УДК 004.056.53

А.А. Демидов, О.Г. Никифоров, И.Б. Саенко

РАЗРАБОТКА КОНЦЕПЦИИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ ОРГАНОВ ГОСУДАРСТВЕННОЙ ВЛАСТИ

Демидов А.А., Никифоров О.Г., Саенко И.Б. **Разработка концепции обеспечения информационной безопасности информационно-телекоммуникационных систем органов государственной власти.**

Аннотация. В статье рассматриваются особенности разработки концепции обеспечения информационной безопасности информационно-телекоммуникационных систем органов государственной власти. Отличительные положения концепции характеризуют объект защиты, угрозы информационной безопасности, средства обеспечения информационной безопасности и организацию обеспечения информационной безопасности. В качестве основных отличительных положений выделены концептуальная модель обеспечения информационной безопасности и концептуальная модель системы обеспечения информационной безопасности. Концептуальная модель обеспечения информационной безопасности представлена в функциональном виде, который позволяет определить зависимость показателей эффективности от полной совокупности условий и факторов, оказывающих влияние на их значения. Концептуальная модель системы обеспечения информационной безопасности представлена в виде ориентированного графа. При этом отмечается, что задача системы обеспечения информационной безопасности состоит в том, чтобы осуществить перекрытие каждого ребра данного графа соответствующими комплексами мер и средств защиты информации.

Ключевые слова: информационно-телекоммуникационная система, органы государственной власти, информационная безопасность, концепция.

Demidov A.A., Nikiforov O.G, Saenko I.B. **Development of the concept of information security for information and telecommunications systems of the State authorities.**

Abstract. The paper deals with design features of the concept of information security for information and telecommunication systems of State authorities. The distinctive concept provisions describe the object of protection, threats to information security, means of ensuring information security, and management of ensuring information security. As main distinctive concept provisions, the conceptual model of ensuring information security and the conceptual model of the system of ensuring information security are selected. Conceptual model of ensuring information security is presented in functional form, which allows determining the dependence of the performance from the full set of conditions and factors influencing their values. A conceptual model of the system of ensuring information security is presented as oriented graph. It is noted that the challenge of the system of ensuring information security is to implement overlay of each edge of the graph of the relevant packages and means of information security.

Keywords: information and communications system, State authorities, information security, concept.

1. Введение. Вопросы обеспечения информационной безопасности (ИБ) информационно-телекоммуникационных систем (ИТКС) органов государственной власти (ОГВ) страны имеют весьма большое

значение, особенно в настоящее время, когда на первый план выдвигаются вопросы информационного противоборства между конфликтующими сторонами. Вместе с тем, проблема обеспечения ИБ ИТКС является многоаспектной, комплексной и предполагающей решение целого ряда разноплановых, но в значительной степени связанных между собой задач.

Начальным этапом решения данной проблемы, как и других проблем такого уровня сложности, является разработка концепции обеспечения ИБ ИТКС ОГВ. С точки зрения понимания сущности задач и путей их решения, данная концепция представляет собой систему взглядов на организацию работ по обеспечению ИБ ИТКС. Если рассматривать вопрос о проведении научных исследований по построению системы защиты информации, то эта концепция воспринимается как метод исследования [1].

Целью настоящей статьи является рассмотрение основных аспектов, касающихся разработки концепции обеспечения ИБ ИТКС ОГВ, включающих отличительные особенности концепции применительно к ИТКС ОГВ как объекту защиты информации, а также концептуальную модель обеспечения ИБ и концептуальную модель системы обеспечения ИБ ИТКС ОГВ.

2. Отличительные особенности концепции обеспечения ИБ ИТКС ОГВ. Анализируя известные разработанные концепции, относящиеся к области защиты информации и к процессу информатизации в целом [2–4], а также руководящие и методические документы по их разработке [5–9], можно предложить следующее общее содержание разрабатываемой концепции обеспечения ИБ ИТКС ОГВ:

общие положения, определяющие предназначение документа;

основные определения;

цели и задачи обеспечения ИБ;

принципы обеспечения ИБ;

угрозы ИБ;

основные направления, методы и средства обеспечения ИБ (модель обеспечения ИБ);

мероприятия по обеспечению ИБ (модель системы обеспечения ИБ).

