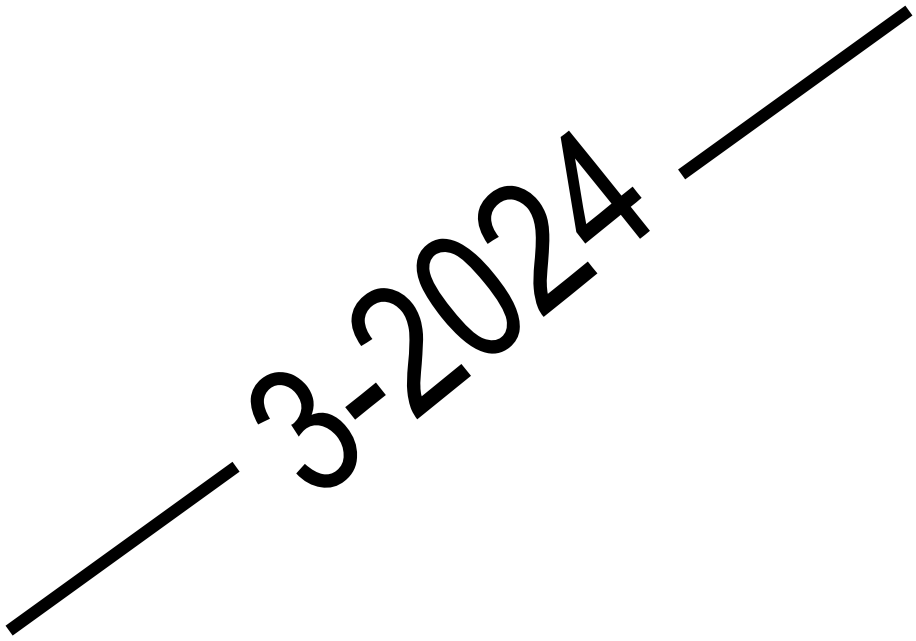
O‘ZBEKISTON RESPUBLIKASI

OLIY TA’LIM, FAN VA INNOVATSIYALAR VAZIRLIGI

FARG‘ONA DAVLAT UNIVERSITETI

FarDU. ILMIY XABARLAR

1995-yildan nashr etiladi
Yilda 6 marta chiqadi



НАУЧНЫЙ ВЕСТНИК. ФерГУ

Издаётся с 1995 года
Выходит 6 раз в год

Aniq va tabiiy fanlar

FIZIKA-TEXNIKA

KIMYO

FarDU. Ilmiy xabarlar – Scientific journal of the Fergana State University

Volume 30 Issue 3, 2024-yil **DOI: 10.56292/SJFSU/vol30_iss3/a127**

UO‘K: 004.056.651.5

AXBOROT XAVFSIZLIGINI TEKSHIRISH USULLARINI TAHLIL QILISH

АНАЛИЗ МЕТОДОВ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ANALYSIS OF INFORMATION SECURITY AUDIT METHODS

Abduraimova Bayan Kuandikovna[1]
[1]Evrosiyo milliy universiteti, Qozog‘iston, texnika fanlari nomzodi, dotsent

Ro‘zaliyev Sherzodjon Avazjonovich[2]
[2]Farg‘ona davlat universiteti, p.f.b.f.d., (PhD)

Kayrat Dinara Kayratkizi[3]
[3]Evrosiyo milliy universiteti, Qozog‘iston, magistrant

Annotatsiya

Ushbu maqolada ma’lumotlarning maxfiyligi, yaxlitligi, mavjudligi va haqiqiyligini ta’minlash, shuningdek majburiyatlarning bajarilishini nazorat qilish uchun zarur bo‘lgan axborot xavfsizligini tekshirish usullari ko‘rib chiqilgan. Tadqiqotchilar tomonidan auditning uchta asosiy usuli taklif etilib, ya’ni faol audit, ekspert auditi va muvofiqlik auditi taklif etilib, faol auditlar axborot tizimining xavfsizlik darajasini tajovuzkor nuqtai nazaridan o‘rganilishi, bu esa zaifliklarni aniqlash va ularni bartaraf etish usullarini ishlab chiqish imkonini berishi, ekspert tekshiruvlari axborot xavfsizligi holatini kompaniya rahbariyati talablari va xalqaro tajriba bilan taqqoslashga asoslangan bo‘lib, ma’lumot to‘plash uchun kompaniya xodimlarini so‘roq qilish usuli qo‘llanilishi, muvofiqlik auditlari axborot tizimlarining turli xavfsizlik standartlariga muvofiqligini baholashi belgilab berilgan. Mualliflar har bir usulning ijobiy va salbiy tomonlarini tahlil qilib, unlarning qo‘llanilish sohalari berilgan. Maqolaning asosiy g‘oyasi, axborot xavfsizligi auditi zaifliklar va xavflarni aniqlashga qaratilgan bo‘lib, bu o‘z navbatida kompaniyaning axborot va biznes jarayonlarini himoya qilish darajasini oshirishga yordam beradi.

