УДК 004.056
DOI 10.33764/2618-981X-2022-6-240-249

# Ранжирование мер обеспечения безопасности значимых объектов критической информационной инфраструктуры

*А. В. Ситская*[1]*, *В. В. Селифанов*[1]

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация

* e-mail: AnSits@yandex.ru

**Аннотация.** Одна из главных задач государства - правильное функционирование внутренних систем, обеспечивающих достойный уровень жизни для граждан. Но что же на самом деле обеспечивает функционирование деятельности государства в разных сферах? Одними из главных систем обеспечения стали критические информационные инфраструктуры и их значимые объекты, а также сети электросвязи, используемые для организации взаимодействия таких объектов. Приказ ФСТЭК России № 239 содержит в себе меры защиты, но не описывает методы оценки эффективности защиты значимых объектов критической информационной инфраструктуры, что в свою очередь ставит под сомнение качество оценивания построенных систем защиты. В данной статье рассматривается ранжирование угроз и разработка метода оценивания эффективности построенной системы защиты на основе весовых коэффициентов. За основу разработанного метода взята методика оценивания уровня защиты безопасности информационной системы Центрального банка России.

**Ключевые слова:** критическая информационная инфраструктура, значимый объект критической информационной инфраструктуры, информационная безопасность, весовые коэффициенты, ранжирование, методика оценивания безопасности информационных систем

# Ranking of security measures of significant objects of critical information infrastructure

*A. V. Sitskaya*[1]*, *V. V. Selifanov*[1]

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation

* e-mail: AnSits@yandex.ru

**Abstract.** One of the main tasks of the state is the proper functioning of internal systems that provide a decent standard of living for citizens. But what actually ensures the functioning of the activities of the state in various areas? Critical information infrastructures and their significant objects, as well as telecommunication networks used to organize the interaction of such objects, have become one of the main support systems. Order of the FSTEC of Russia No. 239 contains protection measures, but does not describe methods for assessing the effectiveness of protection of significant objects of critical information infrastructure, which in turn casts doubt on the quality of assessment of built protection systems. This article discusses the ranking of threats and the development of a method for evaluating the effectiveness of the built protection system based on weighting factors. The developed method is based on the methodology for assessing the level of security protection of the information system of the Central Bank of Russia

**Keywords:** critical information infrastructure, significant object of critical information infrastructure, information security, weight coefficients, ranking, methodology for assessing the security of information systems.

## *Введение*

2021 год охарактеризовался началом плановых проверок значимых объектов критической информационной инфраструктуры (ЗО КИИ). Прошло чуть более трех лет с начала действия федерального закона № 187 «О безопасности критической информационной инфраструктуры Российской Федерации» [1] и внесения сведений о первых объектах в соответствующий реестр.

В соответствии с постановлением Правительства РФ № 162 [2] предметом плановой проверки является соблюдение субъектом КИИ требований по обеспечению безопасности, обеспечивающих устойчивое функционирование ЗО КИИ при проведении в отношении его компьютерных атак.

При этом, приказом ФСТЭК России № 127 [3] установлены положения нормативных правовых актов, выполнение которых подлежит проверке. Их анализ показывает, что существует всего две градации: соответствует и не соответствует. И не дается критериев, по которым можно судить не только о выполнении или невыполнении положений постановлений Правительства РФ и приказов регулятора, а можно сделать вывод о возможности или невозможности совершения нарушителем действий, приводящих к неприемлемым рискам (последствиям).

Анализ практики контрольной деятельности ФСТЭК России в смежных направлениях (контроль защиты информации в государственных информационных системах, государственных информационных системах персональных данных, ключевых системах информационной инфраструктуры) и научных исследований (публикаций) в этих областях показал аналогичную картину.

## *Метод оценивания соблюдения мер ЦБ РФ*

В отличие от документов ФСТЭК России документы ЦБ РФ, а именно ГОСТ Р 57580 [4, 5] имеют строгую систему оценивания, которая содержит в себе качественную и количественную оценки.

