УДК 004.056

# ВОПРОСЫ КЛАССИФИКАЦИИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

**И.Ф. Михалевич**
*Институт проблем управления им. В.А. Трапезникова РАН*
Россия, 117997, Москва, Профсоюзная ул., 65
E-mail: mif-orel@mail.ru

**Ключевые слова:** безопасность, информационная безопасность, класс безопасности, критическая информационная инфраструктура, объект критической информационной инфраструктуры.

**Аннотация:** Развитие киберпространства несет потенциальную угрозу критическим информационным инфраструктурам, в которых функционируют объекты различных типов и категорий значимости. Безопасность критических информационных инфраструктур определяется, в том числе, полнотой нормативной и нормативно-методической базы по защите их объектов. В работе предложена система классов безопасности объектов критической информационной инфраструктуры, относящихся к различным типам, включая информационные системы, автоматизированные системы управления и информационно-телекоммуникационные сети, обеспечивающая, по мнению авторов, требуемое единство походов по их защите.

## 1. Введение

Построение информационного общества, развитие цифровой экономики невозможно без обеспечения безопасности критической информационной инфраструктуры [1-4]. Критическую информационную инфраструктуру Российской Федерации (далее – КИИ) характеризует многообразие объектов, относящихся к разнородным типам систем (информационные системы, автоматизированные системы управления, информационно-телекоммуникационные сети), и обеспечивающих их функционирование сетей связи, категорий важности объектов, видов информации (открытая и ограниченного доступа, включая конфиденциальную и информацию, содержащую сведения, составляющие государственную тайну). В статье изложены подходы по совершенствованию системы классификации объектов критической информационной инфраструктуры как объектов защиты информации, предложения по развитию нормативной и нормативно-методической базы обеспечения безопасности объектов КИИ.

## 2. Основы классификации безопасности объектов критической информационной инфраструктуры

Вне зависимости от типа системы, к которой принадлежит объект КИИ, основным ресурсом, подверженным изменению из киберсреды, является информация. В задачи систем безопасности объектов КИИ входит предотвращение неправомерного доступа, уничтожения, изменения, блокирования, копирования и распространения защищаемой информации, других неправомерных действий в отношении такой информации, недопущения воздействия на технические средства обработки информации, в результате которого может быть нарушено и (или) прекращено функционирование объекта КИИ. От систем безопасности также требуется восстановление функционирования объектов КИИ. Исходя из этого значимые объекты КИИ являются объектами защиты информации, к которым должны быть предъявлены требования по безопасности информации и реализованы меры по защите информации. Каждому значимому объекту КИИ должен быть присвоен класс безопасности.

До настоящего времени обязательные классы защиты устанавливались только для автоматизированных и информационных систем (далее – АС, ИС), обрабатывающих информацию ограниченного доступа, т.е. содержащую сведения, составляющие государственную тайну (далее – ГТ), или конфиденциального характера [5-12]. Одним из критериев значимости объектов КИИ определена социальная значимость, которая выражается, например, в возможном ущербе при нарушении доступа к государственным услугам.

Таким образом, в систему классификации безопасности объектов КИИ необходимо ввести новый параметр, которым является категория значимости объектов КИИ.

## 3. Предложения по системе классов безопасности объектов критической информационной инфраструктуры

К основным признакам классификации безопасности объектов КИИ отнесем уровень конфиденциальности информации, категорию значимости объекта КИИ и режим доступа к информации [13-14].

Учтем все возможные уровни конфиденциальности информации:

– открытая информация, доступ и распространение которой не ограничены. Уровень «5»;

– конфиденциальная информация (служебная, коммерческая, банковская и иные виды информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну). Уровень «4»;

– информация с грифом «секретно». Уровень «3»;

– информация с грифом «совершенно секретно». Уровень «2»;

– информация с грифом «особой важности». Уровень «1».

Присвоим признак классификации «О» объектам, на которых пользователи имеют одинаковые права доступа к информации, и «Р» – если требуется разграничение прав доступа

В зависимости от требуемой категории значимости объекту КИИ назначим признак «1К», «2К» или «3К».

Объекты КИИ рассматриваем как многопользовательские.

Независимо от фактической категории значимости объекту КИИ назначаем первую категорию значимости, если информация имеет гриф секретности. Признак категории

«1К» в обозначении класса таких объектов КИИ указывать не будем, так как в данном случае он является единственным.

