УДК 004.056

**А.Ю. Урзов, С.К. Варлатая**

# Модель защищенной информационной системы на основе автоматизации процессов управления и мониторинга угроз безопасности

Рассмотрена проблема угроз, связанных с действиями администратора защищенной информационной системы, предложено ее решение путем автоматизации процессов управления информационной безопасностью, основанной на включении в состав защищенной информационной сети модулей унификации и автоматической обработки информации и принятия решений, работающих по протоколу автоматизации SCAP.

**Ключевые слова:** автоматическое управление безопасностью, защита информационных систем, информационная безопасность, SCAP.

Современные подходы к созданию защищенных информационных систем (ЗИС) основываются на принципе комплексности – использовании в составе ЗИС взаимосвязанных между собой различных средств защиты информации и централизованном их управлении. Такие системы устойчивы к внешним и внутренним угрозам и хорошо справляются со своими задачами. Тем не менее у современных ЗИС существуют и слабые места, о которых речь пойдет ниже. Целью данного исследования является определение актуальных проблем защищенных информационных систем и предложение их решения в виде модели ЗИС с автоматизацией процессов управления и мониторинга угроз безопасности.

В процессе функционирования ЗИС предприятия возникает огромное количество событий безопасности. Даже правильно настроенное отдельно взятое средство защиты в сутки может регистрировать сотни «нештатных» событий, но из них лишь малый процент представляют действительную опасность. В централизованной системе защиты обязательно настраивается аудит событий на всех автоматизированных рабочих местах (АРМ) и сетевом оборудовании с занесением информации в журнал безопасности на сервере для дальнейшего анализа. Просмотром этого журнала занимается администратор безопасности, на основании полученных данных он создает и корректирует правила безопасности для каждого конкретного устройства или программы. Этот механизм имеет как минимум 2 слабых места:

1. Наличие человеческого фактора. Огромное количество записей журнала событий, которые администратор безопасности должен просматривать и анализировать, делают его работу рутинной, и это в большой степени влияет на качество его работы: могут остаться неучтенные события, представляющие наибольшую опасность, а также велик риск принятия неправильных решений в создании правил безопасности. Это в свою очередь создает потенциальную опасность для секретной и конфиденциальной информации, хранящейся и обрабатываемой в системе, или же может повлиять на удобство работы пользователей.

2. Отсутствие унифицированности описания ошибок, генерируемых различными СЗИ, уязвимостей, настроек безопасности. Этот фактор также усложняет управление системой защиты ЗИС, отсекая возможность полной автоматизации этого процесса.

Теперь стоит рассмотреть угрозы, связанные с человеческим фактором, на фоне других распространенных угроз. Согласно [1, 5–8], одними из основных являются угрозы, связанные с наличием недекларированных возможностей (НДВ) в системном и/или прикладном программном обеспечении (ПО), внедрением вредоносных программ, выявлением паролей и др. Теперь наряду с ними учтем также такие угрозы, как «некомпетентные действия администратора по настройке средств защиты информации (СЗИ)» и «преднамеренное внесение изменений в настройки СЗИ администратором», и определим их действительную опасность.

Согласно методике ФСТЭК России [2], актуальность угроз определяется следующим образом. Вначале рассчитываются вероятность реализации и опасность угрозы. Вероятность (Y2) может принимать значения: 0 (маловероятная), 2 (низкая вероятность), 5 (средняя вероятность) и 10 (высокая

вероятность). Опасность угрозы принимает значения: «низкая», «средняя» и «высокая». Оба параметра определяются экспертным путем.

Далее вычисляется коэффициент реализуемости угрозы $Y$ по формуле

$$Y = (Y_1 + Y_2)/20, \quad (1)$$

где $Y_1$ – показатель исходной защищенности информационной системы (ИС), зависящий от ее технических и эксплуатационных характеристик. Он может принимать значения 0 (для высокой степени исходной защищенности), 5 (для средней степени) и 10 (для низкой степени). Для данной ИС этот показатель примем равным 5. По значению коэффициента реализуемости угрозы $Y$ формируется вербальная интерпретация реализуемости угрозы: «низкая» ($0 \le Y \le 0{,}3$), «средняя» ($0{,}3 \le Y \le 0{,}6$), «высокая» ($0{,}6 \le Y \le 0{,}8$), «очень высокая» ($0{,}8 < Y$).

Рассчитав возможность реализации угрозы $Y$ и ее опасность, можно определить ее актуальность по табл. 1.

