АВТОМАТИЗИРОВАННОЕ УПРАВЛЕНИЕ РИСКАМИ В ТИПОВОЙ ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНОЙ СЕТИ ПОДРАЗДЕЛЕНИЯ ГПС МЧС РОССИИ

В.И. Антюхов, кандидат технических наук, профессор;
О.В. Кравчук.
Санкт-Петербургский университет ГПС МЧС России

Представлены результаты исследований, выполненных по теме: «Формализация процесса управления рисками в информационно-вычислительной сети подразделения ГПС МЧС России». Показан алгоритм управления информационными рисками, в частности, рассмотрены подсистемы управления информационными рисками. Разработана формальная информационная модель управления рисками.

Ключевые слова: риск, информационная безопасность, информационно-вычислительная сеть, управление, методика

AUTOMATED MANAGEMENT BY RISKS IN THE TYPICAL INFORMATION-COMPUTER NETWORK OF DEPARTMENT OF STATE FIRE SERVICE OF EMERCOM OF RUSSIA

V.I. Antyukhov, O.V. Kravchuk.
Saint-Petersburg university of State fire service of EMERCOM of Russia

The article presents the results of a research carried out on the topic: «Formalization of the risk management process in information-computer network of department of State fire service of EMERCOM of Russia. An algorithm for management of information risk management is presented, in particular the subsystem information risk management is considered. The formal information model of risk management is developed.

Keywords: risk, information security, information-computer network, management, technique

На сегодняшний день развитие информационно-вычислительной сети (ИВС) МЧС России выходит на принципиально новый этап, связанный, прежде всего, с началом практического построения Единого информационного пространства МЧС России как части Единого информационного пространства страны.

В МЧС России для поддержки принятия решений по оперативным действиям, связанным с развитием чрезвычайных ситуаций (ЧС) и ходом ликвидации их последствий, а также для сбора и обработки информации о возможном возникновении чрезвычайных ситуаций, созданы специальные автоматизированные системы на базе ИВС МЧС России. Именно эти системы и технические средства их поддержки, в соответствии с положениями Доктрины информационной безопасности Российской Федерации, являются наиболее уязвимыми объектами со стороны злоумышленников в условиях (ЧС).

Особенностью ИВС МЧС России и главным её отличием от большинства других ИВС органов государственной власти является обеспечение решения следующих задач:

– моделирование чрезвычайных ситуаций (ЧС);
– поиск оптимальных путей следования к месту возникновения ЧС;
– распределение сил и средств подразделений при ликвидации ЧС;
– оценка эффективности деятельности подразделений и др.

Зависимость процессов сбора информации и принятия решения от используемых должностными лицами подразделений МЧС России информационных технологий объективно приводит к наступлению в информационно-вычислительной сети случайных событий – информационных рисков (ИР) (информационный риск – это возможность наступления случайного события, приводящего к нарушениям функционирования информационной системы подразделения и снижению качества информации, а также к неправомерному использованию, распространению или противодействию распространения информации во внешней среде путём преодоления защиты, в результате чего наносится ущерб как отдельному подразделению, так и Министерству в целом (рис. 1) [1, 2]. Понятие информационного риска в ИВС возникает при наличии уязвимостей ИВС и угроз информационной безопасности по отношению к рассматриваемой ИВС.

