УДК 004.056.53
DOI: 10.33764/2618-981X-2021-6-3-11

# РАЗРАБОТКА КРИТЕРИЕВ ОЦЕНКИ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ НА ОБЪЕКТЕ ИНФОРМАТИЗАЦИИ

***Владимир Робертович Ан***
Новосибирский государственный технический университет, 630073, Россия, г. Новосибирск, пр. К. Маркса, 20, магистрант кафедры вычислительной техники, тел. (903)939-53-58, e-mail: vovan2011nsk@mail.ru

***Валерия Александровна Табакаева***
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, магистрант кафедры фотоники и приборостроения, тел. (962)831-22-52, e-mail: tabakaeva1997@mail.ru

***Валентин Валерьевич Селифанов***
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, доцент кафедры информационной безопасности, тел. (923)247-25-81, e-mail: sfo1@mail.ru

В данной статье рассматривается проблема оценки состояния уровня безопасности защищаемой информации. Проблема заключается в отсутствие утвержденной методики и недостаточностью подготовки специалистов в области аудита кибербезопасности. Целью исследования является разработка критериев оценки соответствия требованиям безопасности информации. В результате исследования были получены критерии оценки с нормированной шкалой значений и формулами расчёта, разработанные на основе метода анализа иерархий.

**Ключевые слова:** информационная безопасность, кибербезопасность, критерии оценки, государственная информационная система, методика аудита кибербезопасности

# DEVELOPMENT OF CRITERIA FOR ASSESSMENT OF CONFORMITY WITH THE SAFETY REQUIREMENTS AT THE INFORMATION FACILITY

***Vladimir R. An***
Novosibirsk State Technical University, 20, K. Marksa Prospekt, Novosibirsk, 630073, Russia, Graduate, Department of Computer Science, phone: (903)939-53-58, e-mail: vovan2011nsk@mail.ru

***Valeria A. Tabakaeva***
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Graduate, Department of Photonics and Device Engineering, phone: (962)831-22-52, e-mail: tabakaeva1997@mail.ru

***Valentin V. Selifanov***
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Associate Professor of the Department of Information Security, phone: (923)247-25-81, e-mail: sfo1@mail.ru

This article discusses the problem of assessing the state of the security level of protected information. The problem lies in the lack of an approved methodology and inadequate training of specialists in the field of cybersecurity auditing. The aim of the study is to develop criteria for assessing compliance with information security requirements. As a result of the study, assessment criteria were

obtained with a normalized scale of values and calculation formulas, developed on the basis of the hierarchy analysis method.

**Keywords:** information security, cybersecurity, assessment criteria, state information system, cybersecurity audit methodology

## *Список сокращений и специальных терминов*

АВЗ – антивирусная защита;
БД – база данных;
БК – базовая конфигурация;
ВИ – виртуальная инфраструктура;
ВУ – внешние устройства;
ГИС – государственная информационная система;
ЗИ – защита информации;
ИА – идентификация и аутентификаци;
ИБ – информационная безопасность;
ИС – информационная система;
МД – методический документ;
МЭ – межсетевой экран;
НДВ – недекларированные возможности;
ОИ – объект информатизации;
ПО – программное обеспечение;
СБ – события безопасности;
СВТ – средство вычислительной техники;
СЗИ – средство защиты информации;
СОВ – система обнаружения вторжений;
СУБД – система управления базами данных;
ТБИ – требования безопасности информации;
ТС – техническое средство;
УБИ – угрозы безопасности информация;
УЗ – учетные записи;
ФСТЭК – Федеральная служба по техническому и экспортному контролю.

## *Введение*

В настоящее время не уделяется достаточного внимания выполнению работ, связанных с аудитом кибербезопасности ИС [1-2]. Это связано, прежде всего, с отсутствием необходимой нормативной правовой базы и методик в области проведения аудита кибербезопасности. Объектом исследования в данной работе являются системы защиты ГИС. А предметом исследования – аудит кибербезопасности.

