# РАЗРАБОТКА МОДЕЛИ ВЫЯВЛЕНИЯ УГРОЗ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ ВОЕННОГО НАЗНАЧЕНИЯ

**Д.В. Зимонин**[1], *канд. техн. наук, доцент*
**Е.В. Данилин**[1], *канд. техн. наук, доцент*
**А.А. Тимонов**[2], *заместитель председателя НТК*
**Д.В.Юмашев**[1], *курсант*
**А.А. Поповкин**[1], *курсант*
**А.А. Соловьев**[1], *курсант*
**[1]Краснодарское высшее военное орденов Жукова и Октябрьской Революции краснознаменное училище имени генерала армии С.М. Штеменко**
**[2]Научно-технический Комитет**
**[1](Россия, г. Краснодар)**
**[2](Россия, г. Москва)**

*DOI: 10.24411/2500-1000-2020-10195*

***Аннотация.*** *В статье рассмотрены проблемные вопросы выявления компьютерных инцидентов в сегменте автоматизированных систем военного назначения, нарушение работы которых приведет к подрыву национальной безопасности государства. Авторами предложена модель выявления угроз, позволяющая исследовать вероятность атак на всех уровнях возможного доступа к обрабатываемой информации с учетом этапов проведения компьютерных атак и фиксацией подозрительных отклонений в компьютерных системах на нескольких уровнях.*

***Ключевые слова:*** *автоматизированные системы Вооруженных Сил, компьютерные инциденты, компьютерные атаки, система обнаружения вторжений и атак, программно-аппаратные средства, информационные технологии.*

Принятие решений во всех сферах и на всех уровнях деятельности человека, страны и общества осуществляется с использованием информационных технологий. В этой связи существенно возрастает значение информационной безопасности, которая является важнейшим элементом национальной безопасности государств. Первостепенной задачей в области безопасности информации является своевременное выявление и предупреждение инцидентов на критически важных сегментах информационной инфраструктуры России.

Информационная безопасность регламентируется международными стандартами. Российские стандарты и рекомендации также обеспечивают безопасность в этой области. Защиту критической информационной инфраструктуры (КИИ) федеральных органов РФ, включая Вооруженные Силы, обеспечивает Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА).

Зарубежные ученые уже долгое время уделяют особое внимание вопросам обнаружения компьютерных атак, исследуя их признаки, разрабатывая и апробируя методы и средства обнаружения несанкционированного доступа (НСД) к информации.

Информационная безопасность России еще более усугубляется вынужденным наличием в информационной инфраструктуре программно-аппаратных средств и информационных технологий иностранного производства, что может негативно отразиться на «информационном» суверенитете.

Проблемы выявления компьютерных инцидентов сегодня наряду с актуальностью приобрели оттенок тайны. Во время расследования и реагирования на инцидент выявляются уязвимости информационной системы, проверяется работоспособность и эффективность архитектуры и механизмов защиты. При возникновении инцидентов, как правило, о них стараются умалчивать, не дискредитируя себя и не

предоставляя дополнительных возможностей злоумышленникам, проявляющим повышенный интерес к секретной информации.

В соответствии с ГОСТ ИСО/МЭК 27001:2006 п. 3.6 инцидентом информационной безопасности является любое непредвиденное или нежелательное событие, которое может нарушить деятельность и информационную безопасность [1].

Компьютерный инцидент приводит к сбоям в работе информационных систем и сетей, информационных ресурсов, нарушающих их функционирование и приводящих к возможности получения, копирования, распространения, искажения, блокирования информации.

Инцидент компьютерной безопасности является чаще всего результатом комплексного воздействия. Эффективность его выявления определяется декомпозицией на структурные компоненты и их качественной аналитической обработкой.

Важная роль в информационной инфраструктуре принадлежит автоматизированным системам военного назначения (АС ВН), эффективная работа которых обеспечивает надежную обороноспособность страны, устойчивое социально-экономическое развитие и суверенитет государства. В этой связи АС Вооруженных Сил создаются как автоматизированные системы в защищенном исполнении.

Применение статичных механизмов защиты информации, таких как разграничение доступа, межсетевые экраны, системы аутентификации, уже не обеспечивают должной защиты. В этой связи системы обнаружения вторжений и атак (СОА) являются неотъемлемым элементом инфраструктуры безопасности.

Современная классификация СОА включает их деление на сетевые и локальные. Сетевые системы осуществляют анализ трафика, циркулирующего в локальной вычислительной сети с помощью выделенных для этих целей компьютеров. Системные СОА находятся на отдельных компьютерах, в целях их защиты и анализируют различные события.

