УДК 004.056.5, 004.942 ***DOI: 10.46960/1816-210X_2022_4_28***

МОДЕЛИРОВАНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ПРОБЛЕМЫ И РЕШЕНИЯ

В.Ю. Карпычев
ORCID: **0000-0001-8527-2600** e-mail: **kavlyr@yandex.ru**
Нижегородский государственный технический университет им. Р.Е. Алексеева,
Приволжский институт повышения квалификации ФНС России
Нижний Новгород, Россия

Рассмотрены подходы к решению сложной многокритериальной задачи моделирования информационной безопасности организации на основе ряда нормативно-методических документов. Проведен сравнительный анализ особенностей, ограничений и трудностей практической реализации данных подходов. Приведены предпочтительные условия применения различных моделей обеспечения информационной безопасности. Показана вынужденная компромиссность решений в части уровня защищенности информационных активов и экономики обеспечения информационной безопасности.

Ключевые слова: информационная безопасность, моделирование, информационные активы, угроза, ущерб, уязвимость, затраты, риск-менеджмент.

ДЛЯ ЦИТИРОВАНИЯ: Карпычев, В.Ю. Моделирование информационной безопасности: проблемы и решения // Труды НГТУ им. Р.Е. Алексеева. 2022. № 4. С. 28-36. DOI: 10.46960/1816-210X_2022_4_28

CYBER SECURITY MODELING: ISSUES AND OPTIONS

V.Yu. Karpychev
ORCID: **0000-0001-8527-2600** e-mail: **kavlyr@yandex.ru**
Nizhny Novgorod State Technical University n.a. R.E. Alekseev,
Federal State Institution of Advanced Finance Professional Training
Federal Tax Service Training Institute
Nizhny Novgorod, Russia

Abstract. Based on a number of regulatory and procedural guidelines, some approaches are explored to solve the complex multi-objective problem of institutional cyber security modeling. The author performs a comparative analysis of the features, limitations and difficulties of the practical implementation of the approaches. They specify the preferred conditions applicable to the different models of cyber security protection. The trade-off between the protection level of information assets and economics of cyber security protection is shown necessary.

Key words: cyber security, modeling, information assets, threat, harm, vulnerability, costs, risk management

FOR CITATION: V.Ju. Karpychev. Cyber security modeling: issues and options. Transactions of NNSTU n.a. R.E. Alekseev. 2022. № 4. Pp. 28-36. DOI: 10.46960/1816-210X_2022_4_28

Введение

Обеспечение информационной безопасности (ИБ) является самостоятельным, сложным и затратным направлением деятельности организаций. Рассмотрению вопросов, связанных с обеспечением ИБ, посвящено множество научных исследований. Создана обширная база нормативных и методических документов, регламентирующих деятельность в данной области. Тем не менее, задача обеспечения ИБ, как правило, не имеет тривиальных решений при ее практической реализации. Проблемы связаны с определением эффективности по назначению и экономической обоснованности создания систем ИБ. В статье рассмотрены

возможные подходы к решению этих взаимосвязанных задач на основе моделирования информационной безопасности.

Основные подходы к обеспечению информационной безопасности

В качестве теоретической основы обеспечения ИБ можно рассматривать известную *модель безопасности с полным перекрытием* [1], на наш взгляд, в общем случае представляющую идею защиты. В упрощенной версии модели представлены множества:

- $T = \{t_i\},\ i = \overline{1, N}$ – угроз безопасности;
- $O = \{o_j\},\ j = \overline{1, J}$ – объектов безопасности;
- $M = \{m_k\},\ k = \overline{1, K}$ – средств защиты (средств обеспечения безопасности).

Отношения элементов этих множеств можно исследовать на графовой модели. Двухдольный граф $\langle T, O \rangle$ описывает потенциальные угрозы конкретным объектам. Включение в модель множества М позволит перекрыть возможные пути (ребра) реализации угроз. На рис. 1 представлен трехдольный граф $\langle T, M, O \rangle$, отражающий рассмотренные взаимосвязи.

