УДК 621.391

А.В. Снегуров, В.Х. Чакрян

Харьковский национальный университет радиоэлектроники, Харьков

ПОДХОД К ВЫЧИСЛЕНИЮ РЕЙТИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТЕВЫХ УСТРОЙСТВ

В данной статье предлагается подход к вычислению рейтинга информационной безопасности узлов телекоммуникационной сети, на основании которого можно судить о защищенности информации, передаваемой через данный узел. Это позволит повысить управляемость сетью и предоставит возможность более тщательно подойти к вопросу выбора маршрута передачи информации в телекоммуникационной сети, учитывая не только критерии качества обслуживания, но и критерии информационной безопасности.

Ключевые слова: *рейтинг безопасности, безопасность сетевых устройств, информационная безопасность, анализ рисков, метрики безопасности, CCSS, NIST.*

Введение

В современных условиях одним из основных процессов управления телекоммуникационной сетью (ТКС) является процесс управления ее информационной безопасностью (ИБ). Данный процесс должен осуществляться как на этапе проектирования сети, так и на этапе ее функционирования, и подразумевает постоянный анализ рисков ИБ сети. На реализацию данного процесса существенно влияет возможность изменения структуры, топологии и режимов работы ТКС при ее функционировании. Такая ситуация может иметь место вследствие добавления новых устройств в сеть или изменения настроек уже работающих устройств, поломок оборудования, неправильных действий администраторов сети, пользователей и т.п. Подобного рода изменения ведут к неизбежному появлению новых рисков ИБ.

При анализе рисков ИБ одним из основных оцениваемых параметров является степень (уровень) уязвимости элементов сети к информационным атакам. В настоящее время для оценки данного параметра используется вероятностный подход [1 – 4], основанный на расчете вероятности уязвимости сетевых устройств. Недостатком такого подхода является сложность или отсутствие адекватных математических методов расчета данной вероятности для различных сетевых устройств, телекоммуникационных технологий и современных информационных атак, наличие неопределенности относительно задаваемых исходных данных. Это приводит к ошибкам при анализе рисков ИБ, понижению управляемости сети в аспекте информационной безопасности.

Целью статьи является введение комплексного показателя информационной безопасности сетевых устройств - рейтинга их информационной безопасности. Данный показатель позволяет подойти к проектированию и управлению сетью с использованием процесса анализа рисков ИБ.

Концепция рейтинга информационной безопасности сетевых устройств

Введем понятие рейтинга информационной безопасности сетевых устройств (далее – Рейтинг ИБ). Рейтинг ИБ - это величина, которая показывает, насколько безопасна передача трафика через определенное сетевое устройство (маршрутизатор, коммутатор) с учетом заданной конфигурации сети и настроек самого устройства. Под информационной безопасностью в данном случае подразумевается обеспечение конфиденциальности, доступности и целостности информации, передаваемой по сети.

Как видно из определения Рейтинга ИБ при его расчете должны учитываться следующие исходные данные:

1. Текущая или планируемая конфигурация сети.
2. Текущие или планируемые настройки сетевых устройств.

Анализ конфигурации сети позволяет учесть особенности структуры телекоммуникационной сети:

- расположение сетевых устройств;
- типы сетевых устройств;
- технологии передачи данных;
- логическое расположение интерфейсов (какие из интерфейсов соединяются с внешней сетью, а какие с внутренней).

Определение настроек сетевых устройств осуществляется путем автоматизированного анализа конфигурационных файлов устройства на соответствие определенным критериям: включены ли определенные функции безопасности, верно ли задана адресация, корректность настройки сетевых протоколов и т.п.

Наличие вышеуказанной информации позволяет корректно подойти к расчету Рейтинга ИБ. Так, например, для такого расчета необходимо знать тип сетевого устройства: проводной либо беспроводной маршрутизатор; тип используемых в сетевом устрой-

стве программных (программно-аппаратных) средств безопасности: брандмауэр, система предотвращения вторжений и т.д. Не менее важны технологии передачи информации, как логические, так и физические: Ethernet, PPP, Frame Relay, наличие защищенного VPN туннеля для безопасной передачи трафика и т.п. В зависимости от этого изменяется список необходимых настроек безопасности на устройстве, которые требуется проверить: так для обеспечения безопасности в Ethernet сети нужны одни механизмы безопасности, а при передаче информации по PPP каналу совершенно другие. Соответственно при использовании VPN туннеля следует учитывать, насколько безопасные алгоритмы были выбраны для его построения, верно ли заданы параметры, которые указывают, какой поток должен быть защищен.

