УДК 621.391: 004.056.5

Потенциальные угрозы и риски при внедрении автоматизации в информационную безопасность

Ю.В. Титова
студентка 1 курса магистратуры НИЯУ МИФИ, Москва
Email: yuvtitova@mail.ru
В.А. Рычков
старший преподаватель кафедры финансового мониторинга
НИЯУ МИФИ, Москва
Email: varychkov@mephi.ru
В.И. Рычкова
старший преподаватель кафедры финансового мониторинга
НИЯУ МИФИ, Москва
Email: virychkova@mephi.ru

Аннотация: *В статье рассматривается возможность автоматизации рабочих процессов специалистов по информационной безопасности. Делегирование части ежедневных задач программному коду сопряжено с потенциальными уязвимостями, которые могут привести к различным угрозам для информационных систем организации. Рассмотрены виды рисков, возникающих в процессе автоматизации, а также предлагаются методы для их минимизации. Особое внимание уделяется важности комплексного подхода к оценке рисков и внедрению мер по защите от возможных атак, что является критически важным для обеспечения устойчивости и безопасности информационной инфраструктуры организации.*

Ключевые слова: *оптимизация, автоматизация, информационная безопасность, угрозы, риски, данные, внедрение*

Potential threats and risks in the implementation of automation in information security

Y.V. Titova
1st year master’s student at the NRNU MEPhI, Moscow
Email: yuvtitova@mail.ru
V.A. Rychkov
Senior Lecturer of department of financial monitoring
NRNU MEPhI, Moscow
Email: varychkov@mephi.ru

V.I. Rychkova
Senior Lecturer of of department of financial monitoring
NRNU MEPhI, Moscow
Email: virychkova@mephi.ru

Abstract: *The article discusses the possibility of automating the work processes of information security specialists. Delegating some of the daily tasks to the program code is fraught with potential vulnerabilities that can lead to various threats to the organization's information systems. The types of risks that arise in the automation process are considered, and methods for minimizing them are proposed. Particular attention is paid to the importance of an integrated approach to risk assessment and the implementation of measures to protect against possible attacks, which is crucial for ensuring the stability and security of an organization's information infrastructure.*

Keywords: *optimization, automation, information security, threats, risks, data, implementation*

Современные организации сталкиваются с возрастающим числом киберугроз, что делает информационную безопасность (ИБ) одним из ключевых аспектов их функционирования. В условиях стремительного развития технологий автоматизация процессов управления безопасностью становится необходимостью для обеспечения эффективной защиты информации. Однако внедрение автоматизации в ИБ не лишено рисков и угроз, которые могут негативно сказаться на общей безопасности организации.

Автоматизация в контексте информационной безопасности представляет собой процесс внедрения технологий и инструментов, которые позволяют выполнять задачи, связанные с защитой информации, без или с минимальным участием человека. Это включает в себя использование программного обеспечения, алгоритмов и систем для автоматического мониторинга, анализа, реагирования на инциденты и управления безопасностью.

Основные аспекты автоматизации в ИБ включают:

1. Мониторинг и анализ. Автоматизированные системы способны непрерывно отслеживать сетевой трафик, журналы событий и другие источники данных для выявления аномалий и потенциальных угроз. Использование машинного обучения и искусственного интеллекта позволяет улучшить точность обнаружения инцидентов.

2. Реагирование на инциденты. Автоматизация процессов реагирования позволяет быстро и эффективно устранять угрозы. Это может включать автоматическое блокирование подозрительных IP-адресов, изоляцию зараженных систем или уведомление специалистов по безопасности о возникших инцидентах.

3. Управление уязвимостями. Автоматизированные инструменты могут проводить регулярные сканирования систем на наличие уязвимостей, оценивать уровень риска и предлагать меры по их устранению.

4. Соответствие требованиям. Автоматизация позволяет организациям более эффективно управлять соблюдением нормативных требований и стандартов безопасности путем автоматического сбора отчетности и ведения документации.

5. Оптимизация процессов. Внедрение автоматизации снижает вероятность человеческих ошибок, ускоряет выполнение рутинных задач и освобождает специалистов по безопасности для решения более сложных проблем.

Цифровизация охватывает все сферы жизни, и автоматизация процессов становится неотъемлемой частью управления информационной безопасностью: организации стремятся к повышению эффективности и снижению затрат, что делает автоматизацию привлекательным инструментом для защиты информации. Однако с внедрением новых технологий возникают и новые угрозы.