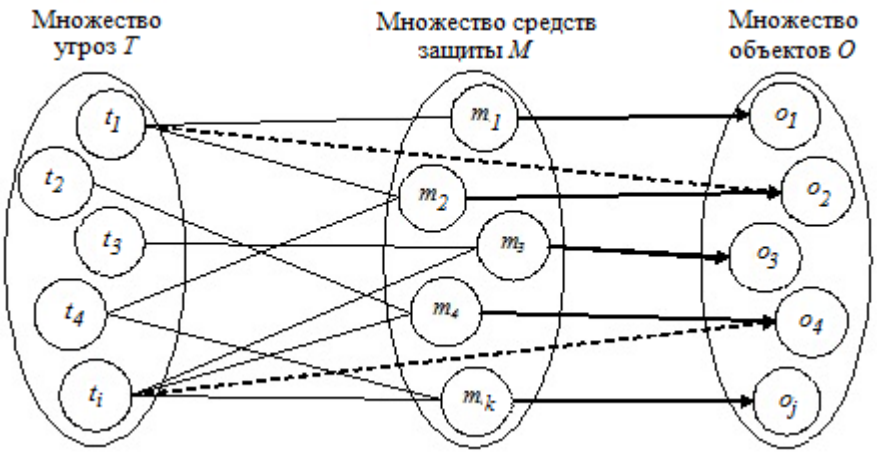

Рис. 1. Полное перекрытие угроз безопасности

Fig. 1. Full overlap of security threats

Для обеспечения безопасности все ребра модели должны иметь вид $\langle t_i, m_k \rangle$ и $\langle m_k, o_j \rangle$. Наличие ребер вида $\langle t_i, o_j \rangle$ означает отсутствие защиты для объекта (ребра $\langle t_1, o_2 \rangle$ и $\langle t_1, o_4 \rangle$ на рис. 1). Тогда полная защищенность объектов достигается при выполнении условия:

$$\forall (t_i) \in T,\ \exists (m_k) \in M, \quad (1)$$

означающего, что реализация каждой угрозы t_i из множества угроз в отношении объекта o_j может быть предотвращена средством m_k из множества средств защиты M.

Предполагается, что используемые средства защиты должны гарантированно противодействовать реализации связанной угрозы. В реальности угрозы могут преодолевать средства защиты, и это желательно отразить в модели. Кроме того, в «реальной» жизни имеют значение *вероятность возникновения угроз и величина ущерба* объекту безопасности в случае реализации угрозы. Однако этими категориями модель не оперирует. Экономические аспекты обеспечения ИБ также остаются за пределами модели с полным перекрытием.

Это означает, что в теоретической модели обеспечения безопасности, представляющей идею полного перекрытия путей реализации угроз, существуют следующие серьезные ограничения, препятствующие практическому применению.

1. Трудности формирования полных множеств угроз *T* и объектов безопасности *O* в контексте конкретной организации. Решение этой задачи влияет на функциональную и экономическую эффективность обеспечения ИБ.
2. Невозможность количественного определения уровня защищенности объектов безопасности, не позволяющая оценивать его изменения, в том числе обусловленные совершенствованием структурно-параметрических характеристик системы ИБ.
3. Отсутствие инструментов адаптации модели к конкретной организации, то есть условиям ее деятельности, структуре и виду объектов безопасности (абстрактность модели).
4. Уникальность принятых решений обеспечения безопасности (т.е. $\langle t_i, m_k \rangle$ и $\langle m_k, o_j \rangle$) конкретных организаций, затрудняющих их тиражирование.
5. Отсутствие инструментов экономического анализа решений по обеспечению ИБ.
6. Невозможность гарантированного обеспечения ИБ (наличие остаточного риска).

Указанные ограничения модели с полным перекрытием оставляют ее теоретической конструкцией без отражения в нормативных документах и, соответственно, практического использования. На практике применяются подходы, частично снимающие эти ограничения: классификационный и рисковый (менеджмент информационного риска).

Классификационный подход к обеспечению ИБ является основным для государственных организаций. В рамках этого подхода проводится категорирование:

- объектов безопасности (объектов информатизации);
- информации (по уровням ограничения доступа);
- средств защиты (по функциональности и реализуемым возможностям);
- нарушителей (по отношению к защищаемой организации, квалификации, доступным техническим средствам) и др.

Рис. 2 раскрывает сущность подхода на примере обеспечения ИБ автоматизированных систем (АС).

