АТТЕСТАЦИЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Малькевич А.А.[1], студент гр.241301

Белорусский государственный университет информатики и радиоэлектроники[1]
г. Минск, Республика Беларусь

Дворникова Т.Н. – магистр технич. наук

Аннотация. В статье рассматриваются проблемы аттестации современных децентрализованных информационных систем, включающих большое количество автоматизированных рабочих мест, серверное оборудование и облачные ресурсы. На основе анализа реальных инцидентов информационной безопасности обосновывается необходимость автоматизации процессов аттестации. Предлагается подход к разработке программного обеспечения для автоматизированной проверки соответствия информационной системы требованиям стандартов *NIST* с учётом особенностей применяемых средств защиты информации и криптографических протоколов.

Ключевые слова. Аттестация, информационная система, инциденты информационной безопасности.

Современные информационные системы (ИС) представляют собой сложные многокомпонентные структуры, включающие сотни автоматизированных рабочих мест (АРМ), распределённые серверные кластеры, облачные ресурсы, а также разнообразные средства защиты информации. В условиях цифровой трансформации и роста числа кибератак вопросы обеспечения информационной безопасности и подтверждения соответствия системы установленным требованиям приобретают критическое значение. Особую сложность вызывает аттестация децентрализованных информационных систем, компоненты которых функционируют автономно, имеют собственные политики безопасности и независимые каналы связи с внешней средой. В рамках настоящего исследования рассматривается информационная система, насчитывающая 190 АРМ, 8 серверных станций, облачные ресурсы *AWS* и *Azure* (5 единиц). В качестве средств защиты информации используются системы мониторинга событий безопасности *SIEM* (*Security Information and Event Management*), системы предотвращения утечек данных *DLP* (*Data Loss Prevention*), межсетевые экраны нового поколения *NGFW* (*Next-Generation Firewall*) и системы предотвращения вторжений *IPS* (*Intrusion Prevention System*). Криптографическая защита информации обеспечивается протоколами шифрования *AES*-256 и *DES*-128, валидация ключей осуществляется через *Active Directory* с использованием службы управления ключами *KMS* (*Key Management Service*). Требования безопасности, предъявляемые к системе, базируются на стандартах Национального института стандартов и технологий США (*The National Institute of Standards and Technology, NIST*), а сама система имеет децентрализованную архитектуру. Перечисленные особенности предопределяют высокую сложность процесса аттестации и требуют разработки новых подходов к её проведению.

Одним из наиболее перспективных вариантов расширения функционала *DLP*-систем является интеграция с *SIEM*-технологией. В симбиозе системы взаимно дополняют друг друга. Компоненты *DLP*-системы осуществляют поиск и классификацию защищаемой информации по установленным критериям. А *SIEM* формирует «единое окно» для администратора безопасности, в котором сводятся данные о выявленных файлах, подлежащих защите, попытках доступа к ним, а также коррелируется технологическая информация, поступающая от операционных систем, систем управления базами данных, сетевого оборудования и других источников, формируя полную картину состояния информационной безопасности в организации. [1].

Анализ реальных инцидентов информационной безопасности, произошедших за последние годы демонстрирует, что недостатки в организации процессов аттестации напрямую приводят к серьёзным последствиям.

Одним из наиболее показательных примеров является атака на *IT*-инфраструктуру крупной авиакомпании «Аэрофлот», произошедшая в 2024 году. Злоумышленники, используя методы социальной инженерии, получили доступ к учётным данным сотрудника технической поддержки, после чего в течение нескольких недель осуществляли латеральное перемещение по корпоративной сети, внедряя вредоносное программное обеспечение. Кульминацией атаки стал вывод из строя веб-сайта, мобильного приложения и внутренних систем бронирования на несколько суток, что привело к многомиллионным убыткам и массовым задержкам рейсов. Расследование показало, что одной из ключевых причин успеха атаки стало несоответствие реальной конфигурации сети утверждённой документации по аттестации: в сети оказались незадокументированные серверы, отсутствовавшие в инвентаризации активов, а система валидации ключей *KMS* функционировала с нарушениями. Еще одним примером инцидента информационной безопасности является кибератака на ОАО «Гродно Азот», показанная на рисунке 1.