Методы обнаружения и анализа несанкционированных воздействий на ресурс информационной системы можно разделить на [2]:

– метод анализа сигнатур, где происходит сравнение трафика с базами сигнатур с целью выявления в базе атаки с подобной сигнатурой. Недостаток метода состоит в уязвимости СОА при незначительном изменении атаки, и особенно при воздействии новых атак. В этой связи необходимо постоянное оперативное внесение данных в базу и применение этого метода с другими;

– метод обнаружения аномального поведения позволяет находить атаки, не встречающиеся ранее. Однако отклонение от обычной активности система может классифицировать как вредоносное, т.е. возможны ложные тревоги, а также возможна оценка администратором реальной угрозы как ложной.

Системы обнаружения вторжений и атак обычно представляют собой программные или аппаратно-программные средства, которые в автоматизированном режиме контролируют и анализируют происходящие события в компьютерной системе или сети с целью обнаружения признаков проблем безопасности [3].

Система обнаружения и предупреждения компьютерных атак на критически важные сегменты информационной инфраструктуры, включая сегменты Вооруженных Сил Российской Федерации, состоит из двух взаимодополняющих подсистем – предупреждения и обнаружения [4].

Подсистема обнаружения осуществляет:

– сбор информации о компьютерных атаках;

– анализ, обобщение информации и принятие решений;

– доведение решений до подразделений, эксплуатирующих информационно-телекоммуникационные системы (ИТС).

Сбор и первичная обработка информации о неправомерных воздействиях на информационные ресурсы производится с использованием средств, позволяющих обеспечить фиксацию происходящих событий и целостность собранной информа-

ции в условиях информационного противоборства.

Весь объем полученной информации проходит аналитическую обработку на наличие вредоносных воздействий с использованием современного математического аппарата и защищенных систем управления базами данных для принятия решений в режиме онлайн.

Решения подсистемы обнаружения компьютерных атак доводятся до подразделений с помощью защищенной высокоскоростной телекоммуникационной системы, где происходит обмен информацией между центрами мониторинга.

Подсистема должна иметь возможность разработки дополнительных модулей, обеспечивающих получение информации от новых источников событий информационной безопасности.

Подсистема предупреждения обеспечивает:

– оперативный мониторинг событий в критически важных сегментах информационной инфраструктуры;

– выявление уязвимостей в программном обеспечении (ПО);

– своевременную актуализацию средств выявления компьютерных атак, в том числе антивирусных средств.

Оперативный мониторинг позволяет определить потенциальные уязвимости автоматизированных систем с целью оценки реальной защищенности. Определение уровня защиты возможно на основе применения высокоэффективных методов и средств, что проблематично в контексте оперативно-технического обеспечения.

Уязвимости в программном обеспечении выявляются при проведении экспертизы сертификационных испытаний ПО. Подсистема предупреждения предусматривает архивирование эталонов сертификационных ПО и оперативное доведение обновлений к ПО до пользователей ИТС.

В целях предупреждения компьютерных атак необходима оперативная актуализация средств их выявления, обеспечивающая эффективность испытаний средств противодействия компьютерным атакам, в том числе антивирусных средств, выявление баз компьютерных атак, включая базы вирусов и своевременное доведения обновлений антивирусных баз по противодействию компьютерным атакам и антивирусных баз до пользователей ИТС.

Подсистема предупреждения компьютерных атак сегодня приобретает особое значение, обусловленное возрастанием ценности обрабатываемой информации и надежности средств защиты. В свою очередь область действия подсистемы обнаружения сужается за счет уменьшения возможностей реализации атак.

Создание эффективной защиты от потенциальных сетевых атак основывается на их детальной классификации, обеспечивающей выявление и активное противодействие. Существующие типы классификаций, к сожалению, не лишены недостатков. Одной из причин является огромное количество сетевых атак и непрерывное их обновление.

В соответствии с отечественной классификацией СОА делятся [5]:

– по поведению после обнаружения (активные и пассивные);

– по расположению источника результатов аудита (регистрационные файлы хоста или сетевые пакеты);

– по методу обнаружения (поведенческие или интеллектуальные).

Предложенная классификация позволяет построить первичные фильтры СОА для эффективного объективного и оперативного анализа информации, разграничения атак, используя необходимые технологии.

Построение системы обнаружения вторжений и атак основано на двух основных технологиях, использующих определенный набор знаний о методах вторжений и знания о «нормальном» поведении наблюдаемого объекта. Датчики-сенсоры аномалий фиксируют отклонение в работе объекта (сети, компьютера, сетевой службы пользователя и т.д.). Система обнаружения аномальной активности осуществляет анализ на основе данных журналов регистрации и текущей деятельности пользователя. Журналы содержат всю важную информацию по произошедшему инциденту, которая служит необходимой доказательной базой при расследовании компьютерных инцидентов (КИ). При сбое

хоста журналы могут быть единственным источником надежной информации, если хост пересылает журналы на центральный сервер.

