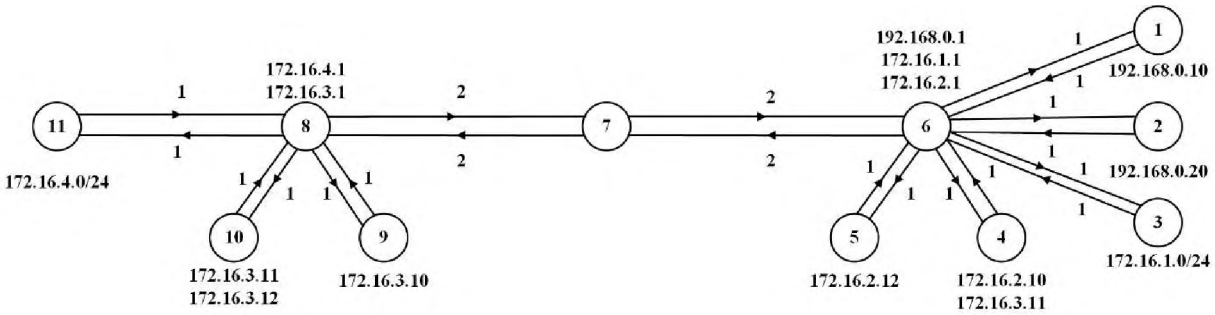

Рис. 2. Модель соответствующей примеру сети

Выбор места размещения ССЗИ в сети зависит от местоположения в сети уязвимой системы и хоста, с которого может быть осуществлена атака злоумышленником. Для размещения ССЗИ в сети могут быть сформулированы следующие правила:

- ССЗИ должно быть размещено на пути трафика от злоумышленника к уязвимой системе. Если путь трафика в сети допускает размещение ССЗИ в нескольких местах, то может быть выбрано любое из этих мест. Например, если в сети, представленной на рис. 2, злоумышленник может осуществить атаку с хоста с номером 11 на уязвимую систему, расположенную в вершине с номером 5, то ССЗИ может быть размещено на любой из дуг $11 \rightarrow 8, 8 \rightarrow 7, 7 \rightarrow 6$ или $6 \rightarrow 5$. Теперь предположим, что атаку на ту же самую систему может осуществить злоумышленник, располагающийся в узле с номером 3, тогда ССЗИ может быть размещено на дуге $3 \rightarrow 6$ или дуге $6 \rightarrow 5$;

- если политика задает возможность размещения ССЗИ в любом из нескольких допустимых мест на пути между атакующим и уязвимой системой (как в приведенных примерах), то выбор места размещения может быть осуществлен на основе дополнительных критериев. Рассмотрение данных критериев выходит за рамки статьи и далее предполагается, что ССЗИ размещается на любой из допустимых дуг.

Если политика задает возможность размещения ССЗИ в нескольких местах, то также может быть применена многоуровневая защита. В случае реализации многоуров-

невой защиты на любом не пустом подмножестве множества допустимых дуг размещаются ССЗИ с одинаковыми функциями, при этом чем на большем количестве дуг размещены ССЗИ, тем выше получаемый в результате суммарный уровень защиты. Однако суммарная стоимость всех ССЗИ не должна превышать значения риска, на снижение которогонаправлено применение таких ССЗИ. Рассмотрение задачи выбора ССЗИ в случае многоуровневой защиты выходит за рамки настоящей статьи.

Задача многокритериальной оптимизации

Классификация ССЗИ позволяет представить каждое $F \in \mathcal{F}$ как совокупность функций (простых ССЗИ), т.е. как вектор

$F = (I_{F_1}(F), I_{F_2}(F), \dots, I_{|\mathcal{F}_s|}(F)) \in 2^{\mathcal{F}_s}$,

где $\mathcal{F}_s$ – множество функций (простых ССЗИ),$2^{\mathcal{F}_s}$– множество всех подмножеств множества $\mathcal{F}_s$. При этом $\forall i \in \{1,2,\dots,|\mathcal{F}_s|\}$, $I_{F_i}(F) \in \{0,1\}$– индикатор, показывающий включена ли в состав ССЗИ Fфункция из класса эквивалентностиF_i. Каждому ССЗИ F может быть присвоен следующий рейтинг R:

$$R(F) = \sum_{i=1}^{|\mathcal{F}_s|} W_{F_i} I_{F_i}(F),$$

где $W_{F_i} > 0$ – весовой коэффициент функции из классаF_i (всем функциям в рамках одного класса присваивается одинаковый весовой коэффициент). Весовой коэффициент определяет значимость конкретной функции и его значение прямо пропорционально количеству уязвимостей, которые позволяет устранить данная функция, и критичности каждой из устраняемых уязвимостей:

$$W_{F_i} = \sum_j V_j^{F_i} S_j,$$

где $V_j^{F_i} \in \{0,1\}$ – индикатор, указывающий на то, что F_i устраняет i-ю уязвимость, $S_j > 0$ – степень критичности j-й уязвимости. Степень критичности уязвимости может быть вычислена на основе данных, полученных из баз уязвимостей и общей системы оценки уязвимостей (CommonVulnerabilityScoringSystem, CVSS) [7].

В общем случае при выборе ССЗИ может оказаться, что ни одно ССЗИ не содержит функции из всех требуемых классов, тогда необходимо производить выбор из комбинаций ССЗИ, включающих требуемые функции. Кроме того, комбинация из нескольких ССЗИ может иметь меньшую стоимость, чем одно ССЗИ, содержащее все требуемые функции. Комбинация из m ССЗИ $F^{i_1}, F^{i_2}, \dots, F^{i_m} \in 2^{\mathcal{F}_s}$может быть определена, как вектор

$$F^{\Sigma} = \bigvee_{j=1}^{m} F^{i_j} = \left(\bigvee_{j=1}^{m} I_{F_1}(F^{i_j}), \bigvee_{j=1}^{mk} I_{F_2}(F^{i_j}), \dots, \bigvee_{j=1}^{m} I_{|\mathcal{F}_s|}(F^{i_j})\right) \in 2^{\mathcal{F}_s},$$

где $\vee$–логическое «или». Другими словами, комбинация ССЗИ рассматривается как ССЗИ (вектор F^{Σ}), включающее в себя функции всех ССЗИ, входящих в состав комбинации. Далее рассматриваются комбинации ССЗИ с учетом того, что одно ССЗИ может быть представлено как комбинация, состоящая из одного данного ССЗИ.

Пусть политика должна быть реализована на lучастках сети (т.е. на дугах графа, моделирующего сеть в соответствии с разделом 2). С этой целью на участке p ($p \in$

$\{1,2,\dots,l\}$) необходимо разместить комбинацию ССЗИF_p^{Σ} с набором функций из классов $F_{i_{1_p}}, F_{i_{2_p}}, \dots, F_{i_{k_p}}$(где k_p – количество функций, необходимых на участке p). При этом $F^{\tilde{\Sigma}} = \{\bigcup_{p=1}^{l} F_p^{\Sigma}\}$ – множество комбинаций, состоящее из комбинаций всех lучастков.

Задача выбора оптимального ССЗИ может является задачей со многими критериями. Так, например, согласно [6] привыборе МЭ могут учитываться: возможность централизованного управления несколькими МЭ и другими ССЗИ; пропускная способность; поддержка возможностей, которые могут потребоваться в будущем (планируемые требования к пропускной способности, поддержка IPv6); нормативно-правовые и другие требования. Требования к выбору МЭ, представленные в [6], также могут быть обобщены на другие ССЗИ.

В общем случае целевые функции и ограничения многокритериальной задачи нахождения оптимального ССЗИ формулируется следующим образом:

$$\varphi_1 \to max/min, \varphi_2 \to max/min, \dots \varphi_n \to max/min,$$
$$F^{\tilde{\Sigma}} \in \{F^{\tilde{\Sigma}*} = \{\bigcup_{p=1}^{l} F_p^{\Sigma*}\} : F_p^{\Sigma*} = \bigvee_{j_p=1}^{m_{p*}} F^{i_{j_p}} \wedge \forall p \in \{1,2,\dots,l\}, \forall i \in \{i_{1_p}, i_{2_p}, \dots, i_{k_p}\} \to I_{F_i}(F_p^{\Sigma*}) = 1\},$$

где n – количество критериев, m_{p*} – количество ССЗИ в составе комбинации $F_p^{\Sigma*}$, устанавливаемой научастке p.

Одной из проблем современных ССЗИ (в частности МЭ нового поколения (англ., Next-generationFirewall, NGFW) [6]), является их пропускная способность. По этой причине пропускная способность относится к одному из важных требований, которые необходимо учитывать при выборе ССЗИ. Требования к пропускной способности могут задаваться для каждого участка сети отдельно. При формулировании задачи выбора ССЗИ могут учитываться его рейтинг, пропускная способность и стоимость, а такженормативно-правовые требования (например, наличие сертификата соответствия).