Подход к математическому описанию рейтинга информационной безопасности сетевых устройств

За основу математического описания Рейтинга ИБ сетевых устройств взят отчет NIST Interagency Report 7502 “The Common Configuration Scoring System (CCSS): Metrics for Software Security Configuration Vulnerabilities” [5]. Описанная в данном документе методика позволяет оценить и измерять уязвимости механизмов безопасности программного обеспечения в заданной среде и с определенными параметрами по 10-ти бальной шкале. Несмотря на то, что разработанный в NIST подход на данный момент применяется для оценки уязвимостей лишь в программном обеспечении, тем не менее, данный подход можно адаптировать для оценки уязвимостей устройств и систем.

Для того чтобы рассмотреть, как можно применить методику CCSS для оценки и измерения уязвимостей в ТКС, разберем основные параметры, используемые для расчетов метрик CCSS. Существуют следующие группы метрик:

- базовые метрики (постоянны и не изменяются со временем);

- временные метрики (не постоянны и могут изменяться со временем);

- метрики окружающей среды (метрики, которые позволяют детализировать базовые и временные метрики и учесть особенности среды, в которой находится оцениваемая уязвимость).

Каждая из групп метрик состоит из подгрупп и локальных метрик, которые используются для расчета групповой метрики. В данной статье рассматриваются лишь базовые метрики, которые позволяют оценить постоянную составляющую степени уязвимости без учета временных параметров и окружения, в которой находится уязвимость.

Базовая группа метрик (англ. “Base Metrics”) состоит из:

a) базовая возможность эксплуатации уязвимости (англ. “Base Eploitability”):

- вектор доступа (англ. “Access Vector [AV]”);

- сложность доступа (англ. “Access Complexity [AC]”);

- требования аутентификации (англ. “Authentication [AU]”);

- уровень привилегий (англ. “Privilege Level [PL]”) – в некоторых случаях используется при расчете временных метрик;

- метод эксплуатации (англ. “Exploitation Method”) - не используется при расчете, однако позволяет группировать уязвимости по определенным критериям;

b) базовый ущерб (англ. “Base Impact”):

- ущерб конфиденциальности информации (англ. “Confidentiality Impact [C]”);

- ущерб целостности информации (англ. “Integrity Impact [I]”);

- ущерб доступности информации (англ. “Availability Impact [A]”).

«Вектор доступа» определяется методом доступа, который необходим злоумышленнику, чтобы эксплуатировать уязвимость. В данной методике определено три метода доступа:

- локальный – злоумышленнику требуется непосредственный физический доступ к объекту, на котором расположена уязвимость;

- смежная сеть – злоумышленнику требуется доступ в пределах одной локальный сети (одного широковещательного домена) с уязвимым объектом;

- сетевой – злоумышленник может эксплуатировать уязвимость удаленно из любого участка сети, в том числе через Интернет.

«Сложность доступа» определяется тем, насколько сложна атака: насколько должны быть глубоки знания злоумышленника при осуществлении доступа в сеть (взлома злоумышленником механизмов защиты от несанкционированного доступа в сеть), насколько сложные действия должен совершить администратор сети при защите сети. В данной методике определено три уровня сложности доступа:

- высокий – злоумышленник должен совершить ряд сложных действий для эксплуатации уязвимости (к примеру: взломать стороннее приложение, чтобы гарантировать уровень доступа для заданной атаки);

- средний – злоумышленник должен выполнить ряд действий средней сложности (например, написать поддельное электронное письмо сотруднику); атака социальной инженерии должна быть незаметной подозрительным сотрудникам телекоммуникационной компании (пример: фишинг, подмена ссылок и т.п.);

- низкий – злоумышленник должен выполнить серию простых действий (пример: отправить поддельный ARP-пакет для проведения атаки ARP spoofing).