Аудит кибербезопасности является одной из важнейших составляющих для решения проблемы обеспечения защищенности информации.

Для решения исследуемой проблемы, а также достижения установленной цели и выполнения поставленных задач в работе рассматриваются следующие документы:

– Приказ ФСТЭК России от 11 февраля 2013 г. №17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» с редакцией от 28 мая 2019 года [3];

– МД. Меры защиты в ГИС [4];

– МД. Методика выявления уязвимостей и НДВ в ПО [5].

Таким образом, целью данной работы является разработка критериев оценки соответствия ТБИ на ОИ. В результате аудита кибербезопасности, ожидается отчет по состоянию уровня безопасности ИС, для дальнейшего анализа и определения перспектив развития с точки зрения менеджмента ИБ.

Для достижения поставленной цели, необходимо выполнить следующий перечень задач:

1) разработать критерии оценки аудита кибербезопасности;

2) разработать метод оценивания;

3) разработать нормированную шкалу значений критериев.

## *Методы и материалы*

В статье предложена система из двух критериев оценки соответствия ТБИ, вычисляемых на основе 16 показателей, содержащих более 45 параметров безопасности.

При разработке критериев применялся экспертно-документальный метод и метод анализа иерархий [6 – 7]. Метод анализа иерархий – это современный метод преобразования качественной информации об исследуемом объекте в количественную. На основе этого метода была составлена схема формирования интегральной оценки защищенности ($S_{\text{защ}}$) объекта информатизации, показанная на рисунке.

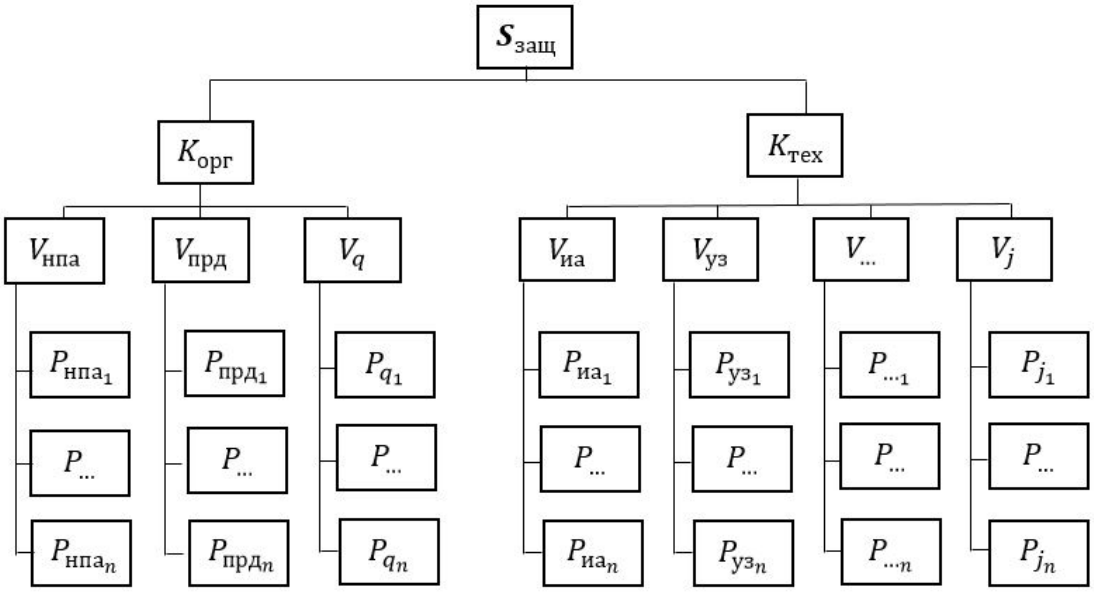


Схема формирования интегральной оценки защищенности

Интегральной оценки защищенности состоит из суммы критериев организационных (q) и технических (j) мер, которые в свою очередь состоят из соответствующих показателей. Каждый показатель содержит n-ое количество параметров безопасности.

