АНАЛИЗ АЛГОРИТМОВ ЗАЩИТЫ SAP-СИСТЕМ ОТ КИБЕРУГРОЗ

Джураев Авазжон Акмалович
магистрант 2-курса Ташкентского университета
информационных технологий имени Мухаммада ал-Хоразмий
e-mail: avazjurayev15@gmail.com

Азизова Зарина Ильдаровна
докторант кафедры “Информационная безопасность” Ташкентского
университета информационных технологий имени Мухаммада ал-Хоразмий
e-mail: z.azizova@tuit.uz

АННОТАЦИЯ

Данная статья описывает восемь ключевых алгоритмов для обеспечения безопасности системы SAP от кибератак. Они включают в себя аутентификацию и авторизацию пользователей, криптографические алгоритмы, обнаружение и предотвращение атак, резервное копирование и восстановление, обновление и патчинг, сегрегацию обязанностей, и мониторинг и анализ данных. Представленный материал представляет собой важный ресурс для профессионалов, ответственных за безопасность системы SAP, а также для всех, кто хочет защитить свою организацию от киберугроз.

Ключевые слова: *SAP, безопасность, обнаружение атак, предотвращение атак, резервное копирование, восстановление, сегрегация обязанностей, мониторинг, анализ данных.*

ABSTRACT

This article describes eight key algorithms for securing an SAP system from cyber-attacks. These include user authentication and authorization, cryptographic algorithms, attack detection and prevention, backup and recovery, updating and patching, duty segregation, and data monitoring and analysis. This material is an important resource for professionals responsible for SAP system security, as well as for anyone who wants to protect their organization from cyber threats.

Keywords: *SAP, security, attack detection, attack prevention, backup, recovery, segregation of duties, monitoring, data analysis.*

ВВЕДЕНИЕ

SAP (Systems, Applications, and Products in Data Processing) – одна из самых популярных и широко используемых ERP-систем в мире. Она используется во многих крупных компаниях для управления бизнес-процессами, финансами, управления персоналом и другими аспектами работы компаний. Однако, такая широкая популярность SAP-систем привлекает к ним внимание хакеров и киберпреступников, которые пытаются получить доступ к конфиденциальной информации и причинить ущерб бизнесу. Для обеспечения безопасности SAP-систем применяются аутентификация и авторизация пользователей, которые помогают убедиться в подлинности пользователя и предоставить ему соответствующие права доступа. Криптографические алгоритмы обеспечивают конфиденциальность, целостность и аутентификацию данных. Обнаружение и предотвращение атак включают в себя механизмы мониторинга и анализа аномальной активности, а также использование систем, которые могут автоматически обнаруживать и блокировать попытки вторжения. Резервное копирование и восстановление помогают минимизировать последствия удачной атаки. Обновление и патчинг позволяют заполнить возможные уязвимости в системе. Сегрегация обязанностей помогает предотвратить возможность злоумышленников получить доступ к критическим данным, разделяя ответственность между несколькими пользователями. Мониторинг и анализ данных позволяют оперативно реагировать на изменения в системе, выявлять и устранять уязвимости.

Оценка текущего уровня защиты системы SAP

С использованием инструментов для сканирования уязвимостей и проверки конфигурации системы, таких как SAP Solution Manager и SAP Security Optimization Service, можно осуществить проверку системы на наличие уязвимостей.

Исходя из основных требований к защите SAP-систем, ключевыми показателями являются:

- реализация меры аутентификации и авторизации пользователей, таких как многофакторная аутентификация, использование сертификатов и ограничение доступа пользователей на основе ролей;
- реализация криптографических алгоритмов для защиты данных в системе, включая шифрование базы данных, шифрование каналов связи и управление ключами шифрования;
- разработка системы обнаружения и предотвращения атак, включая мониторинг событий, интеллектуальный анализ журналов и анализ трафика сети;

- реализация процедур резервного копирования и восстановления данных на случай кибератаки или другого сбоя системы;
- реализация сегрегации обязанностей, чтобы минимизировать возможность внутренних атак и ошибок персонала.
- регулярные обновления системы, для устранения уязвимостей и соответствие стандартам безопасности.

