УДК 004.056.5

**Н.С. Егошин**

# Модель типовых угроз безопасности информации, основанная на модели информационных потоков

Процесс защиты информации подразумевает комплексный подход. Необходимо затронуть все возможные аспекты в области защиты информации, в частности, определить полный перечень угроз и в будущем использовать данный перечень угроз с конкретной системой. Важна именно полнота перечня угроз, так как при отсутствии какого-либо элемента вероятность реализации угрозы резко возрастает. Таким образом, необходимо формирование модели угроз, способной предоставить полноценный перечень угроз. Модели угроз должны стать отправными точками для проектирования будущих систем защиты компьютерных и информационных систем.

**Ключевые слова:** информационная безопасность, защита информации, модель угроз, информационный поток.
**doi:** 10.21293/1818-0442-2021-24-3-21-25

**Актуальность**

Проблематика исследования связана с тем, что на сегодняшний день все имеющиеся модели угроз безопасности информации носят весьма условный характер. Нет единого принципа построения модели угроз. Существуют несколько подходов, и всем им присущи принципиальные недостатки, а именно: отсутствие четкого понятия «модели угроз», разительное отличие структур и принципов функционирования моделей, способов применения модели, избыточность модели в виде слияния с моделью нарушителя и многое другое.

Наличие этих и некоторых других пробелов в существующих подходах отрицательно сказывается на эффективности работы эксперта с самой моделью и на конечном результате, обусловленном отсутствием стандартизованных итоговых оценок одной модели угроз относительно другой. Поэтому задачей настоящего исследования является создание собственной модели угроз информации.

**Описание несанкционированных потоков**

Принцип построения модели угроз основан на модели элементарных информационных потоков [1], а именно на понятии элементарного информационного потока, который представлен на рис. 1 и описывается тройкой

$$g = \{\mathbf{V}_i, \mathbf{E}_z, \mathbf{V}_j\},$$

где $\mathbf{V}_i$, $\mathbf{V}_j$ – множества носителей информации (множество вершин потока); $\mathbf{E}_z$ – множество каналов передачи информации.

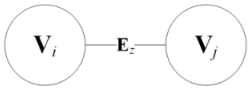


Рис. 1. Графическое представление элементарного информационного потока

Канал передачи информации – это не какой-то абстрактный, а вполне реальный объект, который обладает некоторыми физическими и/или виртуальными свойствами. Из этого следует, что к нему возможен такой же доступ, как и к двум другим элементам потока.

Обозначим и классифицируем виды воздействия. Согласно [2] несанкционированное воздействие на информацию – это воздействие на защищаемую информацию с нарушением установленных прав и (или) правил доступа, приводящее к утечке, искажению, подделке, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Само определение несанкционированного доступа подразумевает появление в системе нового элемента, который будет осуществлять этот самый доступ. Используя обозначенную ранее нотацию, данную ситуацию можно изобразить следующим образом (рис. 2):

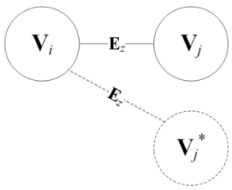


Рис. 2. Возникновение несанкционированного элемента множества $\mathbf{V}_j$*, который получает информацию из элемента $\mathbf{V}_i$

Аналогичная ситуация возможна для любого элемента информационного потока. По аналогии с описанной выше ситуацией (см. рис. 2) доступ может быть осуществлен как к элементу множества $\mathbf{V}_j$, так и к $\mathbf{E}_z$.

Взаимодействие с элементами элементарного информационного потока приводит к угрозам нарушения целостности и доступности, а взаимодействие с информацией, циркулирующей в этом потоке, к угрозам нарушения конфиденциальности [3].

Не все авторы уделяют внимание этому обстоятельству в своих работах. В большинстве случаев говорится о состоянии безопасности информационного потока [4–6], без классификации возможных воздействий и последствий, что является необходимым ввиду разной природы происхождения воздействия [7–9].

**Типовые угрозы целостности и доступности**

Три возможные связи чужеродного элемента $V_j^* \rightarrow V_i$, $V_j^* \rightarrow V_j$, $V_j^* \rightarrow E_z$ описывают ситуации, при

которых оказывается непосредственное воздействие на один из элементов информационного потока, что может привести к искажению информации или её уничтожению.