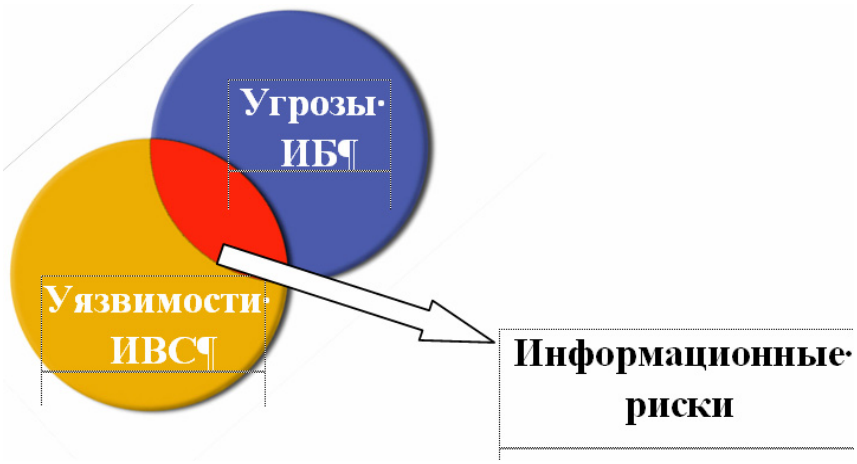

Рис. 1. **Компоненты информационного риска**

Эти риски способствуют нарушению процесса функционирования информационно-вычислительной сети подразделения в соответствии с её целевым предназначением и могут привести к изменению содержания передаваемой по сети информации, к неправомерному использованию, распространению или противодействию распространения информации в сети и телекоммуникационной среде путём преодоления средств защиты сети.

Поэтому задачи обеспечения защиты от возникновения информационных рисков в информационно-вычислительной сети как отдельного подразделения, так и министерства в целом приобретают особую актуальность. Необходимо научиться управлять рисками с целью снижения или компенсации ущерба, наносимого ИВС при наступлении неблагоприятных событий.

Для обеспечения информационной безопасности (ИБ) ИВС подразделений и поддержания её состояния в соответствии с предназначением необходима разработка автоматизированной системы принятия решений по минимизации последствий угроз информационным ресурсам сети, включающая:

– подсистему выявления угроз информационной безопасности сети, их фиксации и журналирования;

– подсистему выбора рационального средства (пути) противодействия угрозам;

– подсистему выработки и реализации управляющего воздействия по нейтрализации угроз;

– подсистему оценивания эффективности управляющих воздействий по нейтрализации угроз.

В работе процесс управления ИР рассматривается на примере системы с управлением. Предполагается, что управление выявленными рисками осуществляют должностные лица, ответственные за информационную безопасность в подразделении, и представляют собой управляющий орган. Объектом управления выступают информационные риски,

возникающие при наличии угроз и уязвимостей, присущих различным элементам ИВС, на различных уровнях сетевого взаимодействия.

С позиций теории принятия решений в такой системе с управлением операцией будем считать выявление угроз информационной безопасности и выработку адекватного управляющего воздействия по локализации и ликвидации этих угроз.

Управление информационными рисками представляет собой процесс выявления и идентификации ИР и выбора в рамках допустимых затрат комплекса средств и методов по нейтрализации уязвимостей ИВС, предупреждению, противодействию и ликвидации последствий реализации информационных атак.

Целью рассматриваемой операции управления ИР будем считать снижение вероятности возникновения информационных рисков, то есть неблагоприятных случайных событий, а также построение эффективной политики информационной безопасности.

По сути, управление информационными рисками предполагает управление политикой информационной безопасности подразделения.

Для построения эффективной политики информационной безопасности подразделения ГПС МЧС России необходимо применить такой подход, который позволял бы комплексно проводить оценку угроз информационным ресурсам, оценку степени защищённости информационной системы, а также разработать экономически оправданную систему мероприятий и средств противодействия угрозам информационной безопасности подразделений.

Таким актуальным подходом является формализация процесса управления рисками ИВС подразделения, начиная от определения исходного множества параметров и заканчивая формированием целевой функции, то есть математической модели процесса управления ИР.

Ввиду недостаточности информации о целях и средствах совершения информационных атак, а также о характере и масштабе ущерба, нанесённого подразделению в результате их реализации, формализация процесса управления ИР осуществляется в условиях неопределённости. Другими словами, имеется информация о различных исходах операции, но нет никаких данных о законах распределения вероятностей на множестве исходов.

Потенциальными объектами угроз ИВС могут выступать:

1) Аппаратные средства ИВС подразделения:

– серверы (почтовый, файловый, сервер БД, Web-сервер, FTP-сервер);

– рабочие станции;

– маршрутизатор;

– сетевые коммутаторы;

– линии связи между узлами ИВС и другими подразделениями.

2) Программное обеспечение (ПО) ИВС:

– системное ПО;

– прикладное ПО, предназначенное для поддержки автоматизированных информационно-управляющих систем (система учёта и информирования ГИМС, система оперативного управления АС НЦУКС, система учёта ЧС и происшествий и др.).

3) Информационные системы ИВС подразделения.

4) Пользователи ИВС подразделения.

