Чмыхалова Анастасия Вячеславовна, Студент
Финансового университета при Правительстве РФ,
Финансовый университет при правительстве РФ,
4-й Вешняковский проезд, 4, Москва, Россия

Сосновский Матвей Владимирович, Студент
Финансового университета при Правительстве РФ,
Финансовый университет при правительстве РФ,
4-й Вешняковский проезд, 4, Москва, Россия

Научный руководитель:
Резниченко Сергей Анатольевич,
Кандидат технических наук, доцент,
доцент департамента информационной безопасности
Финансового университета при Правительстве РФ,
Финансовый университет при правительстве РФ,
Ленинградский пр–кт, 49, Москва, Россия

ПРОБЛЕМЫ В ПРОВЕДЕНИИ АУДИТА ИБ И СПОСОБЫ ИХ РЕШЕНИЯ

Аннотация: Данная статья обсуждает основные проблемы, с которыми сталкиваются процессы аудита информационной безопасности (ИБ) и предлагает методы и стратегии для их преодоления. Путем анализа существующих проблем, авторы предлагают практические рекомендации для улучшения проведения аудита ИБ. Также рассматривается технологические инструменты и методики, которые могут быть применены для устранения данных проблем, направленных на повышение эффективности и точности аудиторского процесса. Статья представляет собой полезный обзор источников проблем в процессе аудита ИБ, предоставляя современные методы их решения.

Ключевые слова: информационная безопасность, аудит ИБ, процесс проведения, проблемы, способы решения.

В современной компьютерной среде аудит информационной безопасности (ИБ) становится все более важным инструментом для защиты компьютерных систем и данных от различных угроз. Аудит позволяет выявлять и анализировать потенциальные уязвимости в системе, а также проверять соответствие установленным стандартам безопасности.

Проведение аудита ИБ позволяет выявлять и устранять слабые места в системе защиты, прежде чем они могут быть использованы злоумышленниками для атак. Кроме того, аудит помогает улучшить процессы управления безопасностью, повысить осведомленность сотрудников о правилах безопасности и обеспечить соответствие компьютерных систем требованиям законодательства.

Однако в ходе проведения аудита информационной безопасности могут возникнуть различные проблемы, которые замедляют или затрудняют процесс проверки и оценки уровня безопасности системы.

Одной из значительных таких проблем является отсутствие универсальных стандартов и регуляций. Данная трудность в проведение аудита заключается в том, что разнообразие практик в разработке собственных методик и процессов аудита различных компаний затрудняет сопоставление и сравнение результатов аудита между ними. Это может привести к

непониманию и неспособности оценить уровень безопасности по стандартным критериям. Различные компании могут упустить важные аспекты безопасности или недооценить определенные уязвимости из-за отсутствия четких регуляций.

Решением данной проблемы будет являться разработка и внедрение общих нормативных актов, которые были бы применимы ко всем организациям. Данные стандарты должны быть разработаны с учетом лучших практик и в соответствии с международными стандартами безопасности информации. Важно также создать механизмы для мониторинга и контроля соблюдения этих стандартов, включить в обучающие программы для специалистов по ИБ обязательное изучение и использование данных стандартов.

Важно отметить проблему ограниченности ресурсов, так как для проведения аудита ИБ требуются определенные средства, включая квалифицированных специалистов, специализированные программные средства, затраченное время, финансовые и материальные ресурсы. Недостаток любого из данных ресурсов может привести к неполной или неэффективной оценке информационной безопасности.

Для устранения данной проблемы необходимо определить приоритетные области и процессы, которые требуют особого внимания при проведении аудита. Это позволит оптимизировать использование ресурсов и сосредоточить усилия на наиболее значимых и уязвимых компонентах ИБ. Также можно использовать автоматизированные инструменты для сбора и анализа данных, что поможет сократить время и ресурсы, затрачиваемые на проведение аудита. Стоит распределить задачи и ответственность между участниками команды аудиторов, чтобы повысить эффективность работы и сэкономить ресурсы.

Следующей проблемой можно выделить недостаточную осведомленность об изменениях в угрозах и уязвимостях. В современном мире угрозы и уязвимости в области ИБ постоянно развиваются, и отслеживание этих изменений обязательно для поддержания безопасности организации. Во время аудита ИБ специалисты должны быть в курсе последних изменений в угрозах и уязвимостях, чтобы обнаружить потенциальные риски и проблемы в системе безопасности и предотвратить возможные кибератаки или утечки данных.

Чтобы избежать данную проблему необходимо регулярно обновлять свои знания по актуальным угрозам и уязвимостям, которые можно найти в Реестре угроз и уязвимостей ФСТЭК, а также следить за изменениями в области ИБ. Обмен опытом и знаниями с другими специалистами в области ИБ, участие в профессиональных сообществах, конференциях, семинарах и других мероприятиях может помочь получить свежие знания и практические советы. Использование современных инструментов и методик также помогут справиться с данной проблемой, ведь с каждым днём появляются новые инструменты для аудита и обнаружения угроз и уязвимостей. Компании, занимающиеся аудитом ИБ, должны постоянно обновлять свой арсенал инструментов, чтобы быть в курсе последних тенденций.

Отсутствие полного понимания бизнес-процессов можно выделить как проблему при проведении аудита информационной безопасности. Аудиторам сложно оценить уровень рисков в информационной безопасности, если они не имеют достаточного понимания того, как работает бизнес и как используются технологии в конкретной организации. В следствие это может привести к неверному выбору методов и технологий для защиты информации.

Для решения этой проблемы необходимо обеспечить аудиторов дополнительным обучением по бизнес-процессам, чтобы они могли более точно оценивать ситуацию и принимать обоснованные решения. Также существует множество инструментов автоматизации, которые позволяют собирать, анализировать и визуализировать данные о бизнес-процессах. Такие инструменты могут значительно облегчить задачу аудиторов и помочь им получить более полное представление о процессах в компании. Комбинация

обучения, вовлечение представителей бизнеса и налаживание с ними коммуникаций для возможных консультаций при возникновении вопросов может значительно повысить эффективность и точность аудита информационной безопасности.

Таким образом проведение аудита информационной безопасности остается актуальной задачей в современном мире, где цифровые угрозы постоянно эволюционируют.

Понимание сложности современных угроз, осознание важности защиты информации и использование современных технологий позволяют предпринимать шаги для улучшения процессов аудита ИБ. Однако важно помнить, что аудит информационной безопасности – это непрерывный процесс, требующий постоянного обновления и адаптации. Для успешного проведения аудита ИБ необходимо постоянное развитие и обучение сотрудников, использование передовых методологий и инструментов, а также постоянное внимание к изменяющимся угрозам и уязвимостям.

Список литературы:

1. Информационная безопасность автоматизированных систем / А.В. Солодянников
2. Проблемы и перспективы проведения аудита информационной безопасности предприятия / Э.Ш. Ганиева
3. Методика проведения аудита информационной безопасности информационных систем
4. Правовые аспекты аудита информационной безопасности: что нужно знать ответственному за ИБ