УДК 004.056

МЕТОДЫ ОРГАНИЗАЦИИ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Залимбекова А.А., Мухамеджанова К.А., Абдулаев А.А.
Кыргызский государственный университет строительства, транспорта и архитектуры имени Н. Исанова

В статье рассмотрены существующие методы организации аудита информационной безопасности. Приведен анализ методов аудита с помощью системы балльных оценок по критериям.

Ключевые слова: аудит информационной безопасности, активный аудит, экспертный аудит, аудит на соответствие стандартам, уязвимость.

МААЛЫМАТТЫК КООПСУЗДУКТУН АУДИТИН УЮШТУРУУ МЕТОДДОРУ

Залимбекова А.А., Мухамеджанова К.А. , Абдулаев А.А.
Н. Исанов атындагы Кыргыз мамлекеттик курулуш, транспорт жана архитектура университети

Макалада маалыматтык коопсуздуктун аудитин уюштуруу боюнча колдонулуп жаткан методдору каралган. Критерийлер боюнча баллдык баалоо тутумунун колдонуу менен аудиттин методдорун талдоо келтирилген.

Баштапкы сөздөр: маалыматтык коопсуздук аудити, жигердүү аудит, эксперттик аудит, стандарттарга шайкештиги, алсыздыгы.

METHODS OF ORGANIZATION OF INFORMATION SECURITY AUDIT

Zalimbekova A.A., Mukhamedzhanova K.A., Abdulaev A.A.
Kyrgyz State University of Construction,
Transport and Architecture named after N. Isanov

The article discusses the existing methods of organizing an information security audit. The analysis of audit methods using a system of scoring by criteria is given.

Keywords: information security audit, active audit, expert audit, audit for compliance with standards, vulnerability.

Введение. На сегодняшний день практически все коммерческие и государственные предприятия не может эффективно функционировать, если не применяют автоматизированные информационные технологии (АИС). Использование АИС можно рассматривать как мощный инструмент для работы с информацией, которой является ценным активом предприятий. И пока информация считается актуальной, тем не менее конфиденциальной, однозначно требует соответсвующей защиты в зависимости от ее степени секретности. Для того, чтобы понять насколько эффективно защищены информационные активы от различных информационных атак злоумышленников, предприятиям необходимо иметь объективную оценку текущего уровня безопасности АИС. Именно для этих целей применяется аудит информационной безопасности [1].

Аудит информационной безопасности – это независимая и объективная оценка системы безопасности ИС.

Методы аудита информационной безопасности.

Мероприятия по проведению аудита можно подразделять на три вида, которые приведены на рис.1.

Рис. 1. Методы аудита информационной безопасности

Рассмотрим более подробно каждого из них.

Экспертный аудит предполагает процесс выявления недостатков в системе мер защиты предприятий на основе имеющегося опыта экспертов, участвующих в процедуре аудита [2]. Данный вид аудита считается актуальным, когда нет необходимости в комплексном обследовании

организации, тем самым аудит проводится в основном на наиболее критичных ресурсах ИС.

Процесс проведение мероприятий экспертного аудита представлен на схеме 1.

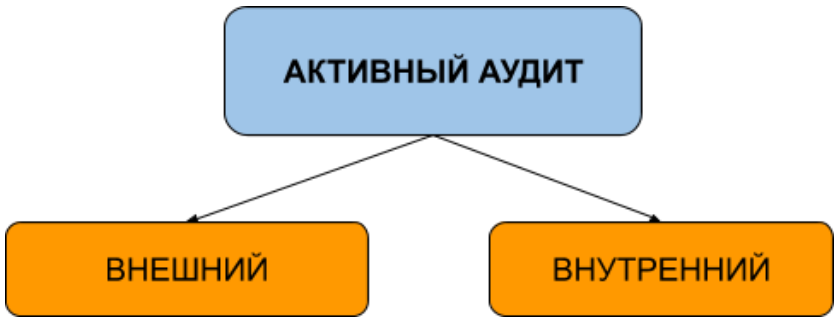
Схема 1. Процесс проведения экспертного аудита

Результаты экспертного аудита могут содержать рекомендации по совершенствованию в основном документационного характера, таких как организационно-распорядительных, методологических, управленческих и процедурных компонентов ИС.

