МЕТОД ВЫЯВЛЕНИЯ ТАРГЕТИРОВАННЫХ АТАК НА РАННИХ ФАЗАХ

Лапсарь А. П.[1], Кенесариева Д. Г.[2]

DOI: 10.21681/2311-3456-2025-2-132-140

Цель статьи: *разработка метода раннего обнаружения таргетированных атак, основанного на ретроспективном анализе состояния защищаемого объекта.*

Методы: *компаративный анализ в рамках системного подхода; синтез структуры ретроспективного метода; синергетика; методы формальной логики.*

Результаты исследования: *выполнен всесторонний анализ свойств таргетированных атак и особенностей их реализации на ранних стадиях, что позволяет глубже понять механизмы, используемые злоумышленниками для достижения своих целей. Рассмотрены закономерности изменения состояния объектов критической информационной инфраструктуры в различных условиях функционирования под воздействием таргетированных атак. Выявлены характерные признаки, сигнализирующие о начале атаки, что служит основой для разработки эффективных методов защиты.*

Для раннего выявления таргетированных атак разработан оригинальный метод, основанный на сравнении состояния исследуемого объекта, подверженного внешнему целенаправленному воздействию, в различные моменты времени. Предложен способ повышения достоверности обнаружения атак с использованием формальной логики.

Научная новизна: *синтезирован метод раннего обнаружения таргетированных атак, основанный на анализе изменения состояния защищаемого объекта под влиянием деструктивного воздействия; предложен способ повышения достоверности выявления скрытой фазы таргетированной атаки на базе оптимальных пороговых значений и применения логических процедур.*

Ключевые слова: *деструктивное информационное воздействие, оценка состояния, объект критической информационной инфраструктуры, раннее обнаружение, информационная безопасность.*

Введение

Стремление ряда недружественных стран к глобальному доминированию в современных условиях проявляется в виде обострения противостояния в информационном пространстве. Воздействие на информационную инфраструктуру Российской Федерации осуществляется как в виде информационно-психологического, так и информационно-технического воздействия. Стремясь нарушить нормальное функционирование информационной инфраструктуры, злоумышленники все активнее используют методы удаленного деструктивного информационного воздействия на сферы, наиболее важные для успешного функционирования отраслей экономики[3]. Тренд на постоянное увеличение количества преступлений и других противоправных действий в информационном пространстве продолжает сохраняться, что подтверждают различного рода аналитические исследования[4].

Меры, принимаемые в рамках реализации федерального закона от 26 июля 2017 г. № 187-ФЗ[5], вынуждают злоумышленников искать новые все более совершенные способы воздействия на атакуемые объекты с целью преодоления созданных на них защитных механизмов. Наиболее известным способом нарушения нормального функционирования важных объектов информационной инфраструктуры является деструктивное воздействие на них путем организации целевых или так называемых таргетированных атак.

Важность задачи противодействия киберпреступникам, повышение устойчивости информационной инфраструктуры к деструктивным информационным воздействиям становится задачей государственного уровня. К ее решению подключилось и научное сообщество, что подтверждается кратным увеличением числа научных публикаций, посвященных

1 Лапсарь Алексей Петрович, кандидат технических наук, доцент, доцент кафедры «Информационная безопасность» ФГБОУ ВО «Ростовский государственный экономический университет», г. Ростов-на-Дону, Россия. E-mail: lapsarap1958@mail.ru

2 Кенесариева Диана Гумаровна, аспирант кафедры «Информационная безопасность» ФГБОУ ВО «Ростовский государственный экономический университет», г. Ростов-на-Дону, Россия. E-mail: diana01102000@yandex.ru

3 Абрамов А. Н. Эксплуатационная надежность технических систем: учебное пособие / А. Н. Абрамов. – М.: МАДИ, 2019. 120 с..

4 МВД РФ На 30% больше IT-преступлений выявлено в 2023 г. в РФ по сравнению с 2022 г. – Интерфакс:новости – 8 февраля 2024 URL: https://www.interfax.ru/russia/945191
Каверин Д. Треть критической инфраструктуры в России подвергалась хакерским атакам – Газета.ru – Декабрь 2023. URL: https://www.gazeta.ru/tech/news/2023/12/25/22000549.shtml
Отчет Positive Technologies [Электронный ресурс] – Режим доступа https://www.ptsecurity.com/ru-ru/research/analytics/hakery-protiv-kompanij-i-lyudej-trendy-i-prognozy/#id6

5 О безопасности критической информационной инфраструктуры Российской Федерации.

6 Калашников А.О., Аникина А. В, Остапенко Г.А., Борисов В. И. Влияние новых технологий на информационную безопасность критической информационной инфраструктуры // Информация и безопасность. 2019. Т. 22. №. 2. С.156–169.

безопасности ключевой информационной инфраструктуры (КИИ)[6]. Вместе с тем, проблема обеспечения устойчивости объектов КИИ к деструктивным информационным воздействиям и повышения их защищенности рассматривается либо как защита от проводимых компьютерных атак, либо как способность минимизировать негативные последствия от их проведения [1].

Применяемые методы защиты объектов КИИ включают в себя ряд стратегий и технологий, направленных на проактивное предотвращение и нейтрализацию угроз. К таким методам относятся:

Мониторинг и анализ трафика: Постоянный анализ сетевого трафика позволяет выявлять аномалии и подозрительные активности, что способствует раннему обнаружению потенциальных атак.