Управление информационными рисками представляет собой процесс выбора управляющим органом оптимального управляющего воздействия (выбор контрмер), в соответствии с информацией о состоянии объекта управления (информацией о наличии выявленных уязвимостей) и информацией о наличии возмущающего воздействия (информацией о наличии угрозы реализации информационной атаки) с целью обеспечения информационной безопасности подразделения.

Для рассматриваемой системы с управлением неуправляемыми характеристиками будем считать:

– средства реализации угроз;

– способы реализации угроз, конкретный сценарий реализации угроз (процесс реализации воздействия);

– источники угроз (субъекты воздействия);

– цель реализации угроз ИБ (предмет воздействия);

– величина нанесенного ущерба в результате реализации атак;

– программное, аппаратное, информационное, кадровое и другие виды обеспечения подразделения ГПС МЧС России (объекты воздействия);

– уязвимости ИВС подразделения;

а управляемыми характеристиками:

– методы защиты ИВС подразделения (R_m);

– средства защиты ИВС подразделения (R_s);

– затраты на обеспечение ИБ (R_z).

Множество значений управляемых характеристик и представляет собой ни что иное, как управляющее воздействие (R_y) (решение) [3].

Выбор решения должен производиться из числа допустимых решений, которые определяются в соответствии с принятыми ограничениями на значения управляемых характеристик [3]:

– должна быть обеспечена совместимость имеющихся в ИВС программных, аппаратных средств со средствами защиты от информационных атак;

– при выборе средств, методов предупреждения, защиты и ликвидации последствий реализации информационных атак, а также управляющих воздействий должно быть выделено не менее одного средства и выбрано не менее одного метода и управляющего воздействия с целью защиты ИВС подразделения ГПС МЧС России;

– применение совокупности средств и методов воздействий должны обеспечивать снижение уровня риска до приемлемого (P_n) (остаточный риск);

– время обнаружения угроз и реализации управляющих воздействий должно быть минимальным и соответствовать реальному масштабу времени.

Для достижения поставленной цели управления информационными рисками в ходе проводимого научного исследования предлагается следующий перечень работ:

1) разработка постановки задачи для автоматизированного оценивания процессов управления рисками в типовой информационно-вычислительной сети подразделения, что было рассмотрено ранее в статье [2];

2) разработка концептуальной, а в последующем – формальной информационной модели процесса управления рисками (рис. 2) [1, 5];

3) разработка методики автоматизированной оценки состояния управления рисками в типовой информационно-вычислительной сети подразделения ГПС МЧС России;

4) разработка математической модели процесса управления рисками в типовой информационно-вычислительной сети подразделения ГПС МЧС России;

5) анализ результатов моделирования для подготовки выводов и рекомендаций по решению проблемы;

6) определение перечня предложений по совершенствованию политики безопасности информационно-вычислительных сетей подразделений ГПС МЧС России и разработка плана реализации предложенных решений.

В соответствии с предложенной моделью имеется возможность определить компоненты выделенных подсистем.

Так, подсистема выявления угроз информационной безопасности сети, их фиксации и журналирования включает:

1. Определение параметров функционирования ИВС в соответствии с её назначением. $A=(a_1, a_2, a_3 \dots a_i)$, где:

a_1 – время реакции на запросы пользователей;

a_2 – пропускная способность сетевого оборудования;

a_3 – средняя задержка передачи пакетов информации;

a_4 – отклонение от среднего значения задержки передачи пакетов информации;

a_5 – коэффициент потери пакетов информации;