«Требования аутентификации» определяется количеством процедур аутентификации, которые должен совершить злоумышленник для эксплуатации уязвимости. В данной методике определено три уровня аутентификации:

- множественная – злоумышленник должен совершить больше одной процедуры аутентификации для эксплуатации уязвимости;

- одноразовая – злоумышленнику достаточно единожды аутентифицироваться для эксплуатации уязвимости;

- отсутствует – злоумышленнику не требуется проходить процедуру аутентификации для эксплуатации уязвимости.

Метрика ущерба определяется тремя метриками ущерба конфиденциальности, целостности и доступности. Данная метрика указывает на то, какой ущерб может быть нанесен ресурсу в случае эксплуатации уязвимости.

«Ущерб конфиденциальности» определяется величиной ущерба конфиденциальности информации в случае успешной эксплуатации уязвимости. В данной методике определено три уровня ущерба конфиденциальности:

- отсутствует – ущерб конфиденциальности информации отсутствует;

- частичный – присутствует частичное разглашение конфиденциальных данных; злоумышленник не имеет возможности контролировать информационную область, к которой получил доступ; присутствует доступ к некоторым системным файлам, однако область утери конфиденциальности ограничена (пример: злоумышленник получил доступ к нескольким таблицам в базе данных);

- полный – присутствует полное разглашение конфиденциальных данных, что приводит к раскрытию всех системных файлов; злоумышленник имеет возможность считывать все системные файлы (память, файлы и т.п.).

«Ущерб целостности» определяется величиной ущерба целостности информации в случае удачной эксплуатации злоумышленником уязвимости. В данной методике определено три уровня ущерба целостности:

- отсутствует – ущерб целостности информации отсутствует;

- частичный – злоумышленник имеет возможность изменять некоторые системные файлы, однако не имеет возможности контролировать всю информационную область, к которой получил доступ;

- полный – злоумышленник имеет возможность изменять любые системные файлы по своему усмотрению, что приводит к полной компрометации целостности информации.

«Ущерб доступности» определяется величиной ущерба доступности информации в случае удачной эксплуатации злоумышленником уязвимости. В данной методике определено три уровня ущерба доступности:

- отсутствует – ущерб доступности информации отсутствует;

- частичный – присутствует частичное уменьшение производительности либо временная недоступность ресурса (пример: DDoS атака определенной службы на ресурсе);

- полный – злоумышленник имеет возможность сделать ресурс полностью недоступным.

«Уровень привилегий» определяется уровнем неавторизованного доступа, который может получить злоумышленник. В данной методике определено четыре уровня привилегий:

– корневой (англ. “Root Level [R]”);

– пользовательский (англ. “User Level [U]”);

– уровень приложения (англ. “Application Level [A]”);

– не определен (англ. “Not Defined [ND]”).

Метод эксплуатации определяет то, каким образом злоумышленником эксплуатируются уязвимости системы. В данной методике определено два уровня метода эксплуатации:

– пассивный – в данном случае злоумышленник использует неправильные настройки системы или отсутствие защитных механизмов для эксплуатации уязвимости);

– активный – в данном случае злоумышленником осуществляется взлом защитных механизмов системы для компрометации ресурса.

Каждому из уровней представленных выше метрик соответствует определенное числовое значение, представленное в табл. 1. Данные значения предоставлены в отчете NIST и являются константами.

Методика CCSS позволяет численно выразить общую базовую метрику заданной уязвимости, а затем изменить полученный уровень на основании оценки временных метрик и метрик окружающей среды для конкретной организации и для определенной ситуации. В данной работе приведен пример оценки лишь базовых метрик.

Формула для расчета Рейтинга ИБ сетевого устройства (без учета временных метрик и метрик окружающей среды) выглядит следующим образом:

$$R_{без} = 10 - \sum_{i=1}^{N} B_{score_i} \Big/ N, \qquad (1)$$

где $R_{без}$ – рейтинг ИБ сетевого устройства в пределах [0; 10]; $\sum_{i=1}^{N} B_{score_i}$ – сумма всех базовых метрик по всем уязвимостям сетевого устройства; N – общее количество оцениваемых уязвимостей сетевого устройства.