Таблица 1

**Определение актуальности угроз**

| Возможность реализации угрозы | Показатель опасности угрозы | | |
|---|---|---|---|
| | Низкая | Средняя | Высокая |
| Низкая | Неактуальная | Неактуальная | Актуальная |
| Средняя | Неактуальная | Актуальная | Актуальная |
| Высокая | Актуальная | Актуальная | Актуальная |
| Очень высокая | Актуальная | Актуальная | Актуальная |

Конечные данные о расчетах актуальности угроз безопасности рассматриваемой ИС сведены в табл. 2. Названия угроз сокращены и идут по порядку в соответствии со списком выше.

Таблица 2

**Актуальность угроз безопасности данных**

| № п/п | Угроза безопасности ПДн | Коэффициент вероятности реализации угрозы ($Y_2$) | Коэффициент реализуемости ($Y$) | Возможность реализации | Опасность | Актуальность |
|---|---|---|---|---|---|---|
| 1 | НДВ | 0 | 0,25 | Низкая | Низкая | – |
| 3 | Вредоносные программы | 0 | 0,25 | Низкая | Низкая | – |
| 4 | Выявление паролей | 2 | 0,35 | Средняя | Средняя | + |
| 5 | Некомпетентные действия администратора | 2 | 0,35 | Средняя | Высокая | + |
| 6 | Преднамеренная настройка СЗИ | 2 | 0,35 | Средняя | Высокая | + |

Как видно из табл. 2, последние две угрозы, связанные с действиями администратора, имеют высокую опасность и отмечены как актуальные, потому что фактически ничто (кроме мер ответственности и норм морали) не мешает администратору безопасности случайно или преднамеренно воздействовать на систему защиты таким образом, что увеличится риск возникновения иных угроз ИС. Для решения этой проблемы предлагается усовершенствовать систему защиты, автоматизировав процесс управления информационной безопасностью, т.е. частично или полностью отстранив администратора от участия. Специфика предлагаемого решения позволяет также установить согласованность функционирования различных средств защиты и обеспечить максимальную производительность всего комплекса.

На рис. 1 представлена типовая схема ЗИС, состоящей из автоматизированных рабочих мест пользователей АРМ ($1 – n$), межсетевого экрана МЭ, сервера безопасности СБ и АРМ администратора, который проводит мониторинг событий от систем защиты разных типов.

Усовершенствование существующей ЗИС осуществляется путем создания новых модулей автоматизации: модуля унификации и модуля автоматической обработки информации и принятия решений.

Компонент унификации представляет собой специальную программу, в задачи которой входит приведение уязвимостей и настроек безопасности различных СЗИ к единому стандарту по типовым формам. Использование средств защиты, поставляемых разными производителями, зачастую влечет за собой несогласованность их работы, сложность в настройке и т.д. Внедрение компонентов уни-

фикации позволит устранить эти проблемы. Компонент устанавливается на сервер безопасности и играет роль шлюза-преобразователя (рис. 2). Его задача – принять и в «прозрачном» режиме привести данные с АРМ и других устройств к утвержденному стандарту, чтобы отправить эти данные в блок автоматической обработки и принятия решений (БАОиПР).

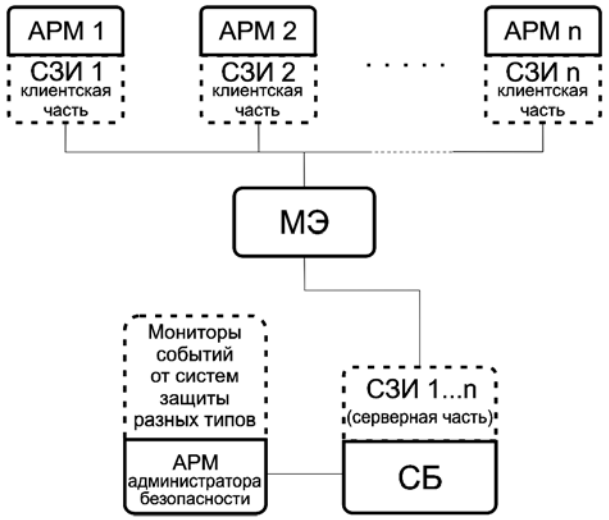


Рис. 1. Типовая схема ЗИС

Шлюз-преобразователь трансформирует описание команд блока принятия решений для отправки по схеме обратной связи на СЗИ. Команды содержат данные о необходимых изменениях настроек безопасности.

Для работы этого программного модуля требуются стандарты – типовые шаблоны для преобразования, в качестве которого предлагается протокол автоматизации контента безопасности SCAP (Security Content Automation Protocol) [4]. Протокол автоматизации SCAP разрабатывается Национальным институтом стандартов и технологий NIST и призван стандартизировать формат описания уязвимостей, автоматизировать процесс управления конфигурациями безопасности, обеспечить информационный обмен между пользователями и производителями средств защиты.