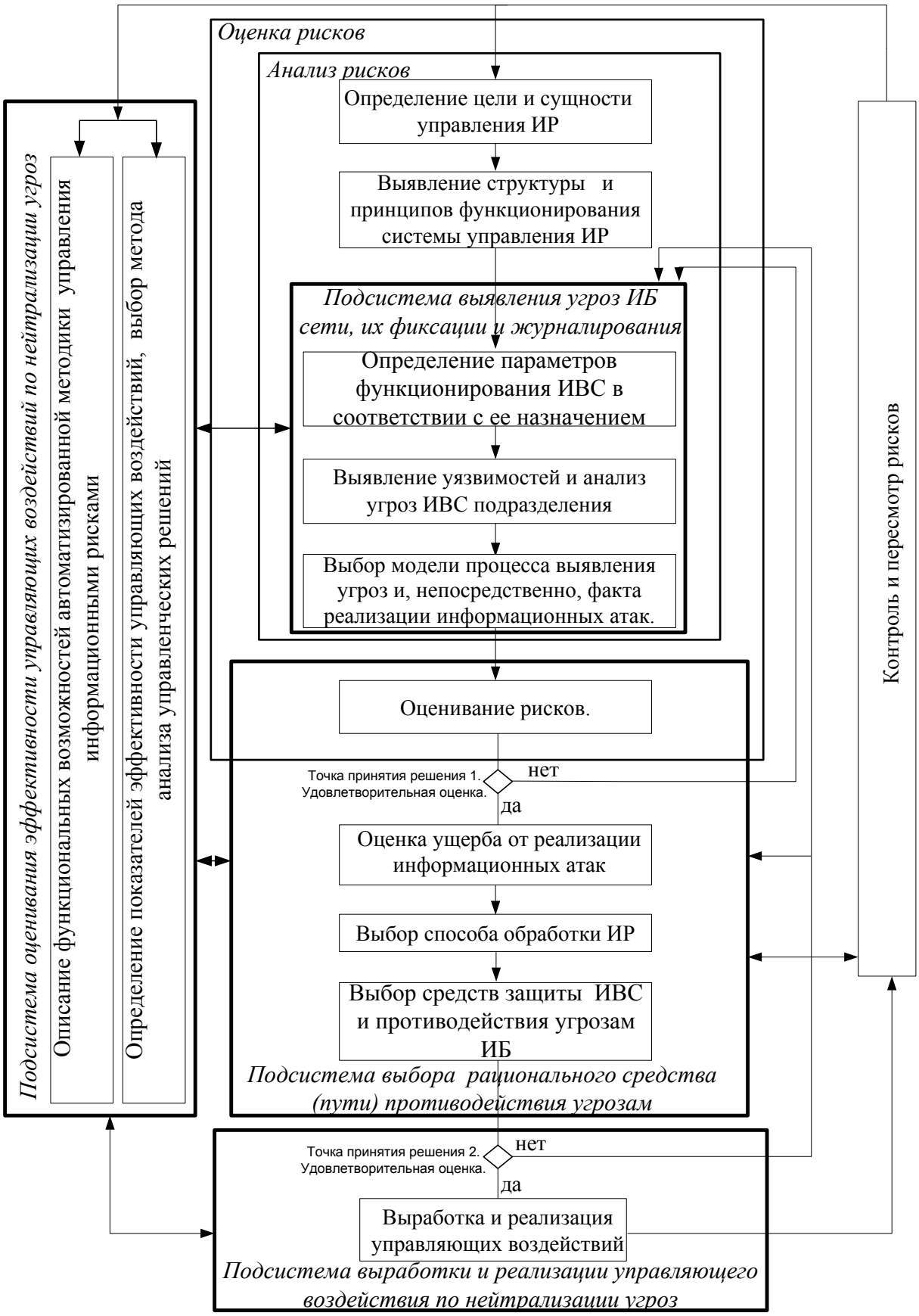

Рис. 2. **Формальная информационная модель управления рисками в типовой информационно-вычислительной сети подразделения ГПС МЧС России**

a_6 – коэффициент ошибок в пакетах информации;

a_7 – штатное время работы пользователей ИВС;

a_8 – количество обращений пользователей к сетевым ресурсам и др.

2. Выявление уязвимостей ИВС. B=(b_1, b_2, b_3 ... b_j), где:

b_1 – отсутствие правил разграничения полномочий должностных лиц по допуску их к информационным ресурсам;

b_2 – незащищённые таблицы паролей;

b_3 – наличие непредусмотренных и пригодных для использования скрытых каналов связи;

b_4 – отсутствие средств авторизации и аутентификации и др.

3. Определение возможных средств обнаружения факта реализации атаки на ИВС. C=(c_1, c_2, c_3 ... c_k), где:

c_1 – анализ сетевых журналов аудита;

c_2 – анализ пакетов данных, передаваемых по сети;

c_3 – срабатывание системы анализа защищённости сети (САЗС);

c_4 – срабатывание системы обнаружения и предотвращения вторжений (СОВ) и др.

4. Выявление угроз, присущих ИВС подразделения ГПС МЧС России. U=(u_1, u_2, u_3 ... u_q), где:

u_1 – внедрение аппаратных закладок;

u_2 – несанкционированное подключение устройств, замена элементов;

u_3 – перехват электромагнитного, магнитного и электрического полей, а также электрических сигналов с информацией;

u_4 – захват каналов телекоммуникационного вещания;

u_5 – перехват информации в/за пределами контролируемой зоны и др.