Системы обнаружения и предотвращения вторжений (IDS/IPS): Эти системы автоматически реагируют на выявленные угрозы, блокируя вредоносные действия и предотвращая доступ к уязвимым ресурсам.

Пенетратное тестирование: Регулярное проведение тестов на проникновение помогает выявить слабые места в системе безопасности и устранить их до того, как злоумышленники смогут их использовать.

Обучение персонала: Повышение осведомленности сотрудников о возможных угрозах и методах защиты является важным аспектом активной безопасности. Регулярные тренинги и симуляции атак помогают подготовить команду к реагированию на инциденты.

Использование средств шифрования: Шифрование данных как в состоянии покоя, так и в процессе передачи помогает защитить информацию от несанкционированного доступа.

Разработка и внедрение планов реагирования на инциденты: Наличие четких и хорошо отработанных планов позволяет быстро и эффективно реагировать на инциденты, минимизируя их последствия.

Эти методы в сочетании с пассивными мерами безопасности создают многоуровневую защиту, способствующую повышению устойчивости объектов КИИ к деструктивным информационным воздействиям[7]. Наиболее перспективным направлением исследований считается раннее обнаружение деструктивных информационных воздействий с целью принятия упреждающих мер [2-3].

В ряде работ для обеспечения безопасности КИИ рассматривается марковская модель ее функционирования в условиях деструктивного информационного воздействия, предполагающая наличие некоторой априорной информации о проводимой компьютерной атаке [3-4]. Однако при проведении злоумышленниками таргетированной компьютерной атаки возникают проблемы с ее обнаружением, что затрудняет использование предложенного подхода. Поэтому усовершенствование названной модели в направлении раннего обнаружения таргетированной атаки позволит существенно расширить область ее применения при создании системы обеспечения безопасности КИИ.

Настоящая работа посвящена повышению защищенности КИИ от деструктивного информационного воздействия путем раннего обнаружения на базе ретроспективного анализа состояния объекта защиты.

1. Особенности таргетированной атаки на объекты КИИ

Таргетированная атака обычно осуществляется путем последовательного прохождения нескольких фаз, каждая из которых имеет свои цели и способы реализации.

Алгоритм поведения злоумышленника в контексте таргетированных атак, представляет собой сложный процесс, состоящий из нескольких ключевых фаз, он может изменяться в зависимости от целей, выбранных методов и особенностей атакуемого объекта. Основные фазы типовой таргетированной атаки включают: разведку, подготовку, внедрение, эксплуатацию, установление присутствия, действия по цели, а также сокрытие следов.

Рассмотренные фазы подчеркивают сложность и многоступенчатость таргетированной атаки, что требует от субъектов КИИ комплексного подхода к кибербезопасности и постоянного мониторинга для выявления и предотвращения угроз. Традиционные меры (разработка политики безопасности, применение систем обнаружения вторжений и средств антивирусной защиты, обновление доверенного программного обеспечения, сегментирование информационной системы) усложняют решение задач злоумышленником, но не обеспечивают надежной защиты от таргетированных атак.

В противоположность массовой, таргетированная атака имеет конкретную цель, хорошо спланирована, используемые ресурсы практически не ограниченные. Реализуется в течение длительного времени, при этом существенную часть времени занимает подготовительный период, включающий первые четыре фазы, могут проводиться не непрерывно, а со значительными паузами, реализуются дискретные воздействия. Наличие на атакуемом объекте эффективной системы защиты не приводит к отказу от атаки, а стимулирует выработку нестандартных решений по ее преодолению. Таргетированная атака проводится скрытно, маскируют сам факт ее проведения, алгоритмы и методы успешных действий

7 Лаврова Д.С., Зегжда Д.П., Зайцева Е.А. Моделирование сетевой инфраструктуры сложных объектов для решения задачи противодействия кибератакам // Вопросы кибербезопасности. 2019. № 2. С. 13–20 DOI: 10.21681/2311-3456-2019-2-13-20.

массово не тиражируются. Злоумышленник не придерживается жесткого плана, он гибко подстраивается под конкретную ситуацию и адаптируется к обстановке, методы и тактики атаки могут изменяться в зависимости от реакции системы безопасности и действий защитников. Неудача злоумышленника не ведет к отказу от замысла реализации атаки. В связи с этим системы защиты должны быть адаптивными, способными быстро реагировать на новые угрозы и изменяющиеся условия. Перспективными направлениями считаются использование машинного обучения и глубокой аналитики для выявления аномалий, а также возможность обновления и модификации защитных мер в реальном времени. Такой подход позволяет не только предотвращать атаки, но и минимизировать их последствия, обеспечивая более высокий уровень безопасности[8]. Технологии успешных таргетированных атак распространяются на другие аналогичные объекты [4], либо могут быть «заморожены» для последующих атак на важнейшие уникальные объекты.

