УПРАВЛЕНИЕ ИНФОРМАЦИОННЫМИ РИСКАМИ В ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ ПОДРАЗДЕЛЕНИЙ ГОСУДАРСТВЕННОЙ ПРОТИВОПОЖАРНОЙ СЛУЖБЫ МЧС РОССИИ

В.И. Антюхов, кандидат технических наук, профессор,
заслуженный работник высшей школы Российской Федерации;
Е.А. Коткова.
Санкт-Петербургский университет ГПС МЧС России

Предложена модель, описывающая процесс управления информационными рисками с помощью системы управления информационными рисками типовой информационно-вычислительной сети подразделения Государственной противопожарной службы МЧС России.

Ключевые слова: управление, информационный риск, информационное обеспечение, модель

MANAGEMENT OF THE INFORMATION RISK IN INFORMATION-COMPUTER NETWORKS OF THE DEPARTMENT OF STATE FIRE SERVICE OF EMERCOM OF RUSSIA

V.I. Antyukhov; E.A. Kotkova.
Saint-Petersburg university of State fire service of EMERCOM of Russia

The model which describes process of information risk managementthrough a system management of the information risk in information-computer networks of the department of State fire service of EMERCOM of Russia.

Keywords: management, information risk, information support, model

Статья является результатом исследований по формализации процесса управления информационными рисками (ИР) с помощью системы управления информационными рисками (СУИР) типовой информационно-вычислительной сети (ИВС) подразделения Государственной противопожарной службы (ГПС) МЧС России.

Применение ИВС приводит к возможному наступлению случайного события – ИР, приводящего к нарушению процесса функционирования или искажению информации ИВС подразделения ГПС МЧС России. ИР – это возможность наступления случайного события, приводящего к нарушениям функционирования ИВС подразделения ГПС МЧС России и снижению качества информации, а также к неправомерному использованию, распространению или противодействию распространения информации во внешней среде путем преодоления защиты, в результате которых наносится ущерб как отдельному подразделению, так и министерству в целом [1]. Возникает необходимость управления ИР, то есть определение совокупности мероприятий, приемов, методик, выбора модели и алгоритма, которые будут способствовать минимизации ИР и обеспечению требуемой информационной безопасности подразделения ГПС МЧС России.

Структуру типовой ИВС подразделения ГПС МЧС России (рис. 1) можно представить состоящей из совокупности связанных подсистем [1]:

– подсистема серверов различного назначения;

– подсистема коммуникаций;

– подсистема автоматизированных рабочих мест (АРМ) должностных лиц подразделения ГПС;

– подсистема средств администрирования ИВС;

– подсистема удаленных АРМ.

Каждая из представленных подсистем включает средства по видам обеспечения:

– организационное (помещения, в которых находятся ресурсы ИВС, в которых хранится и обрабатывается информация; руководящие документы [2–6];

– информационное (системы классификации и кодирования информации; унифицированная система документации (методические и инструкторские материалы); информационные массивы (нормативно-справочная информация, оперативная информация);

– техническое (рабочие станции, серверы, маршрутизаторы, источники бесперебойного питания, сетевые коммутаторы, устройства ввода и вывода информации, линии связи между узлами ИВС и другими подразделениями, министерствами, ведомствами);

– математическое (модели по видам обеспечения: организационного, технического, информационного, программного, кадрового);

– программное (системное (базовое), прикладное, специальное программное обеспечение);

– кадровое (сотрудники подразделения);

– правовое (consultant.ru; nlr.ru) и др.