Так как многие из перечисленных аспектов в той или иной мере уже разработаны и представлены в известных концепциях по защите информации, рассмотрим только особенности настоящей концепции, обусловленные ее ориентацией на ИТКС ОГВ.

В работах [10–13] заложены теоретические основы построения и функционирования систем обеспечения информационной безопасности автоматизированных систем, включая существующие и перспективные ИТКС. Вместе с тем, особенности, присущие информационным процессам, протекающим в ИТКС ОГВ Российской Федерации различного уровня и назначения, а также системам обеспечения их информационной безопасности, обусловливают необходимость уточнения ряда положений, входящих в состав концепции обеспечения ИБ такого класса ИТКС.

На наш взгляд, такими отличительными положениями являются:

в области характеристики объекта защиты:

обоснование принципов структурного представления системы ОГВ как потребителя информации заданного качества с учетом конкретных сфер их деятельности, отношения к организациям с различными организационно-правовыми формами собственности, степени самостоятельности функционирования, взаимосвязей с другими государственными и общественными организациями и структурами;

определение характера информационных процессов в ИТКС ОГВ на основе сформированной структуры информационных ресурсов и потоков в системе управления ОГВ с учетом особенностей формирования и использования информационных ресурсов и специфики информационных потоков в системе обработки информации и управления ОГВ;

системная классификация информации, циркулирующей и обрабатываемой в компонентах ИТКС ОГВ, по степени важности, сферам использования, возможности двойного применения, степени автоматизации информационных процессов в системах управления ОГВ;

уточнение перечня, структуры, классификации, характеристик и особенностей построения и функционирования объектов информационной безопасности ОГВ и их ИТКС;

в области характеристики угроз информационной безопасности:

формирование облика и структурирование среды, в которой функционирует ИТКС ОГВ, выявление, классификация и оценивание возможных дестабилизирующих факторов;

определение угроз информационной безопасности ИТКС ОГВ, оказывающих влияние на защищенность информационной сферы ИТКС, а также источников этих угроз;

в части характеристики средств обеспечения информационной безопасности:

определение способов, методов и средств обеспечения информационной безопасности ИТКС ОГВ и научно-методического инструментария для проведения системных оценок эффективности функционирования системы обеспечения ИБ;

разработка решений по построению системы обеспечения информационной безопасности ИТКС ОГВ с учетом интеграции информационных и телекоммуникационных технологий и особенностей функционирования ИТКС различного назначения и уровня;

определение направлений, путей и способов совершенствования методов, способов и средств обеспечения информационной безопасности ИТКС ОГВ на основе имеющегося и возможного в перспективе уровня развития науки и промышленности страны;

в части организации обеспечения информационной безопасности:

определение целей и задач обеспечения информационной безопасности ИТКС ОГВ, выбор методов их решения и необходимых для этого научных подходов и моделей;

формирование, анализ и уточнение правового поля обеспечения информационной безопасности ИТКС ОГВ как основополагающего базиса любых законных видов деятельности, представляющего систему правовых актов и нормативных документов, определяющих относительно полное множество общественных отношений в информационной сфере и сфере информационной безопасности, а также в других, взаимосвязанных с ними сферах деятельности ОГВ;

разработка системы концептуальных решений, обеспечивающих организацию эффективной защиты ИТКС ОГВ в условиях воздействия любых потенциально возможных угроз ее информационной безопасности и формирование системы условий, обеспечивающих практическую реализацию заданных вариантов и стратегий эффективного обеспечения информационной безопасности ИТКС ОГВ;

формирование основных направлений развития государственной программы обеспечения информационной безопасности ИТКС ОГВ, системы научных исследований, подготовки специалистов на базе действующих и новых образовательных учреждений, а также ведомственных, государственных и межгосударственных органов в области информационной безопасности;

обоснование и последующее уточнение направлений, путей и способов сокращения экономических затрат на обеспечение информационной безопасности ИТКС ОГВ с учетом существующих и перспективных условий социально-экономического, политического, научного и других направлений развития страны.

