УДК 004.056.5
ББК 30.1

ТИПОВАЯ СТРУКТУРА И СОСТАВ АДАПТИВНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ БОЛЬШОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Левкин И. М.[1],
(*Университет ИТМО, Санкт-петербург*)
Володина А. А.[2]
(*Университет ИТМО, Санкт-петербург*)

Целью работы является разработка рекомендаций по построению адаптивной комплексной системы защиты информации за счет определения типовой структуры и состава адаптивной системы защиты информации большой информационной системы. В ходе работы производился анализ типовых схем защиты информации предприятия, определение оптимального набора подсистем защиты информации для адаптивной системы защиты информации. На основании произведенного анализа представлена типовая адаптивная система защиты информации элемента информационной структуры государственной информационной системы. Также, в ходе работы, были выявлены актуальные угрозы, характерные для больших информационных систем. Благодаря произведенной работе осуществляется выработка рекомендаций по построению адаптивной комплексной системы защиты информации.

Ключевые слова: адаптация, информационная система, защита информации.

Для определения возможной структуры и состава средств, входящих в адаптивную систему защиты информации, необхо-

[1] *Игорь Михайлович Левкин*, *доктор военных наук*, *профессор* (*lev.kin@yandex.ru*).
[2] *Анастасия Андреевна Володина*, *аспирант Университета ИТМО* (*nasti.vol@gmail.com*).

димо опираться на типовую схему защиты информации предприятия.

Типовые системы защиты информации могут подразделяться на следующие виды:

- типовая система от угроз несанкционированного доступа (далее – СЗИ от НСД);
- типовая система защиты от угроз вредоносного кода;
- типовая система межсетевого экранирования и защиты каналов связи;
- типовая система анализа защищенности;
- типовая система обнаружения вторжения;
- типовая система мониторинга событий безопасности.

Рассмотрим каждую из них подробнее.

СЗИ от НСД, как правило, решает следующие задачи: производит разграничение доступа, регистрацию и учёт событий безопасности, обеспечивает целостность программно-аппаратной среды. В состав такой СЗИ могут входить различные средства, сертифицированные ФСТЭК России. К ним могут относиться средства централизованного управления средствами защиты от НСД, встроенные в системное программное обеспечение средства идентификации, аутентификации, авторизации, мониторинга событий и контроля целостности, средства удаленного администрирования, а также резервного копирования и восстановления конфигураций и различных параметров настроек.

Типовая система защиты информации от угроз вредоносного кода состоит из сервера управления антивирусным программным обеспечением (далее – ПО), антивирусного ПО, устанавливаемого на сервера и автоматизированные рабочие места (далее – АРМ) работников предприятия и АРМ администратора системы защиты от вредоносного кода. Компонентами такой системы могут являться средства антивирусной защиты информации (далее – АВЗИ) почтовой системы, файловых систем

АРМ и серверов, веб-трафика, обеспечивающие функции фильтрации данных и т. д.

Система межсетевого экранирования и защиты каналов связи включает в себя межсетевые экраны, пограничные маршрутизаторы (обеспечивают подключение к каналам связи внешних информационных систем, ограничения полосы пропускания для отдельных видов трафика, а также контроль доступа и фильтрацию сетевого трафика), сегментообразующие коммутаторы, криптошлюзы, а также АРМ администратора системы межсетевого экранирования и криптографической защиты каналов связи. Средства, включенные в данную СЗИ обеспечивают различные виды фильтрации (сетевого трафика, запросов на установление виртуальных соединений и др.), идентификация и аутентификация администратора при его локальных запросах на доступ по идентификатору, предотвращение доступа неидентифицированного пользователя, регистрация и учет фильтруемых пакетов и множество других функций.

Типовая система анализа защищенности представляет собой комплекс программно-технических и организационных решений, обеспечивающих функции обнаружения уязвимостей программно-аппаратной среды средств вычислительной техники. В такую систему, как правило, входят два сканера безопасности, один из которых сертифицированный, а второй – несертифицированный. Несертифицированный сканер информационной безопасности позволяет расширить функциональные возможности данной СЗИ и повысить уровень обнаружения уязвимостей в программно-аппаратной среде.