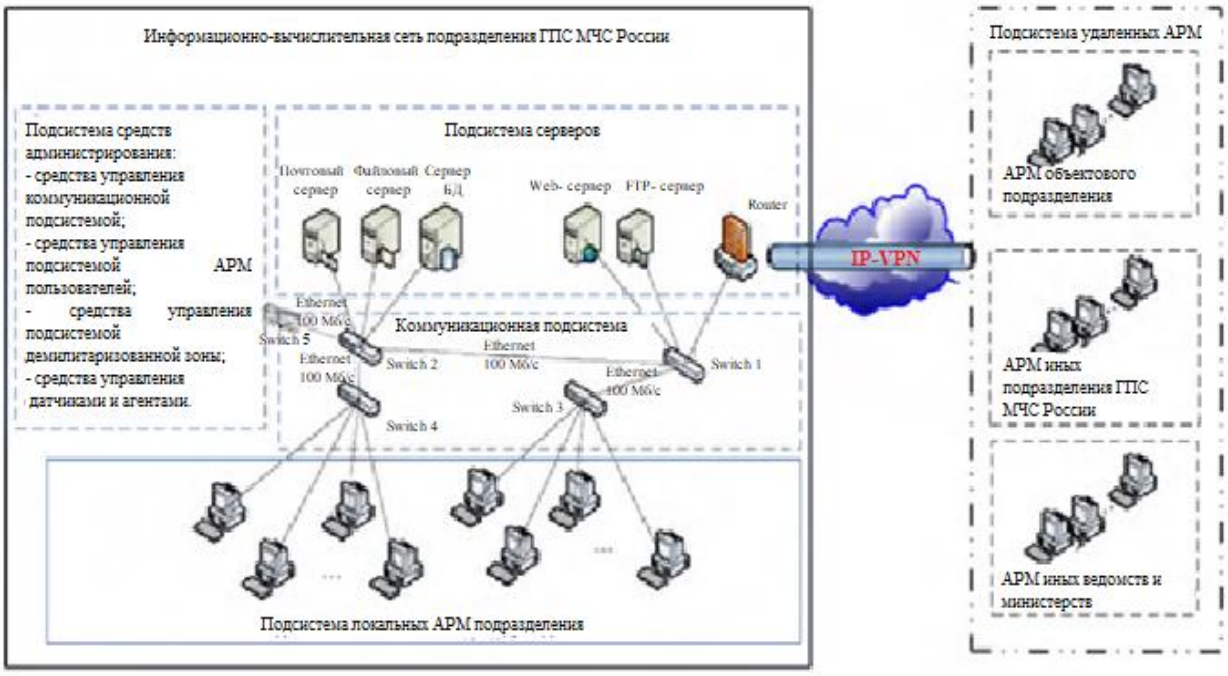

Рис. 1. **Структура типовой ИВС подразделения ГПС МЧС России**

Для автоматизации процессов управления рисками необходима формализация этих процессов и создание автоматизированной системы управления рисками.

СУИР должна выполнять следующие функции и задачи, которые представлены в табл. 1.

Структура предлагаемой СУИР в ИВС подразделений ГПС МЧС России представлена на рис. 2 [7]. В её состав включены:

1) управляющая подсистема (осуществляющая взаимодействие управляющего органа (старший инженер отдела информационных технологий, автоматизированных систем управления и связи (ИТ, АСУиС) с объектом управления (ИР ИВС);

2) подсистема функций управления, включающая, в свою очередь, подсистемы:

– планирования (планирование требований к СУИР; планирование структуры СУИР; планирование документации, сопровождающей процесс управления ИР и т.д.);

– учета (учёт требований к СУИР; учёт структуры СУИР; учёт документации, сопровождающей процесс управления ИР и т.д.);

– контроля (контроль деятельности лиц, ответственных за управление ИР; контроль документации, сопровождающей процесс управления ИР; контроль обновления операционной системы СУИР и т.д.);

– оперативного управления (управление деятельностью лиц, ответственных за управление ИР; оснащение техническими средствами подразделения для выявления угроз; оснащение программными средствами подразделения для выявления угроз);

3) подсистема обслуживания, обработки и предоставления ресурсов для управления системой, состоящей из подсистем:

– МО – математического обеспечения;

– ПО – программного обеспечения;

– ОО – организационного обеспечения;

– ТО – технического обеспечения;

– ИО – информационного обеспечения.

Таблица 1

<table>
<tr><td colspan="5">Функция организации управления риском</td></tr>
<tr><td>Разработка и утверждение политики управления рисками</td><td colspan="2">Разработка внутренних нормативных документов, включающих в себя четкие методы управления риском</td><td colspan="2">Контроль правильности, адекватности и полноты применения утвержденных процедур контроля и управления рисками</td></tr>
<tr><td colspan="5">Функция разработки приёмов и методов управления риском</td></tr>
<tr><td>Разработка методики анализа риска</td><td colspan="2">Разработка приемов и методов контроля риска</td><td colspan="2">Разработка приемов и методов снижения риска</td></tr>
<tr><td colspan="5">Функция контроля рисков</td></tr>
<tr><td colspan="3">Мониторинг состояния технических средств (рабочих станций, камер видеонаблюдения, серверов и т.д.) с целью своевременного выявления «зон риска»</td><td colspan="2">Мониторинг соблюдения и исполнения должностных инструкций, внутренних документов всеми сотрудниками подразделения</td></tr>
<tr><td colspan="5">Функция нивелирования (минимизации) рисков</td></tr>
<tr><td colspan="3">Оценка вероятности наступления события, приводящего к ущербу</td><td colspan="2">Подготовка предложения по минимизации выявленных рисков</td></tr>
<tr><td colspan="5">Функция прогнозирования риска</td></tr>
<tr><td>Идентификация риска</td><td>Анализ риска</td><td>Оценка риска</td><td>Разработка механизмов снижение риска</td><td>Разработка программы мероприятий по ликвидации последствий рисковых ситуаций</td></tr>
</table>

