Сальников Иван Денисович, студент,
Финансовый университет при правительстве
Российской Федерации, г. Москва

АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. ФАКТОРЫ, НА ОСНОВЕ КОТОРЫХ ОСУЩЕСТВЛЯЕТСЯ ПОДБОР СОСТАВА ЭКСПЕРТОВ. ИНДИВИДУАЛЬНЫЕ ХАРАКТЕРИСТИКИ ЭКСПЕРТОВ

Аннотация: Аудит информационной безопасности – сложный процесс, требующий комплексного подхода и, конечно же, должного уровня компетенций членов аудиторской команды.

Ключевые слова: информационная безопасность, аудит информационной безопасности, требования международных стандартов, необходимая квалификация.

Аудит информационной безопасности представляет собой систематическое и независимое исследование, оценку и проверку информационных систем, процессов и мер безопасности с целью выявления уязвимостей, оценки эффективности контрольных механизмов и рекомендаций по улучшению уровня защиты данных. Аудит информационной безопасности играет ключевую роль в обеспечении безопасности информационных систем, так как позволяет выявить уязвимости и проблемы безопасности, прежде чем они станут объектом атак со стороны злоумышленников. Он обеспечивает контроль за соблюдением политик и процедур безопасности, а также соответствием требованиям нормативных актов и стандартов в области ИБ. Аудит позволяет оценить эффективность существующих мер безопасности и выявить необходимость внесения изменений или улучшений для защиты информации. Результаты аудита предоставляют руководству информацию о рисках и угрозах безопасности, что позволяет принимать обоснованные решения по улучшению системы защиты информации.

Цели аудита информационной безопасности заключаются в оценке текущего состояния системы защиты информации, выявлении уязвимостей и разработке рекомендаций по их устранению. Задачи включают в себя анализ архитектуры информационной системы, проверку соблюдения политик безопасности, идентификацию потенциальных угроз и рисков, а также оценку соответствия системы требованиям стандартов и законодательства.

Предметная область аудита информационной безопасности включает в себя анализ технических и организационных аспектов защиты информации. Это может быть проверка конфигурации сетевых устройств, проверка безопасности программного обеспечения, анализ политик доступа и контроля, а также оценка процедур управления уязвимостями и инцидентами.

Аудит информационной безопасности должен соответствовать требованиям международных стандартов и рекомендаций, таких как ISO/IEC 27001, а также национальных нормативных актов и законодательства в области защиты информации. Это включает в себя проверку соблюдения правил хранения и обработки персональных данных, защиту от внешних и внутренних угроз, а также учет особенностей регулирующих органов.

Размер и сложность системы или организации определяют область проведения аудита и объем необходимых работ. Большие и сложные системы требуют более детального и всестороннего анализа, включая оценку всех компонентов информационной инфраструктуры и процессов безопасности. Масштаб проекта также определяет необходимый состав экспертов и временные рамки проведения аудита.

Перечисленные специалисты играют ключевую роль в проведении аудита информационной безопасности:

• Лидер команды: Отвечает за организацию работ, распределение обязанностей между участниками команды, контроль сроков выполнения задач и обеспечение согласованной работы всех участников.

• Технические эксперты по информационной безопасности: Осуществляют анализ технических характеристик информационной инфраструктуры, выявляют уязвимости и рекомендуют меры по их устранению. Это могут быть специалисты по сетевой безопасности, администраторы баз данных, эксперты по безопасности приложений и др.

• Эксперты по анализу данных: Отвечают за сбор и анализ данных, связанных с информационной безопасностью, включая логи аудита, статистику инцидентов, результаты сканирования систем и другую релевантную информацию.

• Юридические консультанты: Оценивают соответствие действующему законодательству в области защиты информации, а также применимым стандартам и регуляторным требованиям. Помогают в составлении правовой документации и рекомендаций.

• Эксперты по взаимодействию с заказчиком: Организуют коммуникацию с клиентом, выявляют его потребности и ожидания, а также обеспечиваю т эффективное взаимодействие между командой аудиторов и представителями заказчика.

Все эти специалисты взаимодействуют для обеспечения всестороннего и качественного проведения аудита информационной безопасности, что позволяет выявить уязвимости и риски, а также разработать рекомендации по их устранению.

Процесс подбора экспертов для аудиторской команды необходимо начинать с определения требований к кандидатам, важно регламентировать необходимые квалификации, навыки и опыт работы, которыми должны обладать кандидаты для успешного выполнения задач аудита информационной безопасности. Требования могут включать как технические компетенции, так и «мягкие навыки», такие как коммуникабельность и способность к работе в команде.

Вторым ключевым этапом процесса подбора экспертов является оценка кандидатов на соответствие требованиям. Он может включать собеседования, тестирование знаний и навыков, проверку профессиональных референсов и анализ предыдущего опыта работы.

Заключительным этапом выступает формирование команды и распределение ролей. После того как кандидаты успешно прошли отбор, формируется аудиторская команда. На этом этапе определяются роли и обязанности каждого члена команды, а также проводится распределение задач в соответствии с их компетенциями и опытом.

Также, можно выделить набор важных характеристик, применяемый к экспертам по информационной безопасности. Чаще всего от аудитора ждут наличия обширного практического опыты работы в сфере информационной безопасности, умения применять передовые методы и технологии для обнаружения и предотвращения угроз. Аудитор должен иметь высшее образование в области информационной безопасности или смежных областях, а также наличие соответствующих профессиональных сертификатов (например, CISSP, CISA, CEH и т. д.). Эксперт обязан специализироваться в конкретной области, например, в сетевой безопасности, защите данных, криптографии, анализе угроз и т.д. Специалисту необходимо обладать достаточными коммуникативными навыками и способностью работать в команде, важно умение эффективно общаться с заказчиком и членами команды, четко выражать свои мысли и идеи, а также успешно взаимодействовать в коллективе, он должен соблюдать высокие стандарты этики и профессионального поведения, а также следовать законодательству и регулятивным требованиям в области информационной безопасности.

Следует помнить, что качество проведения аудита информационной безопасности напрямую зависит от квалификации и опыта членов аудиторской команды. Правильный подбор экспертов является основой успешного выполнения поставленных задач. Нельзя недооценить значения индивидуальных характеристик и профессиональных качеств, каждый член команды должен обладать определенными навыками, знаниями и опытом, необходимыми для решения конкретных задач аудита. Важно учитывать технические компетенции, коммуникабельность, аналитические способности и общий профессионализм. Для эффективного подбора экспертов рекомендуется четко определять требования к кандидатам, составлять список требований самостоятельно, основываясь на программно-аппаратных, технических, производственных особенностях и специфики вашей организации, а также проводить тщательную оценку и анализ кандидатов перед формированием команды. Учитывая эти факторы, можно обеспечить успешное выполнение аудиторских процедур и повысить уровень безопасности информационных систем организации.

Список литературы:

1. Штефан, М. А. Основы аудита: учебник и практикум для вузов – 3-е изд., перераб. и доп. – Москва: Издательство Юрайт, 2024. – 313 с. – (Высшее образование). – ISBN 978-5-534-16651-4

2. Голубева Н.А. Состав аудиторской команды – важнейший фактор гарантии качества внешней верификации корпоративной социальной отчетности.

3. Гильиманова Э.А., Ахметшина Р.И., Исмагилов И.Р. Роль аудита информационной безопасности в жизненном цикле системы обеспечения информационной безопасности объектов критической информационной инфраструктуры – Форум молодых ученых. – 2022. – Том 2 (66). – С.34-37