5. Выбор модели процесса выявления угроз и, непосредственно, факта реализации информационных атак. D=(d_1, d_2, d_3 ... d_c), где:

d_1 – сигнатурные модели (d_{11} – модель контекстного поиска на основе регулярных выражений; d_{12} – модель контекстного поиска на основе специальных языков; d_{13} – модель анализа состояний ИВС; d_{13} – модель на основе экспертных систем; d_{14} – модель, основанная на генетических алгоритмах; d_{15} – модель, основанная на нейросетевых алгоритмах);

d_2 – поведенческие модели (d_{21} – статистические модели; d_{22} – модель, основанная на нейросетевых алгоритмах; d_{23} – модель на основе экспертных систем; d_{24} – модель на основе иммунных систем; d_{14} – модель на основе конечных автоматов-распознавателях).

Подсистема выбора рационального средства (пути) противодействия угрозам включает в себя:

1. Определение вероятности возникновения угроз. P=(p_1, p_2, p_3. ... p_s) [5].

$$P=P_{дос}(N)* P_{реал}(N),$$

где $P_{дос}(i)$ – вероятность доступа ко всем i-м $\left(i=\overline{1,n}\right)$ элементам ИВС, а $P_{реал}(i)$ – вероятность реализации угрозы злоумышленником в i-х элементах ИВС.

2. Определение вероятности противодействия угрозам с использованием экспертных оценок. P*=(p^*_1, p^*_2, p^*_3... p^*_s).

3. Оценка ущерба от реализации информационных атак. W=(w_1, w_2, w_3 ... w_q).

Каждая u-я (U=(u_1, u_2, u_3 ... u_q)) угроза характеризуется вероятностью возникновения угрозы Ps, вероятностью противодействия угрозе Ps* и величиной ущерба от воздействия u-й угрозы на элемент i ИВС подразделения ΔW_u [6]:

$$W = \sum_{u=1}^{U} P_u \cdot P_u^* \cdot \Delta W_i .$$

4. Выбор способа обработки рисков. $O=(o_1, o_2, o_3 \dots o_k)$, где:

o_1 – смягчение рисков (o_{11} – уменьшение вероятности убытков; o_{12} – снижение тяжести потерь);

o_2 – принятие рисков (o_{21} – создание системы резервов ресурсов сети; o_{22} – планирование действий на случай непредвиденных обстоятельств);

o_3 – уклонение от рисков (o_{31} – модификация решений по реализации управляющих воздействий; o_{32} – модификация системы управления информационными рисками);

o_4 – передача рисков (o_{41} – передача полномочий по управлению рисками сторонней организации; o_{42} – страхование рисков).

5. Выбор средств защиты ИВС и противодействия угрозам ИБ в зависимости от их функций. $G=(g_1, g_2, g_3 \dots g_x)$, где:

g_1 – средства выявления и/или устранения уязвимостей ИВС;

g_2 – средства выявления и/или блокирования информационных атак на ИВС;

g_3 – средства выявления и/или устранения последствий информационных атак на ИВС.

6. Выбор средств защиты ИВС и противодействия угрозам ИБ в зависимости от уровня сетевого взаимодействия. $E=(e_1, e_2, e_3 \dots e_v)$, где:

e_1 – средства защиты ИВС и противодействия угрозам ИБ физического уровня;

e_2 – средства защиты ИВС и противодействия угрозам ИБ канального уровня;

e_3 – средства защиты ИВС и противодействия угрозам ИБ сетевого уровня;

e_4 – средства защиты ИВС и противодействия угрозам ИБ транспортного уровня;

e_5 – средства защиты ИВС и противодействия угрозам ИБ прикладного уровня.

6. Выбор средств защиты ИВС и противодействия угрозам ИБ в зависимости от их вида. $H=(h_1, h_2, h_3 \dots h_v)$, где:

h_1 – технические средства защиты ИВС и противодействия угрозам ИБ;

h_2 – программные средства защиты ИВС и противодействия угрозам ИБ;

h_3 – организационные меры защиты ИВС и противодействия угрозам ИБ.