На функциональном уровне в СУИР (рис. 2) выделены задачи по функциям управления (задачи планирования, учёта, контроля и оперативного управления – соответственно табл. 2–5).

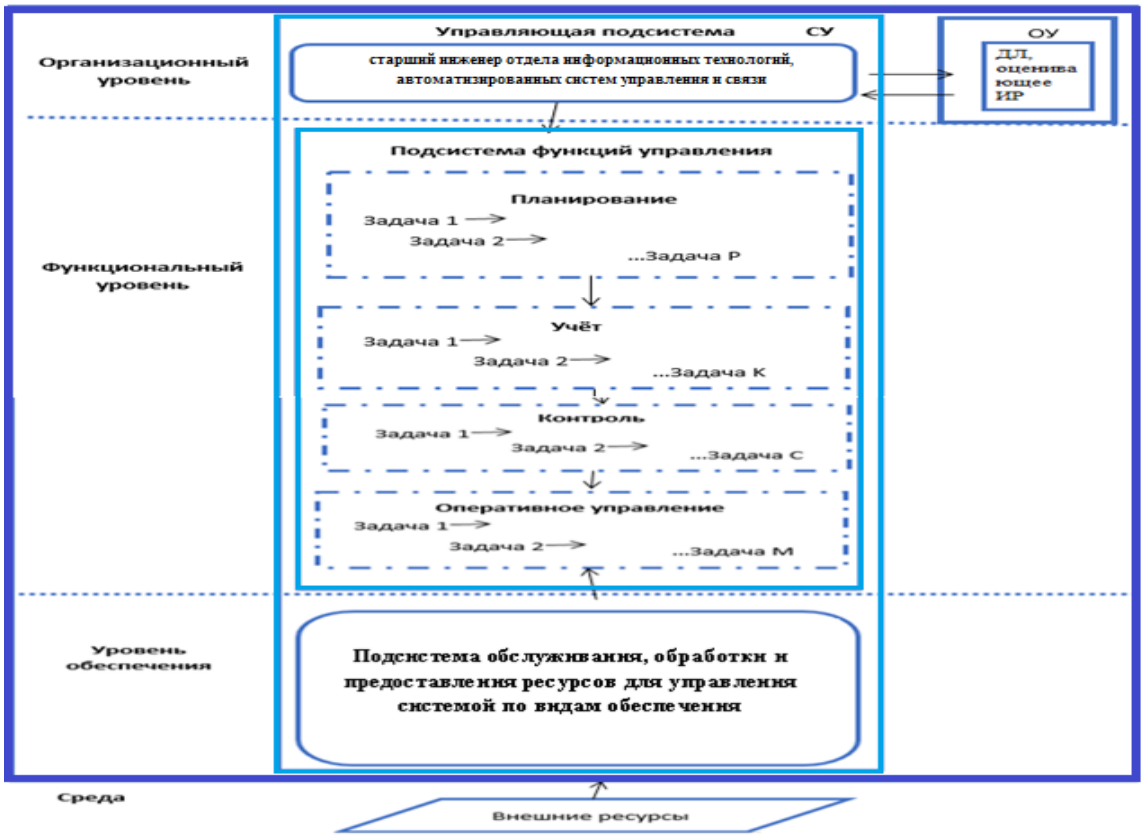

Рис. 2. **СУИР как система с управлением**

Таблица 2

1.	Планирование требований к СУИР
2.	Планирование структуры СУИР
3.	Планирование документации, сопровождающей процесс управления ИР
4.	Планирование правил эксплуатации СУИР
5.	Планирование настройки СУИР
6.	Планирование отладки СУИР
7.	Планирование состава программно-аппаратных средств СУИР
8.	Планирование порядка использования программных средств СУИР
9.	Планирование структуры программного обеспечения СУИР
10.	Планирование организации взаимодействия и взаимообмена СУИР
11.	Планирование порядка оповещения при отказах СУИР
12.	Прогнозирование способов устранения отказов СУИР
13.	Планирование перечня лиц, ответственных за управление ИР