Аннотация

В данной статье рассматриваются методы аудита информационной безопасности, необходимые для обеспечения конфиденциальности, целостности, доступности и аутентичности информации, а также для контроля выполнения обязательств. Автор выделяет три основных метода аудита: активный аудит, экспертный аудит и аудит соответствия. Активные аудиты исследуют уровень защищенности информационной системы с точки зрения злоумышленника, что позволяет выявить уязвимости и разработать методы их устранения. Экспертные аудиты основаны на сопоставлении состояния информационной безопасности с требованиями руководства компании и международным опытом, а для сбора информации используется метод опроса сотрудников компании. Аудиты соответствия оценивают соответствие информационных систем различным стандартам безопасности. Автор анализирует плюсы и минусы каждого метода и выделяет области применения. Основная идея статьи заключается в том, что аудит информационной безопасности может помочь выявить уязвимости и риски, что в свою очередь поможет повысить уровень защиты информации и бизнес-процессов компании.

Abstract

This article discusses information security audit methods necessary to ensure confidentiality, integrity, accessibility and authenticity of information, as well as to monitor compliance with obligations. The author identifies three main audit methods: active audit, expert audit and compliance audit. Active audits examine the level of security of an information system from the point of view of an attacker, which allows you to identify vulnerabilities and develop methods to eliminate them. Expert audits are based on comparing the state of information security with the requirements of the company’s management and international experience, and the method of interviewing company employees is used to collect information. Compliance audits assess the compliance of information systems with various security standards. The author analyzes the pros and cons of each method and highlights the areas of application. The main idea of the article is that an information security audit can help identify vulnerabilities and risks, which in turn will help to increase the level of protection of information and business processes of the company.

Kalit so‘zlar: *axborot xavfsizligi, audit usuli, ekspert tizimi, ekspert tahlili*

Ключевые слова: *информационная безопасность, метод аудита, экспертная система, экспертный анализ*
Key words: *information security, audit method, expert system, expert analysis*

ВВЕДЕНИЕ

В условиях постоянно меняющейся угрожающей среды и растущей важности информационных ресурсов для бизнеса и общества в целом обеспечение информационной безопасности становится приоритетной задачей. Это означает не только защиту информации от несанкционированного доступа, но и обеспечение конфиденциальности, целостности, доступности и аутентичности. В этом контексте аудит информационной безопасности является важным инструментом для оценки текущего состояния систем защиты и выявления уязвимостей, которые могут привести к инцидентам безопасности.

Понимание угроз и уязвимостей является основой для эффективного аудита информационной безопасности. Угрозы представляют собой потенциальные риски для информационной системы или организации, а уязвимости — слабые места в системе, которые могут привести к возникновению этих угроз. Изучение событий и инцидентов в области информационной безопасности может помочь выявить уязвимости и риски и разработать стратегии и меры по их предотвращению.

АНАЛИЗ МЕТОДОВ АУДИТА

Аудиты информационной безопасности позволяют систематически проверять соответствие ваших систем защиты требованиям и стандартам безопасности, а также выявлять области, требующие дополнительных улучшений или обновлений. В этой статье рассматриваются три основных метода аудита информационной безопасности: активный аудит, аудит соответствия и экспертный аудит. Каждый из этих методов имеет свои особенности, преимущества и ограничения, и выбрать подходящий метод можно в зависимости от уникальной ситуации и потребностей организации.

Анализ методов аудита информационной безопасности поможет понять их эффективность, а также определить области применения и ограничения каждого метода. Это позволит разработать наиболее эффективную стратегию аудита, направленную на обеспечение максимальной защиты информационных активов организации.

Информационная безопасность означает обеспечение конфиденциальности, целостности, доступности и подлинности информации, а также надежности систем и контроля над выполнением обязательств [1].

В стандарте [1] также вводятся два важных определения: угрозы и уязвимости информационной безопасности.

Угроза — это потенциальная причина нежелательного инцидента, который может нанести вред информационной системе или компании.

Уязвимость — это отрицательная характеристика актива или группы активов, которая может быть использована для реализации одной или нескольких угроз.

Таким образом, информационная безопасность информационной системы может быть нарушена из-за возникновения угроз информационной безопасности, которые реализуются через уязвимости, существующие в информационной системе [6].