Таблица 1

Параметры базовых метрик

Вектор доступа		
Требуется локальный доступ	Возможен доступ из смежной сети	Возможен доступ из любой сети
0,395	0,646	1,0
Аутентификация		
Требует несколько итераций аутентификации	Аутентификация требуется лишь одноразово	Аутентификация не требуется
0,45	0,56	0,704
Сложность доступа		
Сложная	Средняя	Легкая
0,35	0,61	0,71
Ущерб конфиденциальности		
Отсутствует	Частичный	Полный
0,0	0,275	0,66
Ущерб целостности		
Отсутствует	Частичный	Полный
0,0	0,275	0,66
Ущерб доступности		
Отсутствует	Частичный	Полный
0,0	0,275	0,66

$$B_{score} = \lceil ((0{,}6 \cdot I) + (0{,}4 \cdot E) - 1{,}5) \cdot f(I) \rceil^{1\_dec}, \quad (2)$$

где B_{score} – это показатель базовой метрики;

I – ущерб; E – возможность эксплуатации;

$f(I)$ – это функция от ущерба, расчет которой приведен ниже;

$\lceil \rceil^{1\_dec}$ – округление в большую сторону с точностью до одной десятой.

$$I = 10{,}41 \cdot (1 - (1 - I_c) \cdot (1 - I_i) \cdot (1 - I_a)), \quad (3)$$

где I_c – ущерб от нарушения конфиденциальности;

I_i – ущерб от нарушения целостности;

I_a – ущерб от нарушения доступности информации.

$$E = 20 \cdot A_v \cdot A \cdot A_c, \quad (4)$$

где A_v – это вектор доступа;

A – требования к аутентификации;

A_c – сложность доступа.

$$f(I) = \begin{cases} 0, \text{если } I = 0 \\ 1{,}176, \text{если } I \neq 0 \end{cases}, \quad (5)$$

где $f(I)$ – функция от ущерба;

I – величина возможного ущерба.

Чем больше данный Рейтинг ИБ сетевого устройства, тем более защищено устройство от угроз информационной безопасности.

Пример использования методики CCSS для оценки рейтинга информационной безопасности сетевого устройства

Для более детального описания методики приведем пример расчета Рейтинга ИБ сетевого устройства одной из сетевых уязвимостей. К примеру, на коммутаторе не настроена функция безопасности портов (англ. “Port Security”), что приводит к возможности подключения нелегального устройства в сеть и проведения атаки на коммутатор типа наводнение MAC адресами (англ. “MAC Address Flooding” [12]). Данная уязвимость дает злоумышленнику возможность перехватывать весь трафик в сети. Также будем считать, что пользователи не используют защищенных VPN туннелей и других механизмов безопасности передаваемого трафика. Ниже приведен расчет базовых метрик для заданной уязвимости.

Для расчета базовой метрики используется базовый вектор, в соответствии с которым используются необходимые значения, приведенные в табл. 1.

Для описания вектора необходимо указать метрики и их уровни в прописном формате в одну строку. Метрики отделяются от уровней двоеточием, а метрики от других метрик – косой чертой. Описание базового вектора приведено ниже:

вектор доступа: смежная сеть (англ. “Adjacent Network [A]”); сложность доступа: низкая (англ. “Low [L]”); требование аутентификации: отсутствует (англ. “None [N]”); ущерб конфиденциальности: полный (англ. “Complete [C]”); ущерб целостности: полный; ущерб доступности: полный; уровень привилегий: не определено (англ. “Not Defined [ND]”); метод доступа: активный (англ. “Active [A]”).

Исходя из описания, базовый вектор записывается следующим образом:

AV:A/AC:L/Au:N/C:C/I:C/A:C/PL:ND/AM:A.

Здесь приведен общепринятый формат записи уязвимостей при расчете метрик по данной методике. Все аббревиатуры приведены из английского алфавита, как указано в отчете NIST [5].

Проведем расчет Рейтинга ИБ коммутатора для вышеперечисленных условий на основании формул (1) – (5) и табл. 1:

$$I = 10{,}41 \cdot (1 - (1 - 0{,}66) \cdot (1 - 0{,}66) \cdot (1 - 0{,}66)) = 10{,}00085;$$

$$f(I) = 1{,}176;$$

$$E = 20 \cdot 0.646 \cdot 0.704 \cdot 0.71 = 6{,}457933;$$

$$B_{score} = \left\lceil \begin{matrix} (((0{,}6 \cdot 10{,}00085) + \\ + (0{,}4 \cdot 6{,}457933) - 1{,}5) \cdot 1{,}176) \end{matrix} \right\rceil^{1\_dec} = 8{,}3$$

$$R_{без} = 10 - \frac{8{,}3}{1} = 1{,}4.$$

Как видно из данного примера Рейтинг ИБ оцениваемого коммутатора крайне мал. Наличие на маршруте передачи информации коммутатора с таким Рейтингом ИБ существенно ухудшает возможности обеспечения информационной безопасности передаваемой информации.

