УДК 004.056 DOI: 10.34759/trd-2020-110-16

Модель интеллектуального детектора системы защиты автоматизированной системы управления

Соломатин М.С.*, Митрофанов Д.В.**

Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н.Е. Жуковского и Ю.А. Гагарина»,

ул. Старых Большевиков, 54а, Воронеж, 364064, Россия,

**e-mail: newmihei@gmail.com*

***e-mail: mitrofanovd@mail.ru*

Статья поступила 10.06.2019

Аннотация

В статье рассматривается информационная безопасность автоматизированных систем, в частности автоматизированных систем управления. В качестве одного из методов защиты от несанкционированного доступа предлагается использовать интеллектуальный детектор информационной системы. Дано авторское определение интеллектуального детектора информационной системы. Представлена функциональная модель и структурная схема интеллектуального детектора информационной системы. Описаны требования к интеллектуальному детектору информационной системы. Представленное описание интеллектуального детектора автоматизированной системы управления позволяет создать его программную реализацию.

Ключевые слова: автоматизированная система управления, информационная безопасность, информационная система, безопасность информационных систем,

интеллектуальный детектор автоматизированной системы управления.

Введение

В настоящее время развитие информационных технологий, появление новых угроз информационной безопасности информационных систем, например, автоматизированных систем управления каким-либо процессом, а также с повышением требований к защищенности данных привело к тому, что необходимо создавать или постоянно модернизировать существующие системы защиты информации.

Угрозы целостности, доступности и конфиденциальности информации к хранящимся и обрабатываемым данным в автоматизированных системах управления (АСУ) могут привести к потере престижа организации, финансовым проблемам, угрозам защиты государственной и корпоративной тайне и т.д.

Как отмечено в работе [1] «одним из способов повышения безопасности автоматизированных систем является предотвращение появления новых уязвимостей, которые могут появляться, например, при неправильной конфигурации системы в результате неквалифицированных действий администратора, либо преднамеренного взлома системы».

На этапе организации несанкционированного доступа к защищаемой сети, одной из задач является нарушение внешнего периметра системы защиты информации (СЗИ), реализуемое посредством применения компьютерных атак. Сетевая компьютерная атака – заранее спланированное целенаправленное воздействие на определенные объекты компьютерных сетей программными и

аппаратными средствами через установление соединения на сетевом уровне или попытки установления соединения на канальном или сетевом уровне с объектом данного воздействия. Цель атаки – организация канала утечки информации, блокирование, модификация, уничтожение информационных ресурсов, блокирование СЗИ объекта [1, 2].

К основным первичным задачам любой системы защиты можно отнести сбор статистической информации о работе системы и действиях пользователя, а также выявление атак по каким-либо признакам. К таким признакам относятся цикличность определенных событий или действия, какие-либо аномалии в работе программ и т.д. В настоящее время выделяется два основных метода обнаружения атак: сигнатурный метод и метод обнаружения аномалий [3].

Основным достоинством сигнатурного метода является высокая точность обнаружения известных типов атак. Однако сигнатурный метод не может применяться для обнаружения неизвестных атак. Эту проблему позволяет решить метод обнаружения аномалий, однако такие методы характеризуются высоким количеством ложных срабатываний, когда незначительное отклонение от обычной работы системы может вызвать срабатывание системы защиты.

Становится понятно, что традиционные методы обнаружения атак не позволяют достичь оптимальных характеристик обнаружения внутренних атак. Анализ показывает, что достаточно перспективным является построение систем обнаружения атак на основе технологий искусственных иммунных систем [4]. Этот метод обладает рядом преимуществ по сравнению с другими методами,

обеспечивая:

– высокую скорость работы;

– сравнительно простой алгоритм обучения;

– низкую ресурсоёмкость.

Как следствие искусственных иммунных систем перспективным направлением исследований в области защиты информации автоматизированных систем является разработка средств «интеллектуального детектора» [5-7]. Для дальнейшей программной реализации и внедрения в автоматизированные системы управления необходимо описать требования, которые будут предъявляться к интеллектуальному детектору, основные элементы интеллектуального детектора основные функции его работы.

Интеллектуальный детектор информационной системы

Под автоматизированной системой управления (АСУ) будем понимать комплекс средств автоматизации, который включает в себе как программную, так и аппаратную части, а также персонал, предназначенный для управления различными процессами [8].

Под аудитом с точки зрения информационной безопасности будем понимается «независимая оценка текущего уровня состояния информационной безопасности системы» [6].

Под «интеллектуальным детектором» (ИД) будем понимать систему, которая функционирует в режиме реальном времени, защищает от несанкционированного доступа путем автоматического обнаружения внешних/внутренних воздействий или

угроз и вырабатывает соответствующее решение с целью их ликвидации или их замедления.

