УДК 930.25: 616.98:578

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В АУДИТЕ

Б. Д. Андриюк[1)], А. А. Селицкий[2)]

[1)] *студент, Белорусский государственный университет, г. Минск, Беларусь, andribogdim@gmail.com*
[2)] *студент, Белорусский государственный университет, г. Минск, Беларусь, antonselicky@gmail.com*

Научный руководитель: **Н. И. Шандора**

старший преподаватель, Белорусский государственный университет, г. Минск, Беларусь, shandor@bsu.by

В данной статье рассматривается важность проведения аудита информационной безопасности в современном цифровом обществе, где защита информации становится критически необходимой для компаний. Особое внимание уделяется внедрению технологий искусственного интеллекта, которые способны автоматизировать процессы, обеспечить проактивное реагирование на угрозы и проводить непрерывный мониторинг.

Ключевые слова: информационная безопасность; аудит; киберугрозы; искусственный интеллект; внедрение; мониторинг.

INFORMATION SECURITY IN THE AUDIT

B. A. Andriyuk[1)], A. A. Selitskiy[2)]

[1)] *student, Belarusian State University, Minsk, Belarus, andribogdim@gmail.com*
[2)] *student, Belarusian State University, Minsk, Belarus, antonselicky@gmail.com*

Supervisor: **N. I. Shandora**

senior lecturer, Belarusian State University, Minsk, Belarus, shandor@bsu.by

This article discusses the importance of conducting an information security audit in a modern digital society, where information protection is becoming critically necessary for companies. Special attention is paid to the introduction of artificial intelligence technologies that are able to automate processes, ensure proactive response to threats and conduct continuous monitoring.

Keywords: information security; audit; cyber threats; artificial intelligence; implementation; monitoring.

В условиях современного цифрового общества, где информация является важнейшим ресурсом для многих компаний, обеспечение её защиты стало обязательной задачей. С ростом количества цифровых данных и многообразием угроз, аудит информационной безопасности приобретает решающее значение, позволяя выявлять наиболее слабые места и гарантировать эффективную защиту цифровых ресурсов.

Аудит информационной безопасности – это независимая оценка реального уровня защиты информации в компании. Аудит может быть направлен на комплексное изучение защиты информации и на исследование отдельных систем (серверов, сетей передачи данных, систем хранения данных и др.) и процессов [1].

Классические методы аудита информационной безопасности, несмотря на свою результативность, часто обладают ограниченными возможностями для выявления и предотвращения сложных и современных угроз. В связи с этим появляется потребность в использовании современных подходов, которые способны успешно адаптироваться к стремительно изменяющимся условиям киберугроз.

Аудит информационной безопасности проводится в целях:

- Снижения рисков утечки информации: изначально определяется уровень обеспечения информационной безопасности, затем предоставляются рекомендации, которые позволяют повысить уровень защищенности информации и снизить риски их утечки;

- Оптимизации затрат на средства защиты информации (СЗИ): аудит поможет руководству компании эффективно распределять бюджет на поддержку информационной безопасности, учитывая результаты анализа рисков. Это позволит минимизировать возможные финансовые потери, связанные с инцидентами информационной безопасности;

- Построения бизнес-процессов: аудит даст возможность детально проанализировать текущие ИТ-процессы, а также разработать стратегию, которая обеспечит высокий уровень защиты критически важной информации компании;

- Соответствия законодательству: аудит может стать началом к разработке детализированного плана действий для выполнения законодательных требований в области информационной безопасности и защиты персональных данных.

- Традиционные методы аудита информационной безопасности, несмотря на их широкое применение и по сей день, испытывают трудности в нынешних условиях, которые характеризуются быстрыми изменениями и усложнением киберугроз. Их эффективность часто ограничена при выявлении и устранении новых, сложных атак.

К примеру, ручные проверки безопасности, включающие анализ политик, сканирование уязвимостей и оценку конфигураций, подвержены ошибкам и медлительности из-за человеческого фактора, что затрудняет обнаружение современных угроз.