Применяя метод анализа иерархий, была выполнена линейная свертка разработанных параметров безопасности.

$$S_{\text{защ}}=K_{\text{орг}}w_{\text{орг}} + K_{\text{тех}}w_{\text{тех}}, \quad (1)$$

где $S_{\text{защ}} \leq 1$ – интегральная оценка защищенности, а $w_{\text{орг}} = w_{\text{тех}} = 0{,}5$ – веса (w) организационных и технических критериев (K) оценки соответствия ТБИ.

$$K_{\text{орг}}=\sum_{i=1}^{i=3} w_i^q \, V_i^q, \quad (2)$$

где $K_{\text{орг}} \leq 1$ – значение критерия на соответствие организационным мерам, а $\sum_{i=1}^{i=3} w_i^q \, V_i^q = 1$ – сумма организационных показателей, состоящих из произведения веса (w) и значения соответствующего критерия (V), где (i) – порядковый номер массива.

$$K_{\text{тех}}=\sum_{i=1}^{i=13} w_i^j \, V_i^j, \quad (3)$$

где $K_{\text{тех}} \leq 1$ – значение критерия на соответствие техническим мерам, а $\sum_{i=1}^{i=13} w_i^j V_i^j$=1 – сумма технических показателей, состоящих из произведения веса (w) и значения соответствующего критерия (V), где (i) – порядковый номер массива.

$$V_i^q=\sum_{i=1}^{n} w_i^{i_n} \, P_i^{i_n}, \quad (4)$$

где $V_i^q \leq 1$ – значение показателя на соответствие организационным мерам, а $\sum_{i=1}^{n} w_i^{i_n} \, P_i^{i_n} = 1$ – сумма организационных критериев, состоящих из произведения веса (w) и значения соответствующего параметра безопасности (P), где (i) – порядковый номер массива.

$$V_i^j=\sum_{i=1}^{n} w_i^{i_n}, \quad (5)$$

где $V_i^j \leq 1$ – значение показателя на соответствие организационным мерам, а $\sum_{i=1}^{n} w_i^{\text{нпа}_n} P_i^{i_n} = 1$ – сумма технических критериев, состоящих из произведения веса (w) и значения соответствующего параметра безопасности (P), где (i) – порядковый номер массива.

В данной работе веса критериев, показателей и параметров безопасности равны 1, разделенной на количество их составляющих, то есть они равны по от-

ношению друг к другу. В ходе апробации методики планируется назначать веса на основе выявленной значимости каждого критерия, показателя и параметра безопасности.

## *Результаты*

В результате анализа состояния существующих применяемых методов и методик [8 – 10], а также нормативно-правовых документов в области аудита кибербезопасности были разработаны критерии оценки соответствия ТБИ (табл. 1 и 2).

Диапазон значений качественных характеристик:

– не выполняется – 0;

– выполняется частично – 1;

– выполняется в полной мере – 2.

Порядковый массив организационных показателей:

i = 1 – соответствие нормативно-правовым актам;

i = 2 – соответствие проектной документации ОИ;

i = 3 – соответствие организационно-распорядительной документации ОИ.