Таблица 3

1.	Учёт требований к СУИР
2.	Учёт структуры СУИР
3.	Учёт документации, сопровождающей процесс управления ИР
4.	Учёт конфигурации сети СУИР
5.	Учёт настройки узлов связи
6.	Учёт взаимодействия и взаимообмена СУИР
7.	Учёт состояния и сохранности СУИР
8.	Учёт конфигурации ОС СУИР
9.	Учёт перечня лиц, ответственных за управление ИР
10.	Учёт порядка оповещения при отказах СУИР
11.	Учёт способа устранения отказов СУИР
12.	Учёт структуры программного обеспечения СУИР

Таблица 4

1.	Контроль деятельности лиц, ответственных за управление ИР
2.	Контроль документации, сопровождающей процесс управления ИР
3.	Контроль обновления операционной системы СУИР
4.	Контроль установления программного обеспечения СУИР
5.	Контроль состояния программных средств ИВС
6.	Контроль состояния технических средств ИВС
7.	Контроль состояния СУИР

Таблица 5

1.	Управление деятельностью лиц, ответственных за управление ИР
2.	Оснащение техническими средствами подразделения для выявления угроз
3.	Оснащение программными средствами подразделения для выявления угроз

В ходе исследования поставлена задача выявления приемлемого способа формализованного представления ИР по видам обеспечения. В статье представляется один из возможных способов формализованного описания СУИР (на примере информационного обеспечения СУИР в ИВС подразделения ГПС МЧС России (рис. 3) [8]) – описание на основе теории агрегатов.

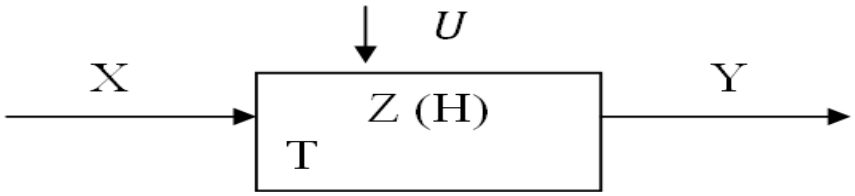

Рис. 3. **Типовой агрегат**

Агрегат (A) представления *ИО,* являющегося элементом *СУИР,* описывается кортежем (1):

$$A = \{T, Z, X, U, Y, H\}, \quad (1)$$

где $T = [0, T_f] \in R$ – процесс моделирования хода функционирования агрегата A (обычно конечный); Z – множество состояний (фазовое пространство) агрегата – переход ИО СУИР из i состояния в состояние j. Фазовое пространство $z = (z_1,\ z_2, \dots z_n)$ представляется фазовыми координатами $z_1,\ z_2, \dots z_n$, изменяющимися с течением t; X – множество входных сигналов ($x = [x^1, \dots x^l]$), где l – число «входных контактов»; U – множество управляющих сигналов ($u = [u^1, \dots u^r]$), где r – число «особенных входных контактов»; Y – множество выходных сигналов; H – оператор переходов, который определяет текущее состояние по предыстории (с учётом множества управляющих и входных сигналов, интервала моделирования СУИР и фазового пространства) (табл. 6).

Результатом моделирования процесса функционирования агрегата A является получение характеристик, определяющих состояние ИО (Z) СУИР: для моментов времени (0; *t)* в зависимости от вида оператора (H), входных (X) и управляющих (U) сигналов. Составляющие элементов кортежа (1) для агрегата управления рисками ИО ИВС представлены соответственно в табл. 6–11.

Информационными ресурсами принято считать массивы документов или отдельно взятые документы, которые хранятся в соответствующих системах отдела ЦУКС (отдела ИТ, АСУиС).

