DOI: 10.5862/JCSTCS.234.2
УДК 681.141.2

А.В. Богданов, И.Г. Малыгин

ТЕХНОЛОГИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КРУПНЫХ МУЗЕЙНЫХ И ВЫСТАВОЧНЫХ КОМПЛЕКСОВ

A.V. Bogdanov, I.G. Malygin

TECHNOLOGY INFORMATION SECURITY OF LARGE MUSEUM AND EXHIBITION COMPLEXES

Выявлена роль и значение информационной безопасности в духовной жизни общества. Проанализированы особенности обеспечения безопасности информационных систем крупных музейных комплексов. Обоснованы состав и структура интегрированной информационной системы обеспечения безопасности музея. Рассмотрены модели функционирования и управления системой защиты информации. Предложен метод моделирования и оценки свойств устойчивости функционирования информационной системы обеспечения безопасности крупных музейных и выставочных комплексов.

МУЗЕЙНЫЙ КОМПЛЕКС; ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ; СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ; МОДЕЛЬ; УСТОЙЧИВОСТЬ.

The paper substantiates the role and importance of information security in the spiritual life of the society, analyses the specifics of the security of large museum complexes, as information systems. We have described the composition and the structure of an integrated information system for ensuring the safety of a museum. Models for operating and managing an information security system have been considered.

MUSEUM COMPLEX; INFORMATION SECURITY; INFORMATION SECURITY SYSTEM; MODEL; STABILITY.

Основными задачами, решаемыми при создании системы безопасности крупных музейных и выставочных комплексов (КМиВК), в общем виде являются [1]:

1) определение целей охраны музейного учреждения и сохранности музейных предметов;

2) постановка задач составным частям системы безопасности;

3) определение возможности построения организационно-технического комплекса безопасности, охватывающего все составные части системы обеспечения безопасности;

4) использование современных технических средств и новых достижений в области безопасности;

5) определение вида охраны;

6) определение уровня и степени надежности с обоснованием экономической целесообразности.

Отличительная особенность построения системы безопасности музейного учреждения, по сравнению с любыми другими объектами, – обеспечение защищенности музейного учреждения по двум равнозначным и важным направлениям:

обеспечение охраны вверенного в управление государственного имущества (территория, здания, сооружения, помещения, отдельные предметы и коллекции и др. материальные ценности и имущество);

обеспечение сохранения объектов культурного наследия и поддержание сохранности музейных предметов.

Такая защищенность должна обеспечиваться в режиме публичного представления музейных предметов и при непрерывной эксплуатации помещений, зданий, сооружений и памятников музейных учреждений, а также природно-ландшафтных территорий.

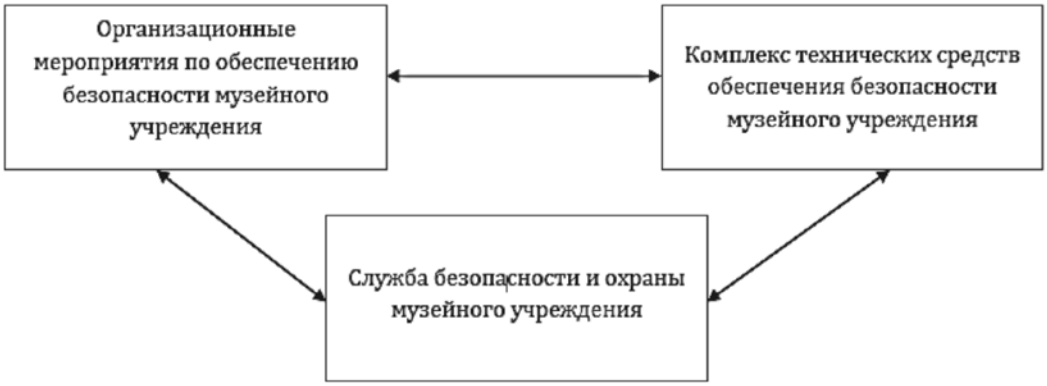


Рис. 1. Комплексный подход к организации безопасности музейного учреждения

Для обеспечения максимальной защищенности на практике применяется комплексный подход к организации системы безопасности музейного учреждения, включающий в себя совокупность мер, направленных на всестороннее пресечение возможных угроз (рис. 1).

Обобщенная структурная схема современной системы безопасности представлена на рис. 2. Ее основой является система сбора и обработки информации.

