АНАЛИЗ ВОЗМОЖНОСТЕЙ АВТОМАТИЗАЦИИ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Пономарев Павел Вячеславович

магистрант, Московский институт электронной техники, РФ, г. Москва

Аудит информационной безопасности (ИБ) представляет собой процесс получения объективных качественных и количественных оценок текущего состояния информационной безопасности в соответствии с определёнными критериями и показателями. В настоящее время можно выделить следующие основные виды аудита информационной безопасности:

• экспертный аудит безопасности, в процессе которого выявляются недостатки в системе мер защиты

информации на основе имеющегося опыта экспертов, участвующих в процедуре обследования;

• активный аудит, включающий механизмы для проверки правильного выполнения существующей политики безопасности, слежения в реальном масштабе времени за отклонениями и выявление вторжения;

• оценка соответствия рекомендациям Международного стандарта ISO 17799, а также требованиям руководящих документов ФСТЭК;

• инструментальный анализ защищённости АС, направленный на выявление и устранение уязвимостей программно-аппаратного обеспечения системы;

• комплексный аудит [2].

Целью аудита безопасности является установление степени соответствия применяемых в организации конкретных параметров конфигурации программного обеспечения объектов информационной системы установленным требованиям безопасности.

Каждый из вышеперечисленных видов аудита может проводиться по отдельности или в комплексе в зависимости от решаемых предприятием задач. В качестве объекта аудита может выступать ИС компании в целом и её отдельные сегменты, в которых проводится обработка информации, подлежащей защите [2].

Помимо требований стандартов обеспечения информационной безопасности организации могут выдвигать внутренние требования безопасности к объектам информационной системы, специфичные для решаемых задач, структурных и функциональных характеристик информационной системы, применяемых информационных технологий, что обосновывает необходимость и важность доработки документации. Процесс автоматизации аудита приведен на рисунке 1 в виде цикла PDCA, согласно ГОСТ Р ИСО 19011-2021 [4]. Такое представление помогает определить ряд необходимых к выполнению задач, также в дальнейшем позволит улучшить процесс аудита.

То есть условно аудит можно разделить на множество различных групп: внутренний и внешний, инструментальный, экспертный, аудит на соответствие стандартам безопасности. В зависимости от целей и типа аудита используются разные методы для получения свидетельств и их характеристики и сопоставление предъявляемым требованиям. Условно математически аудит можно представить совокупность разных множеств, а именно

множество свидетельств аудита, которое является входным потоком для процесса аудита. Множество критериев аудита, положений стандарта, что тоже можно рассматривать как входные данные с точки зрения математической модели, так как аудиты могут иметь разные критерии аудита и их необходимо выработать непосредственно перед проведением аудита. Множество наблюдений аудита, является результатом сравнения входных множеств, что является выходными данным, как и последнее множество заключений по результатам аудита. Это же множество является четко определенным и детерминированным, мощность этого множества равна 3, так как имеется 3 результата: аудит пройден успешно, аудит пройден с замечаниями, аудит не пройдет. Таким образом, с математической точки зрения аудит представляет собой совокупность множеств при отображении одного множество через другое получается результат аудита.

С учетом такой простоты аудита с точки зрения математического моделирования можно сделать вывод, что процесс аудита имеет шаблонный алгоритм, который можно автоматизировать данный процесс, в зависимости от типа аудита.

1.2 Аудит информационной безопасности выделенного помещения

Под выделенным помещением (ВП) понимается служебное помещение, специально предназначенное для проведения конфиденциальных мероприятий (совещаний, переговоров и т.д.). К таким помещениям относятся, прежде всего, комнаты для переговоров на фирмах, где ведутся деловые переговоры, содержащие конфиденциальную информацию [7].

