О НЕКОТОРЫХ ПРОБЛЕМАХ АУДИТА ЗАЩИЩЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ И ПУТЯХ ИХ РАЗРЕШЕНИЯ

Кравченко К.Ю., Утин Л.Л.
Иностранное частное производственное унитарное предприятие «АЛКОПАК» (г. Гомель)

В настоящее время на большинстве отечественных предприятий возникают определенные трудности при проведении аудита информационной безопасности (ИБ), что обусловлено множеством причин, отдельные из которых рассматриваются в докладе.

Под аудитом информационной безопасности понимают системный процесс получения объективных качественных и количественных оценок о текущем состоянии информационной безопасности компании в соответствии с определенными критериями и показателями безопасности [1].

Аудит должен включать в себя комплексное обследование функционирования информационной системы (ИС), проведение тестирование на уязвимость ИС, анализ и оценку защищенности ИС, формирование отчета и разработку рекомендаций.

Проведении аудита ИБ, как правило, осуществляется поэтапно:

На первом этапе, оценивается система управления ИБ. Оценка осуществляется в соответствии со стандартами Республики Беларусь 34 серии [2-3]. Однако на практике использование данных стандартов вызывает некоторые трудности, особенно у молодых специалистов, в области защиты информации, что обусловлено сложностью восприятия отдельных разделов стандартов и недостатком практических методик проведения соответствующих проверок.

На втором этапе проводится технологический аудит защищенности ИС. Следует отметить, что из-за отсутствия четких критериев определения степени защищенности ИС, а также практических рекомендаций по оценке уязвимостей ИС не разработаны перечни проверок, которые должен выполнить аудитор с целью оценки технологической защищенности ИС. В результате на практике данный этап выполняется, как правило, формально в соответствии с опытом и интуицией аудитора. При этом в ходе проведение внутреннего аудита (внутри периметра сети) в лучшем случае осуществляют сканирование уязвимостей и анализ настроек операционной

системы и оборудования с точки зрения ИБ. В результате выполнения только данных операций возможно получение только первоначальной оценки о потенциальном наличии уязвимостей ИС и возможных способах проникновения. Эти сведения носят теоретический характер, так как средства практической реализации обнаруженных уязвимостей у аудитора, как правило, отсутствуют. В результате ответить на вопросы, можно ли реализовать практически обнаруженные уязвимости, каким образом будет действовать реальный взломщик, находясь внутри ИС компании, куда он реально сможет проникнуть, можно лишь предположительно.

Пути разрешения изложенных и некоторых других проблем, выявленных в ходе практической деятельности связанной с аудитом ИБ предприятия предлагаются авторами для обсуждения.

Литература:

1. «Аудит безопасности Intranet». С.А. Петренко. 2002 г.
2. СТБ 34.101.1-2004, СТБ 34.101.2-2004. ОИПИ НАН Беларуси, г. Минск.
3. СТБ 34.101.30-2007. ОИПИ НАН Беларуси, г. Минск.

ОЦЕНКА ДОПОЛНИТЕЛЬНОЙ ТРУДОЕМКОСТИ РАЗРАБОТКИ ЗАЩИЩЕННЫХ ПРОГРАММНЫХ СРЕДСТВ

Лабоцкий В.В.
Академия управления при Президенте Республики Беларусь (г. Минск)

В работе представлена модель оценки дополнительной трудоемкости разработки защищенных ПС. В основе данной модели лежит метод COCOMO II, а также итерационная модель жизненного цикла RUP (ЖЦ RUP - Rational Unified Process). COCOMO II оценивает трудоемкость и сроки разработки ПС только в пределах двух фаз ЖЦ RUP: проектирование (Elaboration) и разработка (Construction). COCOMO II не оценивает следующие работы: научно-исследовательскую работу; системное администрирование; разработку системы (закупка оборудования и ПО, развертывание ПС); создание базы данных; создание нормативно-справочной информации; сопровождение ПС; разработку защищенных ПС.