В 2017 и 2018 годах Центральным банком России была разработана серия ГОСТов 57580. ГОСТ Р 57580.1 – 2017 [4] содержит в себе базовый состав организационных и технических мер, касающихся защиты информации. Данный состав мер получился гибким и подстраивающимся под любые информационные системы, но не менее важной разработкой стал ГОСТ Р 57580.2 [5], содержащий в себе методы оценки эффективности защиты, согласно выбранным мерам ГОСТа 57580.1 [4]. Метод оценки в использовании оказался прост и результативен, что подтверждается эффективной защитой ИС банков. Именно поэтому за основу метода оценки соблюдения мер приказа ФСТЭК России №239 [6] следует взять метод оценки ЦБ России.

Метод ЦБ России основан на весовых коэффициентах, которые, в свою очередь, отражают степень значимости той или иной характеристики по отношению к другим. Наибольшее влияние на конечный результат оказывает именно весовой коэффициент. Весовой коэффициент возможно определить множеством способов, но в случае КИИ целесообразно обратиться к методу графов. Именно граф наиболее наглядно и последовательно отражает взаимосвязь объектов. После его

построения станет возможно описать матрицу, которая покажет связи элементов в числовом виде.

### *Построение графа ранжирования мер*

Приказ ФСТЭК России №239 [6] содержит в себе 17 групп мер, которые регулируют как техническую часть, так и организационную. Построим граф, касающийся проведения аудита безопасности ЗО КИИ (рис. 1).

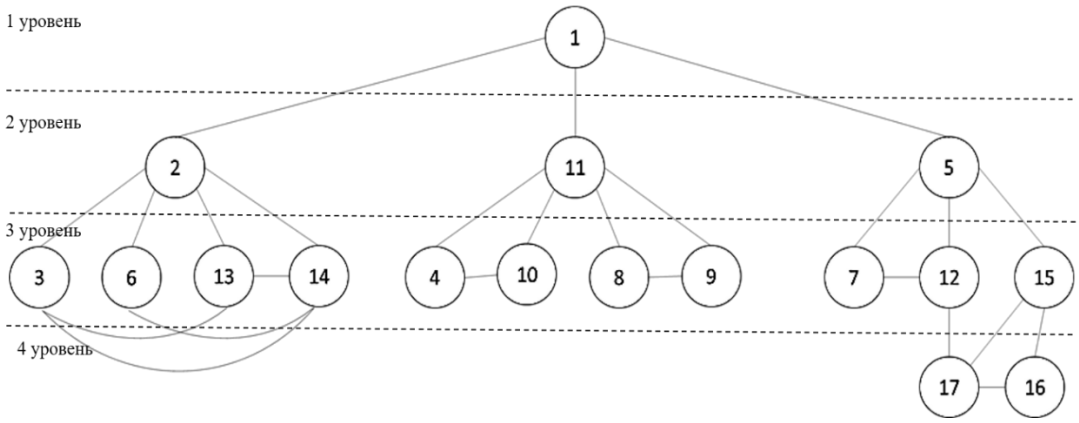


Рис. 1. Граф ранжирования мер обеспечения безопасности ЗО КИИ

Вершины графа обозначены в соответствии с группами мер 239 приказа [6]:

1) идентификация и аутентификация;
2) управление доступом;
3) ограничение программной среды;
4) защита машинных носителей информации;
5) аудит безопасности;
6) антивирусная защита;
7) предотвращение вторжений (компьютерных атак);
8) обеспечение целостности;
9) обеспечение доступности;
10) защита технических средств и систем;
11) защита информационной (автоматизированной) системы и ее компонентов;
12) реагирование на компьютерные инциденты;
13) управление конфигурацией;
14) управление обновлениями программного обеспечения;
15) планирование мероприятий по обеспечению безопасности;
16) обеспечение действий в нештатных ситуациях;
17) информирование и обучение персонала.

Граф построен на основе анализа и систематизации рейтинга SANS CIS Controls 8 [2], анализа литературы [12 – 16] но наибольший вклад в ранжирование мер внес практический опыт ФСТЭК России по сибирскому Федеральному округу в проведении проверок значимых объектов КИИ.