Кроме того, в ее состав входят средства контроля состояния объекта (в частности, средства наблюдения, инженерно-технические средства защиты, защиты информации, контроля технологического оборудования и т. д.); окружающей среды; управления; контроля и управления доступом к объекту информатизации, к информации и к системе безопасности; передачи информации; оповещения; отображения информации; регистрации данных; противодействия и ликвидации угроз; энергопитания, объединенные каналами связи. Перечень средств контроля состояния объекта будет определяться перечнем угроз. Основными функциональными элементами системы безопасности, определяющими ее основные параметры и эффективность, являются:

средства обнаружения;

средства сбора и обработки информации;

средства противодействия угрозам;

соответствующие каналы связи.

Таким образом, современный этап развития проблемы безопасности сложных организационно-технических объектов ха-

Рис. 2. Обобщенная структурная схема системы безопасности

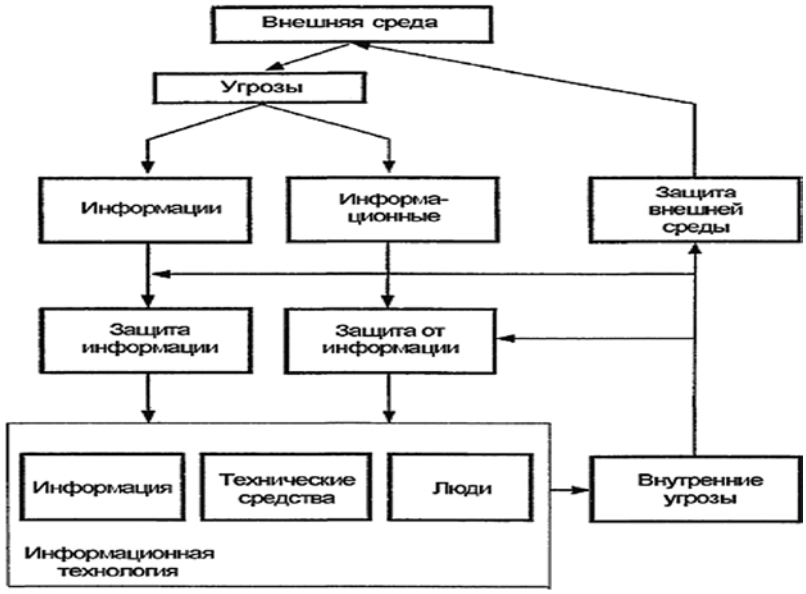


Рис. 3. Объекты защиты информации и угрозы информационной безопасности

рактеризуется переходом от традиционного ее представления как проблемы физической защиты к более широкому пониманию – проблеме безопасности информационной сферы. При этом выделяют три основных направления (объекта) защиты от информационного воздействия: технические средства; информация; человек (рис. 3).

Методика обеспечения безопасности

Современное состояние проблемы безопасности важных объектов, к которым вполне обоснованно относятся КМиВК, определяется множеством факторов. Одним из важных факторов, доминирующих в последнее время, является изменение характера угроз, вызванное повсеместной информатизацией во всех областях жизнедеятельности государства [2]. Угрозами в области духовной жизни и информационной деятельности могут являться: дезорганизация и разрушение системы накопления и сохранения культурных ценностей, включая архивы. В КМиВК движение информации в общем случае происходит в соответствии со схемой, представленной на рис. 4.

Очевидный путь простого увеличения технической оснащенности систем безопасности, без учета информационных особенностей и нюансов проблемы, как правило, не приводит к желаемым результатам.

Предлагаемые сегодня концепции безопасности, являясь, несомненно, полезными и выверенными с точки зрения охраны, чаще всего не учитывают музейную специфику, предполагающую рассмотрение проблемы, как проблемы информационно-технической, обеспечивающей не только интересы и структуру безопасности как таковую, но и (взаимосвязь ее с социологиче-

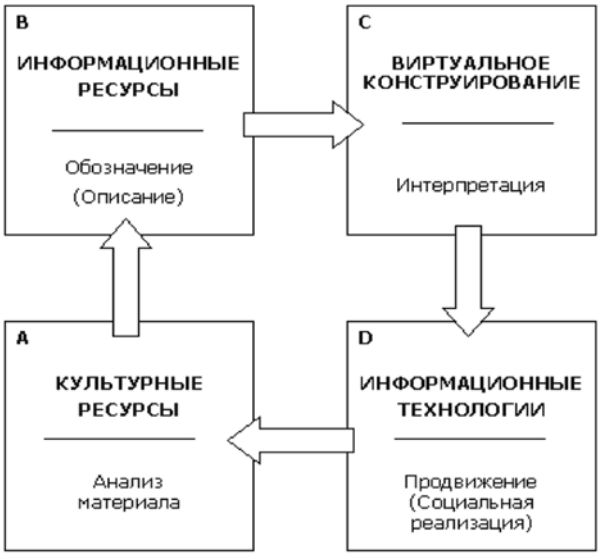


Рис. 4. Общая схема информационного процесса КМиВК

ской организацией колллектива) интересы как посетителей, так и работников музея.