В настоящее время при воздействии на КИИ набольшее распространение получили сетевые и системные таргетированные атаки. Сетевые атаки предполагают захват управления или повышение привилегий для контроля над объектами. К основным видам сетевых атак принадлежат[9] IP-спуфинг, парольные атаки, SQL-инъекции, уязвимости нулевого дня. Системные атаки используют уязвимости в системных программах, основные из них это DoS- и DDoS- атаки (могут быть частью более широкой таргетированной атаки, если злоумышленник пытается отвлечь внимание от других действий), черви, вирусы[10]. Результатами деструктивного информационного воздействия может быть полный или частичный отказ объекта КИИ, нарушение штатного режима функционирования, ухудшение ее качества, снижение эффективности системы безопасности и другие. Кроме прямых потерь от нарушения штатного режима функционирования КИИ, следует учитывать и косвенные [5]. Применительно к субъекту КИИ к ним относятся репутационные потери, судебные издержки, расход ресурсов на отражение деструктивного воздействия и ликвидацию его последствий: расход времени, материальных средств, человеческих ресурсов, блокировка участков памяти и другие.

Исходя из потенциальной опасности таргетированных атак следует, что их своевременное обнаружение и предупреждение является важнейшим условием эффективного противодействия деструктивному воздействию на объект КИИ и обеспечения его информационной безопасности.

2. Функционирование объектов КИИ в условиях угроз деструктивного информационного воздействия

Объекты КИИ, реализующие функции управления важнейшими технологическими и производственными процессами, представляют собой сложные открытые информационно-технические системы. Поскольку процесс управления предполагает информационный обмен с сопряженными информационными сетями, существует вероятность удаленного деструктивного информационного воздействия со стороны злоумышленников в виде таргетированной атаки.

Текущее состояние объекта КИИ, включающее набор отдельных параметров и характеристик, представляет собой многоразмерный вектор. Характеристики объекта КИИ при оценке его состояния могут быть квазистатическими и квазидинамическими. К квазистатическим относят элементный состав объекта, различного рода технические характеристики функционирования объекта, используемое программное обеспечение, показатели надежности элементной базы и софта, сложность и энтропия отдельных фрагментов и так далее. Квазидинамические характеристики отражают изменение привилегий, модификацию алгоритмов, нарушение взаимосвязей, а также интенсивность информационного обмена, объем трафика, используемые адреса.

Поскольку состояние объекта КИИ как сложной системы включает большое число разнородных характеристик, изменение каждой из них приводит к незначительному изменению общего состояния. При этом текущее состояние объекта зависит только от того состояния, в котором он находился в предыдущий момент времени, сколь угодно мало отстоящий от анализируемого, и не зависит от предыстории изменения состояния объекта КИИ. Таким образом, отсутствие последействия и незначительное изменение состояния позволяет синтезировать модель объекта КИИ с использованием марковской теории эволюционных процессов [1].

Считается, что функционирование объекта КИИ происходит в условиях потенциальной угрозы со стороны злоумышленников в форме таргетированной атаки. Поэтому при осуществлении информационного обмена с внешней средой на объекте осуществляются стандартные процедуры обнаружения вторжений и антивирусной защиты с применением методов сигнатурного и эвристического анализа. При отсутствии факта обнаружения деструктивного воздействия объект КИИ продолжает штатную работу, в случае выявления компьютерной атаки оцениваются

8 Безопасность объектов КИИ [Электронный ресурс] – Режим доступа https://www.ptsecurity.com/ru-ru/solutions/bezopasnost-kii/

9 Сетевые атаки. Виды. Способы борьбы [Электронный ресурс] – Режим доступа https://moluch.ru/conf/tech/archive/5/1115/

10 Долбин Р. А., Минин Ю. В., Нуритдинов Г. Н., Высоцкий А. В. Процедура определения критических элементов сетевой информационной системы // Информация и безопасность. 2019. Т. 22. №. 1. С. 108–111.

ее свойства и характеристики с последующей реализацией алгоритмов купирования угрозы [4,6]. Такое поведение системы информационной безопасности достаточно надежно обеспечивает противодействие обычным, а также таргетированным атакам на активной фазе реализации в случае их своевременного обнаружения.

Однако известные методы не позволяют выявить таргетированную атаку на стадии ее подготовки, особенно в том случае, если подготовительные мероприятия осуществляются не непрерывно, в случайные моменты времени, воздействие дозировано и распределено по многим элементам атакуемого объекта. Устранение такой проблемы возможно при использовании нестандартных методов выявления таргетированной атаки на ранних фазах ее реализации. Эти же методы могут быть использованы для поиска «следов» успешно проведенной атаки в том случае, если злоумышленнику удалось успешно замаскировать последствия своего вмешательства в атакуемую систему. Как правило, это происходит при нарушении конфиденциальности при сохранении целостности и доступности информации.

В процессе функционирования объекта КИИ в условиях потенциальной угрозы проведения в отношении его компьютерной атаки рассмотрим три возможных сценария.

А. Нормальная штатная эксплуатация. Атаки не выявлены, система защиты информации объекта КИИ находится в готовности к реагированию.

Б. Выявлен факт деструктивного воздействия. В этом случае оцениваются его свойства и характеристики и принимаются меры по купированию негативных последствий. В качестве реакции системы защиты объекта КИИ на обнаруженную атаку может быть применен алгоритм, предложенный в [1].

В. Есть подозрение на компьютерную атаку или выявлена подготовка к ее осуществлению. Тогда реализуются классические методы обнаружения – анализ «черного списка», сигнатурный и эвристический анализ: исследование изменения трафика, задействование объема памяти и других ресурсов; количество выполняемых операций, скорость и время их выполнения, аномальное поведение, другие характеристики.

