УДК 681.322

ОПТИМИЗАЦИЯ РЕШЕНИЙ ПО ЗАЩИТЕ СИТУАЦИОННОГО ЦЕНТРА ОТ ВНУТРЕННЕГО НАРУШИТЕЛЯ

Зангиев Таймураз Таймуразович
к.т.н., доцент
Институт информационных технологий и безопасности Кубанского государственного технологического университета, Краснодар, Россия

Левчук Екатерина Владимировна
Центр современных компьютерных технологий Кубанского Государственного Технологического Университета, Краснодар, Россия

В статье рассмотрено построение превентивной модели защиты ситуационного центра от внутреннего нарушителя в условиях ограниченности ресурсов

Ключевые слова: СИТУАЦИОННЫЙ ЦЕНТР, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, МОДЕЛЬ ВНУТРЕННЕГО НАРУШИТЕЛЯ, ТЕОРИЯ ИГР

UDC 681.322

OPTIMIZATION OF THE WAYS OF THE PROTECTION OF SITUATIONAL CENTER FROM THE INSIDERS

Zangiev Taymuraz Taymurazovich
Cand.Tech.Sci., associate professor
Institute of information technologies and security of the Kuban State Technological University, Krasnodar, Russia

Levchuk Ekaterina Vladimirovna
Center of modern computer technologies, Kuban State Technological University, Krasnodar, Russia

In this article, we have considered the procedures of the preventive protection model for situational centers from the insiders in the limited resources conditions

Keywords: SITUATIONAL CENTER, INFORMATION SECURITY, SECURITY MODELS, GAMES THEORY

Повышение интенсивности информационного обмена, необходимость оперативного и адекватного реагирования на сложные быстроменяющиеся ситуации, вызывает необходимость более широкого применения современных информационных технологий в системах управления. Процесс принятия решений в условиях дефицита времени актуализирует создание ситуационных центров (СЦ), основными задачами которого является мониторинг состояния объекта управления, прогноз развития ситуации, моделирование последствий управленческих решений. Большая часть бюджета, выделенная на создание СЦ, используется на оборудование и создание интеллектуальных информационных систем, а

формирование систем защиты производится на остаточные средства, поэтому задача разработки рекомендаций по обеспечению оптимального уровня защищенности в условиях ограниченности ресурсов становится весьма актуальной.

Функционирование типового ситуационного центра обеспечивают следующие основные компоненты [2]

1. Модуль мониторинга и анализа данных;
2. Модуль прогнозирования и планирования;
3. Модуль принятия решений;
4. модуль экспертной поддержки;
5. Подсистема управления и визуализации;
6. Подсистема информационной безопасности.

Схема взаимодействия основных внутренних заинтересованных сторон ситуационного центра приведена на рисунке 1.

К внутренним заинтересованным сторонам целесообразно отнести:

-команду, обеспечивающую сопровождение информационных систем СЦ - разработчики, системный администратор и администратор информационной безопасности;

-команду, принимающую управленческие решения – управленческая группа и лицо принимающее решение (ЛПР);

-команду, обеспечивающую подготовку решений – эксперты и аналитики.