Создание интегрированной системы безопасности (ИСБ), обеспечивающей качественное повышение уровня защищенности объектов культуры с учетом всех аспектов безопасности, предусматривает все возможные организационные, социальные и технические мероприятия, позволяющие исключить или уменьшить риск утраты предметов коллекций, дезорганизации работы музея, искажения его информационного облика или, что еще лучше, ликвидировать предпосылки к таким возможностям.

Реализация концепции ИСБ предполагает постоянный мониторинг организационно-технических мероприятий, обеспечивающих:

- всестороннюю защиту всего архитектурного комплекса зданий, представляющих историческую ценность;
- создание условий для сохранности экспонатов, включающих в себя: защиту от краж, вандализма, возможности подмены произведений искусства на различных этапах жизненного цикла, поддержание необходимых климатических параметров (температуры, влажности), обеспечение биологической и химической защиты, реализацию плана эвакуационных мероприятий и действий в чрезвычайных ситуациях;
- защиту информационных ресурсов музея.

Системообразующим элементом ИСБ целесообразно рассматривать комплексную информационную систему, формирующую информационное пространство музея, являющуюся интегрирующим фактором всей ИСБ. Правильно организованное защищенное информационное пространство музея позволит обеспечить достаточную безопасность и при этом создать условия для нормального восприятия архитектурных и художественных ценностей, которые широко представлены в КМиВК.

Мировой опыт создания систем защиты для КМиВК позволяет выделить три основных элемента, входящих в состав любого объекта и требующих обеспечения их безопасности:

1) люди – персонал и посетители, сотрудники охраны;

2) материальные ценности, имущество, оборудование;

3) информация.

Выделенные элементы полностью совпадают с выявленными выше объектами обеспечения информационной безопасности, что подтверждает доминирование этих аспектов в комплексном решении проблемы безопасности.

Каждый из выделенных элементов имеет свои особенности, которые необходимо учесть при определении возможных угроз, каковыми являются:

чрезвычайные обстоятельства, в том числе пожары;

несанкционированное проникновение;

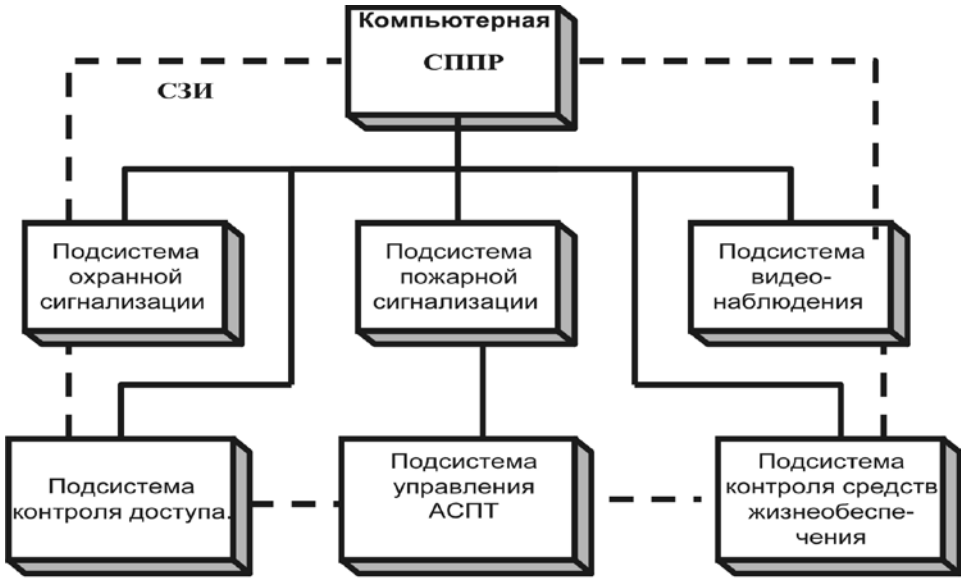
несанкционированный доступ к информации.