*Таблица 1*

Организационные критерии оценки соответствия ТБИ

| i | Наименование параметра безопасности | Диапазон значений | Значения на нормированной шкале |
|---|---|---|---|
| 1 | Класс СЗИ | [-, 6, 5, 4, 3, 2, 1] | $[0,\frac{1}{6},\frac{1}{3},\frac{1}{2},\frac{2}{3},\frac{5}{6},1]$ |
| | Уровень НДВ | [-, 4, 3, 2, 1] | $[0,\frac{1}{4},\frac{1}{2},\frac{3}{4},1]$ |
| | Оценочный уровень доверия | [-, 1, 2, 3, 4, 5, 6, 7] | $[0,\frac{1}{7},\frac{2}{7},\frac{3}{7},\frac{4}{7},,\frac{5}{7},\frac{6}{7},1]$ |
| | Актуальность модели угроз | [0,1,2] | $[0,\frac{P_{\text{нпа}}^{max}(i)}{\max\limits_{i}(\{P_{\text{нпа}}^{max}(i)\})},1]$ |
| | Актуальность уровня нарушителя | [0,1,2] | $[0,\frac{P_{\text{нпа}}^{max}(i)}{\max\limits_{i}(\{P_{\text{нпа}}^{max}(i)\})},1]$ |
| 2 | Выбор мер защиты, подлежащих реализации в системе ЗИ ИС | [0,1,2] | $[0,\frac{P_{\text{пд}}^{max}(i)}{\max\limits_{i}(\{P_{\text{пд}}^{max}(i)\})},1]$ |
| | Определение структуры системы ЗИ ИС (в том числе состав и место размещения её элементов) | [0,1,2] | $[0,\frac{P_{\text{пд}}^{max}(i)}{\max\limits_{i}(\{P_{\text{пд}}^{max}(i)\})},1]$ |
| | Выбор сертифицированных СЗИ | [0,1,2] | $[0,\frac{P_{\text{пд}}^{max}(i)}{\max\limits_{i}(\{P_{\text{пд}}^{max}(i)\})},1]$ |
| 3 | Обнаружение и идентификация инцидентов, в том числе отказов в обслуживании, сбоев (перезагрузок) в работе ТС, ПО и СЗИ | [0,1,2] | $[0,\frac{P_{\text{орд}}^{max}(i)}{\max\limits_{i}(\{P_{\text{орд}}^{max}(i)\})},1]$ |
| | Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий; | [0,1,2] | $[0,\frac{P_{\text{орд}}^{max}(i)}{\max\limits_{i}(\{P_{\text{орд}}^{max}(i)\})},1]$ |
| | Поддержание БК ИС и ее системы ЗИ | [0,1,2] | $[0,\frac{P_{\text{орд}}^{max}(i)}{\max\limits_{i}(\{P_{\text{орд}}^{max}(i)\})},1]$ |

*Окончание табл. 1*

| i | Наименование параметра безопасности | Диапазон значений | Значения на нормированной шкале |
|---|---|---|---|
| | Определение лиц, которым разрешены действия по внесению изменений в БК ИС и ее системы ЗИ; | [0,1,2] | $[0,\frac{P_{\text{орд}}^{max}(i)}{\underset{i}{max}(\{P_{\text{орд}}^{max}(i)\})},1]$ |
| | Контроль (анализ) защищенности информации, содержащейся в ИС; | [0,1,2] | $[0,\frac{P_{\text{орд}}^{max}(i)}{\underset{i}{max}(\{P_{\text{орд}}^{max}(i)\})},1]$ |
| | Документирование процедур и результатов контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в ИС; | [0,1,2] | $[0,\frac{P_{\text{орд}}^{max}(i)}{\underset{i}{max}(\{P_{\text{орд}}^{max}(i)\})},1]$ |

Порядковый массив технических показателей:
i=1 – идентификация и аутентификация в ИС;
i=2 – администрирование учетных записей;
i=3 – ограничение программной среды;
i=4 – защита внешних устройств (жесткие диски, флэш-накопители и т.д.);
i=5 – регистрация событий безопасности;
i=6 – обеспечение антивирусной защиты;
i=7 – администрирование системы обнаружения вторжений;
i=8 – управление сканером уязвимости;
i=9 – администрирование межсетевого экрана;
i=10 – поддержание системы защиты информации в ходе эксплуатации;
i=11 – защита виртуальной инфраструктуры;
i=12 – назначение ответственных лиц;
i=13 – обеспечение криптографической защиты.