Область применения рейтинга информационной безопасности сетевых устройств

На основании рейтинга ИБ могут быть выполнены многие функции управления телекоммуникационной сетью, к примеру:

- передача трафика по наиболее безопасным узлам (выбор наиболее безопасного маршрута передачи трафика);
- динамическое отслеживание устройств с небезопасными либо неверными настройками;
- автоматизированный сбор статистической хронологически упорядоченной информации для проведения внутреннего аудита безопасности телекоммуникационной сети;
- своевременное оповещение ответственных лиц и администраторов системы о возможных некорректных настройках устройств, рисках информационной безопасности и не оптимальной передачи трафика.

К примеру, Рейтинг ИБ сетевых устройств можно учитывать в качестве параметра при расчете метрики маршрута. Подобные научные работы уже проводятся [1-4]. Сервер, который может играть роль анализирующего узла, должен содержать топологию сети и иметь конфигурационные файлы устройств для их анализа. Имеющаяся на сервере карта сети и Рейтинг ИБ каждого из сетевых устройств позволяет использовать подход, который применяется в алгоритмах динамической маршрутизации трафика с контролем линии (англ. “Link State Protocol”), таких как OSPF [6, 7] или OLSR [8].

Объединив учет рисков информационной безопасности с параметрами качества обслуживания, появится возможность выбирать наиболее качественный маршрут с учетом безопасности передаваемого трафика. Такой механизм работы можно реализовать, используя алгоритмы предварительного расчета маршрутов. На эту тему также проводятся исследования, однако, с точки зрения построения отказоустойчивой сети, а не с точки зрения информационной безопасности [9].

Также данный подход позволяет динамически отслеживать возникающие уязвимости на сетевых устройствах, что позволяет своевременно отреагировать и предотвратить возможность компрометации данных. Объединив данное решение с системой защиты конфиденциальной информации от внутренних угроз (англ. “Information Protection and Control [IPC]”) и системой предотвращения утечек (англ. “Data Leak Prevention [DLP]” [13, 14]), которая классифицирует информацию, можно предъявлять определенные требования к формированию маршрутов трафика в сети в зависимости от критичности нарушения доступности, целостности либо конфиденциальности передаваемой информации. Это связано с тем, что все устройства по-разному подвержены определенного рода уязвимостям. В одном случае устройство будет более уязвимо к атакам типа отказ в обслуживании, на других устройствах может быть скомпрометирована конфиденциальность информации. Определив насколько критична для трафика потеря конфиденциальности, целостности и доступности можно будет выдвигать требования к формированию маршрута в зависимости от того какие устройства менее подвержены определенного рода атакам. Чтобы грамотно классифицировать чувствительную информацию в соответствии с критериями критичности для конфиденциальности, целостности и доступности информации можно воспользоваться разработанными стандартами в этой области, к примеру, одним из стандартов NIST [10].

Выводы

Концепция Рейтинга ИБ сетевых устройств телекоммуникационных сетей позволяет динами-

чески отслеживать риск информационной безопасности для каждого из устройств в сети. Данный подход позволяет гибко управлять телекоммуникационной сетью, в том числе передачей трафика в сети с учетом рисков информационной безопасности всех устройств, по которым должен пройти трафик.

В данной статье не приведено типовых ситуаций с динамическим принятием решений о выборе маршрута передачи трафика на основе Рейтинга ИБ сетевых устройств. Также приведенная методика расчета данного показателя не позволяет отдельно оценить риск информационной безопасности для конфиденциальности, целостности и доступности, что уменьшает гибкость принятия решений при выборе маршрута и требует дальнейшего изучения. Данные исследования будут представлены в следующих работах авторов.