Таким образом, под угрозой безопасности крупных музейных комплексов следует понимать событие, действие, процесс или явление, которое посредством воздействия на людей, материальные ценности и информацию может привести к нанесению ущерба объекту, нарушению или прекращению функционирования объекта.

Обеспечение безопасности объекта не может быть одноразовым актом. Это непрерывный процесс, заключающийся в обосновании и реализации наиболее рациональных методов, способов и путей создания, совершенствования и развития интегрированной системы безопасности, непрерывном контроле, выявлении ее слабых мест.

Реализация такого подхода обеспечит:

- получение объективной оперативной информации о состоянии объекта в форме, удобной для оператора системы;
- предоставление оператору возможности принять на основе этой информации правильное решение о реагировании на тревожные и аварийные ситуации и задействовать соответствующие службы реагирования;
- фиксирование в протоколе системы всех событий, представляющих интерес для службы безопасности (подразделения пожарной или вневедомственной охраны), с



(АСПТ – автоматическая система пожаротушения)

Рис. 5. Обобщенная структура ИСБ КМиВК

целью последующего их анализа;

• повышение надежности и самодиагностики системы за счет дублирования разными подсистемами основных функций оповещения, сохранения информации, ее оперативной обработки и последующего анализа;

• повышение устойчивости системы к саботажным действиям путем совмещения на особо важных участках объекта технических средств различных подсистем, которые не могут быть выведенными из строя одновременно;

• простоту эксплуатации и автоматизацию рутинных действий сотрудников охраны, что позволит им сосредоточить внимание на выполнении своих основных функций по предотвращению последствий нештатных ситуаций.

Анализ структуры системы безопасности

Обобщенная структура ИСБ на основе компьютерной системы поддержки принятия решения (СППР) представлена на рис. 5.

Выделение в качестве системообразующего элемента СППР позволяет определить ИСБ как информационную систему обеспечения безопасности (ИСОБ), что обусловливает актуальность первоочередного решения задач защиты информации.

Система защиты информации (СЗИ) в самом общем виде может быть определена как организованная совокупность всех средств, методов и мероприятий, выделяемых (предусматриваемых) на объекте информатизации (ОИ) КМиВК для решения в ней выбранных задач по защите. Введением понятия СЗИ определяется тот факт, что все ресурсы, выделяемые для защиты информации, должны объединяться в единую, целостную систему, которая является функционально самостоятельной подсистемой любого ОИ. К СЗИ предъявляется целый ряд более конкретных, целевых требований (см. рис. 6).

Способность СЗИ эффективно противодействовать деструктивным воздействиям предполагает своевременное разрешение ряда задач: выявление основных угроз для СЗИ; разработку концепции безопасности СЗИ; определение плана конкретных мероприятий по реализации этой концепции; проектирование СЗИ; создание механизма согласования действий всех подразделений и должностных лиц, занимающихся обеспечением безопасности; постоянный мониторинг состояния СЗИ.

Исходя из предположения, что воздействие на защищаемую информацию (нару-

Рис. 6. Требования к системе защиты информации

шение целостности, несанкционированное получение и копирование, хищение, нарушение защищенности) может происходить как на самом объекте, так и при передаче ее по каналам связи, разработана общая модель СЗИ, представленная на рис. 7. Входные сигналы, поступающие в систему защиты информации и преобразующиеся в ней, можно разделить на полезные, несущие конфиденциальные сведения – $x_n(t)$, и сигналы, воздействующие на систему защиты и направленные на изменение структуры конфиденциальных данных или снижение эффективности системы защиты – $x_m(t)$.

При этом под общим названием «сигнал» понимаются сигналы, образы, символы, технические решения и процессы, содержащие конфиденциальные сведения. Сигналы $x_m(t)$ определяются множеством угроз информации (отказы, сбои, ошибки функционирования, стихийные бедствия и др.). Функциональными назначениями системы