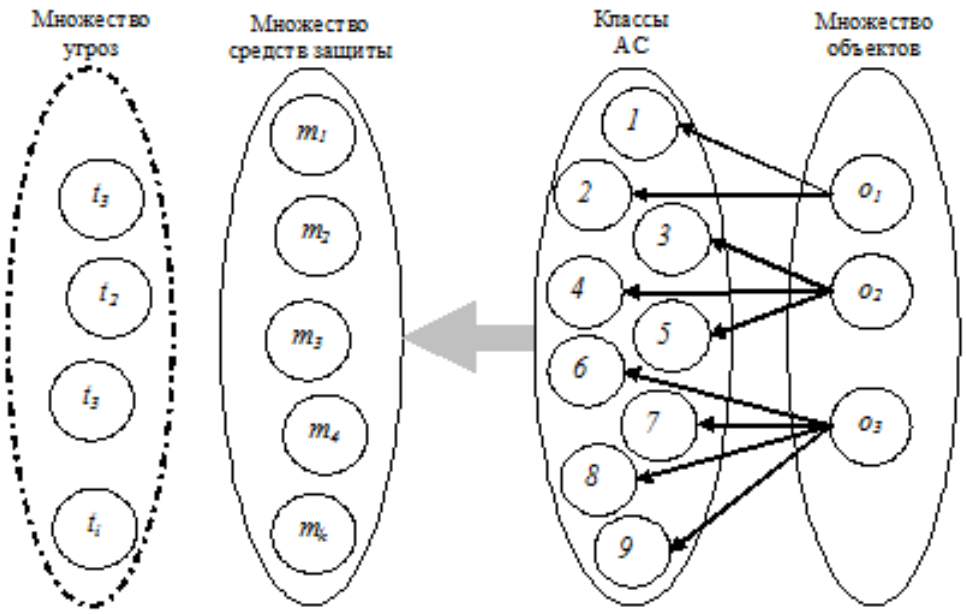

Рис. 2. Классификационный подход к обеспечению ИБ

Fig. 2. Classification approach to CS protection

Руководящий документ[1] устанавливает 9 классов защищенности АС от НСД к информации. Классы объединены в три группы, учитывающие особенности обработки информации. В каждой группе обеспечивается иерархия требований к ИБ в зависимости от уровня ограничения доступа к информации. Для каждого класса АС определен перечень организационно-технических мер безопасности, обязательных для исполнения.

При классификационном подходе к обеспечению ИБ:

- функциональным критерием эффективности является выполнение нормативно заданного набора требований для объектов классификации (категорирования); набор и значения показателей безопасности разработчики нормативных документов не аргументируют;
- без рассмотрения остаются вопросы экономики создания систем ИБ; по умолчанию очевидным критерием экономической эффективности является минимизация обобщенных затрат на выполнение нормативных требований безопасности: $\sum C_k \to \min$, где C_k – затраты на *k-ое* средство защиты.

Таким образом, задача применения классификационного подхода может быть поставлена следующим образом: определить затраты достаточные для достижения в текущих условиях деятельности организации требуемого уровня ИБ, выраженного через нормативно установленные показатели для определенного класса информационных систем (ИС).

Классификационный подход

Классификационный подход обладает следующими особенностями:

- позволяет относить ИС к определенному классу защищенности и определяет соответствующий ему набор мер безопасности;
- обеспечивает в классе одинаковый уровень ИБ для различных организаций путем применения типовых организационно-технических (тиражируемость) решений;
- создает возможность массового применения для близких по отраслевой принадлежности и структуре организаций.

Именно эти свойства, на наш взгляд, определили нормативное закрепление в документах ФСТЭК России классификационных методик обеспечения ИБ, обязательных для применения организациями при защите государственной и служебной тайн. Однако для негосударственных организаций, не связанных жесткими требованиями к уровню безопасности конфиденциальной информации, ценность данных свойств классификационного подхода снижается. Актуализируются ограничения подхода: отсутствие точных значений показателей защищенности для конкретных организаций, характера, вида и условий их деятельности; как следствие, за пределами модели остается планируемая или реальная экономическая эффективность системы ИБ. Иначе классификационный подход не обосновывает необходимость и достаточность предлагаемых решений по обеспечению ИБ и не позволяет производить «тонкую» настройку системы ИБ.

Подход к обеспечению ИБ на основе менеджмента риска

Рассмотренные ограничения классификационного подхода предполагают обращение к иным методам обеспечения ИБ, в том числе, реализующим идею соответствия защиты актуальности угроз. Основная трудность воплощения этой идеи состоит в установлении степени соответствия, т.е. в определении количественных характеристик ИБ и методов вычисления их значений.

[1]РД Автоматизированные системы. Защита от несанкционированного доступа. Классификация автоматизированных систем и требования по защите информации. М.: Гостехкомиссия России, 1992.

Действующие стандарты[1] предлагают альтернативную классификационному подходу методологию менеджмента информационных рисков, предполагающую исследование угроз ИБ, уязвимостей объектов безопасности, оценку и анализ защищенности ИС. В методологии используются несколько специфических понятий. Рассмотрим их в комплексе с ранее введенными понятиями и обозначениями.