Концепция обеспечения ИБ ИТКС ОГВ, содержащая приведенные выше положения, по своей сути представляет программу исследований проблем безопасности в информационной сфере ИТКС ОГВ.

Реализация рассмотренной программы может быть осуществлена на основе представленной ниже *концептуальной модели обеспечения информационной безопасности* ИТКС ОГВ, разработанной с учетом принципов системного подхода.

3. Концептуальная модель обеспечения ИБ ИТКС ОГВ. Данная модель предназначена для выработки основных исходных методологических посылок системного подхода, к числу которых относятся:

семантические, гносеологические, семиотические, физические, синтаксические, коммуникативные, прагматические, когнитивные и другие аспекты и свойства информационной безопасности для ИТКС ОГВ;

понятия информационной сферы ИТКС ОГВ и ее содержание, отражающее объекты информационной безопасности в ИТКС ОГВ и рассматриваемое с позиций системного подхода;

способы и уровни преобразования и обработки информации в ИТКС ОГВ;

формы представления информации, циркулирующей, хранимой или обрабатываемой в ИТКС ОГВ и являющейся объектом воздействия дестабилизирующих факторов, и, соответственно, объектом обеспечения информационной безопасности;

состав, структура и основные особенности информационной инфраструктуры ИТКС ОГВ, являющейся объектом обеспечения ИБ;

основные направления, пути и способы обеспечения информационной безопасности ИТКС ОГВ различных классов;

влияние объективных и субъективных дестабилизирующих факторов на количественные и качественные характеристики информационной безопасности ИТКС;

взаимосвязь элементов системы обеспечения информационной безопасности ИТКС ОГВ на этапах ее жизненного цикла, характеризующихся фазами, состояниями, внешней и внутренней средами;

группирование свойств системы обеспечения информационной безопасности ИТКС ОГВ по признаку подверженности различным дестабилизирующим факторам и времени и характеру проявления негативных последствий.

Концептуальная модель обеспечения ИБ ИТКС ОГВ может быть представлена в виде совокупности следующих взаимосвязанных элементов:

1) множества реальных защищаемых объектов (объектов ИБ) (O);

2) множества угроз со стороны противостоящего нарушителя (Y);

3) множества комплексов мер и средств защиты (S);

4) множества показателей эффективности функционирования системы обеспечения ИБ, отражающих ее основные свойства и особенности (P);

5) множества требований к ИБ ИТКС ОГВ (T);

6) множества ограничений, определяемых спецификой построения и условиями функционирования как самих ИТКС ОГВ, так и системы обеспечения их информационной безопасности (L).

Графически данная модель может быть представлена в виде, показанном на рис. 1.

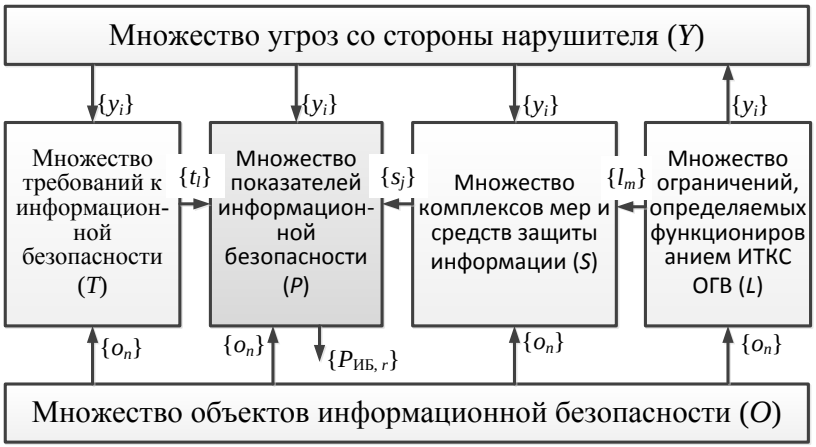

Рис. 1. Концептуальная модель обеспечения ИБ ИТКС ОГВ.