Наиболее информативным источником данных являются журналы операционной системы, сетевых устройств, средств защиты информации. Важными данными, хранящимися в журналах операционных систем, являются данные входа в систему, доступа к данным и подсистемам. Сетевые устройства регистрируют данные, относящиеся к внешним и внутренним сетевым взаимодействиям. Средства защиты информации предоставляют данные о нарушениях информационной безопасности, в частности НСД, компьютерных атаках, вредоносном программном обеспечении.

При построении современной системы обнаружения атак учитываются выявленные и потенциально возможные угрозы информационной безопасности. СОА включает оперативный анализ на основе специализированной обработки большого количества неоднородной информации. В этой связи несомненный интерес представляют критерии ее эффективности, оценивающие, в частности, скорость и точность функционирования.

Методологический подход к обработке данных в современных информационных системах предполагает проведение анализа на нескольких уровнях: прикладное программное обеспечение, система управления базами данных, операционная система, среда передачи.

На выделенных уровнях производится анализ обрабатываемой и передаваемой информации средствами защиты информации и СОА, создается подсистема регистрации событий безопасности в отдельном комплексе информационных зондов СОА, обеспечивающая сбор информации в информационной системе. Комплекс информационных зондов СОА должен иметь модульную архитектуру в целях адаптации к программно-аппаратным платформам объектов информационной системы и изменяющимся условиям применения.

Для надежного выявления атак необходима полная информация о произошедшем событии с возможностью выделения этапов проведения компьютерных атак: сетевая разведка, реализация, развитие, скрытие.

Выделение этапов реализации атаки позволит отследить процесс ее развития, а ее выявление на начальных этапах – спрогнозировать развитие ситуации и предотвратить негативные последствия.

Архитектура современных СОА должна быть направлена на распознавание угрозы на этапе ее подготовки и формирования, чего лишены существующие системы. Распознавание осуществляется с использованием сигнатурного поиска, выявления аномалий, экспертных методов и систем.

Выявление угроз происходит путем агрегации данных о подозрительных действиях и сопоставления шаблонов и статистической фильтрации. Фиксация подозрительных отклонений в компьютерных системах возможна на нескольких уровнях:

– на низшем уровне выявляются незначительные отклонения (совпадение сигнатур, выявление аномалий);

– средний уровень позволяет агрегировать информацию, полученную на нижнем уровне, с помощью конечных сценариев атак, статистического анализа и механизмов пороговой фильтрации;

– высший уровень, основываясь на информации предыдущих уровней, позволяет выявить атаки, их источники и спрогнозировать дальнейший ход событий.

Модель выявления угроз безопасности автоматизированных систем военного назначения представлена на рисунке.

Предлагаемая модель выявления угроз позволит существенным образом повысить эффективность управления информационной безопасностью и приведет к снижению потерь, предотвращению компьютерных инцидентов в части возможностей использования подсистемы предупреждения компьютерных атак в условиях динамично изменяющейся информационной инфраструктуры и угроз информационной безопасности.

Для повышения эффективности мероприятий по выявлению и предупреждению компьютерных инцидентов необходимо:

– замена программно-аппаратных средств и информационных технологий иностранного производства, используемых для выявления компьютерных атак в Вооруженных Силах Российской Федерации, на отечественные программно-технические средства;

– расширение спектра контролируемых параметров системой выявления и предупреждения компьютерных инцидентов в связи с использованием

постоянно изменяющихся подходов и НСД к информации, применение новых алгоритмов по обнаружению и предупреждению компьютерных атак;