Из всего вышесказанного следует, что на любой из элементов элементарного информационного потока, а значит и на информацию, может быть оказано любое из трёх видов несанкционированного воздействия:

– уничтожение;

– искажение;

– подмена.

Снова обратимся к понятию элементарного информационного потока и разберём взаимосвязь между видами воздействия на элементы потока с классическими аспектами информационной безопасности: целостностью и доступностью.

Применительно к вершинам потока:

– уничтожение информации на одной из вершин приводит к нарушению целостности информации;

– искажение информации на одной из вершин приводит к нарушению целостности информации;

– подмена информации на одной из вершин приводит к нарушению целостности информации.

Применительно к каналу передачи информации:

– уничтожение информации в канале приводит к нарушению доступности;

– искажение информации в канале приводит к нарушению целостности;

– подмена информации в канале приводит к нарушению доступности.

Итого: четыре типовые угрозы целостности и две – доступности. Необходимо обратить внимание, что информационный поток имеет две симметричные вершины, и воздействие может быть оказано на любую из них, что приводит к тому, что количество угроз целостности, направленных на вершины, вырастает вдвое, а значит, итоговое их число становится равно семи. Таким образом, разобрав все возможные виды воздействия на информационный поток, можно построить полное множество типовых угроз целостности и доступности информации.

Множество угроз целостности

$$\mathbf{C} = \{c_i \mid c \in \mathbf{C}\},\ i = \overline{1,7},$$

где $c_1$, $c_2$, $c_3$, $c_4$, $c_5$, $c_6$, $c_7$ – типовые угрозы целостности информации.

Множество угроз доступности

$$\mathbf{D} = \{d_1, d_2\},$$

где $d_1$, $d_2$ – типовые угрозы доступности информации.

Зная, что множество элементарных информационных потоков и множество типовых угроз целостности и доступности информации конечны, сопоставим каждый элемент множеств **C** и **D** с каждым элементом множества **G** и получим новое множество, которое будет состоять из всех сочетаний угроз и потоков, т.е. являться их декартовым произведением.

$$\mathbf{G} \times (\mathbf{C} \cup \mathbf{D}) =$$

$$= \{g_1c_1, g_1c_2, g_1c_3, g_1c_4, g_1c_5, g_1c_6, g_1c_7, g_1d_1, g_1d_2,$$
$$g_2c_1, g_2c_2, g_2c_3, g_2c_4, g_2c_5, g_2c_6, g_2c_7, g_2d_1, g_2d_2,$$
$$g_3c_1, g_3c_2, g_3c_3, g_3c_4, g_3c_5, g_3c_6, g_3c_7, g_3d_1, g_3d_2,$$
$$g_4c_1, g_4c_2, g_4c_3, g_4c_4, g_4c_5, g_4c_6, g_4c_7, g_4d_1, g_4d_2,$$
$$g_5c_1, g_5c_2, g_5c_3, g_5c_4, g_5c_5, g_5c_6, g_5c_7, g_5d_1, g_5d_2,$$
$$g_6c_1, g_6c_2, g_6c_3, g_6c_4, g_6c_5, g_6c_6, g_6c_7, g_6d_1, g_6d_2,$$
$$g_7c_1, g_7c_2, g_7c_3, g_7c_4, g_7c_5, g_7c_6, g_7c_7, g_7d_1, g_7d_2,$$
$$g_8c_1, g_8c_2, g_8c_3, g_8c_4, g_8c_5, g_8c_6, g_8c_7, g_8d_1, g_8d_2\}.$$

Посчитаем мощность итогового множества.

$$|\mathbf{G}| * (|\mathbf{C}| + |\mathbf{D}|) = 8 * (7+2) = 72.$$

Из этого следует, что множество типовых угроз целостности и доступности информации в системе можно свести к конечному множеству типовых угроз, мощность которого равна семидесяти двум.

**Типовые угрозы конфиденциальности**

Если говорить исключительно о конфиденциальности информации, то по определению её нарушение не подразумевает нарушения целостности или доступности, хотя и может к этому привести [2]. Из определения информационного потока следует, что нарушение конфиденциальности происходит при подмене любого из его элементов, т. е. возможны следующие случаи:

– подмена любой из двух вершин;

– подмена канала.

