ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

DOI 10.21672/2074-1707.2020.52.4.075-084
УДК 004. 056

АДАПТИВНАЯ СИСТЕМА КОМПЛЕКСНОГО ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КАК ЭЛЕМЕНТ ИНФРАСТРУКТУРЫ СИТУАЦИОННОГО ЦЕНТРА[1]

Статья поступила в редакцию 15.10.2020, в окончательном варианте – 25.10.2020.

Путято Михаил Михайлович, Московский государственный университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,
кандидат технических наук, доцент, ORCID: 0000-0003-0414-6034, e-mail: putyato.m@gmail.com
Макарян Александр Самвелович, Московский государственный университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,
кандидат технических наук, доцент, ORCID: 0000-0002-1801-6137, e-mail: msanya@yandex.ru
Черкасов Александр Николаевич, Московский государственный университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,
кандидат технических наук, доцент, e-mail: cherk@mail.ru
Горин Иван Григорьевич, Негосударственное частное общеобразовательное учреждение "Лицей "ИСТЭК", 350049, Российская Федерация, г. Краснодар, ул. Красных Партизан, 82,
учащийся

В статье рассматриваются вопросы анализа и моделирования адаптивной системы комплексного обеспечения безопасности как элемента инфраструктуры ситуационного центра. Постоянно изменяющиеся условия информационной среды и глобального информационного пространства диктуют возможность автоматизированного или автоматического «приспособления» систем безопасности к требованиям современных программных комплексов. Основными задачами по организации интеграции комплексной системы обеспечения безопасности в систему ситуационного центра и определения регламента взаимодействия с функциональными блоками является анализ и внедрение различных формализованных процедур обеспечения комплексной безопасности. Адаптивная система комплексного обеспечения безопасности рассматривается как объект, реализующий возможность управления и оперативного построения модели защиты ситуационного центра в зависимости от решаемой задачи или предупреждения, или ликвидации инцидента. Предложенный подход продиктован не только повышением функциональности современных технологий, но и требованиями к созданию адаптивных интегрированных решений, масштабируемых в рамках архитектуры для защиты от различного типа угроз. Использование комплексной системы обеспечения безопасности в рамках предложенного подхода позволит оперативно реагировать на инциденты как внешнего, так и внутреннего характера, что позволит своевременно нейтрализовать последствия их влияния. Адаптивная комплексная система обеспечения безопасности как общая платформа обеспечит своевременный мониторинг, контекст и возможности управления в различных ситуациях. Разработка такой платформы интеграции позволит улучшить автоматизацию и повысить качество информации, предоставляемой продуктами для обеспечения информационной безопасности.

Ключевые слова: кибербезопасность, комплексная безопасность, ситуационный центр, информационная безопасность, сложные адаптивные системы, модель с полным перекрытием, математическая модель

ADAPTIVE INTEGRATED SECURITY ASSURANCE SYSTEM AS AN ELEMENT OF THE INFRASTRUCTURE OF THE SITUATION CENTER

The article was received by the editorial board on 15.10.2020, in the final version – 25.10.2020.

Putyato Mikhail M., Moscow State University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,
Cand. Sci. (Engineering), Associate Professor, ORCID: 0000-0003-0414-6034, e-mail: putyato.m@gmail.com
Makaryan Alexander S., Moscow State University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,
Cand. Sci. (Engineering), Associate Professor, ORCID: 0000-0002-1801-6137, e-mail: msanya@yandex.ru
Cherkasov Alexander N., Moscow State University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,
Cand. Sci. (Engineering), Associate Professor, e-mail: cherk@mail.ru

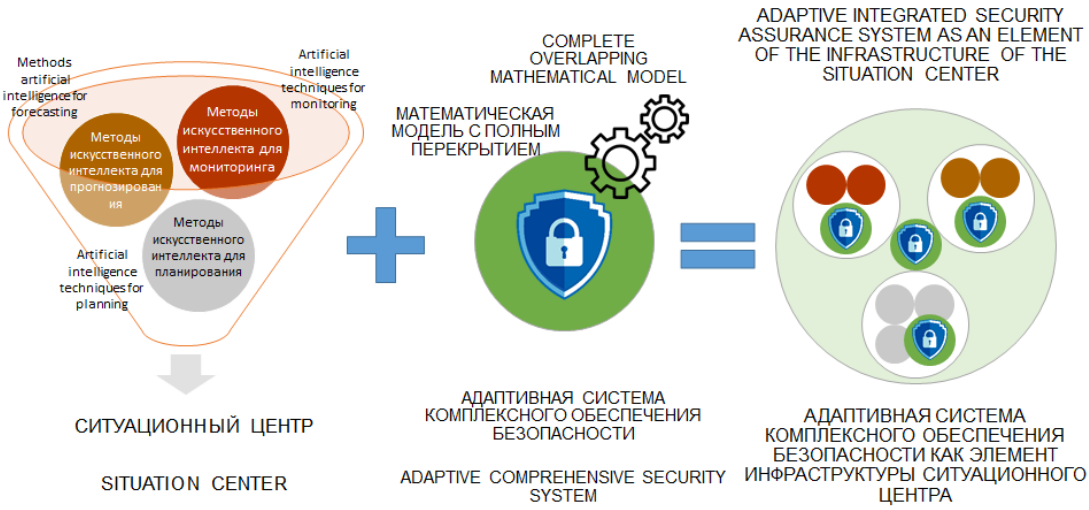
[1] Исследование выполнено при финансовой поддержке РФФИ и администрации Краснодарского края в рамках научного проекта № 19-47-235006 «Разработка теоретических основ и алгоритмов функционирования адаптивных систем управления ситуационных центров на основе методов искусственного интеллекта».