Таблица 6

$T_н$	Момент начала фазы моделирования процесса функционирования агрегата A
$T_к$	Момент окончания фазы моделирования процесса функционирования агрегата A
ΔT	Длительность фазы моделирования процесса функционирования агрегата A, мин

Таблица 7

Z_1	Классификация информационных ресурсов
Z_2	Кодирование информационных ресурсов
Z_3	Унификация систем документации
Z_4	Определение «маршрута движения» информационных ресурсов

Таблица 8

X_1	Информация о количестве документов
X_2	Перечень признаков и значений признаков классификации информационных ресурсов
X_3	Виды методов кодирования информационного ресурса
X_4	Формат документов и требования для их оформления
X_5	Сведения о сопоставимости баз данных
X_6	Сведения о применяемых протоколах

Таблица 9

U_1	Информация о необходимых изменениях в документе
U_2	Информации об изменениях признаков классификации информационных ресурсов для их идентификации
U_3	Информация о видах метода кодирования информационного ресурса (правила кодирования)
U_4	Информация об используемых форматах документов и информация об изменениях, вносимых в требования по оформлению документов
U_5	Информация о сопоставляемых базах данных
U_6	Информация о протоколах

Таблица 10

Y_1	Сводная таблица о вносимых изменениях в текстовые документы, фотодокументы, видеодокументы, коды программ (требующие пароля для авторизации), которые хранятся на АРМе
Y_2	Сводная таблица статистических данных о частоте появления информации, соответствующей значениям признаков классификации информационных ресурсов
Y_3	Информация об используемом способе кодирования информационного ресурса
Y_4	Сводная таблица частот использования форматов при работе на АРМе и информации о вносимых изменениях в требования по оформлению документов
Y_5	Сводная таблица, содержащая информацию о сопоставляемых базах данных
Y_6	Отчёт об окончании работы протокола TCP/IP и информация о правильности сборки файла

Таблица 11

H_1	Описание действий, связанных с определением работоспособности ИО

Схема детализации входного сигнала агрегата A представлена на рис. 4 в виде матрицы размерностью (SxV):

– S – степень детализации входного сигнала;

– V – множество значений детализированных входных сигналов.

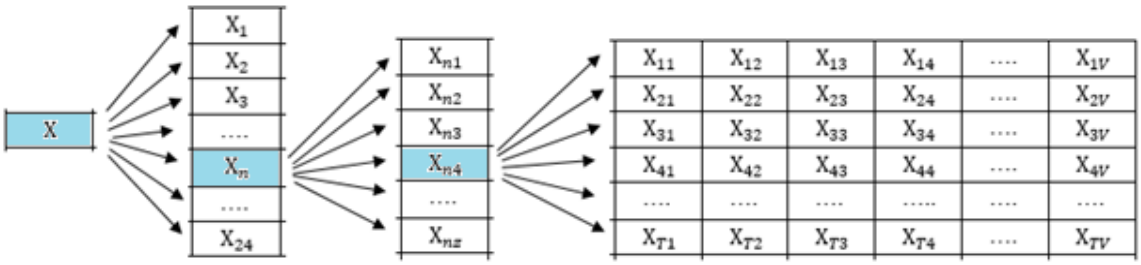

Рис. 4. **Схема детализации входного сигнала агрегата *A***

Аналогичным образом можно представить схемы детализации множества состояний, управляющих и выходных сигналов агрегатов *A* по видам обеспечения (рис. 5).

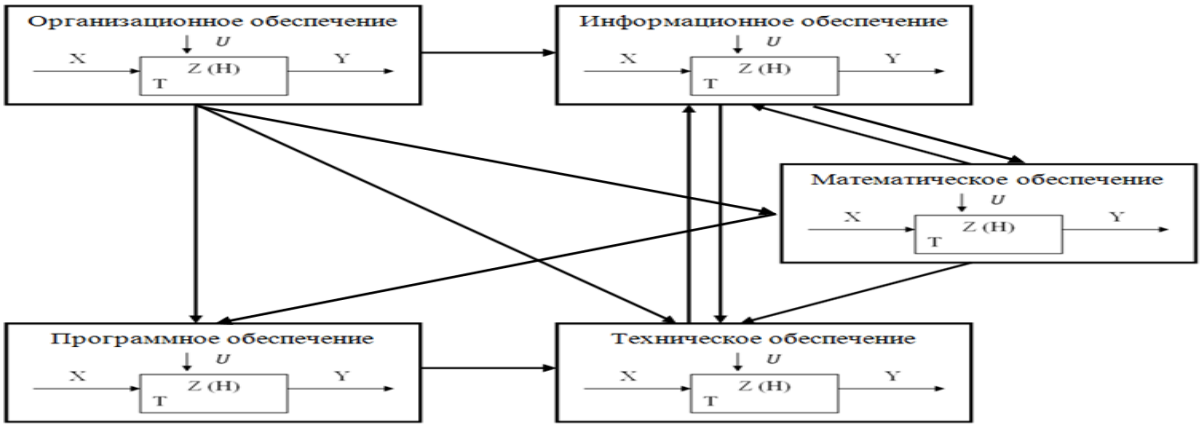

Рис. 5. **Схема взаимодействия агрегатов основных видов обеспечения СУИР**

В результате применения метода агрегатов для описания процесса управления ИР в ИВС сделан вывод, что теория агрегатов позволяет детализировать все реальные процессы, протекающие в СУИР, и тем самым адекватно представляющая эти процессы на формальном уровне.