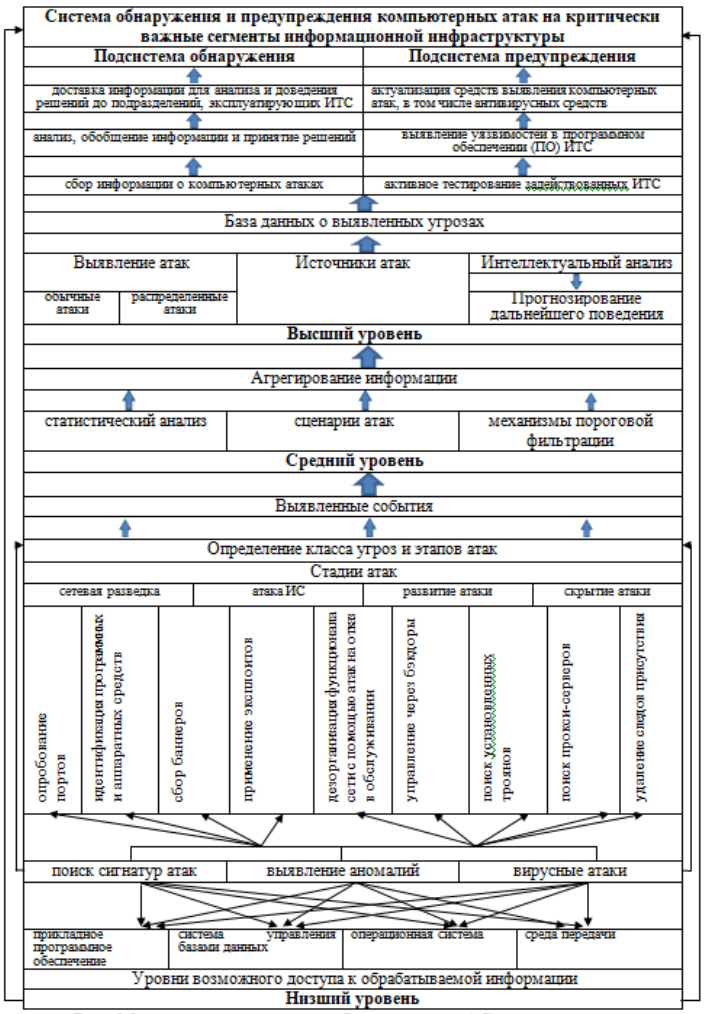

Рис. Модель выявления угроз безопасности АС военного назначения

Рис. Модель выявления угроз безопасности АС военного назначения

– создание интеллектуальных средств обнаружения и предупреждения компьютерных атак, применение механизмов искусственного интеллекта, обеспечивающих качественную обработку большого объема разнородной информации и позволяющих спрогнозировать развитие ситуаций, предотвращая негативные последствия.

Эффективность системы обнаружения и предупреждения компьютерных атак и, соответственно компьютерных инцидентов в Вооруженных Силах Российской Федерации, определяется качественной разработкой и надлежащим использованием российских программно-технических средств, позволяющих обеспечить высокий уровень точности и оперативности процесса выявления компьютерных инцидентов.

**Библиографический список**

1. *ГОСТ Р ИСО*/МЭК 27001:2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. – М.: Стандартинформ, 2006. – [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/1200058325 (дата обращения: 11.11.2019).

2. *Варлатая С.К.,* Кирьяненко А.В. Анализ угроз нарушения информационной безопасности информационных систем, существующие модели и методы противодействия компьютерным атакам // Актуальные проблемы технических наук в России и за рубежом: Сб. науч. тр. по итогам Междунар. науч.-практ. конф. – г. Новосибирск, 10 февраля 2015. – Вып. II.–162 с.

3. *Ганиев А.А.,* Касимова Г.И. Анализ моделей и алгоритмов обнаружения компьютерных атак на основе положений политики безопасности // Молодой ученый. – 2016. – №9. – С. 54-57.

4. *Обзор* Методических рекомендаций ФСБ России по созданию ГосСОПКА. – [Электронный ресурс]. – Режим доступа: https://zlonov.ru/wp-content/uploads/Обзор-Методических-рекомендаций-по-ГосСОПКА.pdf (дата обращения: 10.12.2019).

5.*Аграновский А.В.,* Хади Р.А. Системы обнаружения компьютерных угроз // Сетевые решения. – [Электронный ресурс]. – Режим доступа: http://www.nestor.minsk.by/sr/2008/05/sr80513.html (дата обращения: 09.11.2019).

## DEVELOPMENT OF A MODEL FOR SECURITY THREAT IDENTIFICATION OF AUTOMATED MILITARY SYSTEMS

**D.V. Zimonin**[1], *Candidate of Technical Sciences, Associate Professor*
**E.V. Danilin**[1], *Candidate of Technical Sciences, Associate Professor*
**A.A. Timonov**[2], *Deputy Chairman of NTK*
**D.V. Yumashev**[1], *Cadet*
**A.A. Popovkin**[1], *Cadet*
**A.A. Soloviev**[1], *Cadet*
**[1]The Krasnodar Higher Military Order of Zhukov and the October Revolution, the Red Banner College named after Army General S.M. Shtemenko**
**[2] Scientific and Technical Committee**
**[1](Russia, Krasnodar)**
**[2](Russia, Moscow)**

***Abstract.*** *The article discusses the problematic issues of identifying computer incidents in the segment of automated military systems, the violation of which will lead to undermining the national security of the state. The authors proposed a model for identifying threats that allows you to investigate the probability of attacks at all levels of possible access to the processed information, taking into account the stages of computer attacks and fixing suspicious deviations in computer systems at several levels.*

***Keywords:*** *automated systems of the Armed Forces, computer incidents, computer attacks, intrusion and attack detection system, software and hardware, information technology.*