Итоговая система классов безопасности объектов КИИ включает 15 классов в составе 5 групп.

Пятая группа содержит три класса (5О1К, 5О2К и 5О3К) объектов КИИ с открытой общедоступной информацией для всех зарегистрированных пользователей объектов соответственно первой, второй или третьей категории.

Четвертая группа содержит шесть классов для объектов КИИ с информацией уровня не выше «конфиденциально» с одинаковыми (классы 4О1К, 4О2К и 4О3К) или разными (классы 4Р1К, 4Р2К и 4Р3К) правами доступа пользователей соответственно объектов первой, второй или третьей категории значимости.

Третья группа содержит два класса для объектов КИИ с информацией уровня не выше «секретно» с одинаковыми (класс 3О) или разными (класс 3Р) правами доступа пользователей. Данные объекты КИИ должны соответствовать первой категории значимости независимо от фактической категории.

Вторая группа содержит два класса для объектов КИИ с информацией уровня не выше «совершенно секретно» с одинаковыми (класс 2О) или разными (класс 2Р) правами доступа пользователей. Данные объекты КИИ должны соответствовать первой категории значимости независимо от фактической категории.

Первая группа содержит два класса для объектов КИИ с информацией уровня до «особой важности» включительно с одинаковыми (класс 1О) или разными (класс 1Р) правами доступа пользователей. Данные объекты КИИ должны соответствовать первой категории значимости независимо от фактической категории.

Предложенная система классов безопасности объектов КИИ представлена в таблице 1.

**Таблица 1.** Система классов безопасности объектов КИИ.

| **Требования безопасности информации** | **Классы безопасности объектов КИИ** | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | 5О1К<br>5О2К<br>5О3К | 4О1К<br>4О2К<br>4О3К | 4Р1К<br>4Р2К<br>4Р3К | 3О | 3Р | 2О | 2Р | 1О | 1Р |
| **конфиденциальность** | ОИ | КИ | | С | | СС | | ОВ | |
| **доступность** | + | + | | + | | + | | + | |
| **целостность** | + | + | | + | | + | | + | |

# 4. Заключение

Предложенная система классов безопасности объектов критической информационной инфраструктуры позволяет обеспечить единство подходов по защите объектов критической информационной инфраструктуры, относящихся к различным типам, включая информационные системы, автоматизированные системы управления и информационно-телекоммуникационные сети.

# Список литературы

1. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

2. Доктрина информационной безопасности Российской Федерации (утверждена Указом Президента Российской Федерации от 05.12.2016 № 646).
3. Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы (утверждена Указом Президента Российской Федерации от 09.05.2017 № 203).
4. Программа «Цифровая Экономика Российской Федерации» (утверждена Распоряжением Правительства Российской Федерации от 28.07.2017 № 1632-рп).
5. ГОСТ Р ГОСТ Р 51624-2000 Автоматизированные информационные системы в защищенном исполнении. Общие положения. М.: Стандартинформ, 2000.
6. ГОСТ Р 51583-2014. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. М.: Стандартинформ, 2014.
7. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утв. решением председателя Гостехкомиссии России от 30.03.1992 г.
8. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утв. приказом ФСТЭК России от 11.02. 2013 г. № 17.
9. Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды. Утв. приказом ФСТЭК России от 14.03. 2014 № 31.
10. Требования к защите персональных данных при их обработке в информационных системах персональных данных. Утв. постановлением Правительства РФ от 01.11.2012 г. № 1119.
11. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утв. приказом ФСТЭК России от 18.02.2013 г. № 21.
12. Стандарт Банка России. Обеспечение информационной безопасности организаций банковской системы РФ. Общие положения «СТО БР ИББС-1.0-2014». Принят и введен в действие Распоряжением Банка России от 17.05.2014 № Р-399. М.: Банк России. 48 с.
13. Калашников А.О., Михалевич И.Ф. Анализ систем классификации защищенности автоматизированных и информационных систем значимых объектов критической информационной инфраструктуры Российской Федерации // Информация и безопасность. 2018. Т. 21, Вып. 1. С. 28-37.
14. Калашников А.О., Михалевич И.Ф. Унифицированная система классификации защищенности значимых объектов критической информационной инфраструктуры российской федерации по критериям безопасности информации // Информация и безопасность. 2018. Т. 21, Вып. 1. С. 6-17.