Выявлены следующие достоинства теории агрегатов:

– доступность понимания;

– хорошая формализуемость;

– высокий уровень детализации, составляющих видов обеспечения.

Направлениями дальнейших исследований авторами представляются:

– разработка алгоритма функционирования СУИР и его реализация с поддержкой технологии Windows Forms с помощью программы Microsoft Visual Studio на языке C#;

– применение иных способов формального описания процессов управления ИР в ИВС подразделений ГПС МЧС России;

– определение и формальное представление средств противодействия ИР, которые используются в ИВС подразделений ГПС МЧС России.

Литература

1. Системный анализ и принятие решений / В.С. Артамонов [и др.]. 2-е изд. СПб.: С.-Петерб. ун-т ГПС МЧС России, 2017. 352 с.

2. ГОСТ Р ИСО/МЭК 15408-1–2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Доступ из справ.-правовой системы «КонсультантПлюс».

3. ГОСТ Р ИСО/МЭК 15408-2–2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 2: Функциональные требования безопасности. Доступ из справ.-правовой системы «КонсультантПлюс».

4. ГОСТ Р ИСО/МЭК 15408-3–2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 3: Требования доверия к безопасности. Доступ из справ.-правовой системы «КонсультантПлюс».

5. ГОСТ Р ИСО/МЭК 27001–2006. Информационная технология. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. Доступ из справ.-правовой системы «КонсультантПлюс».

6. ГОСТ РИСО/МЭК 31010–2011. Менеджмент риска. Методы оценки риска. Доступ из справ.-правовой системы «КонсультантПлюс».

7. Кравчук О.В. Формализация процесса управления рисками в информационно-вычислительных сетях подразделений ГПС МЧС России: дис. … канд. техн. наук. СПб., 2014. 159 с.

8. Варфоломеев А.А. Управление информационными рисками. М.: РУДН, 2008. 158 с.

References

1. Sistemnyj analiz i prinyatie reshenij / V.S. Artamonov [i dr.]. 2-e izd. SPb.: S.-Peterb. un-t GPS MCHS Rossii, 2017. 352 s.

2. GOST R ISO/MEHK 15408-1–2002. Informacionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Kriterii ocenki bezopasnosti informacionnyh tekhnologij. Dostup iz sprav.-pravovoj sistemy «Konsul'tantPlyus».

3. GOST R ISO/MEHK 15408-2–2002. Informacionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Kriterii ocenki bezopasnosti informacionnyh tekhnologij. Ch. 2: Funkcional'nye trebovaniya bezopasnosti. Dostup iz sprav.-pravovoj sistemy «Konsul'tantPlyus».

4. GOST R ISO/MEHK 15408-3–2002. Informacionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Kriterii ocenki bezopasnosti informacionnyh tekhnologij. Ch. 3: Trebovaniya doveriya k bezopasnosti. Dostup iz sprav.-pravovoj sistemy «Konsul'tantPlyus».

5. GOST R ISO/MEHK 27001–2006. Informacionnaya tekhnologiya. Metody obespecheniya bezopasnosti. Sistemy menedzhmenta informacionnoj bezopasnosti. Trebovaniya. Dostup iz sprav.-pravovoj sistemy «Konsul'tantPlyus».

6. GOST RISO/MEHK 31010–2011. Menedzhment riska. Metody ocenki riska. Dostup iz sprav.-pravovoj sistemy «Konsul'tantPlyus».

7. Kravchuk O.V. Formalizaciya processa upravleniya riskami v informacionno-vychislitel'nyh setyah podrazdelenij GPS MCHS Rossii: dis. … kand. tekhn. nauk. SPb., 2014. 159 s.

8. Varfolomeev A.A. Upravlenie informacionnymi riskami. M.: RUDN, 2008. 158 s.