С каждым годом количество киберугроз возрастает, и злоумышленники становятся все более изощренными. Автоматизация может как повысить уровень защиты, так и создать новые уязвимости, которые могут быть использованы против организаций. Данная статья направлена на исследование потенциальных угроз и рисков, связанных с внедрением автоматизации в рабочие процессы. В ней рассмотрены задачи, которые подлежат автоматизации, потенциальные угрозы и риски, которые могут возникнуть при внедрении автоматизации, и сформулированы выводы о том, как организации могут эффективно оптимизировать свою работу.

Основная цель исследования заключается в формировании комплексного понимания того, как организации могут эффективно интегрировать автоматизацию процессов без ущерба для уровня безопасности.

Автоматизация в информационной безопасности охватывает несколько типов процессов и задач, которые могут варьироваться от рутинных операций до сложных аналитических процедур. Чтобы определить, какие угрозы могут появиться, важно знать их источники, а для этого необходимо определить задачи, которые могут выполняться программой.

Специалисты по ИБ выполняют широкий спектр задач, включая оценку рисков и уязвимостей, реализацию и управление политиками безопасности, мониторинг событий и активов на предмет инцидентов, реагирование на инциденты и восстановление после атак, обучение сотрудников и повышение их осведомленности, внедрение обновлений и управление конфигурациями. В таблице 1 рассмотрены три отдела департамента

информационной безопасности и определено, какие задачи специалистов могут быть делегированы, а какие нет.

Таблица 1 – Задачи специалистов по ИБ

Роль	Задача	Автоматизация
Сетевые инженеры	Проектирование и внедрение сетевой инфраструктуры	-
	Мониторинг сетевого трафика	+
	Настройка межсетевых экранов и систем предотвращения вторжений (IPS)	+
	Управление виртуальными частными сетями (VPN)	+
	Документирование архитектуры сети	-
Аналитики SOC	Мониторинг событий безопасности	+
	Реагирование на инциденты	-
	Проведение расследований	-
	Создание отчетов о безопасности	-
Специалисты по криптографической защите информации	Аудит существующих систем шифрования	-
	Инициализация ключей шифрования	+
	Обеспечение конфиденциальности данных	-
	Исследование уязвимостей в криптографических протоколах	-

Задачи, отмеченные плюсом в таблице 1, технически автоматизируются с использованием программных скриптов. Например, можно организовать мониторинг сетевого трафика, обнаружение уязвимостей, управление журналами событий, выполнение регулярных проверок безопасности и реагирование на инциденты. Скрипты работают с API различных инструментов безопасности, могут сканировать системы на наличие вредоносного ПО и обеспечивать соответствие требованиям регуляторов.

Скрипт постоянно обрабатывает чувствительные данные, которые перемещаются в сети организации. Эти данные подвержены угрозам, которые представлены на рисунке 1.

Рисунок 1 – Основные каналы воздействия на данные в контексте информационной безопасности

В процессе внедрения программного скрипта в рабочие процессы возникает набор уязвимостей, которые непосредственно влияют на безопасность системы. Существует база данных угроз ФСТЭК, которая содержит информацию обо всех актуальных угрозах безопасности информации. Эта база представляет собой систематизированный ресурс, в котором собраны сведения о различных типах угроз, их характеристиках и способах противодействия. Она служит важным инструментом для организаций, позволяя им проводить анализ рисков и разрабатывать меры по защите информации. Данные из этой базы могут быть использованы для оценки потенциальных угроз при внедрении новых технологий и программных решений, а также для формирования стратегий управления рисками в соответствии с требованиями законодательства и стандартов информационной безопасности.

В дополнение к этому, актуальные уязвимости веб-приложений ежегодно классифицируются некоммерческой организацией OWASP Foundation на основе анализа широкого спектра угроз и атак, а также на основании практического опыта в области кибербезопасности. Отчёт OWASP Top 10 составлен группой экспертов по безопасности со всего мира. Он подвергается регулярным обновлениям, что позволяет учитывать современные тренды и методики, влияющие на безопасность информационных технологий. На момент написания статьи самой актуальной версией документа является отчёт за 2024 год. В состав OWASP Top 10 (2024) были включены следующие уязвимости:

1. Неправильный контроль доступа. Отсутствие адекватной авторизации и аутентификации может привести к эскалации привилегий, позволяя злоумышленникам обходить механизмы контроля доступа (Access Control Lists, ACL) и получать доступ к защищенным ресурсам и данным, что в свою очередь может вызвать утечки конфиденциальной информации и нарушение целостности данных.

2. Криптографические сбои. Неправильная реализация криптографических алгоритмов или использование устаревших протоколов шифрования (например, DES, MD5) может сделать данные уязвимыми для атак "человек посередине" (Man-in-the-Middle) и перехвата, угрожая конфиденциальности передаваемой информации.