В графе меры распределены по уровням согласно их весу в системе защиты, а также последовательности проверки. Граф наглядно демонстрирует всевозможные связи групп мер между собой, которые в свою очередь необходимы при построении эффективной системе защиты. Три ветви графа между собой равноценны, т.к. свидетельствуют о трех параллельных проверках.

В графе два основных уровня: первый и второй. Первый уровень графа содержит одну вершину – группа мер, которая касается идентификации, аутентификации. Данная группа мер стоит выше остальных, поскольку является наиболее весомой. Если не будут организованы идентификации и аутентификации, тогда абсолютно любой пользователь, злоумышленник будут иметь свободный доступ к ЗО КИИ, что, в свою очередь, делает дальнейшую защиту абсолютно бессмысленной и неэффективной.

Второй уровень графа включает в себя три вершины: управление доступом, аудит безопасности, защиты ИС и ее компонентов. Поскольку данный уровень имеет тесную взаимосвязь с последующими, то в какой-то степени можно говорить о том, что он обобщает все последующие группы мер, связанные с той или иной вершиной. Вершина 2, или вершина управления доступом, содержит в себе группы мер напрямую связанные с организацией технической части, а именно ОС и ПО. Вершина 5, или вершина аудита безопасности, так или иначе содержит в себе по большей части организационные меры, связанные с выявлением угроз и реагировании в соответствии с ними, а также обучение персонала. Вершина 11, или вершина защиты ИС и ее компонентов также содержит в себе совокупность технической и организационной частей. Вершина объединяет в себе группы мер связанные с обеспечением безопасности оборудования, доступа к нему и самой ИС.

### *Построение матрицы ранжирования мер*

Чтобы наиболее ярко продемонстрировать связи элементов графа, на его основе строится матрица (рис. 2).

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| 2 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 |
| 3 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 |
| 4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| 5 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 |
| 6 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 |
| 7 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 |
| 8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| 9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| 10 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| 11 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 12 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| 13 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 |
| 14 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 |
| 15 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |
| 16 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 |
| 17 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 0 |

Рис. 2. Матрица графа ранжирования мер обеспечения безопасности ЗО КИИ

В матрице все связи между элементами двухсторонние, за исключением связи элементов 1 и 2. Связь осуществляется от первого элемента (идентификация/аутентификация) ко второму элементу (управление доступом), это обусловлено тем, что самой первой ступенью как в проверке, так и при осуществлении входа в систему является именно идентификация и аутентификация, и только затем идет процесс управления доступом, который в свою очередь заключается в определении права доступа объекта после получения идентификационного кода, именно поэтому связь первого и второго элементов односторонняя.

### *Весовые коэффициенты*

Один из самых важных процессов проведения аудита – определение оценки защищенности ИС. Но для объектов КИИ нет критериев и требований к определению оценки в отличии от ГОСТ Р 57580.2 [5]. И на основании подхода ЦБ РФ к методике расчета количественной оценки, был разработан метод оценивания эффективности соблюдения мер безопасности согласно приказу ФСТЭК России № 239 [6].

Для расчета весовых коэффициентов в первую очередь необходимо проранжировать все меры. Метод разработки весовых коэффициентов частично основан на способах, описанных в статьях [9–11]. Частично ранжировка была сделана при построении графа и матрицы, но она требует детализации. В графе ранжирования мер обеспечения безопасности ЗО КИИ на рисунке 1 в явном виде представлено три ветви, однако на самом деле их четыре. Первая ветвь состоит из элементов с 1 по 17, вторая – 2, 3, 6, 13, 14 элементы, третья – 11, 4, 10, 8, 9 элементы, четвертая – 5, 7, 12, 15, 16, 17 элементы. Таким образом первая ветвь включает в себя все элементы, что связано с тем, что без идентификации и аутентификации защита ИС не может быть эффективной, т.к. становится открытой для любого, именно поэтому можно считать это отдельной ветвью, от которой зависят все остальные элементы графа.