Информационные активы

Поименуем объект ИБ $o_j \in O$ как *актив*. В соответствии с ГОСТ Р 13335-1 в качестве актива организации можно рассматривать «все, что имеет ценность для организации». Эта же позиция отражена и в ГОСТ Р 27005 (приложение В)[2] Тогда *информационный актив* (ИА) – любой актив, используемый в информационном обеспечении организации. В указанных стандартах приводится широкий перечень ИА:

- информация на электронных носителях (базы и файлы данных);
- аппаратно-программные средства, предназначенные для обработки информации;
- различные категории персонала, его компетенции и опыт;
- гудвилл (деловая репутация и имидж организации) и др.

Реализация угрозы в отношении любого ИА ведет к *ущербу* активу, который, исходя из приведенного перечня, может включать:

- *материальный ущерб*, оцениваемый в явном виде в количественном или стоимостном исчислении;
- *нематериальный ущерб* репутации, конкурентным преимуществам и т.п. (виды ущерба и типовые негативные последствия от реализации угроз ИБ приведены в методическом документе «Методика оценки угроз безопасности информации», выпущенном ФСТЭК России (2021)).

Риск нарушения информационной безопасности

Возникновение любой угрозы, например, t_i происходит случайно с вероятностью p_i. Соответственно ущерб ИА o_j в результате реализации угрозы t_i также случайное событие. Ущерб характеризуется величиной u_{ij} и вероятностью p_{ij}. При отсутствии средств защиты ИА, вероятность ущерба активу o_j равна вероятности возникновения угрозы t_i: $p_{ij} = p_i$.

По общему правилу предметную деятельность, сопряженную с возможным ущербом, называют *рисковой,* а показатель, характеризующий вероятность реализации угрозы и размер причиненного ей ущерба – *риском*. Выражение (3) формализует риск ущерба u_j для незащищенного актива o_j при реализации угрозы t_i

$$r_{ij} = p_{ij} \times u_{ij} = p_i \times u_{ij} . \quad (3)$$

Общий риск, создаваемый угрозами T, множеству активов O:

$$R = \sum_i \sum_j r_{ij} . \quad (4)$$

При расширении модели с полным перекрытием риск кроме *вероятности возникновения угрозы и величины ущерба* ИА в случае ее реализации должен учитывать *вероятность использования уязвимости* p_r ИА. Тогда при реализации угрозы t_i в отношении объекта o_j может быть причинен ущерб u_{ij} с вероятностью:

[1] ГОСТ Р 13335-1. Информационная технология. Методы и средства обеспечения безопасности. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий; ГОСТ Р 27001. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования; и др.

[2] ГОСТ Р 27005. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.

$$p_{ij} = p_i \times p_r, \quad (5)$$

где p_{ij} – вероятность ущерба, p_i – вероятность возникновения угрозы, p_r – вероятность использования уязвимости v_r.

Риск в этом случае можно представить выражением (6):

$$r_{ij} = p_i \times p_r \times u_{ij} \quad (6)$$

Такое понимание риска предложено стандартом NIST SP 800-30 Risk Management Guide for Information Technology Systems (США):

$$Risk = R(P(T,V),I), \quad (7)$$

где *риск (R)* – функция вероятности (*P*) использования угрозой (*T*) отдельной уязвимости *(V)* и результата воздействия *(I)* этой угрозы на ИА.

Выражение (7) можно интерпретировать как *остаточный риск*, т.е. риск, не устраненный принятыми мерами ИБ. Эту характеристику можно использовать для оценки стойкости барьера $b_l = \langle t_i, o_j, m_k \rangle$ [2], созданного средством m_k, предназначенным для противодействия угрозе t_i в отношении o_j:

$$Risk_l = p_i u_{ij}(1 - d_k). \quad (8)$$

В выражении (8) переменные p_i и u_{ij} введены нами выше, а переменная d_k характеризует стойкость средства m_k, определяемую вероятностью его преодоления.

Информационные активы подлежат защите. Очевидно, что в настоящее время затраты на ИБ являются обязательной частью ИТ-бюджетов, хотя и не генерируют доходы. Это значит, что их уровень должен быть приемлемым для организации, то есть некоторые виды затрат на ИБ необходимы, а другие могут быть уменьшены или исключены.

