DOI 10.37882/2223–2966.2020.07.09

ОСОБЕННОСТИ ПРОВЕДЕНИЯ АУДИТА И МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

FEATURES OF INFORMATION SECURITY AUDIT AND MONITORING IN DISTRIBUTED INFORMATION SYSTEMS

K. Goryun
S. Klyuev

Summary. In the context of constant changes in the constituent components of a distributed information system, information security is a complex task. To date, in the works of scientists, insufficient attention has been paid to the audit and monitoring of information security in such systems. There is no audit and monitoring methodology, no system of criteria for evaluating the effectiveness of information security; it does not take into account the peculiarities inherent in distributed information systems, which in turn does not allow increasing the efficiency of information security systems in distributed information systems. The aim of this work is to systematize basic information about the stages of audit and monitoring, taking into account the features of their implementation in distributed information systems. When identifying the features of audit and monitoring activities in distributed information systems, methods of system analysis, logical induction and deduction were used. The features and problematic issues identified in the work related to the audit and monitoring in distributed systems can be used to justify the development of new models, methods and algorithms for auditing and monitoring information security of distributed information systems.

Keywords: information security, information security systems, audit and monitoring of information security, distributed information systems.

Горюн Кристина Николаевна
Преподаватель, ФГКОУ ВО «Краснодарский университет Министерства внутренних дел Российской Федерации»
kngoryun@yandex.ru
Клюев Станислав Геннадьевич
К.т.н., доцент, Краснодарское высшее военное училище
s.g.klyuev@mail.ru

Аннотация. В условиях постоянного изменения составляющих компонентов распределенной информационной системы обеспечение безопасности информации является сложной задачей. На сегодняшний день в работах ученых недостаточно внимания уделено проведению аудита и мониторинга информационной безопасности в такого рода системах. Отсутствуют методика проведения аудита и мониторинга, система критериев оценки эффективности обеспечения информационной безопасности, не учитываются особенности присущие распределенным информационным системам, что в свою очередь не позволяет повысить эффективность функционирования систем обеспечения информационной безопасности в распределенных информационных системах. Целью данной работы является систематизация основных сведений об этапах аудита и мониторинга с учетом особенностей их проведения в распределенных информационных системах. При выявлении особенностей мероприятий аудита и мониторинга в распределенных информационных системах использовались методы системного анализа, логической индукции и дедукции. Выявленные в работе особенности и проблемные вопросы, связанные с проведением аудита и мониторинга в распределенных системах, могут быть использованы для обоснования разработки новых моделей, методов и алгоритмов аудита и мониторинга информационной безопасности распределенных информационных систем.

Ключевые слова: информационная безопасность, системы обеспечения информационной безопасности, аудит и мониторинг информационной безопасности, распределенные информационные системы.

При осуществлении обеспечения информационной безопасности (ИБ) распределенных информационных систем наряду с процессами реализации мер защиты информации, специализированной подготовки персонала и внедрения политики безопасности важное значение имеют процессы контроля и проверки состояния информационной безопасности. Данный контроль позволяет проверить целесообразность выбранных методов и средств защиты, а также выявить уязвимости в существующей информационной системе. Среди процессов контроля и проверки состояния информационной безопасности особое место занимают аудит и мониторинг состояния ИБ, основной целью которых является выявления нарушений угроз безопасности информации и уязвимостей, а также формирование независимой оценки состояния информационной безопасности в информационных системах.

На настоящий момент значительное количество ученых освещали тему, посвященную аудиту и мониторингу ИБ. Например, в [1] автор рассматривает конкретные программные комплексы, предназначенные для прове-

дения аудита информационной безопасности, проводит их анализ и приходит к выводу, что при осуществлении аудита информационной безопасности в государственной организации в качестве критериев оценки рисков и управления ИБ выступают требования государственных и международных стандартов, либо анализ рисков. В [2] представлен обзор международных стандартов и практик по проведению аудита ИБ. Автор [3] в качестве средства проведения аудита ИБ рассматривает конкретное программное решение. В целом, в представленных научных работах имеют место решенные научные и практические задачи, однако, не четко определен систематизированный подход к проведению аудита и мониторинга состояния ИБ, классификация и методика проведения данных мероприятий. В большинстве своем авторы рассматривают процесс проведения аудита и осуществление мониторинга в узком направлении, например, проведение аудита в государственных органах как в [4], или исследуют определенный метод или этап, например, в подавляющем большинстве эксперименты по тестированию реальных информационных систем сводятся к «тестированию на проникновение» [5] или к проведению «инструментального аудита». В итоге отсутствуют систематизация знаний об этапах аудита, теоретические и практические принципы проведения аудита.

К тому же терминология и классификация мероприятий аудита и мониторинга, используемые в известных работах, являются достаточно противоречивыми и неоднозначными. Также стоит отметить отсутствие системного подхода в нормативно правовом регулировании вопросов связанных с проведением аудита и мониторинга состояния ИБ.