К возможным требованиям, предъявляемым к системе интеллектуального детектора с целью обнаружения несанкционированного доступа, на наш взгляд, можно отнести:

1. Объективность (достоверность) результата – доказательства того, что уязвимости существуют в информационной системе, а также возможность детально описать последствия их действий.

2. Полнота описания возможных уязвимостей системы.

3. Общепризнанность критериев оценки защищенности. Использование простых и понятных критериев оценки защищенности информационной системы.

Функции системы интеллектуального детектора можно разделить на внешние (выявление и пресечение атак) и внутренние (выявление и устранение уязвимостей). Схематично функции представлены на рисунке 1.

К основным функциям работы интеллектуального детектора мы будем относить следующие:

1. Наличие четкого описания модели нарушителя, в рамках которого будет функционировать система. В качестве нарушителя могут выступать как внутренне сотрудники, так и любой злоумышленник, пытающийся получить доступ к данной системе путем удаленного доступа. Уровень квалификации любого потенциального нарушителя системы всегда считается достаточно высоким для преодоления системы зашиты.

2. Анализ влияния выявленных уязвимостей на защищённость всей информационной системы в целом.

3. Поиск новых уязвимостей.

4. Применение методов социальной инженерии для имитации действий потенциального нарушителя.

Рисунок 1. Функции интеллектуального детектора

С целью обнаружения факта несанкционированного доступа к системе и уведомления администратора интеллектуальный детектор информационной системы, по нашему мнению, должен выполнять следующие функции:

1. Осуществлять сбор информации, поступающей от системы (для обнаружения искажения имеющейся, обрабатываемой и хранящейся информации на рабочем месте/системе).

2. Обрабатывать поступившую информацию для выработки дальнейшего

решения (сравнение информации с хранящейся в банках данных с целью выявления нарушений политики безопасности).

3. Выявлять случаи нарушения политики безопасности (при отличии от информации, находящейся в банках данных необходимо выработать дальнейшее решение реакции системы на действия потенциального нарушителя).

4. Выработать соответствующие реакции системы на нарушения (происходит адекватные действия системы/администратора с целью ликвидации/устранения или замедления/блокирования данной угрозы).

Функциональная модель интеллектуального детектора представлена на рисунке 2. Для более наглядного отображения модель предлагается в виде модели IDEF0 [10, 11], в которой каждая операция представлена в виде функционального блока.