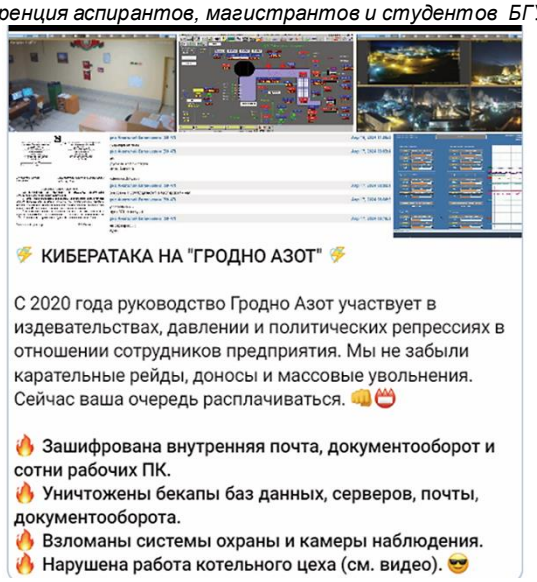

Рисунок 1 – Пример атаки на государственное предприятие

Другой значимой проблемой, выявленной в ходе анализа инцидентов, является недостаточный контроль безопасности облачных ресурсов. В 2024 году крупная международная финансовая организация столкнулась с утечкой данных 10 миллионов клиентов из-за неправильной конфигурации *S*3-бакета в *AWS*. Системный администратор по ошибке установил настройки публичного доступа, в результате чего любой пользователь интернета получил возможность читать и записывать данные в хранилище. Ключевая проблема с точки зрения аттестации заключалась в том, что облачные ресурсы были исключены из периметра аттестации на том основании, что они «находятся под управлением провайдера». Однако стандарты *NIST*, в частности специальная публикация *SP* 800-144, определяют модель разделения ответственности, согласно которой клиент отвечает за безопасность в облаке, включая корректную настройку прав доступа, шифрование данных и управление идентификацией. Игнорирование этого принципа привело к тому, что аттестация оказалась неполной, а облачный сегмент стал уязвимым местом всей системы. [2]

Современное состояние проблемы аттестации информационных систем характеризуется наличием объективного противоречия между растущей сложностью, масштабом и динамичностью информационных систем, с одной стороны, и традиционными, преимущественно ручными и статичными методами оценки их защищённости, с другой стороны. Данное противоречие усугубляется ростом числа кибератак, использующих именно пробелы в процессах аттестации и неактуальность моделей угроз. В качестве примера можно привести не только упомянутые инциденты с «Аэрофлотом» и финансовой организацией, но и множество других случаев, когда утечки данных, внедрение вредоносного ПО, остановка производственных процессов становились возможными именно из-за того, что аттестация не отражала реального состояния системы. Статистика атак на территории Республики Беларусь изображена на рисунке 2. В этой связи становится очевидной необходимость пересмотра подходов к аттестации, смещения акцента с разовых проверок на непрерывный автоматизированный мониторинг соответствия, а также разработки специализированных программных инструментов, позволяющих собирать, анализировать и интерпретировать данные о состоянии защищённости в масштабах современных распределённых и гибридных информационных систем.

Рисунок 2 – Статистика атак на территории Республики Беларусь [3]