Чтобы рассчитать весовой коэффициент каждой ветви графа $r_i$, необходимо узнать сумму значений элементов каждой ветви графа $h_i$ (табл. 1). Значение всего графа равно 92.

*Таблица 1*

Значения элементов графа ранжирования мер обеспечения безопасности ЗО КИИ

| 1 ветвь | | 2 ветвь | | 3 ветвь | | 4 ветвь | |
|---|---|---|---|---|---|---|---|
| элемент | $h_1$ | элемент | $h_2$ | элемент | $h_3$ | элемент | $h_4$ |
| 1 | 3 | 2 | 3 | 4 | 2 | 5 | 3 |
| 2 | 4 | 3 | 3 | 8 | 2 | 7 | 2 |
| 3 | 3 | 6 | 2 | 9 | 2 | 12 | 3 |
| 4 | 2 | 13 | 3 | 10 | 2 | 15 | 3 |
| 5 | 4 | 14 | 4 | 11 | 4 | 16 | 2 |
| 6 | 2 | – | – | – | – | 17 | 3 |
| 7 | 2 | – | – | – | – | – | – |
| 8 | 2 | – | – | – | – | – | – |

*Окончание табл. 1*

| 1 ветвь | | 2 ветвь | | 3 ветвь | | 4 ветвь | |
|---|---|---|---|---|---|---|---|
| элемент | $h_1$ | элемент | $h_2$ | элемент | $h_3$ | элемент | $h_4$ |
| 9 | 2 | – | – | – | – | – | – |
| 10 | 2 | – | – | – | – | – | – |
| 11 | 5 | – | – | – | – | – | – |
| 12 | 3 | – | – | – | – | – | – |
| 13 | 3 | – | – | – | – | – | – |
| 14 | 4 | – | – | – | – | – | – |
| 15 | 3 | – | – | – | – | – | – |
| 16 | 2 | – | – | – | – | – | – |
| 17 | 3 | – | – | – | – | – | – |
| Итого: | 49 | Итого: | 15 | Итого: | 12 | Итого: | 16 |

Из таблицы видно, что сумма значений первой ветви равно 49, второй – 15, третьей – 12, и четвертой – 16.

Далее рассчитаем весовой коэффициент каждой ветви, используя формулу (1)

$$r_i = \frac{h_i}{\sum_{i=1}^{n} h_i}, \quad (1)$$

где $n$ – количество ветвей в графе, $i$ – номер ветви графа.

Результаты представлены в табл. 2.

*Таблица 2.*

Вес каждой ветви в графе

| № ветви | ветвь 1 | ветвь 2 | ветвь 3 | ветвь 4 |
|---|---|---|---|---|
| Вес | 0,5 | 0,2 | 0,1 | 0,2 |

Полученные весовые коэффициенты говорят о том, что меры, регламентирующие идентификацию/ аутентификацию, имеют наибольший вес при оценивании ИС.

Чтобы использовать весовые коэффициенты при расчете оценки эффективности реализованных мер для защиты системы сначала необходимо оценить эти меры.

Эффективную системы оценивания мер предлагает все тот же ГОСТ Р 57580.2, в котором предлагается следующее:

– оценка 1 ставится, если мера реализована полностью;

– оценка 0,5 ставится, если мера реализована не в полном объеме;

– оценка 0 ставится, если мера не реализована.

Но данные оценки справедливы для основной группы мер, однако существуют меры, несоблюдение которых может быть критично, например, меры, ка-

сающиеся идентификации и аутентификации др. В таком случае рационально использоваться следующие оценки:

– оценка 1 ставится, если мера реализована полностью;

– оценка 0 ставится, если мера не реализована или реализована частично.

Такими группами мер становятся первый и второй уровни графа, т.е., меры, касающиеся идентификации/ аутентификации, управления доступом, аудита безопасности и защиты ИС и ее компонентов.

Также необходимо помнить, что каждая система индивидуальна и требует своего, отличного от других подхода. Поэтому общей эталонной системы защиты не существует, а значит для каждой системы защиты необходим свой идеал. Таким идеалом становится система защиты, в которой реализуются в полной мере все разработанные меры защиты.