Основным средством обнаружения компьютерных атак являются системы обнаружения вторжений, требования к которым определены правовыми актами регулятора в области защиты информации. Стандартная конфигурация таких систем включает в себя подсистему сбора событий, связанных с безопасностью; подсистему анализа подозрительных действий в информационном пространстве; базу данных для накопления первичной информации; консоль (панель) управления. Обнаружение вторжений осуществляется путем анализа событий информационного обмена, существенно отличающейся от стандартной[11]: интенсивности сетевого обмена (взаимодействия), задействованных ресурсов, значимых событий безопасности, целостности программного обеспечения и файловых объектов [7–9]. Спектр систем обнаружения вторжений достаточно широк[12]. По способу реагирования они могут быть пассивными и активными, по способу выявления атаки – обнаружение отклонений или злоупотреблений, по способу реализации – на уровне защищаемого объекта или на уровне сети [8,10]. Несмотря на широкое разнообразие таких систем, всем им присущ существенный недостаток: для выявления аномалий требуется установить некоторый порог, превышение которого свидетельствует о наличии факта вторжения. Причем высокий уровень этого порога приводит к возрастанию вероятности необнаруженного вторжения (аналог ошибки второго рода), а низкий – вероятности ложной тревоги (аналог ошибки первого рода). Как отмечалось ранее, на ранних фазах таргетированной атаки злоумышленник «прощупывает» систему защиты объекта воздействиями малого уровня и интенсивности, их выявление существующими методами практически неосуществимо.

Таким образом, для выявления таргетированной атаки на ранних фазах предлагается применить новый метод, основанный на ретроспективном анализе состояния защищаемого объекта и заключающийся в выявлении отличий его квазистатических и квазидинамических характеристик в разные моменты времени. Реализация метода предусматривает создание дополнительной подсистемы, реагирующей на изменение вектора состояния объекта КИИ, и интеграцию ее в общую систему обеспечения безопасности. Это позволит оперативно выявлять и реагировать на угрозы, обеспечивая защиту критической информации и поддерживая стабильность работы информационной инфраструктуры.

3. Ретроспективный анализ состояния объекта КИИ

Ретроспективный анализ состояния объектов КИИ лежит в основе разрабатываемого метода и представляет собой алгоритм оценки и анализа данных о характеристиках системы в прошлом и настоящем.

11 Актуальные вопросы выявления сетевых атак [Электронный ресурс] – Режим доступа http://www.infosecurity.ru/_gazeta/content/030211/article07.html.
Кусакина Н.М. Методы анализа сетевого трафика как основа проектирования системы обнаружения сетевых атак // Труды XLI Междунар. науч.-прак. конф. «International Scientific Review of the Problems and Prospects of Modern Science and Education». Boston: Problems of Science, 2018. С. 28-31.

12 Ansam Khraisat, Iqbal Gondal, Peter Vamplew and Joarder Kamruzzaman Survey of intrusion detection systems: techniques, datasets and challenges // Cybersecurity 2019.

Анализ позволяет выявить тенденции, аномалии и потенциальные угрозы, а также оценить эффективность мер безопасности, позволяет глубже понять динамику изменений и выявить взаимосвязи между различными параметрами. Это, в свою очередь, обеспечивает принятие обоснованных решений по улучшению безопасности объекта и эффективности функционирования системы защиты информации.

В момент времени t_j состояние объекта представлено набором характеристик X_i (x_{i1}, x_{i2}, ..., x_{ii}, ..., x_{in}, ..., x_{in+m}). В некоторый предыдущий момент времени t_i состояние этого же объекта описывается характеристиками X_j (x_{j1}, x_{j2}, ..., x_{ji}, ..., x_{jn}). При этом отличие может касаться хотя бы одной характеристики, а значение m может быть равно некоторой конечной величине. Это означает, что состояния S_j (X_{j1},t_j) и S_i (X_i,t_i) различаются хотя бы в одной позиции. В соответствии со свойством марковости об отсутствии последействия, переход S_i (X_i,t_i) $\rightarrow$ S_j (X_{j1},t_j) определяется переходной плотностью вероятности $p(x,\omega,t)$.

Суть предлагаемого метода состоит в ретроспективном анализе состояния объекта КИИ и заключается в сравнении текущего состояния S_j (X_{j1},t_j) с предшествующим состоянием S_i (X_i,t_i), отстоящим от текущего на некоторый заданный промежуток времени $\Delta t = t_j - t_i$, называемый глубиной ретроспективного поиска. Глубина ретроспективного поиска (или длительность интервала Δt) может быть различной, варьироваться от кратковременного интервала (кратковременный поиск) до длительного. Как указывалось ранее, характеристики объекта КИИ подразделяются на квазистатические и квазидинамические. Квазистатические, или медленно изменяющиеся во времени, оцениваются на временном срезе t_j. К ним относятся как характеристики технических элементов, так и программного обеспечения. Это может быть состав и взаимосвязи элементов, характеристики надежности составных частей объекта КИИ, состав программного обеспечения, распределение вычислительных ресурсов, список адресов взаимодействующих систем, настройки системы защиты и так далее. Квазидинамические как быстроизменяющиеся характеристики предполагают оценку на интервале $[t_j - \tau, t_j]$ при условии $\Delta t >> \tau$. К числу квазидинамических можно отнести объем, интенсивность и распределение во времени информационного обмена (трафика), использование вычислительных ресурсов и памяти, изменения исполняемых файлов, текущие показатели функционирования системы обнаружения вторжений и средств антивирусной защиты, частота и глубина администрирования вычислительной системы, изменение списка адресов и другие. Оперативный контроль названных характеристик может осуществляться либо стандартными техническими и операционными средствами, либо специально созданными подсистемами контроля и анализа. Величина промежутков времени Δt может быть различной в зависимости от глубины ретроспективного поиска. Для углубления исследований можно все характеристики подвергнуть процедуре фрагментации, использовать широкий спектр приемов теории вероятностей и математической статистики, применять элементы теории нечетких множеств и аналогичные математические методы. В этом случае число анализируемых характеристик может достигать десятков или даже сотен, в зависимости от важности защищаемого объекта КИИ и его вычислительных ресурсов.