Целевые функции и ограничения для задачи многокритериального выбора ССЗИ могут быть заданы следующим образом:

$$\varphi_1(F^{\tilde{\Sigma}}) = R(F^{\tilde{\Sigma}}) = \sum_{l=1}^{p} \sum_{j_p=1}^{m_p} R(F^{i_{j_p}}) \to max,$$
$$\varphi_2^1(F_1^{\Sigma}) = \min\left(T(F^{i_{1_1}}), T(F^{i_{2_1}}), \dots, T(F^{i_{m_1}})\right) \to max,$$
$$\dots,$$
$$\varphi_2^l(F_p^{\Sigma}) = \min\left(T(F^{i_{1_l}}), T(F^{i_{2_l}}), \dots, T(F^{i_{m_l}})\right) \to max,$$
$$\varphi_3(F^{\tilde{\Sigma}}) = \sum_{p=1}^{l} \sum_{j_p=1}^{m_p} Cer(F^{i_{j_p}}) \to max,$$
$$\varphi_4(F^{\tilde{\Sigma}}) = \sum_{p=1}^{l} \sum_{j_p=1}^{m_p} C(F^{i_{j_p}}) \to min,$$
$$F^{\tilde{\Sigma}} \in \{F^{\tilde{\Sigma}*} = \{\bigcup_{p=1}^{l} F_p^{\Sigma*}\} : F_p^{\Sigma*} = \bigvee_{j_p=1}^{m_{p*}} F^{i_{j_p}} \wedge \forall p \in \{1,2,\dots,l\}, \forall i \in \{i_{1_p}, i_{2_p}, \dots, i_{k_p}\} \to I_{F_i}(F_p^{\Sigma*}) = 1\}$$

где $\varphi_1(F^{\tilde{\Sigma}})$ – функция, определяющая суммарныйрейтинг комбинаций ССЗИ по всем требуемым участкам сети; $\varphi_2^p(F)$ (где $p \in \{1,2,\dots,l\}$) – функция, определяющая пропускную способностьна участке сети p как минимальную пропускную способность среди всех ССЗИ на данном участке, входящих в соответствующую комбинацию из множества $F^{\tilde{\Sigma}}$ ($T(F)$ – функция, определяющая пропускную способность ССЗИ F); $\varphi_3(F^{\tilde{\Sigma}})$ – функция, определяющая суммарное количество ССЗИ в $F^{\tilde{\Sigma}}$, имеющих сертификат соответствия ($Cer(F) \in \{0,1\}$ – индикатор, показывающий наличие сертификата у ССЗИ F); $\varphi_4(F^{\tilde{\Sigma}})$ – суммарная стоимость всех комбинаций ССЗИ, входящих в $F^{\tilde{\Sigma}}$ ($C(F)$ – стоимость ССЗИ F). Дополнительно могут быть введены ограничения на пропускную способность каждого участка сети, минимальное число ССЗИ, имеющих сертификат соответствия, а также ограничения на бюджет:

$$T(F^{i_{1_1}}), T(F^{i_{2_1}}), \dots, T(F^{i_{m_1}}) \geq T_1,$$
$$\dots,$$
$$T(F^{i_{1_l}}), T(F^{i_{2_l}}), \dots, T(F^{i_{m_l}}) \geq T_l,$$
$$\sum_{p=1}^{l} \sum_{j_p=1}^{m_p} Cer(F^{i_{j_p}}) \geq Cer_{min},$$
$$\sum_{p=1}^{l} \sum_{j_p=1}^{m_p} C(F^{i_{j_p}}) \leq C_{limit},$$

где $T_1, \dots, T_l$ – минимальные пропускные способности на соответствующих участках сети; Cer_{min} – минимальное количество ССЗИ, имеющих сертификат соответствия; C_{limit} – ограничения на бюджет.

Любая из целевых функций может быть заменена соответствующими ограничениями, что приводит к уменьшению количество целевых функций и, как следствие, упрощению задачи. В случае, если ограничениями заменяются все целевые функции, кроме одной (например, кроме φ_1), то задача становится однокритериальной и может быть решена методом динамического программирования [8]. Многокритериальная задача (в изначальной постановке со всеми целевыми функциями или в постановке с некоторым непустым подмножеством целевых функций и заменой остальных функций ограничениями) также может быть решена методом динамического программирования на множествах Парето [8]. Результатом решения многокритериальной задачи методом динамического программирования является множество Парето. Выбор одного решения из этого множества может быть осуществлен, например, методом уступок или методом свертки критериев [8].