Далее необходимо рассчитать значения оценок для каждой из групп мер:

$$E_k = \frac{\sum_{i=1}^{n} M_i}{N}, \tag{2}$$

где $E_k$ – числовое значение промежуточной оценки выбранных организацией групп мер; $M_i$ – оценка $i$ меры; $N$ – число мер, необходимых в системе защиты; $n$ – количество реализуемых мер.

После получения промежуточных оценок реализуемых групп мер необходимо вычислить результативную оценку защищенности ИС. Для этого необходимо определить промежуточные значения по формуле (3)

$$E_{вк} = \sum_{i=1}^{n} E_i , \tag{3}$$

где $E_{\text{Bk}}$ – числовое значение промежуточной оценки выбранной ветви мер; $E_i$ – промежуточная оценка $i$ группы меры, касающейся идентификации и аутентификации; $n$ – число групп мер в ветви;

Для того, чтобы получить взвешенную оценку эффективности защиты ИС используются весовые коэффициенты. Поскольку в системе защиты четыре ветви, то, для получения объективной оценки, необходимо вычислить среднеарифметическое всех полученных оценок. Исходя из вышесказанного получена формула (4)

$$E = \frac{0{,}5 \times E_{B1} + 0{,}2 \times E_{B2} + 0{,}2 \times E_{B3} + 0{,}1 \times E_{B4}}{4}, \tag{4}$$

где $E$ – взвешенная оценка выбранных организацией мер; $E_{B1}$ – промежуточная оценка групп мер 1 ветви; $E_{B2}$ – промежуточная оценка групп мер 2 ветви; $E_{B3}$ – промежуточная оценка групп мер 3 ветви; $E_{B4}$ – промежуточная оценка групп мер 4 ветви.

Используя формулу (4), получают взвешенную оценку, т.к. каждая группа мер проранжирована согласно ее весу (значению) в реализации системы защиты ИС.

Получив оценку эффективности принятых мер, необходимо понять при каком ее числовом значении разработанная система защиты действенна. Для этого необходимы критерии, или диапазон значений эффективности, которых на сегодняшний день нет ни в одном документе ФСТЭК России, однако прописаны в документах ЦБ РФ, а именно в ГОСТ Р 57580.2 [6].

Информационные системы банков России являются огромной ценностью для государства, т.к. нарушения их функционирования может привести к краху финансовой системы страны и, как следствие, тяжелой ситуации в государстве, более подробно описано в статьях [7, 8]. Поэтому критерии их оценивания наиболее строгие, что в свою очередь также необходимо и для ЗО КИИ, т.к. нарушение их функционирования может привести к существенным «негативным социальным, политическим, экономическим, экологическим последствиям, последствиям для обеспечения обороны страны, безопасности государства и правопорядка» [1], а значит критерии ЦБ РФ целесообразно применять как критерии оценки ЗО КИИ. Однако в отличие от категорий ЗО КИИ, Центральный банк разработал пять уровней соответствия, представленных в табл. 3.

*Таблица 3*

Качественная оценка уровня соответствия процессов системы ЗИ

| Оценка | Уровень соответствия |
|---|---|
| E=0 | нулевой |
| 0<E≤0,5 | первый |
| 0,5<E≤0,7 | второй |
| 0,7<E≤0,85 | третий |
| 0,85<E≤0,9 | четвертый |
| 0,9<E≤1 | пятый |

Таким образом становится необходимым адаптировать уровни соответствия защиты, разработанные Банком России под ЗО КИИ. На данный момент для ЗО КИИ целесообразно ориентироваться на три самых высоких уровня соответствия: пятый, четвертый и третий.

### *Выводы*

В данной статье представлена разработка метода оценивания эффективности информационной системы ЗО КИИ. На основе ранжирования групп мер приказа ФСТЭК России № 239 [6], разработаны весовые коэффициенты, на основе которых, в свою очередь рассчитывается количественная оценка качества защиты ИС.