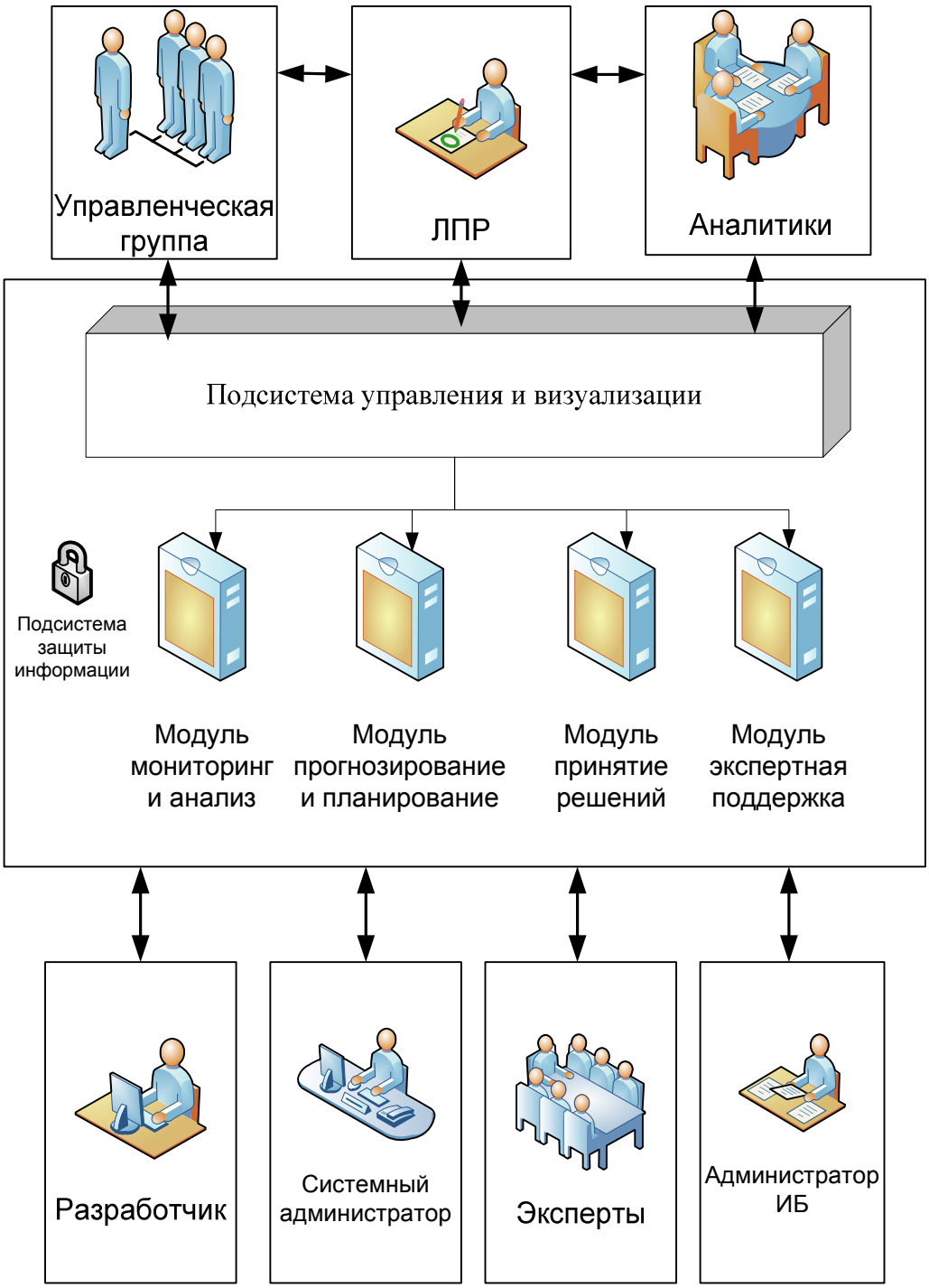

Рисунок 1- Схема взаимодействия основных внутренних заинтересованных сторон ситуационного центра.

В соответствии с [1] защита информации от утечки по техническим каналам, от несанкционированного доступа, от случайных и преднамеренных воздействий, нарушающих целостность информации, обрабатываемой оборудованием СЦ, обеспечивается с помощью

подсистемы информационной безопасности (ИБ), которая создается на основе действующих нормативно-методических документов и правовых актов в области информационной безопасности Российской Федерации.

В [1] предписывается всем проектировщикам при создании СЦ руководствоваться сводом норм, правил, процедур, практических приемов и руководящих принципов. При этом важным вопросом является оценка риска ИБ, которая включает анализ:

- вероятного ущерба, наносимого системе в результате нарушений ИБ с учетом возможных последствий от потери конфиденциальности, целостности или доступности информации и других активов;

- вероятности наступления такого нарушения с учетом существующих угроз и уязвимостей, а также внедренных мероприятий по управлению ИБ.

Как показано в [1], детальные анализы рисков позволяют проводить выбор обоснованных защитных мер, требования к которым фиксируются в политике ИБ, на основании которой разрабатывается концепция СЦ, технико-коммерческое предложение, а затем техническое задание (ТЗ). На этапе разработки ТЗ существует необходимость разработки частного технического задания на систему защиты информации (СиЗИ), разрабатываемой с учетом утвержденной политикой ИБ, которая содержит перечень угроз, модель нарушителя и оценку рисков ИБ.

В общем случае СиЗИ содержит в себе:

- организационно-режимные меры ЗИ;

- криптографические средства ЗИ;

- средства защиты от утечки информации по ТКУИ;

- средства ЗИ от НСД;

-средства ЗИ от уничтожения, защита от стихии, резервное копирование;

- средства ЗИ от программных вирусов и закладок;

- нормативную базу по ЗИ;

- меры по защите от угрозы внутреннего нарушителя.

Последняя угроза – затрудняет выбор мер по защите в связи с непредсказуемостью поведения инсайдера. При разработке базовой модели внутреннего нарушителя, следует учитывать максимум угроз, представленный в Таблице 1. При формировании частной модели внутреннего нарушителя, возможно изменение или добавление нарушителей в зависимости от целевых функций и конкретной конфигурации СЦ.