*Таблица 2*

Технические критерии оценки соответствия ТБИ

| i | Наименование характеристики | Диапазон значений характеристики | Значения характеристики на нормированной шкале |
|---|---|---|---|
| 1 | ИА пользователей, процессов, устройств, ПО, объектов файловой системы и СУБД | [0,1,2] | $[0,\frac{P_{\text{ИА}}^{max}(i)}{\underset{i}{max}(\{P_{\text{ИА}}^{max}(i)\})},1]$ |
| | Многофакторная аутентификация | [0,1,2] | $[0,\frac{P_{\text{ИА}}^{max}(i)}{\underset{i}{max}(\{P_{\text{ИА}}^{max}(i)\})},1]$ |
| | Защита аутентификационной информации | [0,1,2] | $[0,\frac{P_{\text{ИА}}^{max}(i)}{\underset{i}{max}(\{P_{\text{ИА}}^{max}(i)\})},1]$ |
| 2 | Администрирование учетных записей | [0,1,2] | $[0,\frac{P_{\text{АУЗ}}^{max}(i)}{\underset{i}{max}(\{P_{\text{АУЗ}}^{max}(i)\})},1]$ |
| | Управление потоками информации | [0,1,2] | $[0,\frac{P_{\text{АУЗ}}^{max}(i)}{\underset{i}{max}(\{P_{\text{АУЗ}}^{max}(i)\})},1]$ |
| | Реализация защищенного удаленного доступа | [0,1,2] | $[0,\frac{P_{\text{АУЗ}}^{max}(i)}{\underset{i}{max}(\{P_{\text{АУЗ}}^{max}(i)\})},1]$ |
| | Ограничение точек доступа при организации удаленного доступа | [0,1,2] | $[0,\frac{P_{\text{АУЗ}}^{max}(i)}{\underset{i}{max}(\{P_{\text{АУЗ}}^{max}(i)\})},1]$ |