Подозрение на подготовку к таргетированной атаке определяется либо по существенному изменению состояния объекта КИИ больше некоторого допустимого значения $\Delta S(X,t) = S_j(X_j,t_j) - S_i(X_i,t_i) > \Delta S_{доп}(X,t)$, либо по скорости изменения этого состояния, также превышающей установленный допуск $V(X,t) = \Delta S(X,t)\Delta t > V_{доп}(X,t)$.

Дополнительным показателем признака таргетированной атаки может служить корреляция вектора состояния объекта КИИ в моменты времени t_i и t_j соответственно. Корреляция может быть выражена, например, с помощью классического коэффициента корреляции Пирсона

$$K_{ij}(X,t) = \mathrm{Cov}[S_i(X_i,t_i), S_j(X_j,t_j)]\,\sigma[S_i(X_i,t_i)]\,\sigma[S_j(X_j,t_j)].$$

Поскольку объект КИИ является стохастической системой, используемые показатели $\Delta S(X,t)$, $V(X,t)$ и $K_{ij}(X,t)$ определяются с некоторой долей вероятности, а допустимые значения $\Delta S_{доп}(X,t)$, $V_{доп}(X,t)$ и $K_{ijдоп}(X,t)$ назначаются исходя из приемлемых уровней ошибок первого и второго рода.

Структурная схема реализации предлагаемого метода раннего обнаружения таргетированной атаки на базе ретроспективного анализа представлена на рисунке 1.

4. Функционирование системы раннего обнаружения деструктивного воздействия

В условиях потенциальной угрозы деструктивного воздействия, проводится мониторинг обстановки с использованием традиционных методов обнаружения компьютерной атаки. Положительный результат мониторинга служит катализатором мероприятий по оценке степени ее опасности и принятия мер по устранению угрозы. При отсутствии признаков воздействия на объект КИИ проводится дальнейший анализ на основе разработанного метода ретроспективного анализа. Реализация метода предусматривает оценку признаков таргетированной атаки, в качестве которых рассматриваются следующие показатели:

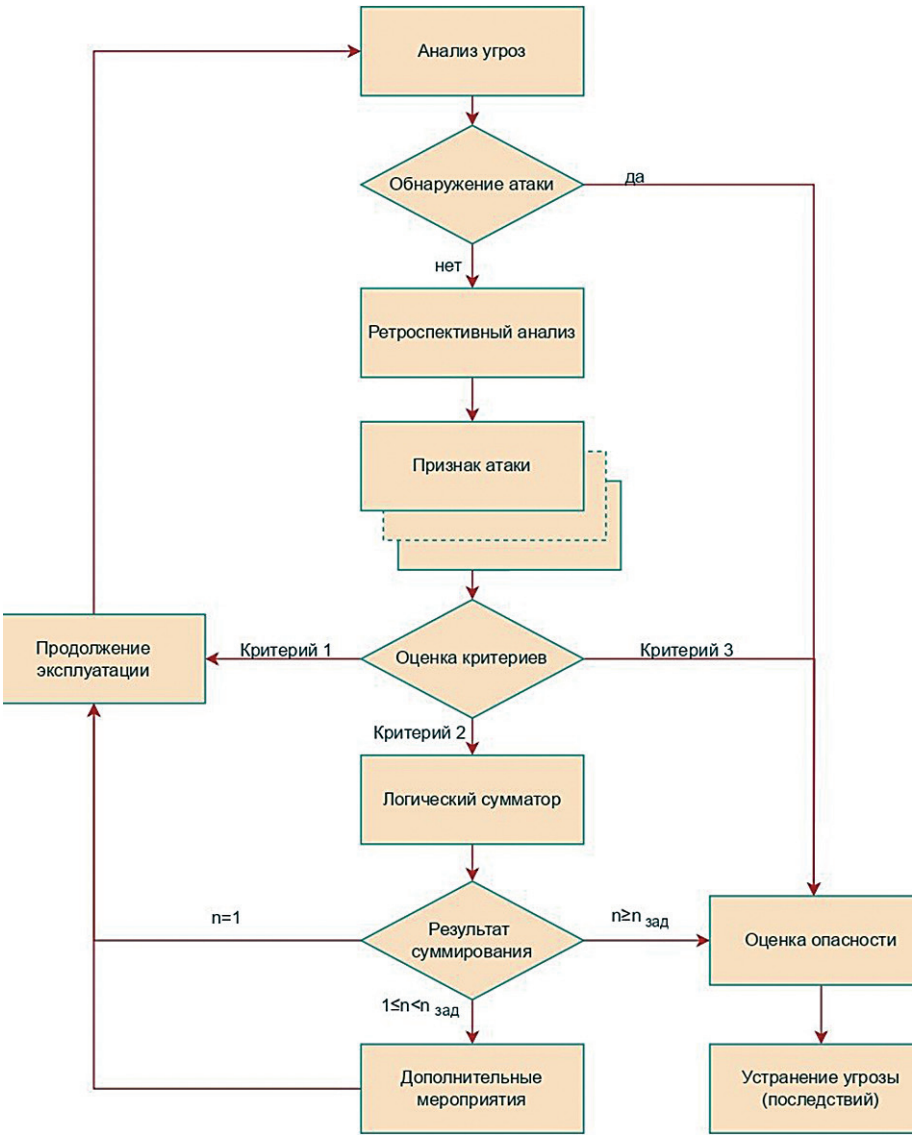

Рис. 1. Схема алгоритма функционирования системы раннего обнаружения таргетированной атаки