Процесс реагирования на инциденты часто является реактивным, а не проактивным. Это означает, что многие угрозы могут оставаться незамеченными до тех пор, пока не произойдет ущерб, что делает традиционные методы недостаточно эффективными для предотвращения атак.

Использование статических правил и сигнатур для выявления атак также имеет недостатки. Эти методы полагаются на уже известные шаблоны угроз, что делает их не такими эффективными против новых, неизвестных атак.

Традиционные методы часто предполагают проведение аудитов на регулярной основе (например, ежегодно или раз в квартал). Это может привести к тому, что уязвимости, выявленные после завершения аудита, могут оставаться открытыми в течение длительного времени, пока не будет проведен следующий аудит.

Анализ журнала событий, хотя и полезен для выявления аномалий, сталкивается с проблемами большого объема данных и частыми ложными срабатываниями [2].

В результате, традиционные подходы остаются важными, но уже не всегда справляются с новыми вызовами киберпространства. В связи с этим, растет интерес к использованию технологии искусственного интеллекта (ИИ), который может помочь преодолеть эти ограничения и улучшить аудит информационной безопасности, выявляя угрозы в реальном времени и адаптируясь к новым типам атак.

Преимущества использования ИИ в аудите информационной безопасности включают в себя:

- Автоматизация и скорость: в отличие от ручных проверок, алгоритмы анализируют политики, сканируют уязвимости и оценивают настройки систем почти мгновенно, снижая вероятность ошибок, вызванных человеческим фактором;

- Проактивное реагирование на угрозы: системы с ИИ способны в реальном времени анализировать данные и прогнозировать потенциальные угрозы. Это помогает компаниям принимать меры до того, как инциденты успеют нанести ущерб, что существенно повышает уровень защиты;

- Гибкость и обучение: ИИ может подстраиваться под новые и неизвестные угрозы, используя опыт прошлых атак и изучая новые модели поведения. Это делает его более эффективным в обнаружении современных киберугроз, в отличие от систем, работающих только на основе заранее заданных правил и сигнатур;

- Непрерывный мониторинг: ИИ обеспечивает постоянный мониторинг сетей и систем, устраняя потребность в периодических проверках. Это помогает сразу же выявлять уязвимости и реагировать на них, не допуская, чтобы слабые места оставались незащищёнными долгое время;

- Повышение качества решений: ИИ формирует аналитические отчёты и предлагает рекомендации на основе практических данных, что помогает специалистам по безопасности принимать более взвешенные решения. Это позволяет значительно улучшить качество аудита и оптимизировать стратегию управления рисками [3].

Таким образом, в условиях стремительного роста технологий и увеличения числа киберугроз аудит информационной безопасности становится ключевым элементом защиты данных в организациях. Традиционные методы, хотя и остаются значимыми, всё чаще сталкиваются с проблемами при обнаружении и предотвращении современных угроз. Внедрение искусственного интеллекта в аудит информационной безопасности становится эффективным способом устранения этих недостатков, однако требует дальнейшего изучения и осторожности. В перспективе использование ИИ не только поможет снизить риски, но и оптимизирует затраты на защиту данных, обеспечивая более надёжное и безопасное будущее в условиях цифровизации экономики.

Библиографические ссылки

1. Аудит информационной безопасности [Электронный ресурс]. URL: https://hoster.by/service/solutions/informatsionnaya-bezopasnost/audit/ (дата обращения: 25.09.2024).

2. *Титков Д. И., Резниченко С. А.* Революция в аудите информационной безопасности: искусственный интеллект [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/revolyutsiya-v-audite-informatsionnoy-bezopasnosti-iskusstvennyy-intellekt/viewer (дата обращения: 25.09.2024).

3. Применение искусственного интеллекта в ИБ: за и против [Электронный ресурс]. URL: https://www.anti-malware.ru/analytics/Technology_Analysis/AI-in-InfoSec-pros-and-cons (дата обращения: 25.09.2024).