Подсистема выработки и реализации управляющих воздействий по нейтрализации угроз объединяет результаты, полученные в предыдущих подсистемах, и позволяет должностному лицу, ответственному за информационную безопасность вовремя выявлять и ликвидировать информационные риски.

Подсистема оценивания эффективности управляющих воздействий по нейтрализации угроз включает в себя:

1. Описание функциональных возможностей автоматизированной методики управления информационными рисками. $Z=(z_1, z_2, z_3 \dots z_m)$, где:

z_1 – точность выявления информационных атак;

z_2 – скорость обработки данных;

z_3 – эффективное реагирование на атаки;

z_4 – наличие механизмов собственной безопасности;

z_5 – масштабируемость;

z_6 – поддержка многопользовательского режима;

z_7 – интеграция с другими средствами защиты;

z_8 – удобство эксплуатации;

z_9 – возможность генерации отчетов;

z_{10} – возможность накопления базы данных о выявленных угрозах и средствах противодействия и др.

2. Определение показателей эффективности управляющих воздействий. $Y=(y_1, y_2, y_3 \dots y_n)$, где:

y_1 – определение временных затрат на реализацию управляющих воздействий;

y_2 – определение экономических затрат на реализацию управляющих воздействий и др.

3. Выбор метода анализа управленческих решений. $Q=(q_1, q_2, q_3 \dots q_m)$, где:

q_1 – метод сравнения;

q_2 – функционально-стоимостный анализ;

q_3 – экономико-математические методы анализа и др.

Практическая значимость полученных результатов заключается в:

1. Разработке концептуальной схемы алгоритма управления рисками в типовой информационно-вычислительной сети подразделений ГПС МЧС России.

2. Формулирование предложений по содержанию методики автоматизированного управления информационными рисками.

3. Формирование исходных данных для разработки математической модели процесса управления рисками типовой информационно-вычислительной сети подразделения ГПС МЧС России.

Направления дальнейших исследований:

1. Разработка математической модели процесса управления рисками в типовой информационно-вычислительной сети подразделения ГПС МЧС России.

2. Анализ результатов моделирования для подготовки выводов и рекомендаций по решению проблемы.

3. Определение перечня предложений по совершенствованию политики безопасности информационно-вычислительных сетей подразделений ГПС МЧС России и разработка плана реализации предложенных решений.

Литература

1. Астахов А.М. Искусство управления информационными рисками. М.: ДМК Пресс, 2010.

2. Росенко А.П. Метод определения вероятности несанкционированного доступа злоумышленника к конфиденциальной информации // Докл. Томск. гос. ун-та систем упр. и радиоэлектроники. 2012. № 1 (25). Ч. 2.

3. Системный анализ и принятие решений: учеб. / под ред. В.С. Артамонова. СПб.: С.-Петерб. ун-т ГПС МЧС России, 2009. 378 с.

4. Антюхов В.И., Кравчук О.В. Моделирование процесса противодействия угрозам информационно – вычислительной сети подразделения ГПС МЧС России // Проблемы упр. рисками в техносфере. 2013. № 3.

5. ISO/IEC 27005:2008. Информационная технология. Методы защиты. Менеджмент рисков информационной безопасности // Практич. менеджмент качества он-лайн. URL: http://www.pqm-online.com /assets /files/ standards/iso_iec_27005-2008(r).pdf (дата обращения: 14.10.2013).

6. Аветисов Р.С. К вопросу оценки ущерба в автоматизированных информационных системах: материалы X Междунар. науч.-практ. конф. «Информационная безопасность». Ч. 1. Таганрог: Таганрог. гос. радиотехн. ун-т, 2008. С. 164–169.

ЗАДАЧИ И РОЛЬ МЧС РОССИИ В РЕШЕНИИ АКТУАЛЬНЫХ ПРОБЛЕМ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ НАСЕЛЕНИЯ ОТ КОСМИЧЕСКИХ УГРОЗ

Л.В. Медведева.
Санкт-Петербургский университет ГПС МЧС России.
К.В. Холшевников;
Л.Л. Соколов.
Санкт-Петербургский государственный университет

Проведён анализ последствий падения метеорита под г. Челябинском, сформулированы ключевые задачи в области обеспечения безопасности при чрезвычайной ситуации планетарного масштаба, изложены фундаментальные основы астероидно-кометной опасности для Земли.