ГОСТ Р 13335-3 предлагал несколько подходов к обеспечению ИБ, отличающихся уровнем формализма при менеджменте риска:

- базовый подход (стандартный или общепринятый уровень ИБ) для всех ИА;
- неформальный подход к безопасности наиболее рисковых ИА, определенных экпертно;
- формальный подход, состоящий в детальном исследовании риска всех ИА;
- комбинированный подход, предполагающий экспертное выявление высокорисковых и/или критически важных ИА, затем детальный анализ их рисков. Для остальных ИА – применение базового подхода[1].

В настоящее время этот ГОСТ заменен на ГОСТ Р 27005, оперирующий двумя последовательно выполняемыми итерациями (приложение Е):

- идентификация высокоуровневых рисков ИБ, для которых возможно использование, по сути, базовых организационных и общих технических мер защиты;
- детальная оценка риска ИБ, включающая определение и оценку вышерассмотренных характеристик риска.

Нетрудно видеть, что ГОСТ Р 27005 содержательно охватывает в рассматриваемой части подходы ГОСТ Р 13335-3. Поэтому полезно остановиться на них более подробно.

Базовый подход

Базовый подход к обеспечению ИБ целесообразен в организациях, которые не имеют критических ИА, и при реализации угроз их восстановление не потребует значительных затрат. В настоящее время базовый уровень обеспечения ИБ рекомендован для любой организации. В общем случае базовый уровень ИБ определяется действующими нормативами и стандартами, лучшими практиками, знаниями и опытом специалистов. Справочные материалы и рекомендации по применению средств защиты на базовом уровне приведены в различ-

[1] ГОСТ Р 13335-3. Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий (отменен).

ных документах (например, Приказ ФСТЭК России № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (2013) и приложение 2 к методическому документу ФСТЭК России «Меры защиты информации в государственных информационных системах» (2014)).

При практическом обеспечении базового уровня ИБ принимаются во внимание характерные угрозы ИА (вирусы, отказы оборудования, НСД и т. д.) Для противодействия угрозам используется типовой набор средств безопасности (антивирусы, фаерволы, средства резервного копирования, системы контроля и управления доступом). Вероятности реализации угроз, уязвимости и ущерб ИА не учитываются, т.е. остаточный риск принимается «как есть». Базовые решения также можно заимствовать у организаций с близкими по отраслевой принадлежности и условиями деятельности. За рубежом получила распространение реализация базового подхода, основанная на поиске инварианта разумных затрат на ИБ. Ведущие консалтинговые организации определили некое значение необходимых затрат на ИБ в пропорции от затрат на информационные технологии и детерминированное конкретными условиями предметной деятельности. Так, Gartner, Inc. определяет, что расходы организаций на обеспечение ИБ составляют 1-13 %, в среднем – 5-6 % ИТ-бюджета [3]. Данные компаний *PricewaterhouseCoopers* и *Forrester Research* находятся в указанном диапазоне, и составляют соответственно 3,7 и 10 % [4].

Результаты исследования, проведенного Deloitte и FS-ISAC, показывают, что средние затраты финансовых организаций на ИБ составляют $1300-3000 на одного работника (10 % ИТ-бюджета) [5]. Это и есть упомянутая выше оценка на основе *best practice*, к которой можно обращаться, не проводя детальные расчеты. В этом случае задача создания системы ИБ может быть интерпретирована следующим образом: при заданном бюджете на ИБ найти оптимальный с функциональной точки зрения набор ИБ-решений в контексте деятельности организации.

Основные преимущества базового подхода:

- исключение затрат (в том числе, временных) на менеджмент рисков;
- повышение защищенности ИА в однородных организациях, имеющих близкие условия предметной деятельности, за счет унификации используемых решений.

Однако этот подход также имеет очевидные недостатки. Для конкретных организаций указанные пропорции являются достаточно абстрактным ориентиром, поскольку на величину ИБ-затрат существенным образом влияют отраслевая принадлежность, регион работы и масштаб организации. При этом не исключена возможность завышения или занижения защищенности ИА по сравнению с реальными, априори неизвестными потребностями организации.

Существуют и более сложные взаимосвязи между компонентами организаций и внешней средой **[4]**. В частности, сравнение затрат со среднеотраслевыми показателями не определяет текущее состояние ИБ в организации, поскольку даже одноуровневые затраты могут не обеспечивать соизмеримую защищенность. Gartner также отмечает, что многие организации некорректно используют средние значения расходов на ИБ, поскольку без учета бизнес-требований, допустимого риска и др. доля расходов на ИБ в ИТ-бюджете не достаточно информативна для бюджетного планирования. Данные о расходах на ИБ не могут служить показателем защищенности ИА [3]. Ориентация на средние показатели также, скорее всего, не позволит привлечь руководство организации к разработке проблем ИБ, поскольку ссылка на общепринятые требования к ИБ, формализованные в стандартах, будет достаточным обоснованием бюджета ИБ.