Функционирование системы обнаружения вторжений направлено на обнаружение сетевых атак на всех уровнях информационной структуры предприятия. В состав системы входят средства обнаружения вторжений на уровне сети, на уровне операционных систем АРМ и серверов, на уровне сетевых узлов, а также АРМ администратора системы обнаружения вторжений.

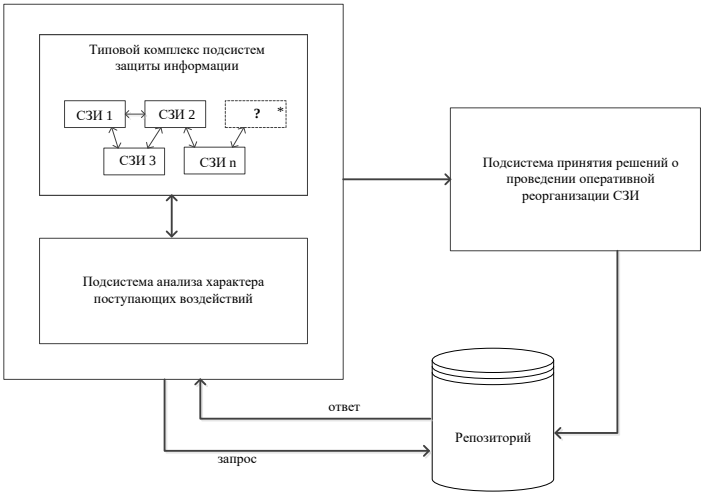
Система централизованного мониторинга событий безопасности информационной системы предназначена для ведения комплексного контроля процессов функционирования систем-

ного и прикладного программного обеспечения применяемых в данной системе средств вычислительной техники и обеспечивает выполнение функций активного и пассивного мониторинга состояния программно-аппаратной среды. Система включает в себя сенсоры регистрации событий безопасности, сервер системы мониторинга, один или несколько серверов файлов регистрации, протоколов и журналов событий.

Таким образом, комплексная система защиты информации (далее – КСЗИ) предприятия должна включать в себя одну или несколько подсистем защиты информации, обеспечивающих сохранность свойств безопасности информации, в зависимости от сложности информационной структуры предприятия.

Адаптивная СЗИ будет включать в себя комплекс подсистем информационной безопасности, а также специальные базы данных (репозитории), аккумулирующие сведения о поступлении новых информационных воздействий на элементы информационной структуры предприятия, подсистему анализа характера поступающих воздействий и подсистему принятия решений о проведении оперативной реорганизации СЗИ.

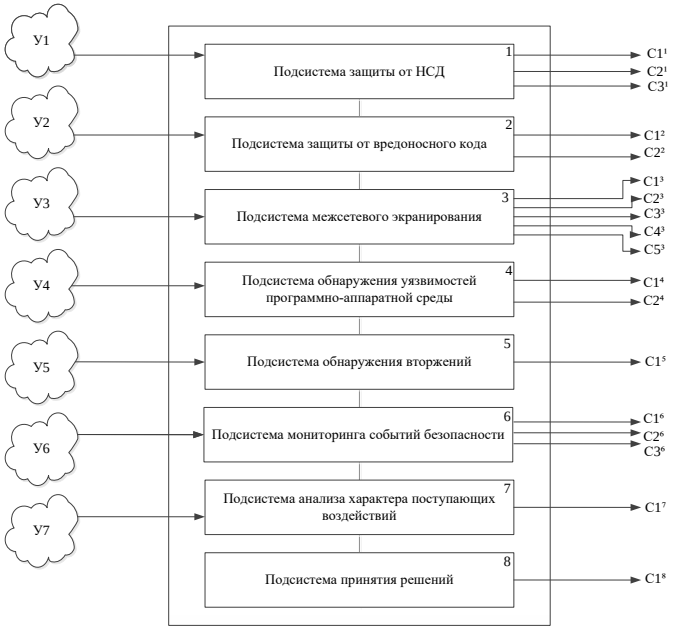
Представим, в качестве примера, типовую адаптивную СЗИ элемента информационной структуры государственной информационной системы. Пример адаптивной СЗИ представлен на рисунке 1.