Событие информационной безопасности — это зафиксированное событие в работе системы, сервиса или сети, которое указывает на возможные нарушения политики информационной безопасности или повреждения средств защиты, а также на ранее неизвестные ситуации, которые могут повлиять на безопасность [1].

Инцидент информационной безопасности – это отдельное нежелательное или неожиданное событие информационной безопасности (или их совокупность), которое может нанести ущерб бизнес-процессам компании или угрожать ее информационной безопасности [1].

Для предотвращения инцидентов информационной безопасности необходимо проводить аудит информационной безопасности вовремя [3].

Ассоциация аудита и управления информационными системами (ISACA) дает следующее определение термина "аудит информационной безопасности". Аудит информационной безопасности – это процесс сбора и анализа информации, позволяющий

определить, обеспечивается ли безопасность ресурсов организации (включая данные), обеспечиваются ли необходимые параметры целостности и доступности данных, и достигаются ли цели организации в области эффективности информационных технологий.

На сегодняшний день существуют три основных метода аудита информационной безопасности, которые представлены на рисунке 1[4].

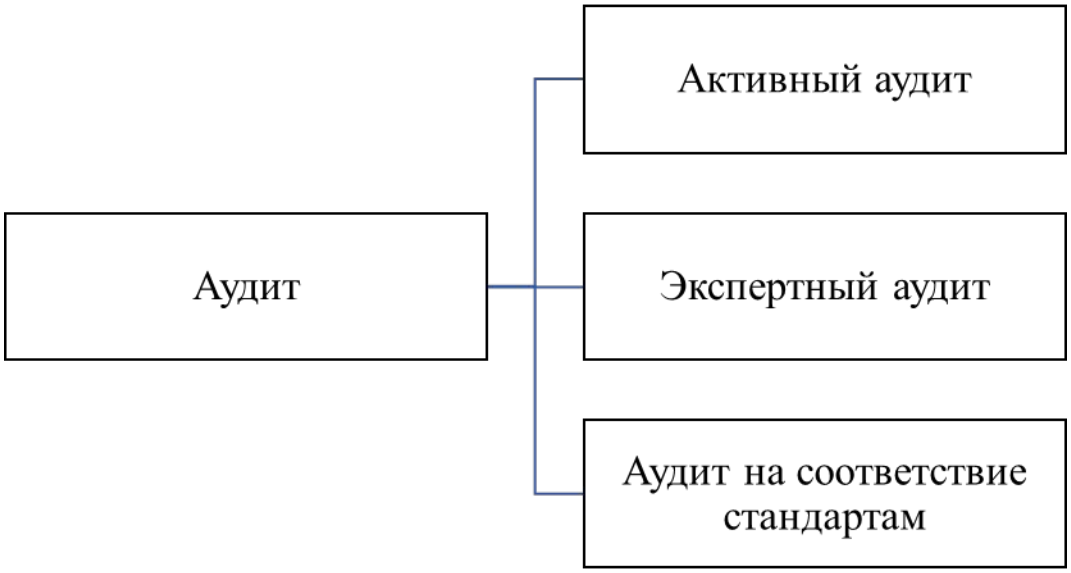


Рис. 1. Виды аудита информационной безопасности

Активный аудит информационной безопасности (ИБ) — это исследование уровня защищенности информационной системы с точки зрения злоумышленника, владеющего информационными технологиями [4]. В ходе такого аудита моделируется максимальное количество атак на системы сетевой безопасности, а аудитору предоставляется только доступная информация из открытых источников. Результатом активного аудита является информация обо всех уязвимостях, их значимости и методах устранения.

Экспертный аудит — это сравнение состояния информационной безопасности на основе требований, предъявляемых руководством компании, с описанием этого состояния на основе мирового и частного опыта, накопленного аудиторской компанией [5]. Для сбора исходных данных об информационных системах используется метод интервьюирования сотрудников компании. Технические эксперты отвечают на вопросы о функционировании информационной системы, а руководящий состав компании рассказывает о требованиях к системе защиты информации. Результаты экспертных проверок включают в себя различные рекомендации по созданию или модернизации системы информационной безопасности.

При проведении аудита на соответствие требованиям состояние информационной безопасности сравнивается с абстрактными описаниями, приведенными в международных и национальных стандартах [3]. Официальный отчет, составляемый по результатам данного вида аудита, содержит информацию о степени соответствия проверяемой информационной системы выбранному стандарту, внутренним требованиям компании в области информационной безопасности, количество и категорию полученных несоответствий, комментарии, а также описание построенной или модифицированной системы информационной безопасности в целях и рекомендации по построению или модификации системы информационной безопасности для приведения ее в соответствие с рассматриваемым стандартом. Отчет также содержит подробную справочную информацию о ключевых документах заказчика, таких как политика безопасности и описание любых кодексов и стандартов, применимых к данной компании.