Gorin Ivan G., Non-state private educational institution "Lyceum "ISTEK", 82 Krasnykh Partizan St., Krasnodar, 350049, Russian Federation,
pupil

The article deals with the analysis and modeling of an adaptive system for integrated security provision as an element of the infrastructure of the situation center. The constantly changing conditions of the information environment and the global information space dictate the possibility of automated or automatic "adaptation" of security systems to the requirements of modern software systems. The main tasks for organizing the integration of an integrated security system into the situation center system and determining the rules for interaction with functional blocks is the analysis and implementation of various formalized procedures for ensuring integrated security. An adaptive integrated security system is considered as an object that implements the ability to manage and quickly build a security model for a situation center, depending on the problem being solved, or preventing or eliminating an incident. The proposed approach is dictated not only by an increase in the functionality of modern technologies, but also by the requirements for the creation of adaptive integrated solutions that are scalable within the architecture to protect against various types of threats. The use of an integrated security system within the framework of the proposed approach will make it possible to promptly respond to incidents of both external and internal nature, which will allow timely neutralization of the consequences of their influence. An adaptive integrated security system as a common platform will provide timely monitoring, context and control capabilities in various situations. The development of such an integration platform will improve automation and improve the quality of information provided by information security products.

Keywords: cybersecurity, integrated security, situation center, information security, complex adaptive systems, full overlap model, mathematical model

Graphical annotation (Графическая аннотация)



Введение. Современные условия развития различных отраслей экономики постоянно предъявляют для информационных систем новые требования:

- минимизация человеческого фактора;
- увеличение автоматизации процессов обработки и управления информацией;
- интеллектуализация решений;
- безопасность информационных технологий, клиентов и организации в целом;
- адаптивность системы к постоянно изменяющимся условиям.

Отдельное место в данной парадигме занимает безопасность IT-систем, особенно критических информационных инфраструктур[1], четко регламентированных нормативными и законодательными актами Российской Федерации.

Изменяющиеся условия информационной среды и глобального информационного пространства диктуют возможность автоматизированного или автоматического «приспособления» систем безопасности к требованиям современных программных комплексов.

Рассматривая ситуационной центр как многоаспектную систему для организации всех этапов принятия решений руководителем, а также обеспечивающих подсистем аппаратно-технического и программного вида работ, необходимо сформулировать задачи о взаимодействии комплексной системы обеспечения безопасности (КСОБ) со структурными элементами ситуационного центра (СЦ).

Особенности функционирования систем поддержки принятия решений [2] (СППР) в ситуационных центрах позволяют построить алгоритм решения задач различного класса на основе синтеза взаимосвязей между факторами, характеризующими задачу и целевое состояние объекта управления [3, 4].

Адаптивная система обеспечения комплексной безопасности как элемент ситуационного центра располагает всеми возможностями, доступными основным элементам распределенной структуры. В частности, для реализации адаптивности состояния защищенности неотъемлемыми этапами интеллектуальной поддержки являются: моделирование ситуации, экспертная поддержка, интеллектуальный поиск в интернете.

Основными задачами по организации интеграции КСОБ в систему СЦ и определения регламента взаимодействия с функциональными блоками является анализ и внедрение различных формализованных процедур обеспечения комплексной безопасности. В работах авторов рассматривались частные случаи использования как существующих средств противодействия несанкционированному доступу к критичным данным [5, 6], так и новых подходов к осуществлению и реализации современных способов защиты [7].

Согласно современным исследованиям [8], адаптивная система защиты информации должна формироваться на применении существующих методов управления и адаптации из других областей научного знания в отношении вопросов информационной безопасности. Использование обобщенных принципов адаптации прикладного характера отражают специфику отдельной сферы. Проведенные исследования [9] показывают, что большинство адаптивных систем управления строятся на основе регламентированных и устоявшихся моделей адаптации систем управления безопасностью. Такие модели предлагают либо параметрическую систему адаптации, позволяющую корректировать или подстраивать параметры системы без изменения принципов работы, либо структурную адаптацию с изменением структуры модели и сохранением параметров системы.

Использование систем защиты информации различного назначения позволяет выполнять достаточно большой спектр функций: мониторинг, обработка и контроль разнородной информации с достаточной большой степенью неопределенности. Обработка информации и использование ее для конкретной ситуации занимает большое количество времени, информационных и аналитических ресурсов [10].

Функционирование различного класса систем [8] в рамках единой адаптивной комплексной системы обеспечения безопасности позволит обеспечить выполнение большего количества задач с минимальным привлечением ресурсов. А использованием математического и интеллектуального аппарата позволит обеспечить методологическую составляющую таких систем.

Рассматривая адаптивную систему с интеллектуальным управлением как необходимое решение, влияющее на скорость реагирования на инциденты информационной безопасности, проведем анализ набора методов искусственного интеллекта, уже предложенных к использованию в распределенной структуре ситуационного центра:

1. Методы искусственного интеллекта для мониторинга.
1.1. Компьютерное зрение.
1.2. Интеллектуальные агенты.
1.3. Обработка естественных языков.
1.4. Экспертные системы.
1.5. Когнитивное моделирование.
2. Методы искусственного интеллекта для прогнозирования.
2.1. Нейронные сети.
2.2. Нечеткая логика.
2.3. Экспертные системы.
3. Методы искусственного интеллекта для планирования.
3.1. Нейронные сети.
3.2. Нечеткая логика.
3.3. Экспертные системы.

На рисунке 1 приведена схема включения адаптивной системы комплексной безопасности в структуру интеллектуального ситуационного центра [11].

Взаимодействие с информационными подсистемами СЦ. Организация функционирования комплексной системы обеспечения безопасности (КСОБ) строится на активном включении в ее работу информационных систем без нарушения работоспособности систем и их быстродействия. КСОБ – интегрированная платформа для быстрого обнаружения и реагирования на угрозы с автоматическим сбором и интеллектуальным анализом данных. Такая платформа постоянно наблюдает за безопасностью системы и не только оповещает о нарушениях и подозрительных событиях, но и создает и формирует модель событий. КСОБ поддерживает процессы мониторинга, прогнозирования, планирования и принятия решений с точки зрения информационной и комплексной безопасности на всех этапах функционирования ситуационного центра [10].

