АУДИТ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Нечаев Андрей Рустамович

студент, РЭУ им. Г.В.Плеханова РФ, г. Москва

Аудит безопасности информационных систем (ISSA) - это независимый обзор и экспертиза системных записей, деятельности и связанных с ними документов. Эти проверки направлены на повышение уровня информационной безопасности, предотвращение ненадлежащих конструкций информационной безопасности и оптимизацию эффективности защитных мер и процессов безопасности.1 термин " структура безопасности" использовался в различных формах в литературе по вопросам безопасности на протяжении многих лет, но в 2006 году он стал использоваться в качестве обобщающего термина для различных документов, некоторых частей программного обеспечения и различных источников, которые дают рекомендации по темам, связанным с безопасностью информационных систем, в частности, в отношении планирования, управление или аудит общей практики информационной безопасности для данного учреждения.

Система Zachman Framework for enterprise architecture была использована в качестве руководства для проведения интервью с экспертами по безопасности и аудиторами для выявления существующих структур, компонентов структуры и мнений по этому вопросу. В дополнение к базовым понятиям безопасности, таким как конфиденциальность, целостность и доступность (CIA), а также эффективность активов, эффективность, надежность, соответствие, подотчетность и аутентификация (E2RCA2), угрозы, уязвимости, риски и средства контроля представлены в онтологической структуре, которая формализуется с помощью стандартного языка веб-онтологий World Wide Web (W3C) (OWL)7 для моделирования. Разработанные концепции безопасности в онтологии были правильно определены и связаны в иерархической основе. Кроме того, общая деятельность MACO предлагается осуществлять с использованием восьми этапов аудита, которые определены в рамках данной структуры.

Предлагаемая Онтологическая Структура

Онтология - это совокупность понятий, представляющих знания более высокого уровня в иерархии знаний в данной организации.8 онтологическая структура помогает нам понять конкретные области, потому что иерархия классов онтологии подобна тому, как люди хранят знания. В настоящее время онтология широко используется для описания знаний конкретной предметной области и достижения многократного использования и обмена знаниями, которые могут быть переданы между людьми и приложениями.9 Чтобы сделать онтологию доступной для информационных систем, были разработаны и предложены для стандартизации различные онтологические языки. Наиболее популярным является OWL, который был стандартизирован консорциумом W3C и был принят в этой онтологической структуре. Концепции, извлеченные из обзора литературы и обзорного исследования, привели к предложенной онтологии, изложенной в этой статье. Разработанная структура онтологии безопасности состоит из трех основных уровней (рис. 1):

Первый уровень иллюстрирует активы организации и ее цель обеспечения безопасности. На этом уровне аудитор или ответственные организационные органы могут идентифицировать активы, принадлежащие организации, и их классификацию, основанную на целях безопасности или свойствах активов CIA и E2RCA2. Этот рамочный уровень не требует привлечения экспертов для определения активов и целей обеспечения безопасности Организации.

Нечаев А.Р. Аудит безопасности информационных систем // Студенческий форум: электрон. научн. журн. 2020. № 2(95). URL: https://nauchforum.ru/journal/stud/95/64825 (дата обращения: 30.08.2025).

Второй уровень фреймворка изображает измерения серьезности атаки с заявленным значением угроз. В явном виде описаны уязвимости и лежащий в их основе анализ рисков для требуемых активов. Таким образом, для эффективного выполнения этих задач на данном уровне требуется определенный обученный персонал и/или участие аудитора.

На третьем уровне онтологии представлены необходимые элементы управления, которые представлены в виде физических, административных и логических элементов управления для бизнес-требований (CIA и E2RCA2). Кроме того, представлены восемь пошаговых процессов аудита безопасности и типы аудита. Этот уровень структуры требует определенного опыта для лучшего достижения цели аудита безопасности.

Основополагающий принцип, лежащий в основе этой онтологии, кратко описывает фундаментальные понятия безопасности и их взаимосвязи. Таким образом, концептуальная модель определяет 10 основных понятий, 21 субконцепт и более 20 взаимосвязей (рис.1). Основными понятиями являются владелец, актив, цели безопасности, уязвимость, угроза, источники, атака, риск, контроль и аудит безопасности, но отношения между компонентами описываются на основе этих фундаментальных понятий:

Актив - это нечто ценное, принадлежащее организациям или частным лицам. Некоторые активы требуют, чтобы другой актив был идентифицируемым и полезным. Актив имеет набор свойств безопасности (CIA) и должен учитывать дополнительные свойства E2RCA2, цель безопасности, на которую влияют как уязвимости, так и источники угроз, а также угрозы, исходящие из источников угроз и эксплуатируемые уязвимостями.

Уязвимости и угрозы повышают вероятность атаки, и чем выше стоимость актива, тем больше вероятность того, что он станет объектом атаки. Более серьезные угрозы и уязвимости делают инциденты атаки более серьезными, а более серьезные атаки приводят к более существенному риску.

Этот риск смягчается с помощью средств контроля, которые являются административными, логическими и/или физическими. Контроль помогает снизить риск, но для того, чтобы сделать контроль над риском практическим, следует использовать надлежащие процессы аудита безопасности (например, восемь этапов аудита).

Наличие надлежащей безопасности должно проверяться и гарантироваться внутренними и внешними аудитами и контролями безопасности и должно обладать превентивными, детективными и корректирующими свойствами. Таким образом, аудит — безопасности-это не разовая задача, а непрерывный процесс (регулярный или случайный).

Внедрение механизмов контроля помогает уменьшить угрозы, блокировать источник угроз, защитить свойства безопасности, защитить уязвимости и сохранить активы в безопасности путем внедрения различных концепций оценки риска и обнаружения атак. Владельцы активов стремятся минимизировать риск, поэтому они должны быть осведомлены об источниках угроз и уязвимостей. Затем они должны ввести различные механизмы контроля для предотвращения угроз от источника и / или обнаружения нарушений и уменьшения ущерба после того, как атака произошла.

Список литературы:

1. Дмитриева, И.М. Бухгалтерский учет и аудит: Учебник и практикум для СПО / И.М. Дмитриева. - Люберцы: Юрайт, 2016. - 323 с.

2. Донцова, Л.В. Учет, аудит и налогообложение в обеспечении экономической безопасности предприятий. т2 / Л.В. Донцова. - М.: Русайнс, 2015. - 304 с.

3. Донцова, Л.В. Учет, аудит и налогообложение в обеспечении экономической безопасности предприятий. т 1 / Л.В. Донцова. - М.: Русайнс, 2017. - 512 с

4. Еленевская, Е.А. Учет, анализ, аудит: Учебное пособие / Е.А. Еленевская, Л.И. Ким, С.Н. Христолюбов. - М.: Инфра-М, 2018. - 319 с.

5. Камысовская, С.В. Банковский финансовый учет и аудит: Учебное пособие / С.В. Камысовская, Т.В. Захарова, Н.Н. Попова. - М.: Форум, 2019. - 64 с.

6. Кобозева, Н.В. Банкротство: учет, анализ, аудит: Практ. пос. / Н.В. Кобозева. - М.: Магистр, 2018. - 368 с.

7. Лустов, Н.С. Учет, анализ и аудит основных и оборотных средств предприятия / Н.С. Лустов. - М.: Русайнс, 2016. - 31 с.

8. Лытнева, Н.А. Учет, анализ и аудит внешнеэкономической деятельности коммерческих организаций: Учебное пособие / Н.А. Лытнева, Т.В. Федорова, Е.А. Боброва. - М.: Форум, 2018. - 208 с.