При этом возможны ситуации, когда будут скомпрометированы сразу несколько элементов. Теперь, зная общее количество элементов и количество состояний этих элементов, можно посчитать общее количество состояний элементарного информационного потока.

Для этого применим формулу расчета мощности множества

$$N = p^i,$$

где $p$ – количество состояний элемента; $i$ – количество элементов.

В нашем случае $p = 2$, так как любой элемент потока может иметь два состояния – скомпрометирован или нет, а $i = 3$, так как элементарный информационный поток состоит из трёх элементов [10]. В итоге общее количество завязанных на компрометации элементов состояний элементарного информационного потока будет равняться восьми. Однако при построении модели угроз нет необходимости рассматривать составные варианты компоновки, так как такой подход приведёт к высокому уровню дублирования различных угроз, потому достаточным будет рассмотрение только четырёх базовых состояний: скомпрометирован один из элементов множества **V**, элемент **E** или ни один из элементов.

Необходимо отдельно разобрать ситуацию, когда ни один из элементов системы не является скомпрометированным. Дело в том, что помимо простой подмены возможна ситуация так называемой «прослушки» элемента, т.е. доступ к хранимой в нём информации из-за пределов контролируемой зоны. Однако «прослушка» уже не будет применима ко всем трём элементам, так как слежение за вершиной подразумевает либо внедрение в уже существующий канал передачи информации, что тождественно прослушиванию канала, либо возникновение нового неразрешенного, что совпадает с подменой канала, и всё же остается вариант, когда скомпрометирована может быть уже вся система целиком.

Таким образом, разобрав все возможные виды вмешательства в информационный поток, построим полное множество типовых угроз конфиденциальности информации.

Обозначим множество типовых угроз конфиденциальности

$$\mathbf{K} = \{k_1, k_2, k_3, k_4\},$$

где $k_1$, $k_2$, $k_3$, $k_4$ – типовые угрозы конфиденциальности информации.

По аналогии с моделью типовых угроз целостности и доступности информации соотнесем каждую типовую угрозу конфиденциальности с каждым элементарным информационным потоком, т.е. построим декартово произведение множеств **K** и **G** и посчитаем итоговую мощность этого множества.

$$\mathbf{G} \times \mathbf{K} = \{g_1k_1, g_1k_2, g_1k_3, g_1k_4,$$
$$g_2k_1, g_2k_2, g_2k_3, g_2k_4,$$
$$g_3k_1, g_3k_2, g_3k_3, g_3k_4,$$
$$g_4k_1, g_4k_2, g_4k_3, g_4k_4,$$
$$g_5k_1, g_5k_2, g_5k_3, g_5k_4,$$
$$g_6k_1, g_6k_2, g_6k_3, g_6k_4,$$
$$g_7k_1, g_7k_2, g_7k_3, g_7k_4,$$
$$g_8k_1, g_8k_2, g_8k_3, g_8k_4\};$$
$$|\mathbf{G} \times \mathbf{K}| = |\mathbf{G}| * |\mathbf{K}| = 8 * 4 = 32.$$

Из этого следует, что множество типовых угроз конфиденциальности информации в системе можно свести к конечному множеству типовых угроз, мощность которого равна тридцати двум.

**Модель угроз и сравнение с аналогами**

Несмотря на то, что описанные в предыдущих пунктах модели угроз имеют разное обоснование полноты, в их основе всё же лежит одинаковый математический аппарат. Благодаря этому результирующие угрозы могут быть объединены в общее множество угроз. Итоговая мощность множества типовых угроз будет равняться сумме мощностей двух множеств, а значит, общее количество типовых угроз по всем трём аспектам будет равняться 104.

Учитывая тот факт, что технологии развиваются нарастающими темпами, мы не можем с точностью предсказать, какие устройства ввода/вывода, хранения или передачи информации в принципе будут существовать через несколько лет. Тем более вряд ли можно рассчитывать на составление полного перечня угроз информации, которая будет обрабатываться с помощью ныне несуществующих приборов.