В сложившейся ситуации достаточно мало ученых рассматривают в качестве объекта мониторинга и аудита распределенные информационные системы.

Распределенная информационная система в соответствии с ГОСТ 34.321–96. «Информационные технологии. Система стандартов по базам данных. Эталонная модель управления данными» представляет собой информационную систему, объекты данных и/или процессы которой физически распределяются на две или более компьютерные системы (34.321–96, 1996).

Распределенные системы должны иметь возможность поддаваться расширению, или масштабированию. Эта характеристика является прямым следствием наличия независимых компонентов, но в то же время не указывает, каким образом эти компоненты на самом деле объединяются в единую систему. Распределенные системы обычно существуют постоянно, однако, некоторые их элементы могут временно выходить из строя. Пользователи и приложения не должны уведомляться о том, что эти компоненты заменены или починены, или что добавлены новые части для поддержки дополнительных пользователей или приложений.

Распределенная система представляется пользователям как единая совокупность. Масштаб системы может измеряться по различным показателям:

1. система может масштабироваться по отношению к её размеру;
2. система может масштабироваться географически, пользователи и набор сервисов могут быть разнесены в пространстве;
3. система может быть разнесена в административном смысле, то есть работать в различных административно разделенных организациях.

Целью данной статьи является систематизация основных сведений об этапах аудита и мониторинга с учетом особенностей их проведения в распределенных информационных системах.

Как правило, аудит информационной безопасности подразделяется на следующие этапы:

- Подготовительный этап, включающий в себя выбор объекта, критериев и методов аудита, средств и способов аудита, определение объёмов и масштаба аудита, установление сроков аудита.
- Основной этап — анализ состояния ИБ объекта, регистрация и проверка статистических данных и результатов измерений уязвимостей и угроз, оценка результатов проверки, формирование отчета по результатам проверки.
- На заключительном этапе происходит формирование рекомендаций по улучшению комплекса мер, направленных на повышение эффективности системы защиты и разработка плана по устранению имеющихся уязвимостей и недостатков в системе обеспечения ИБ.

Однако, когда речь идет о распределенных информационных системах возникает ряд нерешенных вопросов, связанных, например, с проведением инвентаризации аппаратного и программного обеспечения. Современные системы становятся крупногабаритными и динамичными. При наличии большого числа географически распределенных узлов, а также постоянно растущего числа мобильных пользователей трудно иметь четкое представление о том, какое реальное количество аппаратного и программного обеспечения имеется в конкретной информационной системе. Безусловно, возможно воспользоваться специализированным программным обеспечением, но это не решит проблему системного подхода к проведению аудита в распределённых информационных системах.

При осуществлении сбора информации о текущем состоянии, сведений об администрировании и сопровождении информационной системы необходимо учитывать сложность системы, которая определяется как количеством подсистем, так и разнообразием их типов и выполняемых функций; невозможность обеспечения эффективного контроля за доступом к ресурсам, распределенным на больших расстояниях; возможность принадлежности ресурсов сети различным владельцам; необходимость обеспечения гарантированной передачи информации по коммуникационной подсети. Такие сложные системы строятся как адаптивные, в которых обеспечивается постоянный контроль работоспособности элементов системы и возможность продолжения функционирования даже в условиях отказов отдельных подсистем.

Перед аудитором возникает ряд следующих задач, присущих именно процедуре проведения аудита в распределенных системах:

1. Выбрать методы, способы и средства проведения аудита, позволяющие осуществить анализ состава и структуры распределенной информационной системы в условиях постоянного изменения ее составляющих компонентов.
2. Выбрать систему критериев и показателей оценки эффективности функционирования системы обеспечения ИБ.
3. Провести оценку эффективности системы обеспечения ИБ с учетом постоянно меняющихся состава и структуры распределенной информационной системы.
4. Определить наиболее значимые элементы в распределенной информационной системе.

К сожалению, полностью решить вышеуказанные задачи по объективным причинам на данный момент не представляется возможным.

Если говорить о мониторинге информационной безопасности в информационных системах, то этот процесс представляет собой постоянное наблюдение и анализ результатов регистрации событий безопасности с целью выявления нарушений, угроз безопасности информации и уязвимостей в информационных системах.

Мониторинг информационной безопасности в информационной распределенной системе должен предусматривать выполнение следующих мероприятий: контроль за событиями безопасности и действиями пользователей, и состоянием защищенности информации, содержащейся в информационной системе; анализ и оценка функционирования системы защиты информации; периодический анализ изменения угроз безопасности информации в информационной системе.

Процессы сбора и обработки сведений выполняются из разных источников, таких как DLP-системы, IDS-системы, антивирусное программное обеспечение, журналы событий операционных систем. Чем больше и неоднороднее информационная система, тем больше может быть источников.