- изменение состояния объекта за определенный период времени $\Delta S_{ji}(X,t) = S_j(X_j,t_j) - S_i(X_i,t_i)$ и $\Delta S_{j0}(X,t) = S_j(X_j,t_j) - S_0(X_0,t_0)$, где $S_0(X_0,t_0)$ – состояние объекта в момент начала эксплуатации;
- текущая $V_{ji}(X,t) = \Delta S_{ji}(X,t)\,\Delta t_{ji}$ и средняя $V_{j0}(X,t) = \Delta S_{j0}(X,t)\,\Delta t_{j0}$ скорость изменения состояния объекта, где $\Delta t_{ji} = t_j - t_i$, $\Delta t_{j0} = t_j - t_0$;
- снижение корреляционной зависимости между вектором состояния объекта $K_{ji}(X,t)$ и $K_{j0}(X,t)$ в текущий момент t_j и моменты t_i и t_0 соответственно.

Для каждого из показателей признака таргетированной атаки назначаются два пороговых значения, определяемых исходя из особенностей функционирования объекта КИИ, а именно, минимальное (для корреляции – максимальное) и предельно допустимое. Таким образом, диапазон возможных значений показателей признака таргетированной атаки разделяется на три участка, попадание в один из них является критерием, определяющим дальнейшие действия системы защиты объекта КИИ по противодействию компьютерной атаке.

На схеме в качестве критерия 1 представлены условия, когда оценка показателей признака таргетированной атаки находится ниже (для корреляции – выше) установленного порога

$$\Delta S_{ji}(X,t) < \Delta S_{ji\min}(X,t),\ \Delta S_{j0}(X,t) < \Delta S_{j0\min}(X,t),$$
$$V_{ji}(X,t) < V_{ji\min}(X,t),\ V_{j0}(X,t) < V_{j0\min}(X,t),$$
$$K_{ji}(X,t) > K_{ji\max}(X,t),\ K_{j0}(X,t) > K_{j0\max}(X,t).$$

Полученные оценки показателей свидетельствуют об отсутствии признаков атаки, эксплуатация объекта КИИ продолжается в штатном режиме.

Критерий 2 отражает ситуацию, при которой показатели признака таргетированной атаки занимают промежуточные значения

$$\Delta S_{ji\min}(X,t) \le \Delta S_{ji}(X,t) < \Delta S_{ji\text{доп}}(X,t),$$
$$\Delta S_{j0\min}(X,t) \le \Delta S_{j0}(X,t) < \Delta S_{j0\text{доп}}(X,t),$$
$$V_{ji\min}(X,t) \le V_{ji}(X,t) < V_{ji\text{доп}}(X,t),$$
$$V_{j0\min}(X,t) \le V_{j0}(X,t) < V_{j0\text{доп}}(X,t),$$
$$K_{ji\text{доп}}(X,t) < K_{ji}(X,t) \le V_{ji\max}(X,t),$$
$$K_{j0\text{доп}}(X,t) < K_{ji}(X,t) \le K_{j0\max}(X,t).$$

И, наконец, критерий 3 свидетельствует об обнаружении деструктивного воздействия, оценки показателей признаков атаки следующие:

$$\Delta S_{ji}(X,t) \ge \Delta S_{ji\text{доп}}(X,t),\ \Delta S_{j0}(X,t) \ge \Delta S_{j0\text{доп}}(X,t),$$
$$V_{ji}(X,t) \ge V_{ji\text{доп}}(X,t),\ V_{j0}(X,t) \ge V_{j0\text{доп}}(X,t),$$
$$K_{ji\text{доп}}(X,t) \le K_{ji}(X,t),\ K_{j0\text{доп}}(X,t) \le K_{ji}(X,t),$$

на объекте КИИ выполняются мероприятия, аналогичные проводимым при выявлении атаки традиционными методами.

Пороговые значения показателей назначаются исходя из последствий компьютерного инцидента в случае непринятия мер по купированию атаки или прекращения функционирования объекта из-за ошибочного вывода о проводимой атаке. Снижение $\Delta S_{\min}(X,t)$, $V_{\min}(X,t)$ и увеличение $K_{\max}(X,t)$ приводит к уменьшению ошибки второго рода (необнаруженный отказ), но росту вероятности ложного отказа (ошибки первого рода). Соответственно увеличение $\Delta S_{\text{доп}}(X,t)$, $V_{\text{доп}}(X,t)$ и снижение $K_{\text{доп}}(X,t)$ приводит к уменьшению вероятности ложного отказа, но росту вероятности необнаруженного.