Если ни одно ССЗИ не соответствует ограничениям, то из рассмотрения может быть исключена функция с минимальным весовым коэффициентом (тем самым приводя к минимальному остаточному риску, связанному с неполной реализацией политики) и повторно решена та же самая задача, но без учета данной функции. Если решение снова не найдено, до из рассмотрения исключается следующая по значению весового коэффициента функция, первая функция возвращается в число рассматриваемых, и задача решается заново. Данные действия повторяются до тех пор, пока не будет найдено решение. Если на каком-либо этапе исключаемая функция имеет больший весовой коэффициент, чем суммарный весовой коэффициент некоторого подмножества функций, то сначала из рассмотрения исключается данное подмножество (или последовательно исключаются различные подмножества, если таковых несколько). В силу того, что на

каждом шаге величина устраняемого риска изменяется, необходимо следить за тем, чтобы стоимость допустимых решений не превышала значение устраняемого риска.

Заключение

При выборе ССЗИ могут учитываться не только их функциональные возможности, но и другие критерии, например, стоимость, пропускная способность и наличие сертификата соответствия. В статье представлена модель задачи, использующая данные критерии, описаны основные шаги и методы решения задачи. Также в статье представлены модель сети и правила размещения ССЗИ в сети.

СПИСОК ЛИТЕРАТУРЫ:

1. Rees J., Bandyopadhyay S., Spafford E. H. PFIRES: A Policy Framework for Information Security // Communications of the ACM. Vol. 46. Issue 7. 2003. P. 101-106.
2. Chapple M. J., D'Arcy J., Striegel A. An Analysis of Firewall Rulebase (Mis) Management Practices // ISSA Journal. February. 2009. P. 12-18.
3. Cyberthreat Defense Report North America & Europe, CyberEdge Group, 2014.
4. Preda S., Cuppens-Boulahia N., Cuppens F., Toutain L. Architecture-Aware Adaptive Deployment of Contextual Security Policies // Proceedings of International Conference on Availability, Reliability, and Security. 2010. P. 87-95.
5. Rahman M., Al-Shaer E. A Formal Framework for Network Security Design Synthesis // Proceedings of the 2013 IEEE 33rd International Conference on Distributed Computing Systems. 2013. P. 560-570.
6. Scarfone K., Hoffman P. Guidelines on Firewalls and Firewall Policy, NIST Special Publication 800-41 Revision 1, National Institute of Standards and Technology, 2009.
7. Mell P., Scarfone K., Romanosky S. A Complete Guide to the Common Vulnerability Scoring System Version 2.0, 2007 [Электронныйресурс]. URL: http://www.first.org/cvss/cvss-guide.pdf (дата обращения 20.04.2015).
8. Струченков, В.И. Методы оптимизации в прикладных задачах, – М.: Солон-Пресс, 2009. 320 с.

REFERENCES:

1. Rees J., Bandyopadhyay S., Spafford E. H. PFIRES: A Policy Framework for Information Security // Communications of the ACM. Vol. 46. Issue 7. 2003.P. 101-106.
2. Chapple M. J., D'Arcy J., Striegel A. An Analysis of Firewall Rulebase (Mis) Management Practices // ISSA Journal. February. 2009. P. 12-18.
3. Cyberthreat Defense Report North America & Europe, CyberEdge Group, 2014.
4. Preda S., Cuppens-Boulahia N., Cuppens F., Toutain L. Architecture-Aware Adaptive Deployment of Contextual Security Policies // Proceedings of International Conference on Availability, Reliability, and Security. 2010. P. 87-95.
5. Rahman M., Al-Shaer E. A Formal Framework for Network Security Design Synthesis // Proceedings of the 2013 IEEE 33rd International Conference on Distributed Computing Systems. 2013. P. 560-570.
6. Scarfone, K., Hoffman, P. Guidelines on Firewalls and Firewall Policy, NIST Special Publication 800-41 Revision 1, National Institute of Standards and Technology, 2009.
7. Mell P., Scarfone K., Romanosky S. A Complete Guide to the Common Vulnerability Scoring System Version 2.0, 2007 [Электронныйресурс].URL: http://www.first.org/cvss/cvss-guide.pdf (date of access: 20.04.2015).