При всём этом можно с уверенностью сказать, что множество типовых угроз останется неизменным, так как используемый в основе модели угроз аппарат имеет высокую степень абстракции и строится на теории графов, а не на объектах реального мира. В рамках модели любое устройство представляется как канал передачи информации независимо от своей реализации. От специалиста потребуется только обеспечить добавление этого канала (устройства) на этапе описания всей системы. Внедренная абстракция позволяет описать систему вплоть до минимального уровня взаимодействия элементов [11]. Глубину детального описания системы специалист определяет самостоятельно в зависимости от целесообразности и предъявляемых требований [12]. Однако на данном этапе не идет речи об автоматизации процесса формирования полного перечня угроз, так как перечень актуальных угроз бесконечно дополняется и такая задача является попросту невыполнимой [13]. Данное исследование предполагает определение только типовых угроз.

Из проведенного в [14] анализа моделей угроз следует, что перечень угроз из [15] перекрывает все угрозы, обозначенные в остальных моделях. Следовательно, дальнейшее сравнение результатов настоящего исследования будет производиться именно с [15].

Учитывая специфику исследования, а именно обеспечение безопасности информации, обрабатываемой в системе, было произведено сопоставление выделенных из [15] угроз информации с типовыми угрозами, представленными в авторской модели.

По итогам сопоставления всем угрозам из [15] удалось определить соответствующие угрозы из авторской модели. Однако составить полное соотношение не удалось: не для каждой типовой угрозы из авторской модели нашлись угрозы из [15]. В [15] нет примеров для следующих типовых угроз:

– $g_1c_4$ – уничтожение информации, обрабатываемой пользователем;

– $g_1c_5$ – подмена информации, обрабатываемой процессом;

– $g_1c_6$ – подмена информации, обрабатываемой пользователем;

– $g_2c_2$ – передача н/с процессом информации санкционированному пользователю;

– $g_3c_1$ – передача н/с процессом информации санкционированному процессу;

– $g_3c_2$ – передача н/с процессом информации санкционированному процессу;

– $g_3c_5$ – подмена информации, обрабатываемой процессом;

– $g_3c_6$ – подмена информации, обрабатываемой процессом;

– $g_3c_7$ – воздействие на информацию при ее передаче по каналу в электромагнитной среде;

– $g_5c_6$ – подмена информации, обрабатываемой процессом;

– $g_5c_7$ – воздействие на информацию при ее передаче по каналу в электромагнитной среде;

– $g_7c_6$ – подмена информации, хранящейся на носителе информации;

– $g_7c_7$ – воздействие на информацию при ее передаче по каналу в электромагнитной среде.

Все обнаруженные пробелы относятся к угрозам целостности, при этом большая их часть относится к потокам $g_1$, $g_3$, $g_5$ и $g_7$, в которых передача информации осуществляется по электромагнитному каналу.

В модели угроз ФСТЭК были угрозы, которые могли бы подойти указанным типовым угрозам, однако они были отвергнуты в виду того, что в их описании было явно указано, что данная угроза вызвана программно и/или направлена на объект в виртуальной среде. К тому же модель ФСТЭК не учитывает деление канала передачи информации на виртуаль-

ный и электромагнитный, но делит на такие классы носители информации. Ещё одной проблемой является то, что модель ФСТЭК не учитывает направленность угрозы, что вызывает большое количество дублирований при сопоставлении моделей.

**Заключение**

В ходе исследования была разработана и предложена модель типовых угроз конфиденциальности, целостности и доступности информации, которая учитывает модель элементарных информационных потоков и позволяет классифицировать угрозы по направленности на каждую из трёх составляющих элементарного информационного потока.

Сравнение разработанной модели с наиболее полной базой угроз позволило выделить ещё 13 типовых угроз.

Работа выполнена при финансовой поддержке Министерства науки и высшего образования РФ в рамках базовой части государственного задания ТУСУРа на 2020–2022 гг. (проект № FEWM-2020-0037).

*Литература*

1. Новохрестов А.К. Модель угроз безопасности информации и её носителей / А.К. Новохрестов, А.А. Конев, А.А. Шелупанов, Н.С. Егошин // Вестник Иркут. гос. техн. ун-та. – 2017. – Т. 21, № 10. – С. 93–104.

2. Загинайлов Ю.Н. Теория информационной безопасности и методология защиты информации: учеб. пособие. – Москва; Берлин: Директ-Медиа, 2015. – 253 с.

3. Конев А.А. Подход к построению модели угроз защищаемой информации // Доклады ТУСУР. – 2012. – № 1 (25). – С. 34–39.