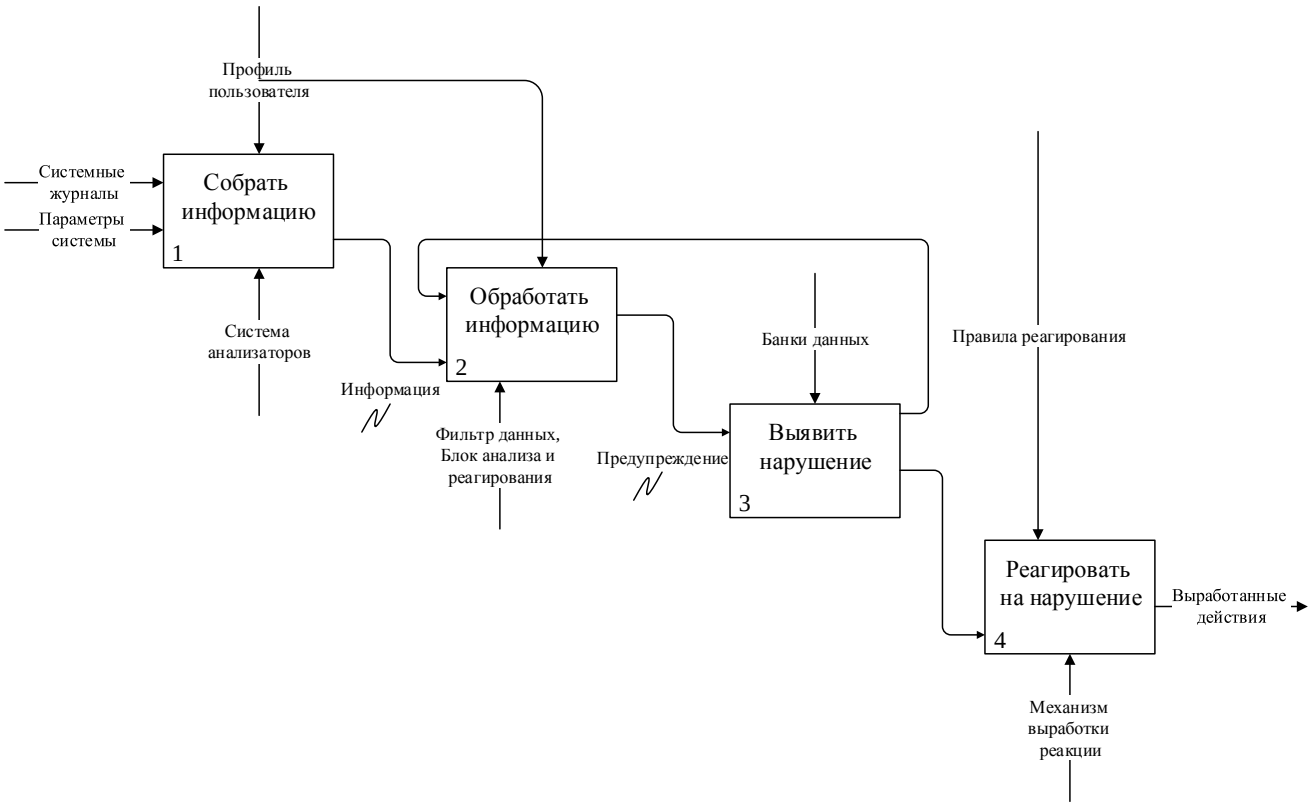

Рисунок 2 – Функциональная модель интеллектуального детектора

Достоинствами данного подхода к декомпозиции системы являются:

простота модели (наглядность);

возможность глубокой декомпозиции нужных блоков до необходимого уровня;

возможность выявления и управления всех обнаруженных недостатков системы еще на этапе проектирования.

Сбор информации включает в себя не только взаимодействие с системами сбора поступающей информации, но и помещение ее в банки данных с целью дальнейшей обработки, систематизации и хранения. В процесс обработки информации входит: получение обрабатываемого информационного блока из банков данных, его сравнении с информации из профиля пользователя, которая выступает в качестве эталонной и дальнейшей выработки соответствующих предупреждений.

Из представленной выше модели становится очевидно, что интеллектуальный детектор информационной системы, на наш взгяд, должен состоять из следующих элементов:

система входных анализаторов;

банки данных, хранящие всю необходимую информацию (эталоны, модели и другие параметры);

система обработки поступивших данных с входных анализаторов;

система реагирования, оказывающая прямое воздействие на информационную систему;

система журналирования для записи процессов, происходящих в информационной системе для хранения отчетов [12].

Структурно это можно представить в виде:

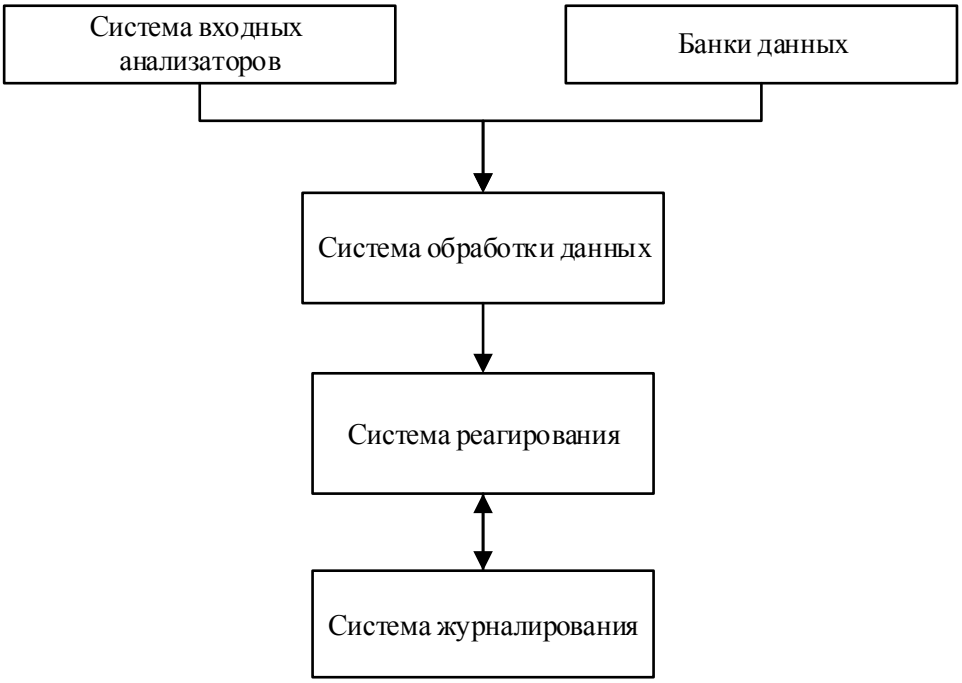

Рисунок 3 – Структурная схема интеллектуального детектора информационной системы

Система входных анализаторов предназначена для анализа параметров системы и действий пользователя или потенциального нарушителя, сравнения их с данными, хранящимися в банках данных, и формирования соответствующих предупреждений для системы обработки данных. Следующим шагом является выработка необходимых действий от системы реагирования. Все действия отражаются в системе журналирования для дальнейшего анализа и пополнения банков данных.