Тогда для решения задачи анализа ИБ, т.е. для определения значений показателей ИБ ИТКС ОГВ, можно использовать следующие обобщенные выражения:

$$\{P_{\text{ИБ},r}\} = F(\{o_n\}, \{y_i\}, \{t_l\}, \{s_j\}), \quad (1)$$

$$\{s_j\} = S(\{o_n\}, \{y_i\}, \{l_m\}), \quad (2)$$

$$\{t_l\} = T(\{o_n\}, \{y_i\}), \quad (3)$$

$$\{l_m\} = L(\{o_n\}, \{y_i\}), \quad (4)$$

где $\{P_{\text{ИБ},r}\}$, $r = 1,\ldots,R$ — множество показателей ИБ ИТКС; $O = \{o_n\}$,

$n = 1,\ldots,N$ — множество реальных объектов информационной безопасности в составе ИТКС; $Y = \{y_i\}$, $i = 1,\ldots,I$ — множество угроз со стороны противника и обслуживающего персонала, приводящих к нарушению ИБ ИТКС; $S = \{s_j\}$, $j = 1,\ldots,J$ — множество комплексов организационных мероприятий и действий должностных лиц, программных и инженерно-технических средств (подсистем) системы обеспечения ИБ, обеспечивающих подавление определенного класса угроз относительно какого-либо объекта ИБ; $T = \{t_l\}$, $l = 1,\ldots,L$ — множество требований должностных лиц и пользователей к системе обеспечения ИБ; $L = \{l_m\}$, $m = 1,\ldots,M$ — множество внешних и внутренних ограничений, определяемых условиями и особенностями функционирования ИТКС ОГВ и системы обеспечения их информационной безопасности.

Необходимо отметить, что анализ информационной безопасности ИТКС ОГВ в соответствии с выражениями (1–4) должен осуществляться с учетом следующих ограничений:

каждый n–й объект информационной безопасности ИТКС ОГВ может быть подвержен воздействию угроз нескольких различных классов;

связь между угрозами и объектами не является только связью типа «каждой угрозе — свой объект»; одна и та же угроза может оказывать воздействия на различное число объектов информационной безопасности из множества $\{o_n\}$;

связь «угроза — объект», т.е. двойка $\langle y_i, o_n \rangle$, существует только тогда, когда существуют реальные пути и способы реализации этих угроз, и имеется нарушитель, способный их осуществить;

наличие уязвимостей какого-либо объекта информационной безопасности определяет возможность осуществления одного или нескольких способов реализации потенциальных угроз.

Рассмотренную концептуальную модель обеспечения ИБ ИТКС ОГВ можно преобразовать в *концептуальную модель системы обеспечения ИБ*.

4. Концептуальная модель системы обеспечения ИБ ИТКС ОГВ. Концептуальную модель системы обеспечения ИБ можно представить в виде графа «объекты $\{o_n\}$ — угрозы $\{y_i\}$», на котором учитываются способы и условия реализации угроз, определяемые ограничениями $\{l_m\}$ (рис. 2).

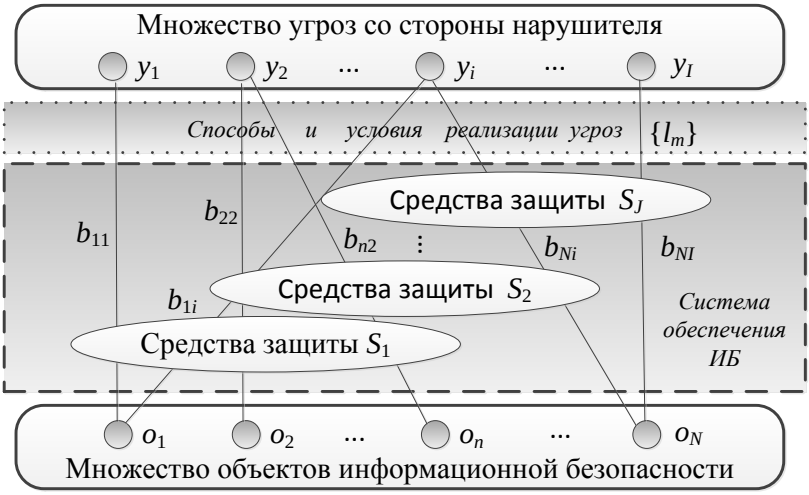

Рис. 2. Концептуальная модель системы обеспечения ИБ ИТКС ОГВ.