? - Неопределенная СЗИ, включаемая в комплекс подсистем в случае возникновения новой информационной угрозы на отражение которой в комплексе нехватает существующих сил и средств

Рисунок 1 - Типовая адаптивная СЗИ

Учитывая специфику, присущую большим информационным системам, обладающим рядом важных свойств сложных систем, а также опираясь на приказ ФСТЭК №21 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», можно сделать вывод, что адаптивная СЗИ, имеющая уровень значимости информации УЗ1 и класс защищенности К1, будет включать в себя следующие подсистемы защиты информации, представленные на рисунке 2.



Список сокращений:
У1-У7 – угрозы ГИС;
Сп¹ -Сп⁸ - средство защиты информации.

Рисунок 2 - Состав и структура адаптивной системы защиты информации государственной информационной системы

Рассмотрим угрозы, характерные для государственных информационных систем.

У1 – в качестве угроз, отражаемых подсистемой защиты информации от НСД могут выступать угрозы, связанные с несанкционированным доступом к ГИС, копированием, модификацией информации, несанкционированным использованием терминалов пользователей, имеющих уникальные физические характеристики и прочие несанкционированные действия, направленные на дестабилизацию работы ГИС.

У2 – в данную группу попадают угрозы, связанные с внедрением вредоносных кодов, программных «закладок», специ-

альных взносов, а также угрозы, возникающие в случае использования ПО с недекларированными возможностями.

У3 – подсистема межсетевого экранирования должна выполнять функции, обеспечивающие отражение угроз типа «отказ в обслуживании», а также выполнять защиту сегментов сети или отдельных хостов от НСД.

У4 – к таким угрозам будут относиться дестабилизирующие воздействия, реализуемые через уязвимости в программно-аппаратной среде средств ВТ.

У5 – под данными угрозами понимаются сетевые атаки, производимые на всех уровнях информационной структуры предприятия.

У6 – угрозы, связанные с процессами функционирования системного и прикладного программного обеспечения.

У7 – подсистема характера поступающих воздействий должна отслеживать угрозы всех типов У1-У6.

Средства зашиты информации, включаемые в подсистемы адаптивной СЗИ государственной информационной системы, должны отвечать классу защищенности К1 и осуществлять своевременное предупреждение и предотвращение угроз информационной безопасности. В качестве средств защиты информации $С1^1$-$С3^1$ могут выступать такие решения, как комплексные системы для защиты рабочих станций и серверов на уровне данных, приложений, сети, операционной системы и периферийного оборудования, например Secret Net Studio и другие решения, являющиеся сертифицированными средствами защиты информации, входящими в реестр сертифицированных средств ФСТЭК России. $С1^2$, $С2^2$ могут быть представлены средства АВЗИ "Лаборатории Касперского" и "Доктор Веб". В подсистему межсетевого экранирования могут быть включены различные средства, например АПКШ "Континент", Security Studio Endpoint Protection и другие средства. Средства защиты информации, включаемые в подсистемы 3-6 также могут быть выбраны из реестра сертифицированных средств защиты информации.

В качестве средства защиты информации $С1^7$ должно выступать средство распознавания угроз, в том числе по сигнату-

рам и аномалиям в протоколах и трафике. Данное средство должно обеспечивать мониторинг трафика, анализ протоколов и автоматическое реагирование, за счёт точного распознавания угроз доля успешных атак будет резко уменьшена.

Для подсистемы принятия решений должно быть разработано программное средство для автоматизации поддержки принятия решений. Не смотря на то, что авторами И.В. Бондарем; А.В. Гуменниковой, к.т.н.; В.В. Золотарёвым, к.т.н.; А.М. Поповым, д.ф.-м.н., была представлена работа «Система поддержки принятия решений по защите информации «Оазис»», на настоящий момент на рынке сертифицированных средств защиты информации не представлено ни одного продукта из такой линейки. Такое средство должно решать задачи поддержки принятия решений при анализе и синтезе существующих подсистем защиты информации и входящих в них средств защиты информации.