Основная цель обеспечения безопасности конфиденциальной информации в переговорных комнатах – исключить доступ к ее содержанию при проведении переговоров (разговоров). При этом защищать необходимо и само помещение, и технические средства, расположенные в нем. Правильная организация ВП позволит защитить конфиденциальную информацию от утечки по техническим каналам и несанкционированного доступа к ней. Именно поэтому уже на стадии проекта важно рассчитать вероятность всевозможных угроз, учитывая расположение помещения в масштабе здания, расположение окон и дверей, коммуникаций, основных и вспомогательных технических средств (ОТСС и ВТСС), мебели и т.д. В настоящее время средства автоматизации аудита информационной безопасности (ИБ) ВП в чистом виде отсутствуют. Иванова М.Е., Напалкова Н.В., Щербаков В.А. предложили СПО для ЭВМ для автоматизации аудита ИБ ВП с заданными параметрами и объектами, которые пользователь желает разместить. Она может быть применима для защиты ВП до 3-ей категории доступа включительно.

1.3 Инструментальный аудит

Проведение инструментального аудита напрямую связано использованием программных и программно-аппаратных средств, позволяющих автоматизировать процесс такого аудита. Одним из основных механизмов формализации требований является протокол SCAP [3]. Большинство сканеров безопасности применяют данный протокол, в рамках которого требования формализуются спецификациями OVAL и XCCDF. Для решения задачи автоматизации аудита могут применяться любые инструменты, совместимые с протоколом SCAP: MaxPatrol 8, Redchek, Joval или бесплатные – OpenScap, ScanOval и Ovaldi.

Помимо сканеров уязвимости для автоматизации процесса аудита ИБ могут использоваться Центры оперативного управления (Security Operations Center – SOC). Современный SOC представляет собой сложную организационно-техническую систему, в состав которой входят сотрудники, процессы и соответствующие технические решения. Здесь среди технических решений выделяется система сбора и корреляции событий ИБ (Security Information and Event Management – SIEM). Данные решения имеют большое количество вариантов и версий от различных вендоров и производителей, поэтому вопрос автоматизации инструментального аудита в целом решен, однако полностью не автоматизирован и требует участия в нем человека, который также пользуется экспертным методом оценки, об автоматизации которого обсуждалось ранее.

Список литературы:

1. Сабанов А.Г. Многоуровневый анализ угроз безопасности процессов аутентификации //Вопросы защиты информации. – 2014. – № 1(104).

2. Иванова Н.В., Коробулина О.Ю. Метод аудита информационной безопасности информационных систем // Известия Петербургского университета путей сообщения. 2010. №4. Режим доступа: https://cyberleninka.ru/article/n/metod-audita-informatsionnoybezopasnosti-informatsionnyh-sistem (режим доступа: 19.09.2023).

3. Автоматизация процедуры проведения аудита информационной безопасности на основе профиля защиты / Л. В. Датская, И. С. Кожевникова, Е. В. Ананьин, В. С. Оладько // Национальная Ассоциация Ученых. – 2015. – № 6-2(11). – С. 18-22. – EDN XYGHQD.

4. Селигеев, С. В. Автоматизация аудита безопасности информационной системы / С. В. Селигеев, В. Г. Жуков // Решетневские чтения : Материалы XXV Международной научно-практической конференции, посвященной памяти генерального конструктора ракетно-космических систем академика М.Ф. Решетнева. В 2-х частях, Красноярск, 10–12 ноября 2021 года / Под общей редакцией Ю.Ю. Логинова. Том Часть 2. – Красноярск: Федеральное государственное бюджетное образовательное учреждение высшего образования "Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева", 2021. – С. 448-449. – EDN YWCKJA [Электронный ресурс]. URL: https://elibrary.ru/item.asp?id=47711986 (дата обращения 25.09.2023).

5. ГОСТ Р ИСО 19011-2021. Оценка соответствия. Руководящие указания по проведению аудита систем менеджмента: национальный стандарт Российской Федерации: издание официальное: Приказом Федерального агентства по техническому регулированию и метрологии от 21 апреля 2021 г. N 261-ст [Электронный ресурс]. URL: https://docs.cntd.ru/document/ 1200179216 (дата обращения 25.09.2023).

6. Разработка алгоритма проведения аудита информационной безопасности на основе профиля защиты. / Л.В.Датская [и др.] // Сборник материалов по III Всероссийской научно-практической конференции «Актуальные вопросы информационной безопасности регионов в условиях глобализации информационного пространства» — 2015. — № 3.— С. 275-279.

7. Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3 т. Т. 1. Технические каналы утечки информации. – М.: НПЦ «Аналитика», 2008. – 436 с.: ил.