С целью снижения ошибок первого и второго рода реализация предлагаемого метода предусматривает включение в схему процедуры логического суммирования. Обнаружение только одного показателя признака атаки, соответствующего критерию 2, не приводит к отмене штатного режима эксплуатации объекта КИИ. Если число таких показателей находится в диапазоне $n = [2, n_{\text{зад}}]$, на защищаемом объекте проводится комплекс дополнительных мероприятий по усилению контроля за эксплуатационными характеристиками в условиях повышенной угрозы деструктивного воздействия. Большое число показателей $n \ge n_{\text{зад}}$ говорит о проведении в отношении объекта компьютерной атаки.

При купировании возникшей угрозы возможно использование подходов, описанных в [4, 5]. Таким образом, использование предлагаемого метода раннего обнаружения таргетированной атаки на базе ретроспективного анализа в дополнение к традиционным позволит не только эффективно обнаруживать признаки таргетированных атак на ранних стадиях и принимать своевременные меры по их предотвращению, но и снизить вероятность принятия ошибочных решений.

Заключение

В данной работе проведен анализ специфических свойств таргетированных атак, которые затрудняют их обнаружение и купирование традиционными способами. Подчеркнуто, что организовать эффективное противодействие атакам возможно при условии их обнаружения на ранних фазах их реализации. Рассмотрены особенности функционирования объектов КИИ в условиях отсутствия, угрозы и наличия факта деструктивного воздействия со стороны злоумышленников. Сделан вывод о том, что надежное купирование скрытых компьютерных атак возможно при условии комплексного применения традиционных методов обнаружения и новых, опирающихся на постулат об изменении состояния защищаемого объекта под воздействием таргетированной атаки, даже если она не обнаружена имеющимися средствами.

Предложенный метод раннего обнаружения таргетированных атак основывается на анализе состояния объекта в текущий момент времени и определенные предыдущие моменты. Наряду с использованием разнообразных оценок показателей признака таргетированной атаки, предусмотрена их градация по уровням. Повышение достоверности выявления скрытой фазы таргетированной атаки достигается оптимальным назначением пороговых значений, а также применением к ним процедуры дизъюнкции. Достоинством предложенного ретроспективного метода является отсутствие необходимости в априорной информации о начальном состоянии объекта КИИ и требований к его значению в момент начала анализа. Для его реализации существенным является только обнаружение разницы между состояниями объекта КИИ в определенные моменты времени. Внедрение предлагаемого метода предполагает дооснащение существующих объектовых систем безопасности дополнительной подсистемой, регистрирующей изменение вектора состояния объекта КИИ.

Предложенный метод может быть положен в основу создания адаптивных систем обнаружения таргетированных атак еще на стадии их подготовки. Использование в современных вычислительных средствах больших объемом памяти позволяет проводить ретроспективный анализ состояния объектов КИИ на большую глубину и создавать системы обнаружения скрытых компьютерных атак, работающие в реальном времени. Очевидно, что эффективность предложенного метода напрямую зависит

от состава анализируемых характеристик и точности их определения. При достаточно большом количестве и разнообразии исследуемых параметров состояния объекта КИИ метод может использоваться в качестве индикатора последствий использования злоумышленником методов социальной инженерии или инсайдерской деятельности.

Направлением совершенствования систем обеспечения безопасности объектов КИИ может быть реализация предложенного метода на основе мультиструктурных алгоритмов функционирования систем защиты объектов, их самоорганизация и адаптация, внедрение нейронных сетей и других методов искусственного интеллекта.

Литература

1. Лапсарь А.П., Назарян С.А., Владимирова А.И. Повышение устойчивости объектов критической информационной инфраструктуры к целевым компьютерным атакам // Вопросы кибербезопасности. 2022, №2. С. 39–51 DOI:10.21681/2311-3456-2022-2-39-51.
2. Скрыль С.В., Гайфулин В.В., Домрачев Д.В., Сычев В.М., Грачёва Ю.В. Актуальные вопросы проблематики оценки угроз компьютерных атак на информационные ресурсы значимых объектов критической информационной инфраструктуры // Безопасность информационных технологий. 2021. Т. 28. № 1. С. 84–94. DOI: 10.26583/bit.2021.1.07
3. Жиленков А.А., Черный С.Г. Система безаварийного управления критически важными объектами в условиях кибернетических атак // Вопросы кибербезопасности. 2020. № 2. С.58-66. DOI:10.21681/2311-3456-2020-2-58-66.
4. Кубарев А.В., Лапсарь А.П., Федорова Я.В. Повышение безопасности эксплуатации значимых объектов критической инфраструктуры с использованием параметрических моделей эволюции // Вопросы кибербезопасности. 2020. № 1. С. 8–17. DOI: 10.21681/2311-3456-2020-01-08-17.
5. Трапезников Е.В. Выбор средств защиты информации в автоматизированных системах на основе марковских моделей кибератак // Безопасность информационных технологий. 2023. Т. 30, № 4. С. 102–113. DOI: http://dx.doi.org/10.26583/bit.2023.4.06.
6. Яковишин А.Д. Способы оптимизации процессов реагирования на инциденты ИБ// Вестник науки. 2024. Т.1, № 2(71). С. 498-504.
7. Болдырихин Н.В., Комоцкий Р.И., Лян Д.И. Исследование систем обнаружения вторжений // Молодой ученый. 2023. №2 (449). С. 6–9.
8. Новикова Е.С., Котенко И.В., Мелешко А.В., Израилов К.Е. Обнаружение вторжений на основе федеративного обучения: архитектура системы и эксперименты // Вопросы кибербезопасности. 2023. № 6. С. 50–66. DOI: 10.21681/2311-3456-2023-6-50-66.
9. Токарев М.Н. Анализ систем обнаружения вторжений (часть 1) // Актуальные исследования. 2024. № 2-1 (184). С. 47–50.
10. Токарев М.Н. SIEM-Система как инструмент обеспечения информационной безопасности в организации // Актуальные исследования. 2024. № 2-1 (184). С. 51–53.