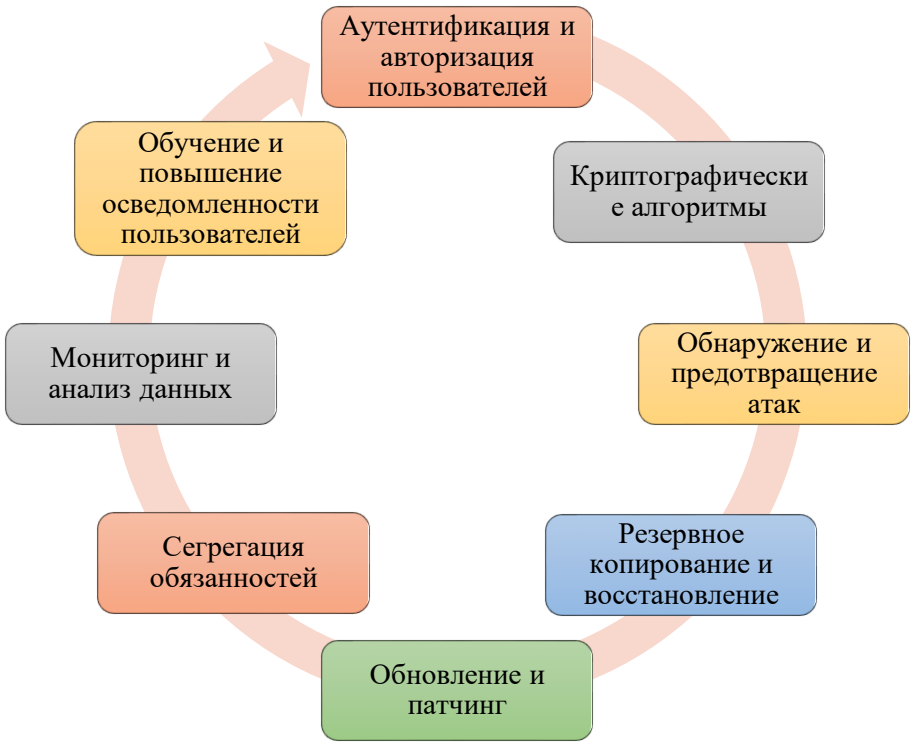

Рис.1. Ключевые этапы защиты SAP-систем

Обучение пользователей правилам безопасности, проведение регулярных тренингов для того, чтобы все сотрудники были в курсе о принятых мерах защиты и знакомы с процедурами реагирования на кибератаки. Рассмотренные этапы образуют цикл непрерывной защиты, который должен регулярно повторяться для обеспечения наивысшей степени безопасности для SAP систем.

ОСНОВНАЯ ЧАСТЬ

Аутентификация и авторизация пользователей

Аутентификация и авторизация пользователей — это ключевые аспекты защиты SAP-систем. Аутентификация — это процесс проверки подлинности пользователя, который пытается получить доступ к SAP-системе. Авторизация — это процесс определения прав доступа пользователя в рамках SAP-системы.

Рис.2. Аутентификация и авторизация пользователей

Процесс аутентификации может включать в себя проверку логина и пароля, использование двухфакторной аутентификации или биометрических методов идентификации, таких как сканирование отпечатков пальцев или распознавание лица. SAP-системы поддерживают различные методы аутентификации, которые могут быть настроены в соответствии с требованиями безопасности компании [1-3].

Процесс авторизации определяет, какие действия и данные пользователь может просматривать, изменять или создавать в рамках SAP-системы. Роли и профили пользователей могут быть настроены в соответствии с ролями и обязанностями внутри компании. Например, пользователи могут быть разделены на группы в зависимости от уровня доступа, и каждая группа может иметь определенный набор прав и привилегий в рамках SAP-системы. Кроме того, SAP-системы могут поддерживать различные методы аутентификации и авторизации для доступа к веб-интерфейсам и мобильным приложениям, таким как OAuth и SAML. Эти протоколы могут обеспечить безопасную и удобную аутентификацию и авторизацию пользователей, используя учетные данные, созданные в других системах [3].

Обеспечение безопасности аутентификации и авторизации пользователей является необходимым условием для защиты SAP-систем от несанкционированного доступа и утечек данных. Компании должны строго следить за использованием сильных паролей, управлять доступом пользователей и регулярно аудитировать свои системы, чтобы обнаруживать и предотвращать возможные уязвимости и угрозы.

Криптографические алгоритмы

SAP предоставляет множество криптографических алгоритмов для защиты данных в своих системах. Эти алгоритмы могут использоваться для шифрования данных в памяти, на диске или в транзакционных логах.