В общем виде задача системы обеспечения информационной безопасности состоит в том, чтобы осуществить перекрытие каждого ребра данного графа путем создания соответствующего комплекса мер и средств защиты или их некоторой совокупности на пути реализации угроз ИБ как по этому ребру, так и в целом по всему графу. При этом необходимо осуществлять оценивание степени противодействия каждой из возможных угроз каждым комплексом защиты в отдельности, а также уровня безопасности ИТКС, обеспечиваемого всей совокупностью средств обеспечения информационной безопасности в целом.

В общем случае каждое из ребер графа, представленного на рис. 2, может перекрываться не одним, а несколькими организационно-техническими и программными комплексами защиты. Это предопределяет необходимость учета уровня защищенности, создаваемого каждым из этих комплексов относительно каждой из возможных угроз, с учетом реализации множеств $\{t_l\}$ и $\{l_m\}$. При этом уровень защищенности ИТКС ОГВ, обеспечиваемый комплексами защиты на v–м ребре от y_i–ой угрозы, может быть определен как

$$B_v(y_i, s_q) = f(b_{v1}, b_{v2}, \ldots, b_{vq}),\ v = \overline{1, K}, \qquad (5)$$

где K — число ребер; b_{vq} — уровень защищенности на v–м ребре, создаваемый q–м комплексом защиты с учетом набора требований

$\{t_l\}$ и ограничений $\{l_m\}$, способствующих предотвращению нарушений информационной безопасности ИТКС ОГВ.

Критериальное значение уровня защищенности на каждом ребре $B_{v,\text{доп}}$ определяется требованиями пользователей или нормативных документов к информационной безопасности ИТКС в целом и к его защищенности от соответствующего вида угроз. Следовательно, с учетом выражения (5) критерием достаточности защиты от данной угрозы является условие $B_v(y_i, s_q) \geq B_{v,\text{доп}}$.

Заключение. Концепция обеспечения ИБ ИТКС ОГВ, разработанная на основании изложенных выше предложений, позволяет анализировать существующие направления в сфере обеспечения ИБ ИТКС ОГВ, определять пути преодоления существующих противоречий в теоретических и практических аспектах решения задач комплексного обеспечения ИБ, выделить перспективные проблемы и направления развития информационной сферы ИТКС ОГВ и ее составляющих, в первую очередь в области ИБ.

Рассмотренные концептуальные модели обеспечения ИБ и системы обеспечения ИБ ИТКС ОГВ отражают в наиболее общем виде основы многоуровневой комплексной защиты, обеспечивающей заданный уровень ИБ ИТКС ОГВ.

В то же время данная концепция предполагает необходимость проведения дальнейших исследований в направлении разработки модели объекта ИБ, моделей угроз и нарушителя и модели построения и функционирования системы обеспечения ИБ. Кроме того, она требует разработки методов, способов и средств обеспечения ИБ и формирования системы показателей, характеризующих информационную безопасность с учетом вероятностного характера функционирования ИТКС ОГВ и системы обеспечения ИБ, а также воздействующих на ИТКС угроз и дестабилизирующих факторов.

Литература

1. Значение слова «Концепция» в Большой Советской Энциклопедии // http://bse.sci-lib.com/article064302.html.
2. Концепция защиты персональных данных в информационных системах персональных данных оператора связи // http://admin.smolensk.ru/www.fstec.ru/pers/koncepcia.doc.
3. Концепция защиты информации в Смоленской области. Утверждена постановлением Администрации Смоленской области от 20.11.2004 № 366. http://admin.smolensk.ru/www.fstec.ru/smol/366_04.doc.
4. *Корсак А.Б.* О Концепции информационной безопасности Москвы // Информационное общество, 2005, Вып. 2. С. 14–17.

5. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. М.: ВИ. ГТК. – 1997. 12с.
6. Доктрина информационной безопасности. Утверждена Президентом Российской Федерации от 9 сентября 2000г. // Рос. Газ. 2000. 28 сентября.
7. Курс «Безопасность Информационных Технологий». Глава 17. Концепция информационной безопасности организации. http://asher.ru/security/book/its/17.
8. Разработка концепции информационной безопасности. http://www.insave.ru/index.php?option=com_content&view=article&id=36&Itemid=118.
9. *Саенко И.Б., Агеев С.А., Шерстюк Ю.М., Полубелова О.В.* Концептуальные основы автоматизации управления защищенными мультисервисными сетями // Проблемы информационной безопасности. Компьютерные системы. №3, 2011. С. 30-39.
10. *Герасименко В.А., Малюк А.А.* Основы защиты информации: Учебник. – М: МОПО, МИФИ, 1997. 537 с.
11. *Фисун А.П.* Теоретические основы информационной безопасности информационно-телекоммуникационных систем. Монография. М.: 2000. 276 с.
12. *Котенко И.В., Саенко И.Б., Полубелова О.В., Чечулин А.А.* Применение технологии управления информацией и событиями безопасности для защиты информации в критически важных инфраструктурах // Труды СПИИРАН. Вып.1 (20). СПб.: Наука, 2012.
13. *Котенко И.В., Саенко И.Б., Полубелова О.В., Чечулин А.А.* Технологии управления информацией и событиями безопасности для защиты компьютерных сетей // Проблемы информационной безопасности. Компьютерные системы. № 2, 2012.

Демидов Александр Алексеевич — кандидат технических наук; председатель комитета по информатизации и связи Правительства Санкт-Петербурга. Область научных интересов: информационные и телекоммуникационные сети, информационная безопасность. Число научных публикаций — 45. demidov@kvmsu.gov.spb.ru; Правительство Санкт-Петербурга, Комитет по информатизации и связи, Смольный, Санкт-Петербург, 191060, РФ, р.т. +7(812)576–7123, факс +7(812)576–7345. Научный консультант — В.И. Курносов.

Demidov Alexandr Alexeevich — PhD; the Chairman of the Committee on information and communications of the Government of St Petersburg. Research interests: information and telecommunication systems, information security. The number of publications — 45. demidov@kvmsu.gov.spb.ru; Government of St Petersburg, Committee on information and communications, Smolny, St Petersburg, 191060, Russia; office phone +7(812)576–7123, fax +7(812)576–7345. Scientific consultant — V.I. Kurnosov.

Никифоров Олег Гелиевич — кандидат технических наук, доцент; ведущий научный сотрудник ФГУП «НИИ «Рубин». Область научных интересов: информационные и телекоммуникационные сети, информационная безопасность. Число научных публикаций — 96. inforubin@rubin-spb.ru; ФГУП «НИИ «Рубин», Кантемировская ул., дом 5, Санкт-Петербург, 197342, РФ, р.т. +7(812)295–0129, факс +7(812)596–3581. Научный консультант — Ю.И. Стародубцев.

Nikiforov Oleg Gelievich — PhD, associate professor; leading research scientist of the FSUE “SII “Rubin”. Research interests: information and telecommunication systems, information security. The number of publications — 96. inforubin@rubin-spb.ru; FSUE “SII “Rubin”, Kantemirovskaya str., 5, St. Petersburg, Russia, office phone +7(812)295–0129, fax +7(812)596–3581. Scientific consultant — Y.I. Starodubtsev.

Саенко Игорь Борисович — д-р техн. наук, проф.; ведущий научный сотрудник лаборатории проблем компьютерной СПИИРАН. Область научных интересов: автоматизированные информационные системы, информационная безопасность. Число научных публикаций — 250. ibsaen@mail.ru; СПИИРАН, 14-я линия В.О., 39, Санкт-Петербург, 199178, РФ; р.т. +7(812)328–2642, факс +7(812)328–4450.

Saenko Igor Borisovich — Ph.D., Doctor of Technical Sciences, professor; leading research scientist of laboratory of computer network security of SPIIRAS. Research interests: automated information systems, information security. The number of publications — 250. ibsaen@mail.ru; SPIIRAS, 14-th line, 39, St. Petersburg, 199178, Russia; office phone +7(812)328–2642, fax +7(812)328–4450.

Поддержка исследований. В публикации представлены результаты исследований, поддержанные Министерством образования и науки Российской Федерации (государственный контракт 11.519.11.4008), грантом РФФИ (проект 11–07–00435–а), программой фундаментальных исследований ОНИТ РАН (проект 2.2) и проектами Седьмой рамочной программы Европейского Союза SecFutur и MASSIF.