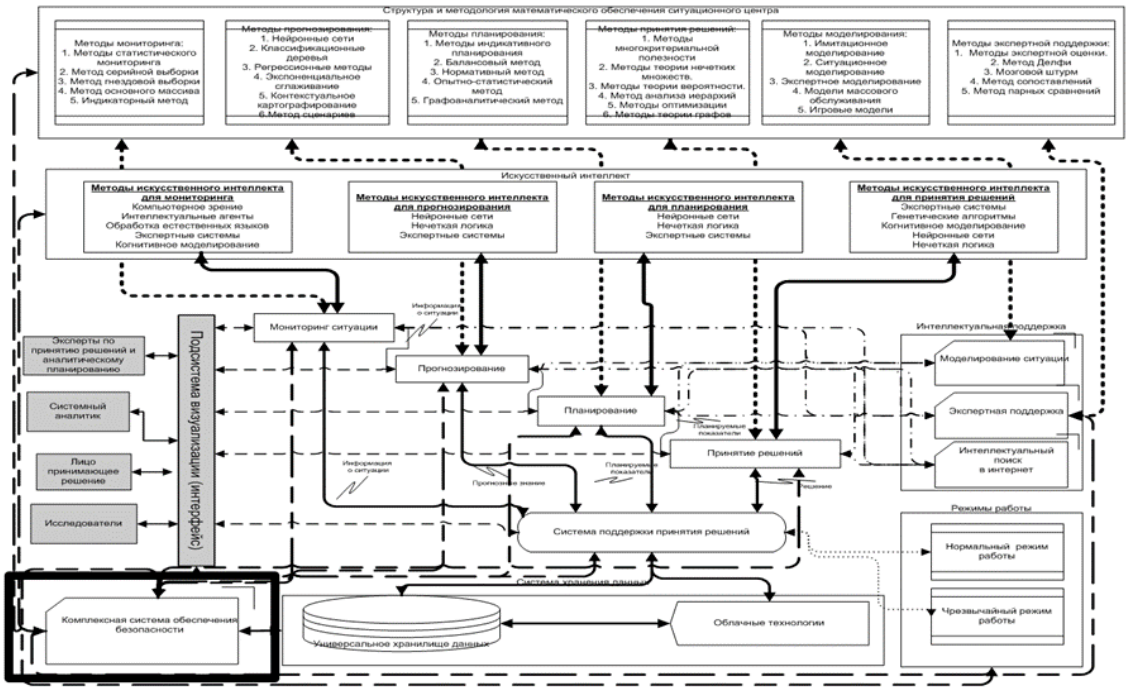


Рисунок 1 – Схема включения адаптивной системы комплексной безопасности в структуру интеллектуального ситуационного центра

Применение интеллектуальных технологий для обеспечения безопасности. Использование математических методов и технологий искусственного интеллекта позволит минимизировать участие некомпетентных специалистов в обеспечении безопасности. Речь идет о некоторой компиляции или синергии знаний и опыта в определенных направлениях обеспечения безопасности, которая позволила бы в рамках одной подсистемы закрыть вопрос с обеспечением безопасности объекта путем объединения направлений обеспечения безопасности через определенный набор маркеров или систему критериев в комплексную систему безопасности СЦ.

Контроль функционирования СЦ в различных режимах. Работа ситуационного центра предусматривает переходы в различные режимы для создания оптимальной структуры, предназначенной для обеспечения эффективного взаимодействия и координации работы всех компонентов системы ситуационного центра. В таком случае КСОБ обеспечивает структурную, параметрическую и ситуационную безопасность при функционировании интегрированного комплекса как в режиме реального времени, так и в режиме офлайн [10].

Формирование новых моделей безопасности на основе систем моделирования и экспертного мнения. При рассмотрении многоаспектных проблем и развития ситуации активно могут применять системы имитационного, агентного и дискретно-событийного моделирования. Включение процедур экспертной поддержки позволит получить дополнительную информация по проблемам безопасности. Эффективность использования таких процедур обеспечит возможность уменьшения времени на принятие решений [10], использование эвристического аппарата экспертов для накопления соответствующей базы знаний.

Организационно-правовое сопровождение. Как свидетельствуют результаты исследования, которое провели PonemonInstitute и компания Fasoo [12], безалаберность сотрудников – главная причина утечек. Именно она – причина более половины инцидентов (56 %). В 37 % случаев утечка происходит в результате утери или кражи устройства. 35 % инцидентов объясняется ошибкой третьей стороны. Лишь в 22 % случаев конфиденциальная информация пропадает по вине злоумышленников, не связанных с компанией [13].

КСОБ должна включать и функции нормативно-правового и организационного сопровождения безопасности, особенно относительно сотрудников ситуационного центра, обладающих достаточным объемом знаний и информации.

Хранилище данных. Безопасность БД и ХД. Облачные технологии. Распределенные технологии передачи и хранения данных. Подсистема визуализации. Рассматривается группа пользователей для работы в защищенном периметре закрытой части ситуационного центра. Системы идентификации с использованием комбинированных методов доступа: биометрические, аппаратно-программные, организационные, пароли и ключи доступа.

Адаптивная система комплексного обеспечения безопасности рассматривается как объект, реализующий возможность управления и оперативного построения модели защиты ситуационного центра в зависимости от решаемой задачи или предупреждения, или ликвидации инцидента. Рассмотрим подробно связи и взаимодействие КСОБ со всеми элементами ситуационного центра.