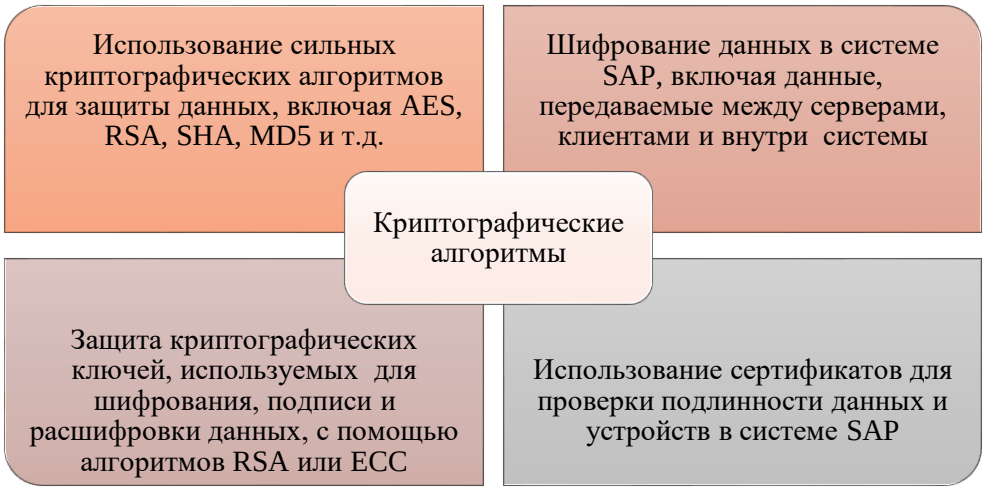

Рис 3. Криптографические алгоритмы, используемые в системе SAP

Некоторые из наиболее распространенных криптографических алгоритмов, используемых в SAP, представлены в таблице 1.

SAP также предоставляет различные инструменты для управления криптографическими алгоритмами, такие как SAP Cryptographic Library (SAPCRYPTOLIB) и SAP Secure Store and Forward (SSF). SAPCRYPTOLIB предоставляет API для шифрования, расшифровки данных и для работы с цифровыми подписями и сертификатами. SSF обеспечивает защиту данных в интеграции между системами SAP. Правильное использование криптографических алгоритмов в SAP требует тщательного планирования и настройки. Необходимо учитывать различные факторы, такие как тип данных, с которыми работает система, уровень конфиденциальности этих данных, и степень защиты, которая необходима для каждого типа данных. Все это должно быть учтено при разработке стратегии безопасности в SAP [4,5].

Таблица 1. Распространенные криптографические алгоритмы, используемые в SAP

Название	Тип	Применение
AES (Advanced Encryption Standard)	Симметричный алгоритм шифрования	Используется для защиты данных в памяти и на диске
RSA (Rivest-Shamir-Adleman)	Асимметричный алгоритм шифрования	Используется для обеспечения подлинности и целостности данных
SHA (Secure Hash Algorithm)	Криптографическая хэш-функция	Используется для создания цифровых отпечатков и проверки целостности данных
MD5 (Message-Digest Algorithm 5)	Криптографический хэш-алгоритм	Применяется для вычисления контрольной суммы данных
S/MIME (Secure/Multipurpose Internet Mail Extensions)	Набор стандартов	Используется для защиты электронной почты с помощью шифрования и цифровой подписи
SSL/TLS (Secure Sockets Layer/Transport Layer Security)	Протоколы защиты транспорта	Применяется для обеспечения безопасности соединений между приложениями и серверами

Обнаружение и предотвращение атак

Обнаружение и предотвращение атак в SAP являются критическими компонентами стратегии безопасности в SAP. Некоторые из наиболее распространенных типов атак в SAP включают в себя SQL-инъекции, переполнение буфера, кражу сессии, атаки типа "человек посередине" (Man-in-the-Middle) и атаки на пароли. Для обнаружения и предотвращения таких атак в SAP можно использовать методы, приведённые в таблице 2.

Для достижения максимальной защиты необходимо использовать несколько методов, включая мониторинг системных журналов, использование средств обнаружения вторжений, защиту в режиме реального времени, обновление системы, проведение аудита безопасности, управление доступом, шифрование данных, использование специализированных инструментов и обучение пользователей [4].