Для автоматизации процесса сбора и анализа информации о событиях безопасности, поступающих из различных источников целесообразно использовать систему мониторинга событий информационной безопасности, которая состоит из программно-аппаратной части (агенты мониторинга, сервер событий, хранилища данных); документационной части (набор документов, описывающих основные процессы, связанные с выявлением и реагированием на инциденты безопасности); кадровой составляющей (сотрудники, ответственные за работу с системой мониторинга ИБ).

В распределенных информационных системах мониторинг информационной безопасности осуществляется на следующих уровнях:

- уровень источников данных;
- уровень сбора данных;
- уровень хранения и обработки данных;
- уровень представления информации мониторинга потребителям.

Причем на каждом из перечисленных уровней должна быть обеспечена возможность реализации многомерности, то есть обеспечения вертикальной интеграции процесса мониторинга информационной безопасности в организационную структуру управления безопасности организации, а также горизонтальную — по структурным элементам информационной системы; масштабируемость за счет подключения новых источников информации о событиях безопасности; адаптивность к новым компьютерным атакам и иным видам нарушений безопасности информации за счет развития правил сопоставления событий безопасности и регистрации нарушений безопасности информации, унификация протоколов взаимодействия различных элементов, участвующих в процессе мониторинга информационной безопасности.

Автоматизированный и непрерывный мониторинг безопасности является главным условием быстрого выявления и устранения угроз.

Тем не менее, при осуществлении мониторинга состояния ИБ возникают неразрешенные задачи, связанные с неоднородностью и неопределенностью структуры распределенной информационной системы, отсутствии системы критериев и оценок, позволяющих оценить эффективность защищенности системы, неопределенности воздействия угроз.

Таким образом, для повышения точности оценки эффективности функционирования систем обеспечения информационной безопасности распределенных информационных систем необходимо:

Во-первых, разработать динамическую модель осуществления аудита распределенной информационной системы с учетом изменения ее состава и структуры.

Во-вторых, разработать систему критериев, показателей и алгоритм оценки эффективности функционирования систем обеспечения информационной безопасности в распределенных информационных системах с учетом изменения ее состава и структуры, а также всех факторов, воздействующих на безопасность защищаемой информации.

В-третьих, разработать метод выявления значимых элементов распределенной информационной системы и уязвимостей в системе обеспечения информационной безопасности для формулирования мер защиты в условиях неопределенности воздействия.

Только при наличии данных трех составляющих возможен системный подход к проведению аудита и мониторинга в распределенных информационных системах, позволяющий повысить эффективность защиты информационных систем.

ЛИТЕРАТУРА

1. Серова А. Г. Теоретические основы и программные средства аудита //Системы Управления информационной безопасностью государственного учреждения, Санкт-Петербургский университет технологий управления и экономики, 2017. С. 560–569.
2. Сёмкина Н.С., Виды и методы проведения внутреннего аудита //Системы Управления Информационной Безопасностью Московский институт электроники и математики НИУ ВШЭ, 2017.С. 340–341.
3. Бутакова Н. Г. Интеграция средств мониторинга и аудита информационной безопасности корпоративной сети // Электронный Научный Журнал. 2017. № 4–1 (19). С. 152–155.
4. Ермаков А.С., Клименко А. П. Методы Аудита Информационной Безопасности Государственного Предприятия 2017. С. 8–14.
5. Чуб В. Молодой исследователь дона // Аудит безопасности информационной системы с использованием тестов на проникновение. 2018. № 6. С. 88–90.
6. Аверичников В.И., Рытов М. Ю., Кувылкин А. В., Рудановский М. В. //Аудит информационной безопасности органов исполнительной власти: учебное пособие.— М.: Флинта, 2011–100 с.
7. Кульба В.В., Шелков А. Б., Гладков Ю. М., Мониторинг и аудит информационной безопасности автоматизированных систем.— М.: ИПУ им. В. А. Трапезникова РАН, 2009–94 с.
8. Марков А.С., Цирлов В. Л., Барабанов А. В. Методы несоответствия средств защиты информации / под ред. А. С. Маркова.— М.: Радио и связь, 2012–192 с.
9. Хомяков В. А. Аудит как метод модернизации системы обеспечения информационной безопасности //Экономический вестник университета. 2013 № 2 С. 48–52.
10. Симонов С. Аудит безопасности информационных систем // Jet Info.1999 № 9 (76). С. 3–24.
11. Котенко И.В., Степашин М. В. Анализ защищенности компьютерных сетей на основе моделирования действий злоумышленников и построении графа атак // Труды Института системного анализа РАН. 2007 Т. 31 С. 126–207.
12. Скабцов Н. Аудит безопасности информационных систем.— СПб.: Питер, 2018–272 с.

Журнал «Современная наука: актуальные проблемы теории и практики»