1. Связь КСОБ с информационно-аналитическими системами мониторинга, планирования, прогнозирования [10] и принятия решений в ситуационном центре:
   a. предотвращение вторжений;
   b. обеспечение реализации политик безопасности;
   c. оперативное предупреждение о нарушениях и инцидентах;
   d. визуализация ключевых показателей по результатам мониторинга безопасности;
   e. программно-аппаратная защита;
   f. техническая защита.
2. Связь КСОБ в рамках универсального хранилища данных отражает следующие функции:
   a. резервное копирование данных;
   b. безопасность информационных баз;
   c. передача данных без потерь;
   d. бесперебойная работа систем.
3. Взаимодействие КСОБ со структурой и методологией математического обеспечения и искусственного интеллекта ситуационного центра обеспечивает:
   a. модели и политики комплексной безопасности;
   b. методы искусственного интеллекта в безопасности;
   c. принципы реализации комплексной безопасности;
   d. прогнозирование новых угроз и уязвимостей.
4. Связь КСОБ с сотрудниками ситуационного центра:
   a. мониторинг показателей деятельности КСОБ;
   b. реализация пропускного режима на физический объект;
   c. обеспечение нормативно-правового аспекта безопасности

Математическая модель комплексной системы обеспечения безопасности. Математическая модель представляет собой формализованное описание сценариев в виде логических алгоритмов, представленных последовательностью действий нарушителей и ответных мер. Количественные характеристики модели определяют основные функциональные зависимости, которые используются для оценки уязвимости объекта, построения системы защиты и последующего рассмотрения ее эффективности.

Различают несколько типов моделей в зависимости от факторов:

- модели минимизации рисков [14];
- модели на основе анализа угроз в системе [15];
- модели конечных состояний [16];
- модели на основе дискретных компонент [17].

Формальные подходы к решению оценки защищенности системы не получили широкого практического распространения из-за трудностей, связанных с формализацией.

Для выбора необходимой модели системы защиты необходимо произвести их сравнение по параметрам, обусловливающим функционирование системы защиты и разрешение выполнения операции над объектом защиты либо запрещение (табл.).

Таблица – Сравнение моделей построения комплексной системы информационной безопасности

Критерии модели	**Механизм реализации**	**Динамика изменения системы**	**Финансовые затраты**	**Оценка степени уязвимости и ущерба**
Модели минимизации рисков	Средний	Средняя	Высокие	Средняя
Модели на основе анализа угроз в системе	Сложный	Высокая	Низкие	Высокая
Модели конечных состояний	Сложный	Средняя	Высокие	Средняя
Модели на основе дискретных компонент	Простой	Низкая	Низкая	Низкая

Как видно из представленной таблицы, лучшей моделью для обеспечения эффективной работы интеллектуального ситуационного центра являются модели анализа угроз систем. Одной из наиболее популярных и эффективных моделей на основе анализа угроз в системе является модель с полным перекрытием [18], которая должна иметь, по крайней мере, одно средство (субъект) для обеспечения безопасности на каждом возможном пути проникновения в систему. Для учета количественных факторов состояний комплексной системы обеспечения безопасности ситуационного центра определена модель системы защиты с полным перекрытием, которая относится к типу моделей анализа угроз в системе. Данная модель позволит вести постоянный мониторинг и контроль количественных показателей, позволяющих отслеживать набор защищаемых объектов, который сопряжен с некоторой величиной ущерба, и некоторое множество действий, к которым может прибегнуть злоумышленник для получения несанкционированного доступа к объекту.

Модель с полным перекрытием рассматривается в непосредственном взаимодействии «области угроз», «системы защиты» и «защищаемой области». Такая модель может быть описана следующими множествами:

$T = \{t_i\}$ – множество угроз;

$O = \{o_j\}$ – множество объектов защищенной системы;

$M = \{m_k\}$ – множество механизмов безопасности СЦ.

Отношения элементов множеств описывают систему защиты. Для описания системы защиты в таком случае обычно используют графовую модель, в которой множество отношений угроза – объект образует двудольный граф. Цель защиты состоит в перекрытии всех возможных ребер в графе. Это достигается введением третьего набора – M. Стандартная модель с полным перекрытием приведена на рисунке 2.

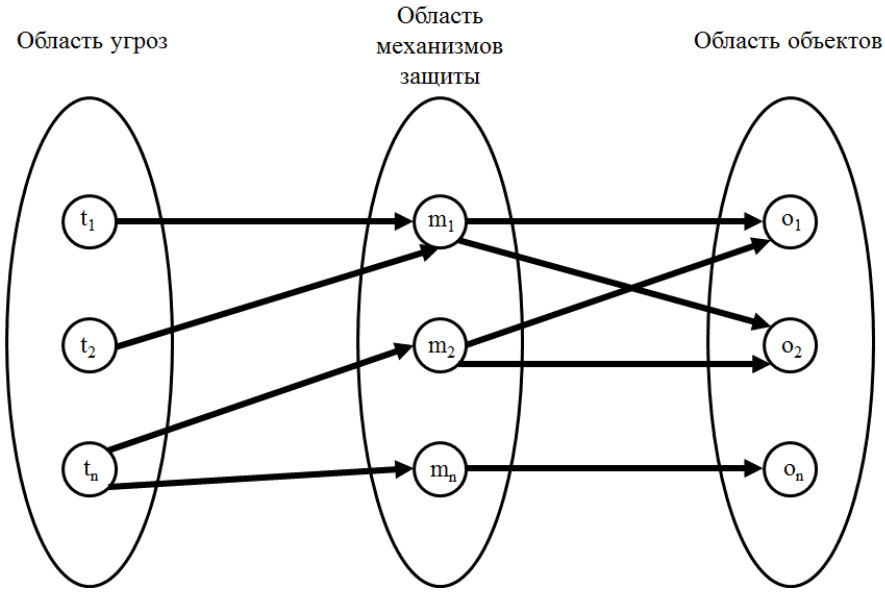


Рисунок 2 – Стандартная модель комплексной системы обеспечения безопасности с полным перекрытием

В последнее время наиболее эффективной показала себя модель, которая уточняет общую модель с полным перекрытием, где производится введение набора уязвимостей V и набора барьеров B.