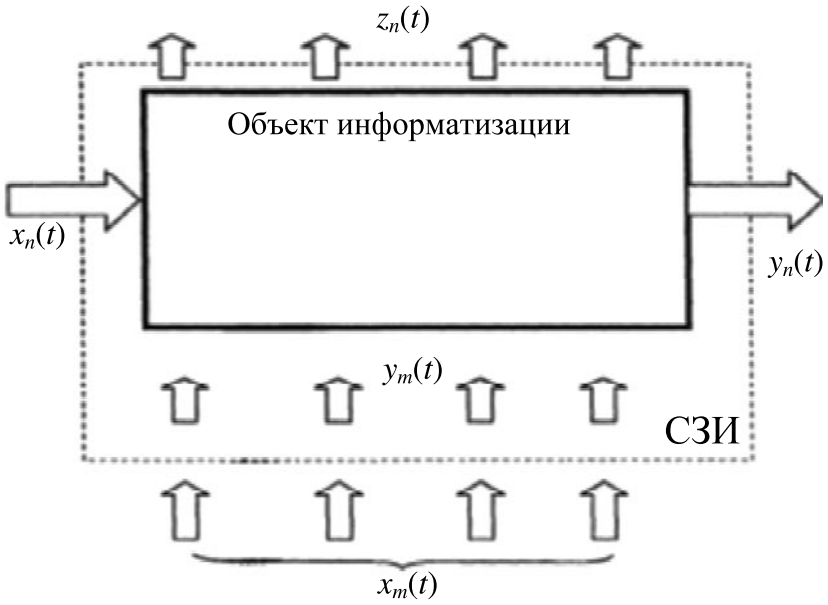


Рис. 7. Общая модель системы защиты информации

Рис. 8. Обобщенная модель процесса защиты информации

защиты информации являются перекрытие каналов несанкционированного доступа и утечки информации. Математически это можно представить преобразованием сигнала $x_n(t)$ в форму либо не доступную для раскрытия содержания конфиденциальных сведений – $y_n(t)$, либо не позволяющую распознать информационный сигнал – $z_n(t)$, а сигнала $x_m(i)$ – в форму, не оказывающую разрушающего воздействия на полезный сигнал – $y_m(t)$, то есть выполнить функцию нейтрализации вредных воздействий: $y_n(t) = f_1(x_n(t))$, $z_n(t) = f_2(x_n(t))$, $y_m(t) = f_3(x_m(t))$ [6].

Системное представление проблемы обеспечения безопасности возможно на основе обобщенной модели процесса защиты информации (рис. 8).

Возможность реализации процессов защиты информации, характеризующихся соответствующими показателями, во многом определяется эффективностью управления процессами функционирования СЗИ. Общая модель управления защитой информации представлена на рис. 9. Как следует из представленной модели, исходной основой для управления защитой служат планы обработки информации, а на основе анализа параметров подлежащей обработке информации обосновываются требования к защите информации, которые в самом общем виде могут быть выражены вероятностью требуемой защиты $P_{тр}$. В соответствии с требуемым значением показателя защищенности должны быть определены оптимальные наборы средств защиты (технических {Т}, программных {П}, организационных {О}, законодательных {З}, морально-этических {М}), обеспечивающих требуемый уровень защищенности. Обоснование таких наборов средств защиты является общей задачей механизмов управления средствами защиты. Выбранные наборы средств защиты способны обеспечить вполне определенный ожидаемый уровень защищенности информации ($P_{ож}$), который может отличаться от требуемого.

Если это отличие будет превышать допустимые значения ($P_{доп}$), то, очевидно, надо скорректировать выбранные наборы средств защиты.

Обсуждение предлагаемой методики

Перечисленные средства обеспечения безопасности можно рассматривать как последовательность барьеров или рубежей защиты информации, комплексное использование которых в рамках ИСБ позволит обеспечить требуемый уровень безопасности КМиВК (рис. 10).

Критерием оптимизации СЗИ может быть минимизация затрат на реализацию СЗИ в КМиВК при условии обеспечения