Рекомендовано лабораторией проблем компьютерной безопасности, заведующий лабораторией Котенко И.В., д-р техн. наук, проф.
Статья поступила в редакцию 08.05.2012.

РЕФЕРАТ

Демидов А.А., Никифоров О.Г., Саенко И.Б. **Разработка концепции обеспечения информационной безопасности информационно-телекоммуникационных систем органов государственной власти.**

В статье рассматриваются особенности разработки концепции обеспечения информационной безопасности информационно-телекоммуникационных систем органов государственной власти. Отличительные положения концепции разделяются на группы, характеризующие объект защиты, угрозы информационной безопасности, средства обеспечения информационной безопасности и организацию обеспечения информационной безопасности. Концепция обеспечения информационной безопасности, содержащая рассмотренные отличительные положения, может восприниматься как программа исследований, проводимых в области проблем безопасности в информационной сфере информационно-телекоммуникационных сетей органов государственной власти.

В качестве основных отличительных положений выделены концептуальная модель обеспечения информационной безопасности и концептуальная модель системы обеспечения информационной безопасности.

Концептуальная модель обеспечения информационной безопасности представлена в виде совокупности следующих взаимосвязанных элементов: множества реальных защищаемых объектов; множества угроз со стороны нарушителя; множества комплексов мер и средств защиты; множества показателей эффективности и требований системы обеспечения информационной безопасности; множества ограничений, определяемых спецификой построения и условиями функционирования информационно-телекоммуникационной системы и системы обеспечения информационной безопасности. При этом определены ограничения, налагаемые на связи между объектами защиты и угрозами безопасности. Модель носит стохастический характер и представлена в функциональном виде, который позволяет определить зависимость показателей эффективности от полной совокупности условий и факторов, оказывающих влияние на их значения.

Концептуальная модель системы обеспечения информационной безопасности представлена в виде ориентированного графа, увязывающего объекты защиты и угрозы безопасности. Ребра данного графа отображают уровни защищенности, создаваемые комплексами мер и средств защиты относительно возможных угроз, которые учитывают возможности данных комплексов мер и средств защиты и требования по информационной безопасности. При этом отмечается, что задача системы обеспечения информационной безопасности состоит в том, чтобы осуществить перекрытие каждого ребра данного графа соответствующими комплексами мер и средств защиты информации.

Приведен формальный вид критерия достаточности защиты от данной угрозы с учетом того, что критериальное значение определяется требованиями пользователей или нормативных документов.

SUMMARY

Demidov A.A., Nikiforov O.G, Saenko I.B. **Development of the concept of information security for information and telecommunications systems of the State authorities.**

The paper deals with design features of the concept of information security for information and telecommunication systems of State authorities. The distinctive provisions of the concept are divided into groups that characterize the object of protection, threats to information security, means of ensuring information security, and organization of ensuring information security. The concept of information security, which contains these distinctive provisions, might be perceived as a program of research conducted in the area of security problems in the information sphere of information and telecommunication systems of State authorities.

As main distinctive provisions of the concept, the conceptual model of ensuring information security and the conceptual model of the system of ensuring information security are selected.

Conceptual model of ensuring information security is represented as the set of the following interrelated elements: the set of real securable objects, the set of threats made by the malefactor, the set of security packages and tools; the set of performance indicators and requirements of information security, the set of restrictions as determined by the specifics of developing and operation of information and telecommunication system and the system of ensuring information security. In this case, the restrictions imposed on the relationships between objects of protection and security threats are identified. The model has a stochastic character and is presented in functional form, which allows determining the dependence of the performance from the full set of conditions and factors influencing their values.

A conceptual model of the system of ensuring information security is presented by oriented graph. Each arc of the graph shows the level of protection caused by packages and means for possible threats that take into account the possibility of packages and means of protection and the requirements for information security. It is noted that the challenge of ensuring information security consists in the implementation of overlay of each arc of the graph of the relevant systems and means of information security.

The formal form of the criterion of adequacy of protection against the threat, given that the criterion value is determined by user requirements or regulations are listed.