4. Тарасенко А.И. Критерии оценки эффективности обеспечения информационной безопасности при управлении информационными потоками на основе динамических приоритетов // Science Time. – 2016. – № 4. – С. 816–825.

5. Верешник А.В. Способ защиты информационных потоков в многооператорных информационно-телекоммуникационных сетях / А.В. Верешник, В.Г. Федоров, А.В. Попова // Матер. IV Всерос. науч.-практ. конф. «Современные информационные технологии. Теория и практика». – Череповец: Изд-во Череп. гос. ун-та. – 2018. – С. 154–158.

6. Десницкий В.А. Реализация средств верификации сетевых информационных потоков с использованием метода «Проверка на модели» // Матер. 9-й конф. по проблемам управления «Информационные технологии в управлении». – СПб.: Концерн «Центральный научно-исследовательский институт «Электроприбор»». – 2016. – С. 680–683.

7. Mouna Jouini, Latifa Ben Arfa – Threat classification: State of art. – May 2016 // Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security [Электронный ресурс]. – Режим доступа: https://www.researchgate.net/publication/313241139_Threat_classification_State_of_art, свободный (дата обращения: 22.09.2021).

8. Ruf L. Threat Modeling in Security Architecture – the Nature of Threats / L. Ruf, A. Thorn, T. Christen, B. Gruber, R. Portmann, H. Luzer // ISSS Working Group on Security Architectures [Электронный ресурс]. – Режим доступа: https://scribd.com/document/47730732/ISSS-AG-Security-Architecture-Threat-Modeling-Lukas-Ruf, свободный (дата обращения: 22.09.2021).

9. Geric S., Hutinski Z. Information system security threats classifications // Journal of Information and Organizational Sciences. – 2007. – P. 31–51 [Электронный ресурс]. – Режим доступа: https://www.researchgate.net/ publication/ 26596385_Information_system_security_threats_classifications, свободный (дата обращения: 22.09.2021).

10. Ануфриенко С.А. Введение в теорию множеств и комбинаторику: учеб. пособие. – Екатеринбург: УрГУ, 1998. – 62 с.

11. Егошин Н.С. Модель угроз безопасности информации, передаваемой через Интернет / Н.С. Егошин, А.А. Конев, А.А. Шелупанов // Информация и безопасность. – 2018. – Т. 21, № 4. – С. 530–533.

12. Новохрестов А.К. Оценка качества защищенности компьютерных сетей / А.К. Новохрестов, А.А. Конев // Динамика систем, механизмов и машин. – 2014. – № 4. – С. 85–87.

13. Шелупанов А.А. Актуальные направления развития методов и средств защиты информации / А.А. Шелупанов, О.О. Евсютин, А.А. Конев, Е.Ю. Костюченко, Д.В. Кручинин, Д.С. Никифоров // Доклады ТУСУР. – 2017. – Т. 20, № 3. – С. 11–24.

14. Новохрестов А.К. Обзор подходов к построению моделей информационной системы и угроз ее безопасности / А.К. Новохрестов, А.А. Конев // Актуальные проблемы обеспечения информационной безопасности: Тр. межвуз. науч.-практ. конф. – Самара: Инсома-Пресс, 2017. – С. 151–155.

15. Банк данных угроз безопасности информации. ФСТЭК России [Электронный ресурс]. – Режим доступа: http://bdu.fstec.ru (дата обращения: 22.09.2021).

---

**Егошин Николай Сергеевич**
Ст. преп. каф. комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) Томского университета
систем управления и радиоэлектроники (ТУСУР)
Красноармейская ул., 146, г. Томск, Россия, 634034
ORCID: 0000-0003-4770-0701
Тел.: +7-961-095-54-18
Эл. почта: ens@fb.tusur.ru

Egoshin N.S.

**Model of typical threats to information security based on the model of information flows**

The information security process involves an integrated approach. It is necessary to cover all possible aspects in the field of information protection to define a complete list of threats and in the future use this list of threats according to a specific system. It is important to make it more complete possible, since if ever it is missing any element, the chances for the threats to appear increase dramatically. Thus, it is necessary to form a threat model allowing to provide a complete list of threats. The threat models should become the starting points for the design of future security systems for computer and information systems.