Таблица 2. Методы обнаружения и предотвращения распространенных атак в SAP

Название	Назначение
Мониторинг системных журналов	Запись и хранение всех событий в системе, включая аутентификацию и авторизацию пользователей, попытки входа в систему, изменения конфигурации и т. д. Применяется для обнаружения подозрительной активности и реагировать на нее.
Использование средств обнаружения вторжений	В SAP можно использовать специализированные IDS-системы для обнаружения атак на SAP-систему.
Использование средств защиты в режиме реального времени	Средства защиты в режиме реального времени (Real-time Protection) позволяют мониторить трафик и данные в системе в режиме реального времени, обнаруживать и предотвращать атаки на основе заранее определенных правил.
Обновление системы	Регулярное обновление SAP-системы позволяет устранять уязвимости в системе и предотвращать возможные атаки.
Аудит безопасности	При проведении аудита безопасности можно выявить уязвимости и потенциальные угрозы безопасности, а также определить наилучшие методы защиты и улучшения безопасности в SAP.
Управление доступом	В SAP можно настроить управление доступом на уровне пользователей, ролей, объектов и т. д. Это помогает предотвратить несанкционированный доступ к системе и снизить риск атак.
Шифрование данных	В SAP системах используется шифрование при передаче данных между системами, хранении данных на дисках или отправке данных по электронной почте.
Использование специализированных инструментов	В SAP можно использовать специализированные инструменты, такие как SAP Solution Manager, SAP Enterprise Threat Detection (ETD), SAP NetWeaver Identity Management (IdM) и др., которые помогают обеспечить безопасность в системе.

Резервное копирование и восстановление

Резервное копирование и восстановление — это важная часть стратегии безопасности в SAP, которая помогает обеспечить сохранность и доступность данных в случае непредвиденных сбоев в системе. В SAP существует несколько методов резервного копирования, включая резервное копирование базы данных и файловой системы, а также инкрементное и дифференциальное резервное копирование. Восстановление может быть произведено на уровне базы данных, приложения или операционной системы.

В SAP существует несколько подходов к резервному копированию и восстановлению данных. Например, SAP HANA может быть скопирована с

помощью инструментов SAP HANA Studio или SAP HANA Cockpit, а также с помощью резервного копирования на уровне операционной системы [6,7].

В SAP NetWeaver AS ABAP существует несколько методов резервного копирования, таких как резервное копирование базы данных с помощью инструментов SAP Backup или SAP BR*Tools, а также инкрементное и дифференциальное резервное копирование. Кроме того, в SAP можно использовать такие инструменты, как SAP Solution Manager и SAP Data Intelligence, для автоматизации процесса резервного копирования и восстановления данных.

Рис.4. Возможности резервного копирования и восстановления в SAP-системах

Процесс резервного копирования и восстановления данных должен быть тщательно спланирован и протестирован. Необходимо определить частоту и время выполнения резервного копирования, а также определить процедуры восстановления данных. Важно также проводить регулярное тестирование процедур восстановления данных для убедительности, что они работают правильно и корректно восстанавливают данные в случае их потери или повреждения. Как правило резервное копирование и восстановление — это важные компоненты стратегии безопасности в SAP, которые помогают обеспечить сохранность и доступность данных в случае непредвиденных сбоев в системе [9].

Обновление и патчинг

Обновление и патчинг – это важные меры по обеспечению безопасности SAP-систем. Разработчики SAP регулярно выпускают обновления и патчи, которые устраняют уязвимости и исправляют ошибки. Необходимо следить за релизами обновлений и патчей и своевременно устанавливать их [8].

Сегрегация обязанностей

Сегрегация обязанностей (SoD) в SAP — это концепция, основанная на принципе, что один пользователь не должен иметь возможности выполнения двух или более функций, которые могут привести к мошенничеству или ошибкам в системе. Примером таких функций могут быть управление финансами и снабжением, а также создание поставщиков и оплату счетов [8].

Для обеспечения сегрегации обязанностей в SAP используется модуль безопасности, известный как SAP GRC (Governance, Risk, and Compliance). SAP GRC включает в себя набор инструментов и функций, которые позволяют организациям управлять рисками, связанными с нарушением сегрегации обязанностей, а также удовлетворять требованиям законодательства и стандартов отчетности.