Уязвимость системы защиты – возможность осуществления угрозы t_i в отношении объекта o_j. Набор уязвимостей V определяется подмножеством декартова произведения T*O: $vr = <t_i,o_j>$.

Барьеры определяются декартовым произведением V*M: $b = <t_i,o_j,m_k>$. Под барьерами понимают пути осуществления угроз безопасности, перекрытые средствами защиты.

Для системы с полным перекрытием для любой уязвимости имеется барьер. Другими словами, для всех угроз безопасности существуют механизмы защиты, препятствующие осуществлению данных угроз.

Механизмы защиты обеспечивают некоторую сопротивляемость угрозам, поэтому в качестве характеристик барьера может рассматриваться набор $<P_i, D_i, R_i>$, где P_i – вероятность появления i-й угрозы, D_i – потенциальный ущерб при осуществлении i-й угрозы, а R_i – степень сопротивляемости механизма защиты.

Прочность барьера характеризуется величиной остаточного риска X_i, связанного с возможностью осуществления угрозы t_i в отношении объекта o_j при использовании механизма защиты s_k:

$$X_i = P_k * D_k (1 - R_k). \quad (1)$$

Для определения величины защищенности используют соотношение:

$$Z = \frac{1}{\sum_{\forall b_k \in B} P_k * D_k (1 - R_k)}, \quad (2)$$

где $P_k, D_k, R_k \in (0,1)$.

На практике получение точных значений приведенных характеристик барьеров затруднено, поскольку понятия угрозы, ущерба и сопротивляемости механизма защиты трудно формализовать.

Для защиты информации, допускающей оценку ущерба, актуальны стоимостные методы оценки эффективности средств защиты. Эти методы характеристики барьеров дополняет величина F_i – затраты на построение барьера b_i. В данном случае выбор оптимального набора СЗИ связан с минимизацией суммарных затрат $A = \{a_i\}$, состоящих из затрат на создание барьера $F = \{f_i\}$ и возможных потерь от осуществления угроз $N = \{n_i\}$.

Модифицированная модель комплексной системы обеспечения безопасности с полным перекрытием приведена на рисунке 3.

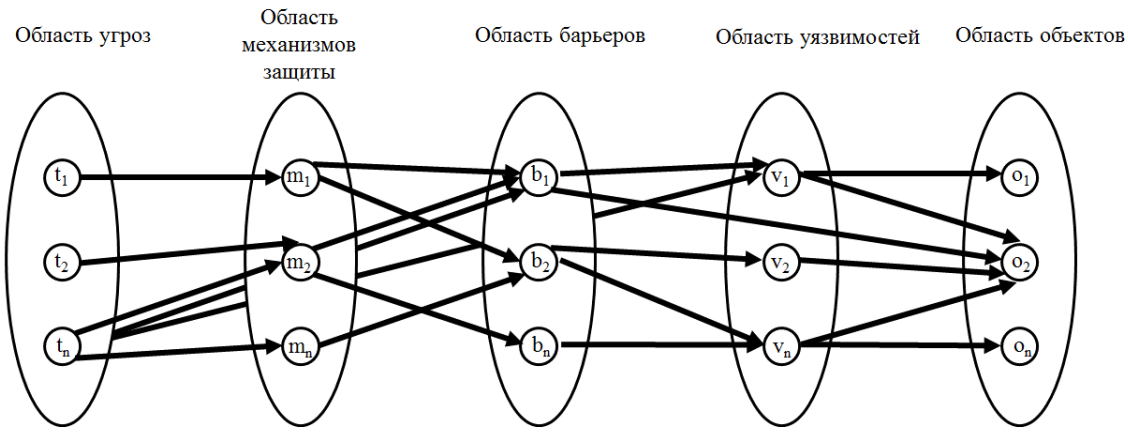


Рисунок 3 – Стандартная модель комплексной системы обеспечения безопасности с полным перекрытием

Данная модель является общей и не полностью отражает концептуальное построение КСОБ в рамках ситуационного центра. Предлагается использовать адаптивную модифицированную модель с полным перекрытием. Предлагаемая модель позволит в зависимости от целей и решаемых задач организовать множество математических моделей как части системы комплексной защиты, которые еще на стадии проектирования системы позволяют оценить ее эффективность (рис. 4).

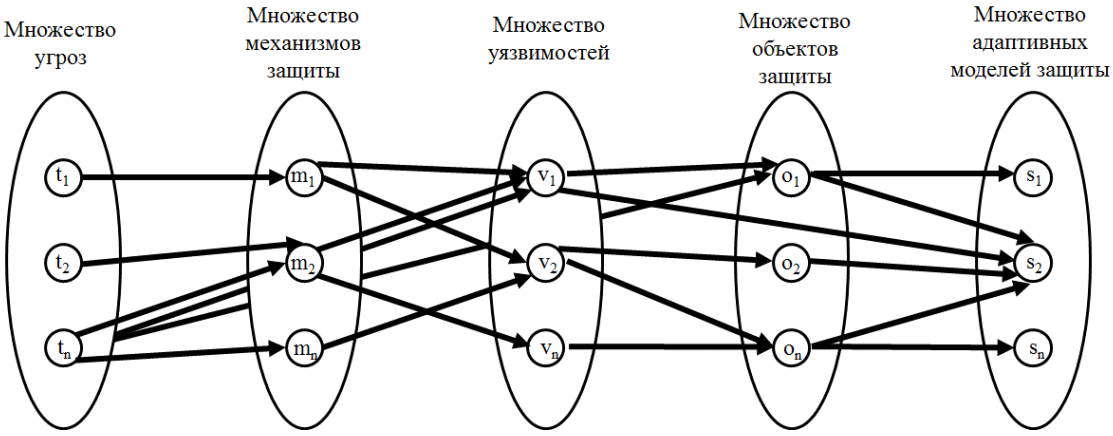


Рисунок 4 – Стандартная модель комплексной системы обеспечения безопасности с полным перекрытием

Модель адаптивного управления безопасностью предлагается описывать формулой *Безопасность = Мониторинг + Аудит + Анализ риска + Политика безопасности + Средства защиты + Реализация контрмер + Реагирование*. Процесс определения эффективности комплексной системы обеспечения безопасности состоит из обоснования показателей (критериев) оценки эффективности и методики расчета этих показателей. Предлагается выбрать оптимизационный подход для оценки комплексной системы обеспечения безопасности. При этом решается задача оптимизации вида: максимизировать некую функцию при заданных ограничениях. В случае адаптивных систем указанную методику предлагается расширить параметром k, характеризующим этапы адаптивного процесса.