Таблица 1 – Базовая модель внутреннего нарушителя

Категория	Квалификация, техническая оснащенность	Характер возможных действий	Последствия	Контрмеры
К1. Пользователь ситуационного центра	Знает минимум о техническом оснащении и топологии СЦ, занимается сбором информации, моделирует проблемные ситуации, оценивает и оптимизирует принимаемые решения	Сбор информации некорректно, изменение информации при моделировании ситуации, субъективная оценка управленческих решений	Искажение проблемной ситуации, принятие неправильного решения	Р1. Параллельный сбор информации, сохранение её в базе данных при полном совпадении некоторых параметров
				Р2. Помощь нескольких экспертов, сравнение индивидуальных оценок и общей
К2. Разработчик программного обеспечения	Имеет право на создание и запуск собственных программ с новыми функциями по обработке информации, занимается разработкой ПО для обработки информации	Нарушение нормальной работы СЦ, внесение программных закладок, ошибок, разрушение информации, информационной модели	Потеря конфиденциальной информации	Р3. Проверка целостности ПО, обрабатывающего информацию, моделирующего ситуацию, проверка получившейся модели
				Р4. Проверка ПО на наличие программных закладок, ошибок.

Продолжение таблицы 1 – Базовая модель внутреннего нарушителя

Категория	Квалификация, техническая оснащенность	Характер возможных действий	Последствия	Контрмеры
К3. Системный администратор	Управление функционированием СЦ, воздействие на базовое ПО системы, и на конфигурацию оборудования	Нарушение нормальной работы СЦ	Выход из строя программно-аппаратного обеспечения	Р5. Проверка целостности системы и отдельных подсистем, программных продуктов
К4. Администратор информационной безопасности	Специалист высшей квалификации, обладает полными правами и знаниями о системе СЦ и средствах защиты	Нарушение работы СЦ, отключение средств защиты	Возникновение уязвимости системы	Р6. Установка комплексных систем защиты информации (СЗИ), предотвращающих вторжения, отключение, модификацию СЗИ

При неизвестном поведении внутреннего нарушителя, ситуацию можно описать как модель с нечеткими исходными данными. Мероприятия по предотвращению реализации угроз требуют ресурсов, поэтому необходимо определить, на что обратить особое внимание, чтобы снизить риски реализации угроз. Описанная ситуация рассматривается «игра с природой», и ее решение возможно получить с использованием алгоритмов теории статистических решений. Для этого необходимо определить возможный выигрыш. За выигрыш здесь принята вероятность реализации угрозы, причем ниже вероятность, тем соответственно выигрыш больше. Выигрыш целесообразно оценить в условных единицах от 1 до 3. Выигрыш при каждой паре стратегий оценивается эффективностью каждой из стратегий против угрозы: угроза неосуществима – 3; угроза частично реализуема – 2; угроза реализуема полностью – 1 и задан матрицей (таблица 2), где $К_j$ – действия нарушителя, $Р_i$ – стратегия поведения (рекомендации).

Таблица 2 - Матрица выигрышей.

P_i \ K_j	K_1	K_2	K_3	K_4
P_1	3	1	1	1
P_2	3	1	1	1
P_3	2	3	2	2
P_4	1	3	2	2
P_5	1	3	3	2
P_6	1	2	2	3

Матрица игры показана в таблице 3, в дополнительном правом столбце приведен – минимум выигрыша из каждой строки, а в дополнительной нижней строке – максимум выигрышей из столбцов.

Таблица 3 - Матрица игры.

P_i \ K_j	K_1	K_2	K_3	K_4	α_i
P_1	3	1	1	1	1
P_2	3	1	1	1	1
P_3	2	3	2	2	2
P_4	1	3	2	2	1
P_5	1	3	3	2	1
P_6	1	2	2	3	1
β_j	3	3	3	3	

Согласно принципу максимина, оптимальной стратегией является P_3, Уточнить оптимальную стратегию, можно руководствуясь критерием min риска Сэвиджа, для этого составляется матрица риска (таблица 4). Риском [3] игрока P при пользовании стратегией P_i в условиях K_j названа разность между выигрышем, который был бы получен, если бы были известны условия K_j, и выигрышем, который был бы получен, при неизвестных условиях и выборе стратегии P_i.

Таблица 4 – Матрица риска.