Рис.5. Сегрегация обязанностей в SAP системах

Один из ключевых инструментов SAP GRC — это SAP Access Control, который предоставляет возможность анализировать и управлять правами доступа пользователей в SAP. SAP Access Control позволяет установить политики и правила, которые определяют, какие пользователи могут получить доступ к каким объектам и функциям в системе. Это позволяет организациям обеспечить сегрегацию обязанностей и предотвратить нарушения. Другим важным инструментом SAP GRC является SAP Process Control, который позволяет организациям управлять процессами в рамках SAP, в том числе контролировать выполнение задач и процедур, и отслеживать нарушения сегрегации обязанностей. Также SAP GRC включает в себя инструменты для мониторинга и анализа активности пользователей в системе. Это помогает организациям выявлять и предотвращать потенциальные нарушения сегрегации обязанностей. Сегрегация обязанностей — это не только технический вопрос, но

и вопрос процессов и организации. Для успешной реализации сегрегации обязанностей в SAP необходимо провести анализ бизнес-процессов и установить политики и правила, которые определяют, какие пользователи могут выполнять какие функции в системе [7].

Мониторинг и анализ данных

Мониторинг и анализ данных являются ключевыми аспектами безопасности в SAP. Мониторинг включает в себя постоянное отслеживание системы на наличие потенциальных угроз безопасности, анализ и реагирование на обнаруженные инциденты. Анализ данных помогает выявлять тенденции, паттерны и потенциальные риски в системе, что позволяет предотвращать возможные нарушения безопасности [8].

Рис.6. Мониторинг и анализ данных в SAP системах

Система мониторинга в SAP предоставляет администраторам и безопасности доступ к инструментам, которые позволяют отслеживать события в режиме реального времени. Это позволяет быстро обнаруживать и реагировать на нарушения безопасности, такие как несанкционированный доступ, попытки взлома и другие угрозы. В SAP также существуют инструменты анализа данных, которые помогают выявлять потенциальные риски и аномалии в системе. Один из таких инструментов — это SAP Fraud Management, который использует аналитические технологии, чтобы обнаружить возможные проблемы и риски в бизнес-процессах. SAP Fraud Management анализирует большие объемы данных и выделяет аномалии, которые могут указывать на нарушения безопасности [9,10].

SAP Access Control позволяет администраторам мониторить права доступа пользователей и анализировать доступ к чувствительным объектам и функциям в системе. Это позволяет обнаруживать нарушения сегрегации обязанностей и другие потенциальные угрозы безопасности.

Мониторинг и анализ данных — это непрерывный процесс, который должен быть регулярно обновляется и настраивается. Администраторы и безопасность должны уделять достаточно внимания мониторингу и анализу данных, чтобы обеспечить безопасность системы и предотвратить возможные угрозы мониторинг и анализ данных в SAP могут помочь в предотвращении мошенничества. Например, анализ данных может помочь выявить ненормальные транзакции, которые могут указывать на мошенничество или другие несанкционированные действия. Это позволяет предотвратить потери и сохранить данные и репутацию компании.

Исходя из этого мониторинг и анализ данных в SAP должны соответствовать правилам безопасности и конфиденциальности. Следует использовать только те инструменты, которые полностью соответствуют требованиям безопасности и конфиденциальности, чтобы избежать потенциальных угроз безопасности. Мониторинг и анализ данных — это важный аспект безопасности в SAP. Использование инструментов мониторинга и анализа данных помогает обнаруживать и предотвращать потенциальные угрозы безопасности, а также предотвращать мошенничество и сохранять данные и репутацию компании [8,10].

Обучение пользователей

Обучение пользователей — это важная часть стратегии безопасности в SAP. Обучение пользователей помогает повысить осведомленность о безопасности информации и снизить вероятность несанкционированных действий, которые могут привести к атакам. целях повышения кибербезопасности.

Обучение пользователей является важным аспектом обеспечения безопасности систем SAP. Пользователи, как правило, являются слабым звеном в цепочке безопасности, так как могут стать жертвами фишинговых атак, не использовать достаточно сложные пароли или нарушать правила обработки конфиденциальной информации. Для повышения уровня кибербезопасности необходимо регулярно проводить обучение пользователей, которое поможет им узнать о возможных угрозах и научиться их предотвращать. Обучение должно проводиться как для новых сотрудников, так и для уже работающих [10].

Кроме того, необходимо проводить тестирование пользователей на знание правил безопасности и регулярно напоминать им о необходимости соблюдения этих правил. Например, можно отправлять регулярные электронные письма с напоминанием о правилах безопасности или проводить тренинги и семинары.