*Окончание табл. 2*

| i | Наименование характеристики | Диапазон значений характеристики | Значения характеристики на нормированной шкале |
|---|---|---|---|
| | Контроль использования ВУ в ИС | [0,1,2] | $[0,\frac{P_{\text{АУЗ}}^{max}(i)}{\underset{i}{max}(\{P_{\text{АУЗ}}^{max}(i)\})},1]$ |
| 3 | Доверенная загрузка СВТ | [0,1,2] | $[0,\frac{P_{\text{ОПС}}^{max}(i)}{\underset{i}{max}(\{P_{\text{ОПС}}^{max}(i)\})},1]$ |
| | Ограничение программной среды | [0,1,2] | $[0,\frac{P_{\text{ОПС}}^{max}(i)}{\underset{i}{max}(\{P_{\text{ОПС}}^{max}(i)\})},1]$ |
| 4 | Защита учтенных ВУ | [0,1,2] | $[0,\frac{P_{\text{ЗВУ}}^{max}(i)}{\underset{i}{max}(\{P_{\text{ЗВУ}}^{max}(i)\})},1]$ |
| | Управление доступом к учтенным ВУ | [0,1,2] | $[0,\frac{P_{\text{ЗВУ}}^{max}(i)}{\underset{i}{max}(\{P_{\text{ЗВУ}}^{max}(i)\})},1]$ |
| | Затирание остаточной информации | [0,1,2] | $[0,\frac{P_{\text{ЗВУ}}^{max}(i)}{\underset{i}{max}(\{P_{\text{ЗВУ}}^{max}(i)\})},1]$ |
| 5 | Регистрация СБ | [0,1,2] | $[0,\frac{P_{\text{РСБ}}^{max}(i)}{\underset{i}{max}(\{P_{\text{РСБ}}^{max}(i)\})},1]$ |
| | Реагирование системы защиты на сбои при регистрации СБ | [0,1,2] | $[0,\frac{P_{\text{РСБ}}^{max}(i)}{\underset{i}{max}(\{P_{\text{РСБ}}^{max}(i)\})},1]$ |
| | Мониторинг журнала безопасности | [0,1,2] | $[0,\frac{P_{\text{РСБ}}^{max}(i)}{\underset{i}{max}(\{P_{\text{РСБ}}^{max}(i)\})},1]$ |
| | ЗИ о СБ | [0,1,2] | $[0,\frac{P_{\text{РСБ}}^{max}(i)}{\underset{i}{max}(\{P_{\text{РСБ}}^{max}(i)\})},1]$ |
| 6 | Администрирование АВЗ | [0,1,2] | $[0,\frac{P_{\text{ОАЗ}}^{max}(i)}{\underset{i}{max}(\{P_{\text{ОАЗ}}^{max}(i)\})},1]$ |
| | Актуальность БД АВЗ | [0,1,2] | $[0,\frac{P_{\text{ОАЗ}}^{max}(i)}{\underset{i}{max}(\{P_{\text{ОАЗ}}^{max}(i)\})},1]$ |
| 7 | Администрирование СОВ | [0,1,2] | $[0,\frac{P_{\text{АСОВ}}^{max}(i)}{\underset{i}{max}(\{P_{\text{АСОВ}}^{max}(i)\})},1]$ |
| | Актуальность сигнатур СОВ | [0,1,2] | $[0,\frac{P_{\text{АСОВ}}^{max}(i)}{\underset{i}{max}(\{P_{\text{АСОВ}}^{max}(i)\})},1]$ |
| 8 | Администрирование сканера уязвимости | [0,1,2] | $[0,\frac{P_{\text{УСУ}}^{max}(i)}{\underset{i}{max}(\{P_{\text{УСУ}}^{max}(i)\})},1]$ |
| | Актуальность БД выявляемых уязвимостей | [0,1,2] | $[0,\frac{P_{\text{УСУ}}^{max}(i)}{\underset{i}{max}(\{P_{\text{УСУ}}^{max}(i)\})},1]$ |
| 9 | Администрирование МЭ | [0,1,2] | $[0,\frac{P_{\text{АМЭ}}^{max}(i)}{\underset{i}{max}(\{P_{\text{АМЭ}}^{max}(i)\})},1]$ |
| | Актуальность правил фильтрации трафика МЭ | [0,1,2] | $[0,\frac{P_{\text{АМЭ}}^{max}(i)}{\underset{i}{max}(\{P_{\text{АМЭ}}^{max}(i)\})},1]$ |
| 10 | Контроль установки обновлений ПО и СЗИ | [0,1,2] | $[0,\frac{P_{\text{ПСЗИ}}^{max}(i)}{\underset{i}{max}(\{P_{\text{ПСЗИ}}^{max}(i)\})},1]$ |
| | Контроль состава ТС, ПО и СЗИ | [0,1,2] | $[0,\frac{P_{\text{ПСЗИ}}^{max}(i)}{\underset{i}{max}(\{P_{\text{ПСЗИ}}^{max}(i)\})},1]$ |
| | Контроль целостности ПО и СЗИ | [0,1,2] | $[0,\frac{P_{\text{ПСЗИ}}^{max}(i)}{\underset{i}{max}(\{P_{\text{ПСЗИ}}^{max}(i)\})},1]$ |
| 11 | ИА субъектов и объектов доступа в ВИ | [0,1,2] | $[0,\frac{P_{\text{ЗВИ}}^{max}(i)}{\underset{i}{max}(\{P_{\text{ЗВИ}}^{max}(i)\})},1]$ |
| | Администрирование учетных записей в ВИ | [0,1,2] | $[0,\frac{P_{\text{ЗВИ}}^{max}(i)}{\underset{i}{max}(\{P_{\text{ЗВИ}}^{max}(i)\})},1]$ |
| | Регистрация СБ в ВИ | [0,1,2] | $[0,\frac{P_{\text{ЗВИ}}^{max}(i)}{\underset{i}{max}(\{P_{\text{ЗВИ}}^{max}(i)\})},1]$ |
| 12 | Разделение функций по управлению ИС и ЗИ | [0,1,2] | $[0,\frac{P_{\text{НОЛ}}^{max}(i)}{\underset{i}{max}(\{P_{\text{НОЛ}}^{max}(i)\})},1]$ |
| 13 | Администрирование средства криптографической ЗИ | [0,1,2] | $[0,\frac{P_{\text{ОКЗ}}^{max}(i)}{\underset{i}{max}(\{P_{\text{ОКЗ}}^{max}(i)\})},1]$ |

## *Заключение*

В данной работе рассмотрена проблема разработки критериев оценки соответствия требованиям безопасности на объекте информатизации.