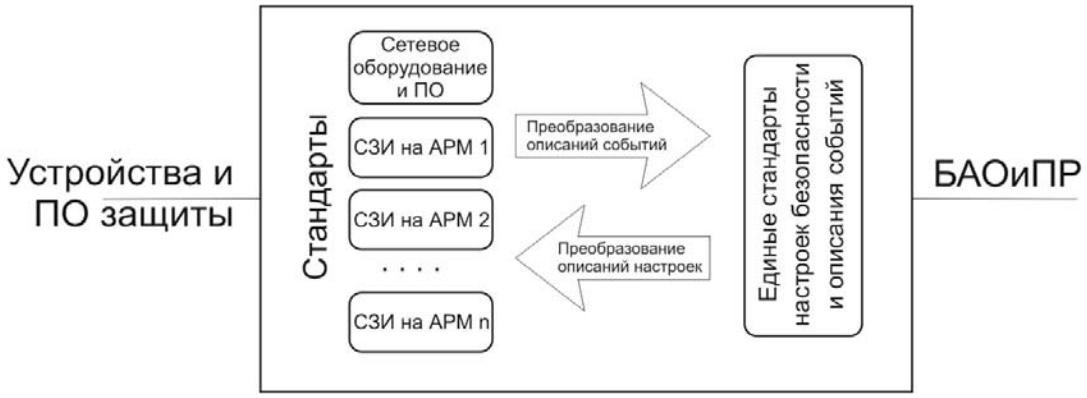


Рис. 2. Устройство шлюза-преобразователя

Использование SCAP выгодно по многим параметрам:

– имеется доступ к репозиторию SCAP-контента – большой базе сигнатур уязвимостей для наиболее распространенных программных и программно-аппаратных средств защиты, а также отправлять данные об уязвимостях из своей системы для анализа;

– наличие готовых конфигураций безопасности, разрабатываемых специализированными лабораториями на основе анализа уязвимостей;

– в проекте SCAP, имеющем статус международного, принимают участие специалисты в области ИБ во всем мире;

– ведущие мировые производители средств защиты в последних версиях своих продуктов уже предусматривают поддержку SCAP;

– SCAP содержит единые стандарты представления данных, основанные на лучших мировых практиках;

– наличие в SCAP встроенного открытого языка описания уязвимостей и проведения оценок OVAL (Open vulnerability and assessment language).

Международный статус проекта, его безусловные качества, описанные выше, и быстрый рост популярности также дают основание полагать, что использование протокола SCAP в очень скором времени станет «правилом хорошего тона» в информационной безопасности.

Второй модуль ЗИС – блок автоматической обработки информации и принятия решений. Это наиболее сложный элемент, поскольку в его функции входит анализ возникающих событий безопас-

ности в системе, самостоятельная оценка угроз, просчет рисков и автоматическая подстройка СЗИ в соответствии с заданными критериями безопасности, т.е. обеспечение адаптивности системы. Для настройки работы анализатора этого блока должен быть предусмотрен режим обучения. В качестве базы спецификаций уязвимостей используется собственная база и репозиторий SCAP, что позволяет эффективно обнаруживать и устранять угрозы. Подсистема анализа событий также умеет сопоставлять данные, полученные из разных источников, находить закономерности и связь между угрозами. Это дает возможность определять распределенные несанкционированные воздействия на систему и предугадывать примерный сценарий действий нарушителя.

Система с внедренными компонентами показана на рис. 3.