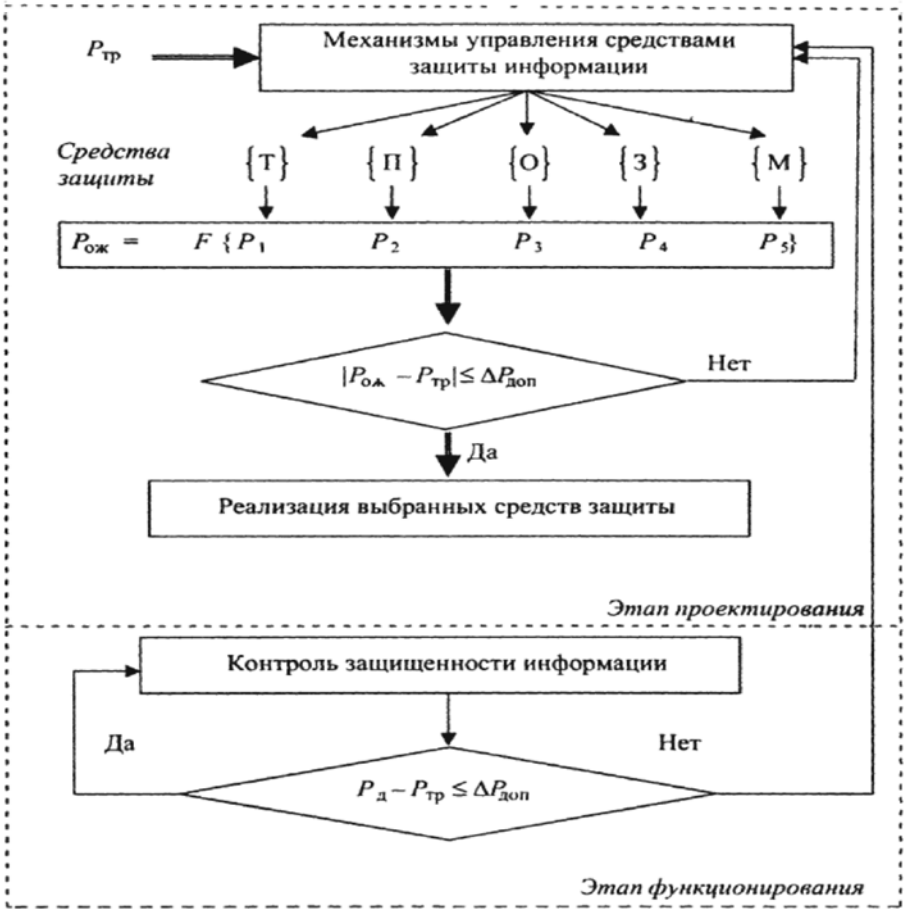


Рис. 9. Общая модель управления защитой информации

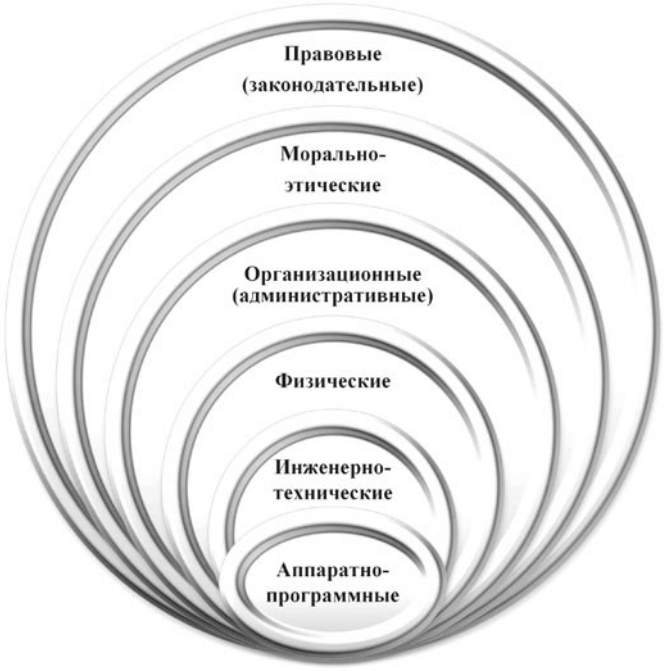


Рис. 10. Система рубежей защиты

заданных уровней защищенности информации от несанкционированных действий со стороны всех вероятных стратегий нападения [4], то есть

$$C = \sum_j C_j = \sum_j \sum_i d_{ij} S_i \to \min$$

$$\log P = U \le U_0 = \log P_0,$$

где S_i – затраты на реализацию i-й меры;

$$d_{ij} = \begin{cases} 1, \text{ если } i\text{-я мера защиты входит } в\ j\text{-й} \\ \text{набор мер;} \\ 0, \text{ если } i\text{-я мера защиты не входит } в\ j\text{-й} \\ \text{набор мер;} \end{cases}$$

$U = \log P$ – уровень защищенности информации в АСОД.

$$P = \sum_{k=1}^{S} \sum_{i=1}^{m_k} \left(1 - q_i \sum_{j=1}^{n_k} Pij \right),$$

где q_i – вероятность применения стратегии; S – число возможных подсистем стратегий нападения; m_k – число возможных стратегий нападения в составе k-й подсистемы нападения; $N_к$ – число мер защиты, направленных на противодействие k-й подсистеме стратегий нападения; P_{ij} – вероятность преодоления j-й меры противодействия i-й стратегии нападения.