Примерная схема функционирования интеллектуального детектора для обнаружения несанкционированного доступа представлена на рисунке 4. Алгоритм работы следующий: на вход интеллектуального детектора по различным каналам от 1 до N поступает входная информация, которая проходит проверку на ее соответствие с информацией, хранящейся в банках данных. В случае обнаружения искажений либо выявления потенциальных угроз, которые могут нанести вред автоматизированной системе управления, происходит выработка адекватных действий системы/администратора с целью ликвидации/устранения или замедления/блокирования данной угрозы интеллектуальным детектором. При полном совпадении поступающей информации по различным каналам с имеющейся/хранящейся в банках данных информация поступает в автоматизированную систему управления для дальнейшей обработки.

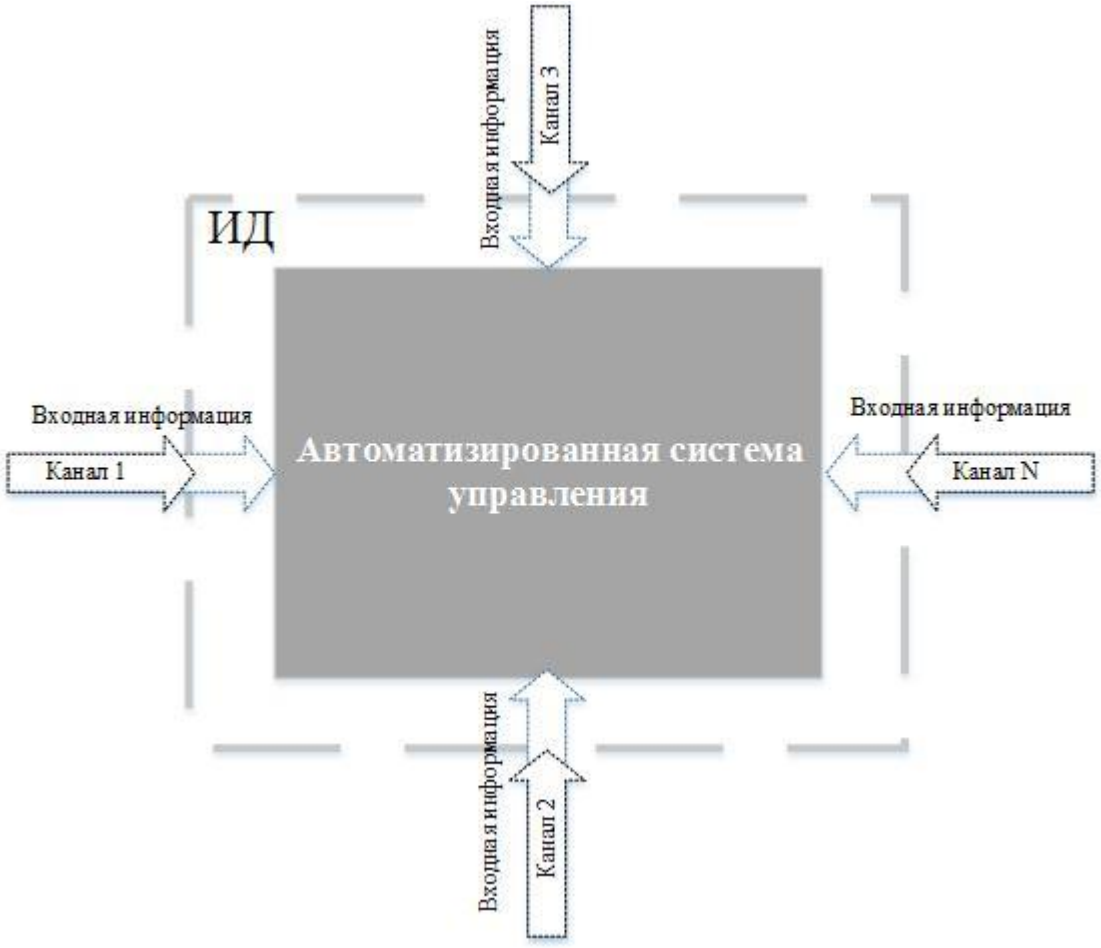

Рисунок 4 – Схема функционирования интеллектуального детектора

Выводы

Таким образом, с целью выявления (замедления, блокирования или устранения) несанкционированного доступа к автоматизированной системе управления и для повышения ее защищенности предлагается использовать интеллектуальный детектор. Приведенное авторское определение интеллектуального детектора автоматизированной системы управления позволило описать его функции, структуру и основные элементы, что позволит в дальнейшем программно реализовать интеллектуальный детектор и внедрить его в АСУ, что будет способствовать совершенствованию ее системы защиты.