P_i \ K_j	K_1	K_2	K_3	K_4
P_1	0	2	2	2
P_2	0	2	2	2
P_3	1	0	1	1
P_4	2	0	1	1
P_5	2	1	0	1
P_6	2	0	1	0

По данному критерию доминирует стратегия P_3, так как риск при ней минимален, что позволяет определить начальную стратегию.

Итак, определилась начальная стратегия поведения, к реализации которой можно приступать, и в дальнейшем осуществляется переход к методу решения конечной игры, который позволит определить наиболее вероятные угрозы со стороны нарушителей; конкретизировать модель защиты и определить смешанную стратегию поведения (таблица 5).

Рассчитывается первые десять шагов итерационного процесса по методу Брауна – Робинсон, с началом стратегии P_3. В первом столбце – номер партии (пары выборов) h, во втором – номер i выбранной в данной партии стратегии игрока Р.

В последующих четырех столбцах – «накопленный выигрыш» за первые h партий при тех стратегиях, которые применяли игроки в предыдущих партиях и при стратегиях K_1, K_2, K_3, K_4 игрока К в данной партии (получается прибавлением элементов соответствующей строки к тому, что было строкой выше).

В последних трех столбцах даны: $\underline{\upsilon}$ – нижняя оценка цены игры, равная минимальному накопленному выигрышу, деленному на h, υ – верхняя оценка цены игры, равная максимальному выигрышу, деленному на h, υ^* - среднее арифметическое между ними (лучшая, приближенная оценка цены игры).

Таблица 5 – Итерационный процесс по методу Брауна-Робинсона

h	i	K_1	K_2	K_3	K_4	j	P_1	P_2	P_3	P_4	P_5	P_6	$\underline{\upsilon}$	υ	υ^*
1	3	3	1	1	1	2	1	1	3	3	3	2	1	3	2
2	3	5	4	3	3	3	2	2	5	5	6	4	1,5	3	2,25
3	5	6	7	6	5	4	3	3	7	7	8	7	1,67	2,67	2,17
4	5	7	10	9	7	1	6	6	9	8	9	8	1,75	2,25	2
5	3	9	13	11	9	1	9	9	11	9	10	9	1,8	2,2	2
6	3	11	16	13	11	1	12	12	13	10	11	10	1,83	2,17	2
7	3	13	19	15	13	1	15	15	15	11	12	11	1,86	2,14	2
8	1	16	20	16	14	4	16	16	17	13	14	14	1,75	2,13	1,9
9	3	18	23	18	16	4	17	17	19	15	16	17	1,78	2,1	1,34
10	3	20	26	20	18	4	18	18	21	17	18	20	1,8	2,1	1,95

Подсчитаем по таблице 5 частоты стратегий игроков:

$p_1 = 1/10 = 0,1$, $p_2 = 0/10 = 0$, $p_3 = 7/10 = 0,7$, $p_4 = 0/10 = 0$, $p_5 = 2/10 = 0,2$, $p_6 = 0/10 = 0$

$q_1 = 4/10 = 0,4$, $q_2 = 1/10 = 0,1$, $q_3 = 1/10 = 0,1$, $q_4 = 4/10 = 0,4$

Итак, применение смешанной стратегии 1, 3 и 5 позволит предотвратить все угрозы. Программные продукты, позволяющие реализовать параллельный сбор информации; проверку целостности программного обеспечения, обрабатывающего информацию, моделирующего ситуацию; контрольную проверку получившейся модели; проверку целостности отдельных подсистем и системы в целом, потребуют меньших затрат, чем весь комплекс и могут обеспечить требуемый уровень защищенности.

Предложенный подход позволяет при наличии информации о конфигурации СЦ, штатном расписании и функциональных обязанностях работников обеспечить приемлемый уровень защищенности от внутреннего нарушителя в условиях ограниченных ресурсов.

Список использованной литературы:

1. Ильин Н.И., Демидов Н.Н., Новикова Е.В./Ситуационные центры. Опыт, состояние, тенденции развития.-М.:Медиапресс, Москва, 2011. – С. 96, 255-256.

2. Симанков, В.С. Разработка теоретических основ и построение интеллектуальных систем мониторинга, анализа и поддержки принятия политических, социально-экономических и технологических решений регионального уровня для ситуационных центров органов власти/ В.С. Симанков, А.П. Редько, А.Н.Черкасов и др. // Матер. конф. получателей грантов регион. конкурса РФФИ. – Краснодар: ООО «Просвещение - Юг», 2008. – С. 176 –177.

3. Вентцель Е.С./Исследование операций: задачи, принципы, методология: учеб. пособие.-5-е изд., стер. – М.:КНОРУС, 2010. – С. 173-186.