Список литературы

1. Snigurov A. Approach of routing metrics formation based on information security risk / A.Snigurov., V.Chakryan // Experience of Designing and Application of CAD Systems in Microelectronics (CADSM). - IEEE, 2013. – P. 339-340.

2. Snegurov A.V. The approach for selection of a routing metric in special-purpose wireless networks under the influence of radio-electronic investigation / A.V. Snegurov, V.K. Chakryan, A.A. Mamedov / //Microwave and Telecommunication Technology (CriMiCo), 2013 23rd International Crimean Conference. – IEEE, 2013. – P. 470-471.

3. Снегуров А.В. Метод формирования метрик маршрутизации, основанный на рисках информационной безопасности / А.В. Снегуров, В.Х. Чакрян // Системи управління, навігації та зв'язку, 2012. – вип.4 (24). - С. 105 – 109.

4. Снегуров А.В. Механизм повышения живучести телекоммуникационной сети путем выбора метрики маршрутизации с использованием теории риска информационной безопасности / А.В. Снегуров, В.Х. Чакрян // Проблемы инфокоммуникаций. Наука и технологии (PICS&T'2013). - 2013. – С. 81 – 84.

5. Scarfone K. The common configuration scoring system (ccss): Metrics for software security configuration vulnerabilities / K. Scarfone, P. Mell //National Institute of Standard and Technology. – 2010. – 36 p.

6. Moy J. OSPF version 2 / J. Moy. – 1998. – 244 p.

7. Coltun R. et al. OSPF for IPv6 / R.Coltun //IETF RFC2740. – 2008. – T. 2. – C. 839-841.

8. Clausen, T. RFC 3626. Optimized link state routing protocol (OLSR) / T. Clausen, P. Jacque. – 2003. - 75 p.

9. Lemeshko A.V. Probabilistic-temporal model of QoS-routing with precomputation of routes under the terms of non-ideal reliability of telecommunication network / A.V. Lemeshko // Telecommunications and Radio Engineering. – 2007. – T. 66. – №. 13. – P. 1151-1166.

10. Stine K. SP 800-60 Rev. 1. Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories; Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories / K. Stine., R. Kissel, W. C. Barker – 2008. - 53 p.

11. Kraemer S. Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists / S. Kraemer, P. Carayon // Applied Ergonomics. – 2007. – T. 38. – №. 2. – C. 143-154.

12. Spangler R. Packet sniffing on layer 2 switched local area networks / R. Spangler // Packetwatch Research. – 2003. – 5 p.

13. Liu S. Data loss prevention / S. Liu, R.Kuhn // IT professional. – 2010. – T. 12. – №. 2. – C. 10-13.

14. McCallister E. SP 800-122. Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) / E. McCallister, T. Grance, K. Scarfone – 2010. – 59 p.

Поступила в редколлегию 16.12.2013

Рецензент: д-р техн. наук, проф. А.В. Лемешко, Харьковский национальный университет радиоэлектроники, Харьков.

ПІДХІД ДО ОБЧИСЛЕННЯ РЕЙТИНГУ БЕЗПЕКИ МЕРЕЖЕВИХ ПРИСТРОЇВ

А.В. Снігуров, В.Х. Чакрян

В даній статті пропонується підхід до обчислення рейтингу інформаційної безпеки вузлів телекомунікаційної мережі, на основі якого можна робити висновки щодо захищеності інформації, що передається через цей вузол. Це дозволить підвищити управління мережею і та надасть змогу більш ретельно підійти до питання вибору маршруту в передачі інформації в телекомунікаційній мережі, враховуючи не тільки критерії якості обслуговування, але й критерії інформаційної безпеки.

Ключові слова: *рейтинг безпеки, безпека мережевих пристроїв, інформаційна безпека, аналіз рисок, метрики безпеки, CCSS, NIST.*

APPROACH OF CALCULATION OF NETWORK DEVICES SECURITY RATING

A.V. Snigurov, V.K. Chakrian

In this paper it is proposed an approach of calculation of network devices security rating that can be used as an index that shows if information is secure when it transfers through this node. This approach allows to increase the network manageability and provides the more thoroughly way of choosing the route for information transferring in telecommunication network, considering not only the criterions of quality of service, but also the criterions of information security.

Keywords: *rating of safety, safety of networkings issues, informative safety, analysis of risks, birth-certificates of safety, CCSS, NIST.*