Библиографический список

1. Бухарин В.В., Кирьянов А.В., Стародубцев Ю.И. Способ защиты информационно-вычислительных сетей от компьютерных атак // Труды МАИ. 2012. № 57. URL: http://trudymai.ru/published.php?ID=31145

2. Бухарин В.В., Кирьянов А.В., Стародубцев Ю.И., Трусков С.С. Метод обнаружения сетевого перехвата информационного трафика информационно-телекоммуникационной сети // Труды МАИ. 2012. № 57. URL: http://trudymai.ru/published.php?ID=31144

3. Мизина Е.Г. Особенности выявления и оценки информационных угроз // Безопасность информационных технологий. 1999. № 2. С. 57 - 59.

4. Мухамедиева Д.Т., Саманова М.М. Анализ применения искусственных иммунных систем для интеллектуальной обработки информации // Молодой ученый. 2016. № 18. С. 7 - 10.

5. Новиков А.А., Шарков А.Е., Сердюк В.А. Новые продукты активного аудита информационной безопасности // Тезисы докладов X юбилейной конференции «Методы и технические средства обеспечения безопасности информации», Санкт Петербург, 2002. С. 153 - 154.

6. Галатенко А.В. Активный аудит // Jet Info. 1999. № 8. С. 2 - 28.

7. Галатенко А.В. Защитные средства Intranet // Журнал сетевых решений/LAN. 1996. Т. 2. № 8. С. 14.

8. Литвиненко А.О. Программный комплекс автоматизированного планирования задействования средств наземного автоматизированного комплекса управления //

Труды МАИ. 2016. № 86. URL: http://trudymai.ru/published.php?ID=67829

9. Тузик С. Зачем проводить аудит информационных систем? // Jet Info. 2000. № 10. С. 8 - 16.

10. Шумский А.А., Шелупанов А.А. Системный анализ в защите информации. - М.: Гелиос АРВ, 2005. - 224 с.

11. Черемных С.В., Семенов И.О., Ручкин В.С. Моделирование и анализ систем. IDEF-технологии: практикум. - М.: Финансы и статистика, 1997. - 188 с.

12. Гураков М.А., Костюченко Е.Ю. Показатели качества систем распознавания пользователей по динамике подписи на основе наивного классификатора Байеса и нейронной сети // Труды МАИ. 2016. № 86. URL: http://trudymai.ru/published.php?ID=67851

13. Романчев И.В., Романчева Н.И. Методы защиты информации в АСУ // Труды международного симпозиума «Надежность и качество». 2010. Т. 2. С. 260 – 262.

14. Чернов Д.В., Сычугов А.А. Современные подходы к обеспечению информационной безопасности АСУ ТП // Известия Тульского государственного университета. Технические науки. 2018. № 10. С. 58 – 64.

15. Карантаев В.Г. Система защиты информации как составная часть АСУ ТП // Информатизация и системы управления в промышленности. 2017. № 2 (68). URL https://isup.ru/articles/2/11118/

16. Кульба В.В., Курочка Н.П. Математическая модель обеспечения безопасности информации в базах данных // Науковедение. 2015. Т. 7. № 3 (28). С. 108.

17. Никонов А.И., Павлов Н.О. Системы защиты информации и их место в политики

безопасности // Вестник Нижегородского государственного инженерно-экономического института. 2016. № 8 (63). С. 48 – 54.

18. Скрыпников А.В., Хвостов В.А., Чернышова Е.В., Самцов В.В., Абасов М.А. Нормирование требований к характеристикам программных систем защиты информации // Вестник Воронежского государственного университета инженерных технологий. 2018. Т. 80. № 4 (78). С. 96 – 110.

19. Пищук Б.Н. Безопасность АСУ ТП // Вычислительные технологии. 2013. Т. 18. № S1. С. 170 - 175.

20. Дудаков Н.С., Макаров К.В., Тимошенко А.В. Методика проектирования баз данных для автоматизированных систем управления специального назначения // Труды МАИ. 2016. № 90. URL: http://trudymai.ru/published.php?ID=74844