Обозначена важность данной проблемы, описаны причины её возникновения, рассмотрен и обобщен нормативно-методический аппарат аудита кибербезопасности, на основе которого разрабатывались критерии оценки, а также сформулированы и поставлены цели и задачи для решения данной проблемы.

В результате работы были выполнены все поставленные задачи, а именно разработаны критерии оценки аудита кибербезопасности, с учетом метода оценивания, формул расчёта и нормированной шкалой значений критериев, на основе которых в настоящее время разрабатывается вспомогательное программное обеспечение

В дальнейшем будет разработана полноценная методика аудита кибербезопасности ИС и рекомендации по использованию этой методики.

Значимость результатов обуславливается возможностью достаточно быстро, эффективно, с высокой точностью оценивать состояние уровня защищенности ИС при проведении аудита кибербезопасности, учитывая индивидуальность ОИ и соблюдение соответствующих федеральных законов.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Буковшин В.А., Болдырихин Н.В. Современные проблемы информационной безопасности. 2018. – С. 47–51 [Электронный ресурс] // Научная электронная библиотека «eLibrary». – URL: https://www.elibrary.ru/item.asp?id=36765246 (дата обращения: 05.03.2021).

2. Байнов А.М. Проблемы и задачи обеспечения информационной безопасности. 2018. – С. 18–21 [Электронный ресурс] // Научная электронная библиотека «eLibrary». – URL: https://www.elibrary.ru/item.asp?id=36617652 (дата обращения: 5.04.2021).

3. Приказ ФСТЭК России от 11 февраля 2013 г. №17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах». [Электронный ресурс] – URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702-prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17 (дата обращения: 17.01.2021).

4. Методический документ. Меры защиты в государственных информационных системах. Утвержден ФСТЭК России 11 февраля 2014 г. [Электронный ресурс] – URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/805-metodicheskij-dokument (дата обращения: 17.01.2021).

5. Методический документ. Методика выявления уязвимостей и недекларированных возможностей в программном обеспечении. Утвержден ФСТЭК России 11 февраля 2019 года. [Электронный ресурс] URL: http://new.groteck.ru/images/catalog/ 70840/e 75c72a254fcc880fa65657fdb144063.pdf (дата обращения: 11.01.2021).

6. Волокобинский М.Ю., Пекарская О.А., Рази Д.А. Принятие решений на основе метода анализа иерархий // Финансы: теория и практика. – 2016. – № 2. – С. 91–93.

7. Картвелишвили В.М., Лебедюк Э.А. Метод анализа иерархий: критерии и практика // Вестник РЭА им. Г.В. Плеханова. – 2013. – № 6. – С. 59–61.

8. Каратунова Н.Г. Аудит комплексной и информационной безопасности объекта. 2017. – С. 63–65 [Электронный ресурс] // Научная электронная библиотека «eLibrary». – URL: https://www.elibrary.ru/item.asp?id= 29505431 (дата обращения: 16.02.2021).

9. Ситнов А.А. Организация аудита информационной безопасности. 2016. – С. 107–110 [Электронный ресурс] // Научная электронная библиотека «eLibrary». – URL: https://www.elibrary.ru/item.asp?id= 28743214 (дата обращения: 17.03.2021).

10. Аверченков В.И. Аудит информационной безопасности, 3-е издание. 2016. – С.261–264 [Электронный ресурс] // Научная электронная библиотека «eLibrary». – URL: https://www.elibrary.ru/item.asp?id= 25083492 (дата обращения: 17.01.2021).