В качестве системы защиты принимается такой набор мер защиты R_t, для которого $C_t = \min\{C_j\}$.

В этом случае ИСОБ можно рассматривать как информационно-управляющую систему, обеспечивающую оперативное взаимодействие и реагирование сил и средств обеспечения безопасности КМиВК, от устойчивости (надежности, живучести) функционирования которой во многом зависит реализация функций, возложенных на КМиВК.

Создание и эксплуатация сложных ИСОБ предполагает широкое применение аналитических методов, основным содержанием которых является установление связей (зависимостей) между показателями устойчивости и соответствующими показателями устойчивости систем. Эти методы обладают следующими положительными свойствами:

абсолютной точностью (в рамках принятых допущений);

представлением результата в явной аналитической форме;

возможностью использования моделей при решении оптимизационных задач.

К числу основных недостатков этих методов обычно относят:

большую размерность моделей;

упрощение моделей, не учитывающее всех особенностей исследуемых систем.

Следует заметить, что другим эффективным средством совершенствования методов моделирования является разработка комбинированных аналитико-статистических методов. Используемые в качестве базовых методов исследования устойчивости методы надежности можно классифицировать следующим образом:

1) методы, основанные на перечислении путей и сечений. Они различаются способами формирования путей и сечений, приемами ортогонализации, организацией вычислений и представлением промежуточных результатов. В наиболее законченном виде идея перечислений путей (сечений) воплощена в логико-вероятностном методе (ЛВМ);

2) методы, основанные на перечислении состояний графа. Они различаются способами формирования состояний, проверки наличия связанности в конкретном состоянии и вычислении результирующих, что позволяет как производить расчет соответствующих количественных характеристик устойчивости, так и использовать эти зависимости непосредственно в качестве целевых функций при решении задач оптимизации.

В случае громоздкости и трудоемкости проведения точных расчетов показателей надежности используются приближенные методы, которые можно, в общем случае, разделить на методы граничных оценок и методы частичного перебора состояний.

Среди известных в теории надежности средств математического моделирования, базирующихся на структурных схемах, в последнее время интенсивное развитие получил ЛВМ. Привлекательность этого метода заключается в исключительной четкости, однозначности и больших возможностях

анализа влияния отдельных элементов на устойчивость функционирования системы в целом. ЛВМ основывается на сопоставлении в моделях надежности элементам рассматриваемой системы логических (двоичных, булевых, переключательных) переменных: $\tilde{i} = \{i, \bar{i}\}$.

Здесь арифметическое значение переменной $i = \overline{1, N}$ соответствует порядковому номеру элемента в модели надежности системы.

Прямым логическим значением переменной $\tilde{i} = i$ будем обозначать событие, состоящее в том, что на рассматриваемом интервале времени функционирования системы соответствующий элемент проработал безотказно, или в данный момент времени этот элемент находится в состоянии собственной (независящей от состояния других элементов) работоспособности. Инверсной логической переменной $\tilde{i} = \bar{i}$ обозначается противоположное событие.

При рассмотрении возможности использования указанной логической модели функционального элемента в моделях живучести и отказоустойчивости необходимо отметить, что отличие от надежности здесь состоит, в основном, не в форме проявления изменений состояния элемента (и там, и там – нарушение или не нарушение способности элемента функционировать), а лишь в причинах возникновения этих событий и степени их детерминированности. Поэтому логическая форма представления функциональных элементов является вполне приемлемой в различных моделях устойчивости. Кроме того, простые случайные события, представляющие причины возникновения, распределения и характер воздействия поражающих факторов на функциональные элементы в моделях живучести, и причинно-следственные связи в моделях отказоустойчивости могут быть также сопоставлены двоичным переменным. Это позволяет говорить о принципиальной возможности использования арсенала логико-вероятностных средств теории надежности при разработке моделей отдельных и комплексных свойств устойчивости ИСОБ КМиВК.