Неформальный и формальный подходы

В организациях, где наличие проблем в области ИБ имеет большое значение для предметной деятельности, ГОСТ Р 13335-3 рекомендовал оценивать информационные риски, используя неформальный (экспертный) подход. Преимуществом неформального подхода по сравнению с рассматриваемым ниже детальным подходом являются меньшие затраты в том числе времени на менеджмент риска. Особенности подхода: субъективные результаты оценки риска, возможные трудности обоснования мер защиты, ограниченность числа специалистов, обладающих необходимыми компетенциями. Эти особенности являются, по сути, ограничениями на применение неформального подхода к менеджменту риска.

В основе формального подхода лежат количественные методы детального анализа риска: проводится спецификация всех рисков путем идентификации активов и их уязвимостей, угроз и возможного ущерба в случае реализации угроз. Детальный анализ риска позволяет определить для каждого ИА актуальные угрозы и адекватные им меры защиты, а также разработать соразмерные рискам мероприятия для совершенствования системы ИБ (достоинства подхода). Однако использование формального подхода предполагает значительные затраты материальных ресурсов и времени квалифицированных, в том числе сторонних специалистов. Поэтому подход целесообразно использовать при критически высокой ценности ИА и необходимости «тонкой» настройки системы ИБ.

При этом актуальным является выбор допустимого уровня риска, поскольку существует вариативность способов выбора. Например, можно полагать, что текущий уровень обобщенного риска на определенную величину превышает максимально допустимое значение и провести соответствующие мероприятия по его обработке.

Также возможно итеративное нахождение наилучшего значения риска в области допустимых значений. В этом случае менеджмент риска является скорее творчеством, чем проектной работой, поскольку нормативные документы, например, ГОСТ 27005 рекомендует лишь общий алгоритм процесса.

Заключение

Методологии моделирования ИБ в целом подвержены общим ограничениям и сопряжены с трудностями практического применения:

- несовершенство моделей ИБ, включая трудности количественной оценки параметров ИБ;
- отсутствие формализованных зависимостей между уровнями безопасности, величинами среднегодовых потерь от реализации угроз ИА и затратами организации на обеспечение ИБ;
- высокая доля субъективных процедур в менеджменте ИБ;
- большая трудоемкость моделирования ИБ;
- необходимость привлечения к разработке моделей квалифицированных специалистов;
- отсутствие доступного программного инструментария поддержки моделирования ИБ и т.п.

Таким образом, моделирование (менеджмент) ИБ представляет собой нетривиальную задачу, особенно при недостаточности необходимого опыта у исполнителей.

Изложенные обстоятельства определяют актуальность дальнейших исследований, направленных на разработку научно-методологической базы, прикладных методов и инструментальных средств менеджмента ИБ, разработки научно обоснованных подходов к созданию безопасных ИС, а также подготовки специалистов в области ИБ.

Библиографический список

1. **Хоффман, Л.Дж.** Современные методы защиты информации / Л.Дж. Хоффман. – М.: Сов. радио, 1980. – 264 с.
2. **Астахов, А.** Анализ защищенности корпоративных систем // Открытые системы. 2002. № 7-8
3. Gartner, Inc. [Электронный ресурс] // Режим доступа: https://www.gartner.com/en/newsroom/press-releases/2016-12-09-gartner-says-many-organizations-falsely-equate-it-security-spending-with-maturity/ (дата обращения 20.07.2022).
4. **Asen, A.** Are You Spending Enough on Cybersecurity? / A. Asen, W. Bohmayr, S. Deutscher et al. [Электронный ресурс] // Режим доступа: https://www.bcg.com/publications/2019/are-you-spending-enough-cybersecurity (дата обращения 20.07.2022).
5. **Comtois, J.** Financial services firms spend 6% to 14% of IT budget on cybersecurity – survey/ [Электронный ресурс] // Режим доступа: https://www.pionline.com/article/20190501/ONLINE/190509988/financial-services-firms-spend-6-to-14-of-it-budget-on-cybersecurity-survey (дата обращения 20.07.2022).

Дата поступления
в редакцию: 20.07.2022

Дата принятия
к публикации: 18.10.2022