Введем нижеследующие обозначения:

T = $\{t_j\}$ – множество угроз безопасности, j = 1, … n;

$M^k = a_i^k$ – множество механизмов безопасности, используемых на k-м этапе адаптивного процесса, k = 0...R;

V = $\{v_i\}$ – множество уязвимостей, i = 1…n;

$C^k = c_i^k$ – допустимые затраты на создание защиты объекта (объем затрат на сопровождение системы с учетом реализации k-го этапа адаптивного процесса), причем c_i – это затраты на начальную разработку, обучение и первоначальный запуск адаптивной системы;

$d^k\ i,j$ – эффективность нейтрализации i-м механизмом безопасности j-й угрозы на k-м этапе.

Для построения математической модели вводят переменную p(i, j), равную 1, если j-я угроза устраняется с помощью i-го механизма, и нулю – в противном случае и q, такую, что

$$q\ i,j\ = \begin{matrix} 1 - \text{если},\ i - \text{й механизм без} - \text{ти используется для устранения } j - \text{й угрозы} \\ 0 - \text{в противном случае} \end{matrix} \quad (3)$$

Если информационные угрозы между собой не связаны, то требуется найти максимальный эффект от нейтрализации множества информационных угроз T с помощью задекларированных в системе средств защиты S при ограничениях на общий объем затрат C:

$$\sum_{k=1}^{r} \sum_{j=1}^{m} \sum_{i=1}^{n} d^k\ i,j\ p(i,j) \to max \quad (4)$$

при ограничениях

$$\sum_{i=1}^{n} c\ i\ * sign \sum_{u_j \in U}^{n} p(i,j) \le C \quad (5)$$

$$p(i,j) \in (1,0).$$

Несколько видоизменив постановку задачи и введя понятие функции принадлежности $\mu^S(x_i)$, получим вариант оценки эффективности информационной системы защиты в нечетких показателях. Пусть W – счетное множество показателей $W = w_i$, i = 1…h, h – количество показателей. Принадлежность к определенному уровню безопасности определяем на заданном промежутке $0,T$. Тогда множество значений модели S, определяющих выполнение требований безопасности определяется как: $S = \sum_{i=1}^{n} \frac{\mu^A(x_i)}{x_i}$, где $\frac{\mu^A(x_i)}{x_i}$ – пара «функция принадлежности/элемент».

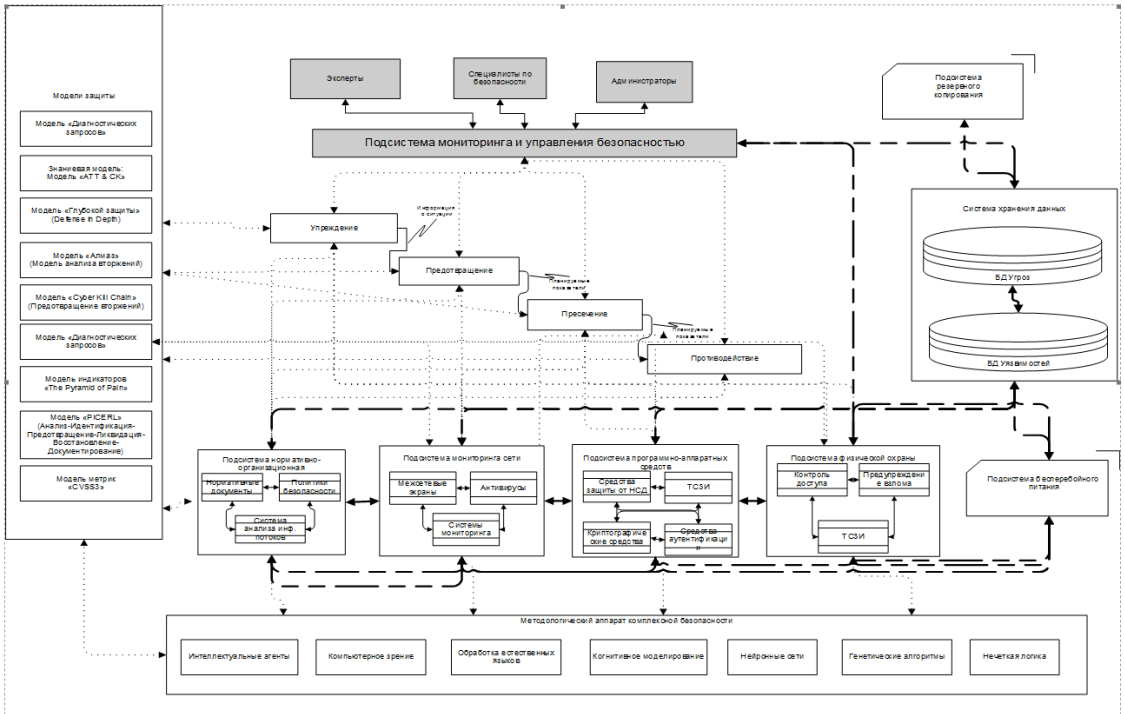


Рисунок 5 – Структурная схема комплексной системы обеспечения безопасности

Разные состояния безопасности системы выделяются в виде подмножеств нечёткого множества, а вероятность взлома оцениваемой системы может соответствовать кардинальному числу (мощности) нечёткого множества. При таком подходе для оценки эффективности защищённости адаптивной системы комплексной безопасности необходимы данные о необходимых требованиях защищённости и данные о полноте выполнения этих требований. Подобный подход позволит добиться постоянного мониторинга состояния безопасности ситуационного центра, выполнить прогноз возможности осуществления атак, провести изменение требований к переменным безопасности. Получаем возможность контролировать вновь возникающие угрозы, устранять уязвимости, которые могут привести к реализации угрозы, анализировать условия, приводящие к появлению уязвимостей. На рисунке 5 представлена структурная схема комплексной системы обеспечения безопасности.