Правильно рассчитанная оценка защиты ИС позволяет своевременно обнаружить уязвимые места в построенной системе безопасности. Раннее обнаруже-

ние уязвимостей позволяет вовремя их устранить, а значит обеспечить необходимый уровень безопасности ЗО КИИ.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК


1. Федеральный закон от 26 июля 2017 г. N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» от 19.06.2017.
2. Постановление Правительства РФ от 17 февраля 2018 г. N 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».
3. Приказ ФСТЭК России от 26.06.2019 № 127 «Об утверждении обзора правоприменительной практики ФСТЭК России в рамках контроля за соблюдением российскими участниками внешнеэкономической деятельности законодательства Российской Федерации в области экспортного контроля за 2018 год».
4. ГОСТ Р 57580.1-2017 Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер. введ. 2018-01-01.
5. ГОСТ Р 57580.2-2018 Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия. введ. 2018-09-01.
6. Приказ ФСТЭК России от 25 декабря 2017 г. N 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».
7. Ситская, А. В. Вопросы автоматизации проведения аудита в соответствии с ГОСТ р 57580.2-2018 / А. В. Ситская, В. А. Табакаева, В. В. Селифанов // Интерэкспо Гео-Сибирь. – 2021. – Т. 6. – С. 268-275. – DOI 10.33764/2618-981X-2021-6-268-275.
8. Заведенская, А. А. Соотнесение мер защиты информации, указанных в ГОСТ Р 57580.1-2017, с мерами защиты из приказа ФСТЭК России от 18 февраля 2013 г. № 21 / А. А. Заведенская, Т. Ю. Зырянова // Безопасность информационного пространства : Сборник трудов XIX Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых, Екатеринбург, 08–11 декабря 2020 года. – Екатеринбург: Уральский государственный экономический университет, 2021. – С. 93-97.
9. Григорьев А.В., Козин П.А., Остапчук А.В. Методика определения значений весовых коэффициентов //Имущественные отношения в Российской Федерации. – 2004, №8. - С. 73-83.
10. Постников В.М., Спиридонов С.Б. Методы выбора весовых коэффициентов локальных критериев // Машиностроение и компьютерные технологии. – 2015, №6 – С. 267 –287.
11. Постников В.М., Спиридонов С.Б. Выбор методов взвешивания локальных критериев // Наука и образование МГТУ им. Баумана. – 2015. DOI: 10.7463/0615.0780334
12. Забегалин, Е. В. Логическая модель деятельности по комплексному техническому диагностированию информационной безопасности организаций и значимых объектов критической информационной инфраструктуры / Е. В. Забегалин // Системы управления, связи и безопасности. – 2019. – № 3. – С. 145-178. – DOI 10.24411/2410-9916-2019-10308.
13. Экспертная ситема поддержки принятия решений в процессе аудита информационной безопасности / В. И. Васильев, Т. З. Хисамутдинов, А. С. Красько, П. В. Матвеев // Информационное противодействие угрозам терроризма. – 2005. – № 4. – С. 98-102.
14. Краснов, А. Е. Оценивание устойчивости критических информационных инфраструктур к угрозам информационной безопасности / А. Е. Краснов, А. С. Мосолов, Н. А. Феоктистова // Безопасность информационных технологий. – 2021. – Т. 28. – № 1. – С. 106-120. – DOI 10.26583/bit.2021.1.09.
15. Поздняк, И. С. Контроль состояния защищенности информации в объектах критической информационной инфраструктуры / И. С. Поздняк, Ч. Р. Абдулганеева // XXVIII Россий-

ская научно-техническая конференция профессорско-преподавательского состава, научных сотрудников и аспирантов университета с приглашением ведущих ученых и специалистов родственных вузов и организаций, Самара, 05–08 апреля 2021 года. – Самара: Поволжский государственный университет телекоммуникаций и информатики, 2021. – С. 62-63.

16. Нестеровский, О. И. Методический подход к организации проведения контроля защищенности информации на объектах критической информационной инфраструктуры / О. И. Нестеровский, Е. С. Пашковская, Е. Е. Бутрик // Вестник Воронежского института МВД России. – 2021. – № 2. – С. 126-133.