Анализ методов аудита

Анализ методов аудита информационной безопасности помогает определить их преимущества, недостатки и области применения[9].

Метод аудита	Преимущества	Недостатки
Активный аудит	1. Проверка безопасности путем моделирования реальных атак. 2. Обнаружение конкретных уязвимостей. 3. Практические рекомендации по устранению проблемы.	1. Является дорогостоящим и требует много времени 2. Не охватывает все аспекты безопасности. 3. Конфиденциальность данных проблематична.
Аудит на соответствие стандартам	1. Оценка соответствия различным стандартам безопасности. 2. Систематические аналитические методы. 3. Демонстрация соответствия.	1. Может не обнаружить некоторые уязвимости. 2. Требует значительных усилий и ресурсов для подготовки к аудиту.
Экспертный аудит	1. Использование опыта специалистов для оценки системы; 2. Выявление незамеченных уязвимостей и рисков. 3. Глубокое понимание специфических потребностей.	1. Зависимость от профессиональной квалификации. 2. Значительные временные и ресурсные затраты. 3. Субъективность и непредсказуемость результатов.

Таблица-1. Анализ методов аудита ИБ

Дополнительно можно отметить, что проведение анализа методов аудита информационной безопасности способствует повышению осведомленности и понимания управленческого персонала об инструментах и стратегиях обеспечения безопасности [10]. Это также способствует оптимизации бюджетных затрат и ресурсов организации, а также помогает снизить риски потенциальных угроз для информационных систем. Такой анализ является важным этапом в разработке и реализации политики информационной безопасности, позволяя адаптировать подходы к конкретным потребностям и характеристикам каждой организации.**ЗАКЛЮЧЕНИЕ**

Рассматриваются основные методы аудита информационной безопасности, анализируются их преимущества, недостатки и области применения. Активные аудиты позволяют моделировать атаки, выявлять уязвимости и давать полезные рекомендации, но требуют значительных ресурсов и могут вызывать проблемы с конфиденциальностью данных. Аудиты соответствия оценивают соблюдение стандартов безопасности, но могут не заметить некоторые уязвимости и требуют значительных усилий для подготовки. Экспертные аудиты опираются на опыт экспертов и могут помочь выявить риски, но зависят от квалификации эксперта и требуют значительных ресурсов.

Выбор наиболее подходящего метода аудита информационной безопасности должен основываться на всестороннем анализе целей, ресурсов и ситуации в организации. Также важно учитывать динамично меняющуюся среду угроз и эволюцию методов и технологий для обеспечения защиты информационных активов и бизнес-процессов организации. Правильно проведенный аудит информационной безопасности является ключевым

элементом в обеспечении безопасности информации и бесперебойного функционирования организации.

СПИСОК ЛИТЕРАТУРЫ

1. Международный стандарт ISO/IEC 17799:2005. Информационные технологии. Технологии безопасности. Практические правила по управлению информационной безопасностью. – http://www.dsec.ru/. – 123 с.

2. ISACA. (2022). Information Security Audit and Assurance. [Online]. Available: https://www.isaca.org/resources/isaca-journal/issues/2022/volume-7/information-security-audit-and-assurance.

3. Браун, Дж., Джонс, М. (2018). Аудит информационной безопасности: лучшие практики и методы. Москва: Издательство "БИНОМ".

4. Гарднер, Дж., Мур, Р., Шрифф, Н. (2019). Методы аудита ИБ: теория и практика. Санкт-Петербург: Питер.

5. Хоул, Д., Леонов, В. (2020). Экспертный аудит в информационной безопасности. Москва: Издательство "Питер".

6. Перекрестов, В., Казаков, А. (2017). Основы аудита информационной безопасности. Москва: Издательство "Эксмо".

7. Стандарт ISO/IEC 27001:2013. (2013). Информационная технология. Методы обеспечения информационной безопасности. Системы менеджмента информационной безопасности. Требования. Москва: Издательский дом стандартов.

8. Аверичников В. И., Рытов М. Ю., Кувылкин А. В., Рудановский М. В. Аудит информационной безопасности органов исполнительной власти: учебное пособие. – М.: Флинта, 2011. – 100 с.

9. Макаренко С. И. Аудит информационной безопасности: основные этапы, концептуальные основы, классификация мероприятий // Системы управления, связи и безопасности. 2018. № 1. С. 1–29.

10. Онлайн ресурс: http://izvestiapgups.org/assets/pdf/04_2010.pdf.

11. Избавиться от заблуждений. Виды аудита информационной безопасности / Р. Е. Просянников // Connect! Мир связи. – 2004. – № 12. – С. 148–151.