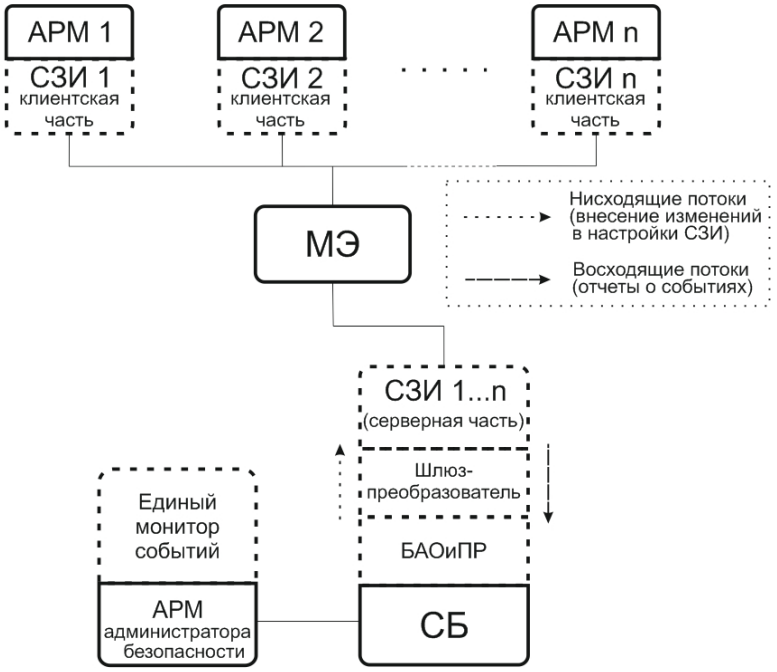


Рис. 3. Схема ЗИС с внедренными модулями автоматизации

Предложенная модель ЗИС с модулями автоматизации способствует решению проблемы угроз, обусловленных некомпетентными действиями и злоумышленным внесением изменений в настройки СЗИ администратором безопасности. Внедренные модули автоматизации процессов управления информационной безопасностью практически полностью исключают участие администратора безопасности в настройке системы защиты, и, таким образом, угрозы, связанные с его действиями, переходят в разряд неактуальных. В функции администратора обновленной системы входит лишь задание критериев безопасности для всей системы в соответствии с нормативной документацией на начальном этапе внедрения системы. Последующее изменение критериев должно строго документироваться и не осуществляться без крайней необходимости.

*Литература*

1. Специальный нормативный документ Федеральной службы по техническому и экспортному контролю Российской Федерации (ФСТЭК РФ) от 15 февраля 2008 г. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» [Электронный ресурс]. – Режим доступа: http://b-152.ru/npb/FSTEK_bazovaya_model_ugroz/, свободный (дата обращения: 01.03.2013).

2. Специальный нормативный документ Федеральной службы по техническому и экспортному контролю Российской Федерации (ФСТЭК РФ) от 14 февраля 2008 г. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» [Электронный ресурс]. – Режим доступа: http://b-152.ru/npb/FSTEK_metodika_opr_aktual_ugroz, свободный (дата обращения: 01.03.2013).

3. Montesino R. Automation Possibilities in Information Security Management / R. Montesino, S. Fenz – [Электронный ресурс]. – Режим доступа: http://www.sba-research.org/wp-content/uploads/publications/PID1947709.pdf, свободный (дата обращения: 25.02.2013).

4. The Security Content Automation Protocol (SCAP) [Электронный ресурс]. – Режим доступа: http://scap.nist.gov/, свободный (дата обращения: 03.03.2013).

5. Прищеп С.В. Подходы и критерии оценки рисков информационной безопасности / С.В. Прищеп, С.В. Тимченко, А.А. Шелупанов // Безопасность информационных технологий. – 2007. – № 4. – С. 15–21.

6. Оценка рисков информационной безопасности телекоммуникационной системы / А.А. Кускова, А.А. Шелупанов, Р.В. Мещеряков, С.С. Ерохин // Информационное противодействие угрозам терроризма. – 2009. – № 13. – С. 90–92.

7. Миронова В.Г. Реализация модели Take-Grant как представление систем разграничения доступа в помещениях / В.Г. Миронова, А.А. Шелупанов, Н.Т. Югов // Доклады Том. гос. ун-та систем управления и радиоэлектроники. – 2011. – № 2–3. – С. 206–210.

8. Миронова В.Г. Методология формирования угроз безопасности конфиденциальной информации в неопределенных условиях их возникновения / В.Г. Миронова, А.А. Шелупанов // Изв. Южного федерального ун-та. Технические науки. – 2012. – Т. 137, № 12. – С. 39–45.

---

**Урзов Александр Юрьевич**
Студент каф. информационной безопасности Дальневосточного федерального университета (ДВФУ), г. Владивосток
Тел.: +7-908-982-25-50
Эл. почта: verronyvl@gmail.com

**Варлатая Светлана Климентьевна**
Канд. техн. наук, профессор каф. информационной безопасности ДВФУ
Тел.: +7-924-244-40-33
Эл. почта: sk-varl@yandex.ru

Urzov A.Y., Varlataya S.K.

**Development of the model of secure information system (SIS) with automation of security assets management and monitoring**

The article shows the problem of assets associated with activity of an information security manager. We offer a solution by means of automation of management of security assets, which is based on the integration of special modules of unification and automated information processing and decision-making, working with the SCAP automation protocol.

**Keywords:** automatic security management, information system security, information security, SCAP.

---