Также можно использовать различные обучающие материалы, такие как видеоуроки, интерактивные онлайн-курсы и обучающие программы. Важно не только предоставить информацию о правилах безопасности, но и научить

пользователей их понимать и применять на практике. Обучение пользователей в сочетании с другими аспектами безопасности, такими как аутентификация, криптографические алгоритмы и мониторинг, поможет обеспечить надежную защиту систем SAP от киберугроз.

ОБСУЖДЕНИЕ

Статья описывает основные алгоритмы защиты систем SAP от киберугроз. В целом, эти алгоритмы важны для обеспечения безопасности информации в системах SAP и их использование может помочь предотвратить серьезные последствия, связанные с кибератаками.

Наличие надежной системы аутентификации и авторизации гарантирует, что только правильно аутентифицированные и авторизованные пользователи могут получить доступ к системе и выполнять необходимые действия. Например, использование многофакторной аутентификации (MFA) может существенно повысить уровень безопасности.

Шифрование помогают защитить данные от несанкционированного доступа и обеспечивают конфиденциальность, целостность и доступность информации. Важно использовать сильные криптографические алгоритмы, такие как AES, RSA, SHA, и правильно настроить их параметры.

Системы обнаружения и предотвращения атак помогают автоматически обнаруживать и предотвращать попытки несанкционированного доступа или других видов атак. Это может быть достигнуто путем настройки правил, обнаружения подозрительной активности или использования машинного обучения для выявления новых типов атак.

Резервное копирование помогает сохранить критически важную информацию и восстановить данные в случае их потери или повреждения. Важно проводить регулярные резервные копии и тестировать процедуры восстановления, чтобы убедиться в их работоспособности.

Периодические обновления и патчи позволяют исправлять уязвимости и улучшать безопасность системы. Важно следить за обновлениями и патчами, выпущенными SAP, и применять их в срок.

Дополнительные методы защиты могут включать в себя использование белых списков (whitelisting) для разрешения только определенных программ и сервисов, а также ограничение доступа к определенным частям системы только для авторизованных пользователей и приложений.

Также важно подчеркнуть, что для обеспечения безопасности системы SAP необходимо обновлять ее регулярно и применять все доступные патчи и обновления. Это позволит устранять уязвимости и предотвращать возможные атаки на систему.

И наконец, необходимо убедиться, что все сотрудники компании осведомлены о методах защиты системы SAP и обучены соблюдению соответствующих правил и процедур. Это может включать в себя проведение регулярных тренингов и тестирований на соответствие политикам безопасности компании.

Защита системы SAP от киберугроз требует комплексного подхода и использования различных методов защиты, описанных выше. Только таким образом можно обеспечить надежную защиту от кибератак и сохранить целостность и конфиденциальность бизнес-данных компании.

ЗАКЛЮЧЕНИЕ

В заключение, защита SAP-систем является комплексным процессом, включающим множество аспектов. Необходимо использовать все доступные инструменты и методы защиты, чтобы обеспечить надежную защиту от угроз внутреннего и внешнего характера. Это позволит сохранить конфиденциальность и целостность данных, обеспечить непрерывность бизнес-процессов и защитить репутацию компании. Также обучение пользователей должно быть важной частью политики безопасности компании и происходить регулярно. Это поможет снизить риск уязвимостей и атак, связанных с ошибками персонала.

Литература:

1. "SAP Security for Beginners" by Tanya Duncan.
2. "SAP Security and Authorizations: Risk Management and Compliance with Legal Regulations in the SAP Environment" by Mario Linkies.
3. "SAP Security Configuration and Deployment: The IT Administrator’s Guide to Best Practices" by Joey Hirao and Jim Stewart.
4. "SAP Security Essentials" by Jim Stewart.
5. "SAP Security Interview Questions, Answers, and Explanations" by Stuart Lee.
6. "SAP Security Optimization" by Ariel Litvin and Maxim Chuprunov.
7. "SAP GRC for Dummies" by Denise Vu Broady and Holly A. Roland.
8. "SAP Audit and Control Features: SAP Governance, Risk, and Compliance" by Michael L. Schiller.
9. "SAP Security and Risk Management" by Rajeev Kasturi and Arun K. Murthy.
10. "SAP Security and Risk Management, Second Edition" by Mario Linkies and Gunnar Landwehr.