Активный аудит является одним из самых распространенных видов аудита. Также данного вида аудита называют как инструментальный. Под активным аудитом моделируется реальные воздействия на исследуемую систему с точки зрения злоумышленника или же противника (имея в виду, некоего хакера, обладающего высокой квалификацией в сфере информационных технологии).

Данный вид аудита преимущественно на обследование защиты технических подсистем.

Существует два вида данного аудита: внешний и внутренний аудит.



1. Внешний аудит имитирует действия злоумышленника извне удаленно или через Интернет.
2. Внутренний аудит аналогичен, как и внешний, но имитирует действия злоумышленника изнутри предприятий.

Результатами активного аудита является аналитический отчет о текущей состояние системы защиты, т.е. перечень уязвимостей со степенью их критичности, а также данные найденные извне сети, которые не должны быть общедоступными.

По окончании исходя из анализа исследовании дополнительно может быть предложен план работы по совершенствованию системы защиты, от внутренних и внешних угроз.

Аудит на соответствие стандартам ИБ основывается на применение стандартов информационной безопасности (СИБ). В СИБ дается наборы требований безопасности в зависимости от уровня защищенности ИС для различного класса, и ее принадлежности будь это коммерческая организация, либо государственное учреждение. Важно правильно определить набор требования стандарта, чтобы соответствовало для исследуемой ИС. Необходимо правильно выбрать методику, позволяющая оценить это соответствие.

На практике данный метод аудита распространен из-за своей простоты, т.е. заранее определен стандартный набор требований для проведения аудита и позволяет делать обоснованные выводы о состоянии ИС указанной рекомендации в стандартах.

У нас в Кыргызской Республике отсутствует национальные стандарты, методика проведения аудита, кроме в банковской сфере. Однако, частично

для государственных учреждений можно использовать нормативные акты, такие как:

- Постановление Правительства КР от 21 ноября 2017 года № 762 "Об утверждении Требований к защите информации, содержащейся в базах данных государственных информационных систем".
- Постановление Правительства КР от 21 ноября 2017 года № 760 "Об утверждении Требований к обеспечению безопасности и защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных.

По результатам данного аудита составляется отчеты, содержащие следующую информацию:

− степень соответствия проверяемой ИС выбранным стандартам;

− количество и категории полученных несоответствий и замечаний;

− рекомендации по построению или модификации СОИБ, позволяющие привести ее в соответствие с требованиями рассматриваемого стандарта.

Анализ методов аудита ИБ с помощью системы балльных оценок по критериям

В таблице 1. приведены достоинства и недостатки методов аудита ИБ.

Таблица 1. Достоинства и недостатки методов аудита ИБ

Методы	Достоинства	Недостатки
Экспертный аудит	-не требуется спец. ПО; -не требуется прекращение работы ИС на время проведения аудита; -наличие необходимых нормативной базы; -покрытие огромного количества уязвимостей, за счет тщательного исследование.	-необходимость привлечения внешних экспертов-аудиторов; -длительные работы (трудоемкий сбор данных и анализ); - Отсутствуют средства автоматизации процесса; - необходимость доверия оценкам экспертов

Активный аудит	-автоматизация процесса; -большое количество спец-х ПО для аудита; -возможно производить аудит собственными силами организации; - выявляет неизвестных уязвимостей;	-во время аудита требуется прекращение работы системы; -отсутствуют нормативные базы для проведение аудита;
Аудит на соответствия стандартам	-порядок проведения аудита регулируется соответствующими стандартами - не требуется остановка работы ИС при проведении аудита -в результате аудита возможность получить сертификат безопасности; - наличие описания отчетных документов и лучшие практические рекомендации в стандартах.	-необходимость привлечения внешних экспертов-аудиторов; -вероятность длительного проведения процедуры аудита; - необходимость доверия оценкам экспертов - при изменении состояние ИС требуется повторное проведение аудита -стандарты постоянное обновляются.