Исходя из произведенного анализа можно сделать вывод, что при формировании состава и структуры адаптивной СЗИ большой информационной системы необходимо опираться на данные проведенных предпроектных обследований, специфику большой информационной системы, обрабатываемые в ней данные, их актуальность, насколько они интересны злоумышленникам, учитывать размах информационной системы, а также опираться на базовую модель КСЗИ предприятия.

Литература

1. АЛЕКСАНДРОВ А. Г. О*птимальные и адаптивные системы: Учеб. пособие для вузов по спец. «Автоматика и упр. в техн. системах»* // М.: Высш. шк, 1989. — 263 с.
2. ВОЛОДИНА А.А. *Алгоритм выбора рациональной структуры системы защиты информации предприятия* // сборник трудов международной конференции “Проблемы управления безопасностью сложных систем” - 2016. - С. 158-161.

3. ВОЛОДИНА А.А., ЛЕВКИН И.М. *Модель формирования информационных угроз информационной структуры предприятия* // Региональная информатика (РИ-2016): Материалы конференции (Санкт-Петербург, 26-28октября 2016г.) - 2016. - С. 252.
4. КОЗЕНКО З.Н., РОГАЧЁВ А.Ф., НАХШУНОВ А.Л., КАРАПУЗОВ И.А. *Поддержка принятия управленческих решений: инструментально-информационное обеспечение* // Козенко З.Н., Рогачёв А.Ф., Нахшунов А.Л., Карапузов И.А.; Под. ред. Рогачёва А.Ф. — Волгоград: Изд-Во Волгоградского Государственного Университета,2001. — 124 С. 2001.
5. ЛЕВКИН И.М., ВОЛОДИНА А.А. *Агрегированная операционно-временная модель оценивания эффективности отражения информационных угроз в больших информационных системах* // Известия высших учебных заведений. Приборостроение - 2016. - Т. 59. - № 5. - С. 335-341
6. ПЕТУХОВ Г.П., ЯКУНИН В.И. *Методологические основы внешнего проектирования целенаправленных процессов и целеустремленных систем* // Г.Б. Петухов, В.И. Якунин. – М.: АСТ, 2006.
7. СРАГОВИЧ В.Г. «*Теория адаптивных систем»*. – 1976. – 320 с.
8. *Приказ ФСТЭК России от 18 февраля 2013 г. N 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»* / Федеральная служба по техническому и экспертному контролю. URL: http://fstec.ru/normotvorcheskaya/akty/53-prikazy/691-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21 (дата обращения: 27.03.2017).
9. https://iitrust.ru/region/vpn/primery/ (дата обращения: 15.03.2017.

THE TYPICAL STRUCTURE AND COMPOSITION OF THE ADAPTIVE INFORMATION SECURITY SYSTEM OF THE BIG INFORMATION SYSTEM

Anastasia Volodina, ITMO University, Saint-Petersburg, Graduate Student (nasty.vol@gmail.com).
Igor Levkin, , ITMO University, Saint-Petersburg, Doctor of Military Science, professor (lev.kin@yandex.ru).

Abstract: *The aim of the article is development of recommendations how to make an adaptive complex information security system by dint of the definition of the typical structure and composition of the adaptive information security system of the big information system. During the science working an analysis of the typical information security systems was carried and the definition of the optimal set of information protection subsystems for the adaptive information security system was carried too. The typical adaptive information security system of the element from information structure of the Government information system was developed by based on the analysis. Moreover, the typical composition and structure of the adaptive information security system of the Government information system was developed. Also, during the science working, the actual information security threats for big information systems were revealed. Owing to the performed work the development of recommendations how to make an adaptive complex information security system is carried out.*

Keywords: adaptation, information system, information security.

Статья представлена к публикации
членом редакционной коллегии ...заполняется редактором…

Поступила в редакцию ...заполняется редактором…
Опубликована ...заполняется редактором…