Анализ приведённых инцидентов позволяет выделить ключевые проблемы, характерные для традиционных подходов к аттестации информационных систем. Во-первых, это статичность: традиционная аттестация представляет собой разовое событие, в то время как система непрерывно изменяется. Между периодами аттестации в системе происходят сотни изменений: обновления программного обеспечения, замена оборудования, подключение новых АРМ, изменение конфигураций средств защиты. Во-вторых, это высокая трудоёмкость и подверженность ошибкам при ручной проверке. Проверка конфигураций 190 АРМ на предмет использования корректных протоколов шифрования, валидации ключей в *KMS*, настроек локальных межсетевых экранов физически не может быть выполнена вручную с требуемой полнотой и периодичностью. В-третьих, это недостаточный охват гибридных и облачных сегментов, которые часто выпадают из периметра оценки или оцениваются по упрощённым методикам. Для решения указанных проблем целесообразно использовать подход, предлагаемый стандартами *NIST*, в частности *Risk Management Framework* (*RMF*), описанный в публикации *NIST SP* 800-37. Данный подход предполагает не разовую проверку с выдачей сертификата соответствия, а непрерывный цикл, включающий категоризацию информационной системы, выбор средств защиты, их внедрение, оценку эффективности, авторизацию и непрерывный мониторинг состояния безопасности. В *NIST SP* 800-37 указано, что *Risk Management Framework*, в целом, указывает на важность разработки и внедрения возможностей по обеспечению безопасности и конфиденциальности в *IT*-системах на протяжении всего жизненного цикла (*system development life cycle, SDLC*), непрерывной поддержки ситуационной осведомленности о состоянии защиты ИТ-систем с применением процессов непрерывного мониторинга (*continuous monitoring, CM*) и предоставления информации руководству для принятия взвешенных риск-ориентированных решений. В *RMF* выделены следующие типы рисков: программный риск, риск несоответствия законодательству, финансовый риск, юридический риск, бизнес-риск, политический риск, риск безопасности и конфиденциальности (включая риск цепочки поставок), проектный риск, репутационный риск, риск безопасности жизнедеятельности, риск стратегического планирования. [4].

В контексте рассматриваемой информационной системы, имеющей децентрализованную архитектуру и включающей 190 АРМ, 8 серверов, облачные ресурсы *AWS* и *Azure*, а также средства защиты *SIEM*, *DLP*, *NGFW*, *IPS*, реализация принципов непрерывного мониторинга требует разработки специализированного программного обеспечения. Такое программное обеспечение должно обеспечивать автоматизированный сбор данных о состоянии защищённости всех компонентов системы, включая проверку корректности применения протоколов шифрования (*AES*-256, *DES*-128), валидацию ключей в *Active Directory* через *KMS*, анализ конфигураций *NGFW* и *IPS*, а также интеграцию с *SIEM*-системой. Разрабатываемое программное обеспечение должно реализовывать алгоритм, включающий следующие основные этапы: загрузка шаблона требований безопасности на основе стандартов *NIST*; сканирование сети для выявления всех активных компонентов системы; проверка конфигураций каждого компонента на соответствие установленным требованиям; анализ логов *SIEM* для выявления нарушений безопасности; формирование отчёта о соответствии с указанием выявленных несоответствий. Экономическая эффективность предлагаемого подхода обусловлена сокращением трудозатрат на проведение аттестации. Внедрение автоматизированного программного обеспечения позволяет сократить время на сбор и анализ данных с нескольких недель до нескольких часов, а также снизить влияние человеческого фактора на результаты оценки.

Таким образом, традиционные подходы к аттестации информационных систем, основанные на ручных проверках и статичных документах, неэффективны для современных децентрализованных систем. Разработка специализированного программного обеспечения для автоматизации процессов аттестации позволяет сократить временные и финансовые затраты, повысить полноту и достоверность оценки, а также обеспечить поддержание информационной системы в состоянии соответствия требованиям безопасности на постоянной основе.

Список использованных источников:

1. Андриянова, Т. А. Симбиоз SIEM и DLP / Т. А. Андриянова, С. Б. Саломатин // Технические средства защиты информации: тезисы докладов XV Белорусско-российской научно-технической конференции, Минск, 6 июня 2017 г. / Белорусский государственный университет информатики и радиоэлектроники. – Минск, 2017. – С. 38–39.

2. NIST Special Publication 800-144. Guidelines on Security and Privacy in Public Cloud Computing. – National Institute of Standards and Technology, 2011. – 80 p.

3. Positive Technologies. Анализ угроз информационной безопасности за 2024 год. – 2025. – 62 с.

4. NIST Special Publication 800-37 Rev. 2. Risk Management Framework for Information Systems and Organizations. – National Institute of Standards and Technology, 2018. – 183 p.