Методы аудита ИБ можно оценить по следующим критериям

- К1- вероятность автоматизации процесса аудита
- К2-наличие специализированного ПО для проведения аудита
- К3-необходимость участие сотрудников организации в процессе проведения аудита
- К4-Вероятность длительного проведения процедуры аудита.
- К5-Наличие необходимых нормативно-правовых, стандартных методических документов
- К6-Вероятность на влияние работы ИС во время проведения аудита

- К7-Вероястность выявление неизвестных угроз и уязвимостей

Каждый критерий можно оценить по шкале от 0 до 3

- К1= {3-высокая, 2-средняя, 1-низкая, 0-отсутствует}
- К2= {3-имеются,2-частично, 0- отсутствует}
- К3= {0-необходимо, 3-необязательно}
- К4= {0-высокая,2-средняя, 3-низкая}
- К5= {3-имеются,2-частично,0- отсутствует}
- К6= {3-низкая,2-средняя, 0-высокая}
- К7= {3-высокая, 2-средняя, 1-низкая}

Общая оценка рассчитывается по формуле (1)

$$S = \sum_{i=1} K_i$$

В таблице 2. отображена оценка методов в соответствии свыше указанными критериями.

Таблица №2. Оценка методов аудита ИБ

Критерии	**Экспертный аудит**	**Активный аудит**	**Аудит на соответствие стандартам**
К1-вероятность автоматизации процесса аудита	1	3	2
К2-вероятность применение специализированного ПО для проведения аудита	1	3	2
К3-Необходимость участие сотрудников организации в процессе проведения аудита	0	3	0
К4-Вероятность длительного	2	3	0

проведения процедуры аудита.			
k5-Наличие необходимых нормативно-правовых, стандартных методических документов	3	0	3
К6-Вероятность на влияние работы системы во время проведения аудита	3	0	3
К7-Вероястность выявление неизвестных угроз и уязвимостей	2	3	2
Итого	10	15	13

Из таблицы №2 видно, что лучшим методом аудита безопасности будет являться - Активный аудит.

Вывод. На сегодняшний день многие исследовательские работы направлены на исследование аудита [1, 2].

При этом, активный аудит является недостаточно изученной теоретической областью аудита.

Однако в работе [3] рассматривается один из методик активного аудита “тест на проникновение”, в котором носят в большей степени практический характер, чем теоретический.

Тест на проникновение представляет собой демонстрацию возможности проникновение в ИС, тем самым позволяет эффективный способ показать уязвимостей в системе защиты. Такой подход имитирует действия злоумышленника, максимально приближая к реальной среде функционирования ИС.

Тест на проникновение можно считать гибким инструментом, чем, например, мероприятия оценка соответствия стандартам, поскольку его

проведение на ограничивается рамками существующих стандартов или регламентов.

Такой способ предоставляет возможность более широкий выбор средств и методов тестирования (оценивания) защищенности АИС. А также может быть гораздо избирательном в достижении цели аудита. Например, тестирование систем к угрозам, дает возможность выявлять уязвимости, в которых еще отсутствует в базах угроз и уязвимостей. Именно поэтому активный аудит как отдельный область аудита ИБ должна рассматриваться более актуальной, важной и ведущей относительно действующих стандартов ИБ.

Таким образом, исходя из вышеприведенного анализа самым лучшим является активный аудит, и является дальнейшим направлением нашей исследовательской работе.

ЛИТЕРАТУРА

1. Кравчук Д. И., Коркушко Д. А. Аудит безопасности корпоративных информационных систем // Молодой ученый. — 2015. — №10. — С. 697-700. — URL https://moluch.ru/archive/90/19022/ (дата обращения: 04.04.2020).

2. Макаренко С. И. Аудит информационной безопасности: основные этапы, концептуальные основы, классификация мероприятий // Системы управления, связи и безопасности. 2018. № 1. С. 1–29. URL: http://sccs.intelgr.com/archive/2018-01/01-Makarenko.pdf

3. Курило А. П., Зефиров С. Л., Голованов В. Б. и др. Аудит информационной безопасности. – М.: Издательская группа «БДЦ-пресс», 2006. – 304 с.