**Keywords:** information security, information protection, threat model, information flow.
**doi:** 10.21293/1818-0442-2021-24-3-21-25

*References*

1. Novokhrestov A.K, Konev A.A, Shelupanov A.A, Egoshin N.S. [Information and information carrier security threat model]. *Proceedings of Irkutsk State Technical University*, 2014, vol. 21, no. 10, pp. 93–94 (in Russ.).

2. Zaginaylov Yu.N. *Teoria informacionnoy bezopasnosti I metodologii zashiti informacii: uchebnoe posobie* [Information security theory and information security methodology: a tutorial]. *M. Berlin: Direct-Media*, 2015, 253 p. (in Russ.).

3. Konev A.A. [Approach to creation protected information model]. *Proceedings of TUSUR University*, 2012, no. 1-2 (25), pp. 34 –39 (in Russ.).

4. Tarasenko A.I. *Kriterii ocenki effektivnosti obespecheniya informacionnoj bezopasnosti pri upravlenii informacionnymi potokami na osnove dinamicheskih prioritetov* [Criteria for assessing the effectiveness of information security in managing information flows based on dynamic priorities]. *Science Time*, 2016, no. 4, pp. 816–825 (in Russ.).

5. Vershnik A.V., Fedorov V.G., Popova A.V. [Method of protecting information flows in multi-operator information and telecommunication networks]. *Materials of the IV All-Russian Scientific and Practical Conference «Modern Information Technologies. Theory and practice»* Cherepovets: Cherepovets State University, 2018, pp. 154–158 (in Russ.).

6. Desnickiy V.A. [Implementation of verification tools for network information flows using the «Model check» method]. *Materials of the 9th Conference on Management Problems «Information Technologies in Management»*, St. Petersburg: Concern «Central Research Institute Electropribor», 2016, pp. 680–683 (in Russ.).

7. Mouna Jouini, Latifa Ben Arfa. Threat classification: State of art. *Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security*, 2016. – Available at: https://www.researchgate.net/publication/313241139_Threat_classification_State_of_art, free (Accessed: September 22, 2021).

8. Ruf L., Thorn A., Christen T., Gruber B., Portmann R., Luzer H. Threat Modeling in Security Architecture - The Nature of Threats. *ISSS Working Group on Security Architectures.* Available at: https://scribd.com/document/47730732/ISSS-AG-Security-Architecture-Threat-Modeling-Lukas-Ruf, free (Accessed: September 22, 2021).

9. Geric S, Hutinski Z. Information system security threats classifications. *Journal of Information and Organizational Sciences*, 2007, vol. 31, no. 1. Available at: https://jios.foi.hr/index.php/jios/article/view/29, free (Accessed: September 22, 2021).

10. Anufrienko S.A. Vvedenie v teoriu mnozhestv I kombinatoriku: uchebnoe posobie [Introduction to set theory and combinatorics: tutorial]. Ekb., 1998, 62 p. (in Russ.).

11. Egoshin N.S., Konev A.A., Shelupanov A.A. [Security threats model of information transmitted by internet]. *International Scientific Conference on Electronic Devices and Control Systems*, 2018, vol. 21, no. 4, pp. 530–533 (in Russ.).

12. Novokhrestov A.K., Konev A.A. [Assessment the quality of computer network security]. *Dinamica system, mekhanizmov i mashin*, 2014, no. 4, pp. 85–87 (in Russ.).

13. Shelupanov A.A., Evsutin O.O., Konev A.A., Kostychenko E.Yu., Kruchinin D.V., Nikiforov D.S. [Modern trends in development of methods and means for information protection]. *Proceedings of TUSUR University*, 2017, vol. 20, no. 3, pp. 11–24.

14. Novokhrestov A.K., Konev A.A. [Review of approaches to building models of an information system and threats to its security]. *Actual problems of information security: Proceedings of the Interuniversity Scientific and Practical Conference*, Samara: Insoma-Press, 2017, pp. 151–155 (in Russ.).

15. Databank of information security threats. FSTEC of Russia – Available at: http://bdu.fstec.ru/, free. (Accessed: September 22, 2021).

---

**Nikolay S. Egoshin**
Senior Lecturer of Department of Complex Information Security of Computer Systems, Tomsk State University of Control Systems and Radioelectronics
146, Krasnoarmeyskaya st., Tomsk, Russia, 634034
ORCID: 0000-0003-4770-0701
Phone: +7-961-095-54-18
Email: ens@fb.tusur.ru