Заключение. Проанализировав основные функции и характеристики адаптивной комплексной системы обеспечения безопасности на основе ситуационного центра, определим, что:

1) предложенный подход продиктован не только повышением функциональности современных технологий, но и требованиями к созданию адаптивных интегрированных решений, масштабируемых в рамках архитектуры для защиты от различного типа угроз;

2) использование КСОБ в рамках предложенного подхода позволит оперативно реагировать на инциденты как внешнего, так и внутреннего характера, что позволит своевременно нейтрализовать последствия их влияния.

Адаптивная комплексная система обеспечения безопасности как общая платформа обеспечит своевременный мониторинг, контекст и возможности управления в различных ситуациях. Разработка такой платформы интеграции позволит усовершенствовать процесс автоматизации и значительно улучшить качество информации, предоставляемой продуктами для обеспечения ИБ.

Библиографический список

1. Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». – 2017.

2. Курейчик В. М. Особенности построения систем поддержки принятия решений / В. М. Курейчик // Известия Южного федерального университета. Технические науки. – 2012. – Тематический выпуск. – С. 92–98.

3. Симанков В. С. Международная конференция по мягким вычислениям и измерениям / В. С. Симанков, А. Н. Черкасов, П. Ю. Бучацкий, В. В. Бучацкая, С. В. Теплоухов // Синтез системы поддержки принятия решений на основе интеллектуального ситуационного центра. Санкт-Петербург, 2020. – С. 260–263.

4. Тарасов Е. С. Методологические основы принятия решений с использованием автоматизации неформальных процедур / Е. С. Тарасов, В. С. Симанков, М. М. Путято // Естественные и технические науки. – 2010. – № 4 (49). – С. 292–297.

5. Власенко А. В. Дистанционные образовательные технологии / А. В. Власенко, М. М. Путято, А. С. Макарян // Возможности совершенствования кибербезопасности мобильных устройств на основе интеграции динамических биометрических методов. – Симферополь, 2020. – С. 369–372.

6. Макарян А. С. Классификация мессенджеров на основе анализа уровня безопасности хранимых данных / А. С. Макарян, М. М. Путято // Прикаспийский журнал: управление и высокие технологии. – 2019. – № 4 (48). – С. 135–143.

7. Очередько А. Р. Исследование SIEM-систем на основе анализа механизмов выявления кибератак / А. Р. Очередько, В. С. Герасименко, М. М. Путято, А. С. Макарян // Вестник Адыгейского государственного университета. Серия «Естественно-математические и технические науки». – 2020. – № 2. – С. 25–31.

8. Тюкин Ю. А. Адаптация в нелинейных динамических системах / Ю. А. Тюкин, В. А. Терехов. – Санкт-Петербург : ЛКИ, 2008. – С. 384.

9. Масаев С. Н. Оценка системы управления компанией на основе метода адаптационной корреляции к внешней среде / С. Н. Масаев, М. Г. Доррер // Проблемы управления. – 2010. – № 3. – С. 45–50.

10. Симанков В. С. Структура и методология функционирования интеллектуальной системы ситуационного центра / В. С. Симанков, А. Н. Черкасов // Глобальный научный потенциал. – 2015. – № 12 (57). – С. 32–37.

11. Федотова М. А. Интеллектуальные системы в информационно-аналитических (ситуационных) центрах в условиях перехода к цифровой экономике / М. А. Федотова, И. А. Мартынов // Московский экономический журнал. – 2019. – № 1.

12. Ponemon Institute и Fasoo проанализировали причины утечек корпоративных данных. – 2016. – Режим доступа: https://securenews.ru/ponemon_institute_fasoo_report/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 25.10.2020).

13. Эволюция угроз и стратегии защиты. – 2016. – Режим доступа: https://habr.com/ru /company/smart_soft/blog/304764/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 10.23.2020).

14. Баранкова И. И. Минимизация рисков информационной безопасности на основе моделирования угроз безопасности / И. И. Баранкова, У. В. Михайлова, М. В. Афанасьева // Динамика систем, механизмов и машин. – 2019. – Т. 7.

15. Любимов А. В. Модели угрозы в методологии общих критериев / А. В. Любимов // Научно-технический вестник информационных технологий, механики и оптики. – 2006. – С. 75–81.

16. Шушляпин Е. А. Модели конечного состояния для непрерывно-дискретных систем / Е. А. Шушляпин, Л. Н. Каное // Радіоелектроніка, інформатика, управління. – 1999. – С. 129–132.

17. Гутова Г. Особенности дискретного моделирования динамических объектов / Г. Гутова, Я. Карташов // Вестник Кемеровского государственного университета. – 2010. – № 4 (44). – С. 63–67.

18. Максименко В. Н. Основные подходы к анализу и оценке рисков информационной безопасности / В. Н. Максименко, Е. В. Ясюк // Экономика и качество систем связи. – 2017. – № 2. – С. 42–-48.

References

1. *Federal Law of July 26, 2017 no. 187-FL "On the security of the critical information infrastructure of the Russian Federation"*, 2017.

2. Kureychik V. M. Osobennosti postroyeniya sistem podderzhki prinyatiya resheniy [Features of building decision support systems]. *Izvestiya Yuzhnogo federalnogo universiteta. Tekhnicheskiye nauki* [Bulletin of the Southern Federal University. Technical science], 2012, thematic issue, pp. 92–98.