A METHOD FOR DETECTING TARGETED ATTACKS IN EARLY PHASES

Lapsar A. P.[13], Kenesarieva D. G.[14]

Keywords: *destructive information impact, state assessment, critical information infrastructure object, early detection, information security.*

Purpose of the study: *development of a method for early detection of targeted attacks based on retrospective analysis of the state of the protected object.*

Methods of research: *comparative analysis within the framework of the system approach; synthesis of the structure of the retrospective method; synergetics; methods of formal logic.*

Result(s): *a comprehensive analysis of the properties of targeted attacks and the peculiarities of their implementation at early stages is performed, which allows for a deeper understanding of the mechanisms used by attackers to achieve their goals. The regularities of changes in the state of critical information infrastructure objects in different operating conditions under the influence of targeted attacks are considered. Characteristic signs signaling the beginning of an attack are revealed, which serves as a basis for the development of effective defense methods.*

For early detection of targeted attacks, an original method based on the comparison of the state of the object under study, subjected to external targeting, at different points in time is developed. A method of increasing the reliability of attack detection using formal logic is proposed.

Scientific novelty: *synthesized method of early detection of targeted computer based on the analysis of changes in the state of the protected object under the influence of destructive impact; proposed a way to increase the reliability of detection of the hidden phase of a targeted attack on the basis of optimal threshold values and the use of logical procedures.*

13 Alexey P. Lapsar, Ph.D., Associate Professor, Associate Professor of the Department of Information Security, Rostov State University of Economics, Rostov-on-Don, Russia. E-mail: lapsarap1958@mail.ru

14 Diana G. Kenesarieva, Postgraduate Student of the Department of Information Security, Rostov State University of Economics, Rostov-on-Don, Russia. E-mail: diana01102000@yandex.ru

References

1. Lapsar' A. P., Nazarjan S. A., Vladimirova A. I. Povyshenie ustojchivosti ob#ektov kriticheskoj informacionnoj infrastruktury k celevym komp'juternym atakam // Voprosy kiberbezopasnosti. 2022, № 2. S. 39–51 DOI:10.21681/2311-3456-2022-2-39-51.
2. Skryl' S. V., Gajfulin V. V., Domrachev D. V., Sychev V. M., Grachjova Ju. V. Aktual'nye voprosy problematiki ocenki ugroz komp'juternyh atak na informacionnye resursy znachimyh ob#ektov kriticheskoj informacionnoj infrastruktury // Bezopasnost' informacionnyh tehnologij. 2021. T. 28. № 1. S. 84–94. DOI: 10.26583/bit.2021.1.07.
3. Zhilenkov A. A., Chernyj S. G. Sistema bezavarijnogo upravlenija kriticheski vazhnymi ob#ektami v uslovijah kiberneticheskih atak // Voprosy kiberbezopasnosti. 2020. №. 2. S. 58–66. DOI:10.21681/2311-3456-2020-2-58-66.
4. Kubarev A. V., Lapsar' A. P., Fedorova Ja. V. Povyshenie bezopasnosti jekspluatacii znachimyh ob#ektov kriticheskoj infrastruktury s ispol'zovaniem parametricheskih modelej jevoljucii // Voprosy kiberbezopasnosti. 2020. № 1. S. 8–17. DOI: 10.21681/2311-3456-2020-01-08-17.
5. Trapeznikov E. V. Vybor sredstv zashhity informacii v avtomatizirovannyh sistemah na osnove markovskih modelej kiberatak // Bezopasnost' informacionnyh tehnologij. 2023. T.30, № 4. S. 1022113. DOI: http://dx.doi.org/10.26583/bit.2023.4.06.
6. Jakovishin A. D. Sposoby optimizacii processov reagirovanija na incidenty IB// Vestnik nauki. 2024. T. 1, № 2(71). S. 498–504.
7. Boldyrihin N. V., Komockij R. I., Ljan D. I. Issledovanie sistem obnaruzhenija vtorzhenij // Molodoj uchenyj. 2023. № 2 (449). S. 6–9.
8. Novikova E. S., Kotenko I. V., Meleshko A. V., Izrailov K. E. Obnaruzhenie vtorzhenij na osnove federativnogo obuchenija: arhitektura sistemy i jeksperimenty // Voprosy kiberbezopasnosti. 2023. № 6. S. 50–66. DOI: 10.21681/2311-3456-2023-6-50-66.
9. Tokarev M. N. Analiz sistem obnaruzhenija vtorzhenij (chast' 1) // Aktual'nye issledovanija. 2024. № 2-1 (184). S. 47–50.
10. Tokarev M. N. SIEM-Sistema kak instrument obespechenija informacionnoj bezopasnosti v organizacii // Aktual'nye issledovanija. 2024. № 2-1 (184). S. 51–53.