Классический ЛВМ применяется для анализа систем, функционирование которых с достаточной, в рамках рассматриваемой задачи, точностью характеризуется статическими моделями надежности. Под статическими моделями будем понимать модели, в которых значения системных характеристик не зависят от реальной последовательности (порядка, очередности) случайных изменений состояний элементов и определяются только их составом, на рассматриваемом интервале времени, или в заданный момент времени функционирования системы. Кроме того, существующие приемы построения логико-вероятностных моделей надежности систем в большинстве случаев малопригодны для прямой реализации на ЭВМ в силу своей слабой формализации и исходной ориентации на ручное применение. Поэтому все более широкое распространение начинают получать разработки новых методов системного анализа, непосредственно ориентированные на машинную реализацию процессов моделирования. К этому классу относится общий логико-вероятностный метод (ОЛВМ), используемый в качестве методологической базы автоматизированного моделирования. Он является развитием классического монотонного ЛВМ.

Необходимость обеспечения многовариантного и точного анализа устойчивости ИСОБ КМиВК в процессе их разработки, а также оперативного управления устойчивостью в процессе эксплуатации предполагает реализацию метода в виде автоматизированной системы моделирования и расчета показателей устойчивости, осуществляющей функции справочника, расчета, прогноза и анализа.

Возможности метода моделирования сложных систем могут быть значительно расширены за счет внедрения соответствующих процедур учета групп несовместных событий, заданной последовательности отказов элементов и расчета дополнительных характеристик надежности как не восстанавливаемых, так и восстанавливаемых систем.

СПИСОК ЛИТЕРАТУРЫ

1. **Богданов А.В., Малыгин И.Г., Синещук Ю.И.** Неформальная модель нарушителя безопасности объектов культуры // Вестник Санкт-Петербургского университета ГПС МЧС России. 2013. № 3. С. 109–113. [электронный ресурс]/URL: vestnik.igps.ru

2. **Корчагин С.И., Павлов В.Г., Бутов А.Н., Ткаченко Д.Г.** Подходы к созданию систем обеспечения безопасности особо важных объектов // Системы безопасности. 2010. № 4.

3. **Семкин С.Н., Беляков Э.В., Гребенев С.В., Козачок В.И.** Основы организационного обеспечения информационной безопасности объектов информатизации: Учеб. пособие. М.: Гелиос АРВ, 2005.

4. **Климов С.М.** Методы и модели противодействия компьютерным атакам. Люберцы: КАТАЛИТ, 2008.

REFERENCES

1. **Bogdanov A.V., Malygin I.G., Sineshchuk Yu.I.** Neformalnaya model narushitelya bezopasnosti obyektov kultury [Informal model of the violator of security culture object], *Vestnik Sankt-Peterburgskogo universiteta GPS MChS Rossii*, 2013, No. 3, Pp. 109–113. Available: vestnik.igps.ru

2. **Korchagin S.I., Pavlov V.G., Butov A.N., Tkachenko D.G.** Podkhody k sozdaniyu sistem obespecheniya bezopasnosti osobo vazhnykh obyektov [Approaches to the development of security systems of critical facilities]. *Sistemy bezopasnosti* [*Systems of security*], 2010, No. 4. (rus)

3. **Semkin S.N., Belyakov E.V., Grebenev S.V., Kozachok V.I.** *Osnovy organizatsionnogo obespecheniya informatsionnoy bezopasnosti obyektov informatizatsii* [*Fundamentals of organizational information security facilities information*]. Moscow: Gelios ARV Publ., 2005. (rus)

4. **Klimov S.M.** *Metody i modeli protivodeystviya kompyuternym atakam* [*Methods and models to counter computer attacks*]. Lyubertsy: KATALIT Publ., 2008. (rus)

БОГДАНОВ Алексей Валентинович – *доцент кафедры радиоэлектронных средств защиты информации Санкт-Петербургского политехнического университета Петра Великого.*
195251, Россия, Санкт-Петербург, ул. Политехническая, д. 29.
E-mail: bogdanov@hermitage.ru

BOGDANOV Alexey V. *Peter the Great St. Petersburg Polytechnic University.*
195251, Politekhnicheskaya Str. 29, St. Petersburg, Russia.
E-mail: bogdanov@hermitage.ru

МАЛЫГИН Игорь Геннадьевич – *профессор Института проблем транспорта имени Н.С. Соломенко РАН, доктор технических наук.*
199178, Россия, Санкт-Петербург, 12-я линия ВО, д. 13.
E-mail: malygin_com@mail.ru

MALYGIN Igor G. *IPT RAS.*
199178, 12th line of Vasilievsky Island, 13, St. Petersburg, Russia.
E-mail: malygin_com@mail.ru