3. Simankov V. S., Cherkasov A. N., Buchatsky P. Yu., Buchatskaya V. V., Teploukhov S. V. Mezhdunarodnaya konferentsiya po myagkim vychisleniyam i izmereniyam [International Conference on Soft Computing and Measurements]. *Sintez sistemy podderzhki prinyatiya resheniy na osnove intellektualnogo situatsionnogo tsentra* [Synthesis of a decision support system based on an intelligent situational center]. St. Petersburg, 2020, pp. 260–263.

4. Tarasov E. S., Simankov V. S., Putyato M. M. Metodologicheskiye osnovy prinyatiya resheniy s ispolzovaniyem avtomatizatsii neformalnykh protsedur [Methodological foundations of decision-making using the automation of informal procedures]. *Yestestvennyye i tekhnicheskiye nauki* [Natural and Technical Sciences], 2010, no. 4 (49), pp. 292–297.

5. Vlasenko A. V., Putyato M. M., Makaryan A. S. Distantsionnyye obrazovatelnyye tekhnologii [Distance educational technologies]. *Vozmozhnosti sovershenstvovaniya kiberbezopasnosti mobilnykh ustroystv na osnove integratsii dinamicheskikh biometricheskikh metodov* [Opportunities for improving the cybersecurity of mobile devices based on the integration of dynamic biometric methods]. Simferopol, 2020, pp. 369–372.

6. Makaryan A. S., Putyato M. M. Klassifikatsiya messendzherov na osnove analiza urovnya bezopasnosti khranimykh dannykh [Classification of messengers based on analysis of the security level of stored data]. *Prikaspiyskiy zhurnal: upravleniye i vysokiye tekhnologii* [Caspian Journal: Control and High Technologies], 2019, no. 4 (48), pp. 135–143.

7. Ochelyko A. R., Gerasimenko V. S., Putyato M. M., Makaryan A. S. Issledovaniye SIEM-sistem na osnove analiza mekhanizmov vyyavleniya kiberatak [Investigation of SIEM-systems based on the analysis of cyberattack detection mechanisms]. *Vestnik Adygeyskogo gosudarstvennogo universiteta. Seriya «Yestestvenno-matematicheskiye I tekhnicheskiye nauki»* [Bulletin of the Adyghe State University. Series "Natural-mathematical and technical sciences"], 2020, no. 2, pp. 25–31.

8. Tyukin Yu. A., Terekhov V. A. *Adaptatsiya v nelineynykh dinamicheskikh sistemakh* [Adaptation in nonlinear dynamic systems]. St. Petersburg, LKI Publ., 2008, p. 384.

9. Masaev S. N., Dorrer M. G. Otsenka sistemy upravleniya kompaniey na osnove metoda adaptatsionnoy korrelyatsii k vneshney srede [Assessment of the company management system based on the method of adaptation correlation to the external environment]. *Problemy upravleniya* [Problems of Management], 2010, no. 3, pp. 45–50.

10. Simankov V. S., Cherkasov A. N. Struktura i metodologiya funktsionirovaniya intellektualnoy sistemy situatsionnogo tsentra [The structure and methodology of functioning of the intellectual system of the situational center]. *Globalnyy nauchnyy potentsial* [Global Scientific Potential], 2015, no. 12 (57), pp. 32–37.

11. Fedotova M. A., Martynov I. A. Intellektualnyye sistemy v informatsionno-analiticheskikh (situatsionnykh) tsentrakh v usloviyakh perekhoda k tsifrovoy ekonomike [Intelligent systems in information and analytical (situational) centers in the transition to a digital economy]. *Moskovskiy ekonomicheskiy zhurnal* [Moscow Economic Journal], 2019, no. 1.

12. *Ponemon Institute i Fasoo proanalizirovali prichiny utechek korporativnykh dannykh* [Ponemon Institute and Fasoo analyzed the reasons for corporate data leaks], 2016. Available at: https://securenews.ru/ponemon_institute_fasoo_report/ (accessed 10.25.2020).

13. *Evolyutsiya ugroz i strategii zashchity* [The evolution of threats and defense strategies], 2016. Available at: https://habr.com/ru/company/smart_soft/blog/304764/ (accessed 10.23.2020).

14. Barankova I. I., Mikhailova U. V., Afanasyeva M. V. Minimizatsiya riskov informatsionnoy bezopasnosti na osnove modelirovaniya ugroz bezopasnosti [Minimization of information security risks based on modeling security threats]. *Dinamika sistem, mekhanizmov i mashin* [Dynamics of systems, mechanisms and machines], 2019, vol. 7.

15. Lyubimov A. V. Modeli ugrozy v metodologii obshchikh kriteriyev [Threat models in the general criteria methodology]. *Nauchno-tekhnicheskiy vestnik informatsionnykh tekhnologiy, mekhaniki i optiki* [Scientific and technical bulletin of information technologies, mechanics and optics], 2006, pp. 75–81.

16. Shushlyapin E. A., Kanoe L. N. Modeli konechnogo sostoyaniya dlya nepreryvno-diskretnykh sistem [End-state models for continuous-discrete systems]. *Radioyelektronika, informatika, upravlinnya* [Radioelectronika, informatics, control], 1999, pp. 129–132.

17. Gutova G., Kartashov Ya. Osobennosti diskretnogo modelirovaniya dinamicheskikh obektov [Features of discrete modeling of dynamic objects]. *Vestnik Kemerovskogo gosudarstvennogo universiteta* [Bulletin of Kemerovo State University], 2010, no. 4 (44), pp. 63–67.

18. Maksimenko V. N., Yasyuk E. V. Osnovnyye podkhody k analizu i otsenke riskov informatsionnoy bezopasnosti [Basic approaches to the analysis and assessment of information security risks]. *Ekonomika i kachestvo sistem svyazi* [Economy and quality of communication systems], 2017, no. 2, pp. 42–48.