3. SQL-инъекции (SQL Injection). Скрипты, взаимодействующие с реляционными базами данных через SQL-запросы, могут быть подвержены инъекциям SQL при отсутствии должной валидации и экранирования пользовательского ввода. Злоумышленник может выполнять произвольные SQL-команды, что приводит к компрометации базы данных, утечке конфиденциальной информации или модификации/удалению данных.

4. Уязвимости межсайтового скриптинга (XSS). Если скрипт не применяет соответствующие меры по экранированию пользовательского ввода (например, HTML-экранирование), злоумышленник может внедрять вредоносные скрипты в контент страниц. Эти скрипты будут выполняться в контексте браузеров других пользователей, что может привести к кражам токенов сессий, cookies и другим атакам на клиента (например, фишинг).

5. Уязвимости удаленного выполнения кода (RCE). Скрипт может принимать ввод от пользователя и выполнять его без достаточной проверки или фильтрации. Это создает возможность для злоумышленника выполнить произвольный код на сервере или клиенте через механизмы интерпретации языка программирования или командной строки.

6. Уязвимые и устаревшие компоненты. Представляют собой критическую уязвимость, возникающую при использовании устаревших библиотек и фреймворков, которые содержат известные уязвимости, задокументированные в базах данных, таких как CVE (Common Vulnerabilities and Exposures). Неподдерживаемые версии компонентов могут быть подвержены эксплуатации со стороны злоумышленников, что повышает риск атак, использующих известные эксплойты, а также может привести к компрометации системы через небезопасные функции и API, несовместимые с современными стандартами безопасности.

7. Недостаточная идентификация и аутентификация. Если скрипт не реализует надежные механизмы аутентификации (например, двухфакторная аутентификация) и не использует безопасные методы хранения паролей (например, хеширование с солью), это может привести к несанкционированному доступу к ресурсам.

8. Сбои в работе программного обеспечения и целостности данных. Скрипт может ошибочно выводить чувствительную информацию в логи или интерфейсы отладки (debugging interfaces), такие как пароли или ключи API. Утечка этих данных может привести к компрометации учетных записей и систем.

9. Сбои в ведении журнала безопасности и мониторинге. Недостаточная реализация логирования событий безопасности затрудняет обнаружение инцидентов безопасности и их расследование, что увеличивает время реакции на атаки.

10. Подделка запросов на стороне сервера (SSRF). Уязвимость SSRF позволяет злоумышленникам инициировать HTTP-запросы от имени сервера к внутренним сервисам или внешним ресурсам. Это может привести к утечке внутренних данных или атакам на другие сервисы внутри сети через доступные API или интерфейсы управления.

При интеграции автоматизированных систем в работу, руководство заведомо идёт на риски, связанные с возможными угрозами и уязвимостями в области информационной безопасности. Эти риски могут повлиять на конфиденциальность, целостность и доступность информации. Для оценки рисков применяются реестры уязвимостей и угроз, представленные в базах данных ФСТЭК. В отношении каждой уязвимости предоставляется информация о следующих параметрах:

- Тип ошибки: классификация уязвимости по характеру проблемы.
- Класс уязвимости: определение категории, к которой относится данная уязвимость (например, код выполнения, утечка информации и т.д.).
- Уровень опасности: оценка степени риска, связанного с эксплуатацией данной уязвимости.
- Наличие эксплойта: информация о том, существует ли готовый инструмент для эксплуатации данной уязвимости.
- Способы эксплуатации: описание методов, которыми злоумышленники могут воспользоваться для реализации атаки на данную уязвимость.
- Способы устранения: рекомендации по исправлению или минимизации риска, связанного с данной уязвимостью.
- В отношении угроз предоставляется следующая информация:
- Описание угрозы: детальное изложение сути угрозы.
- Источник угрозы: указание на возможные источники возникновения угрозы (например, внутренние или внешние злоумышленники).
- Объект воздействия: определение целевых систем или данных, которые могут быть подвержены атаке.
- Последствия реализации угрозы: анализ потенциальных последствий для организации в случае успешной реализации угрозы.

Чтобы идентифицировать риски, каждая организация должна пройти через ключевые этапы: определить активы, выявить уязвимости и угрозы, оценить вероятность их возникновения и последствия для бизнеса. Этот процесс является основой для управления рисками и должен основываться на специфике бизнеса и инфраструктуры каждой конкретной организации. В рамках данной статьи рассматриваются только риски, связанные с внедрением автоматизации.

Уязвимости, рассмотренные ранее, оказывают непосредственное воздействие на:

- программное обеспечение;
- персонал;
- существующие процессы;
- пользовательские данные;
- финансовые ресурсы;
- информационные системы.

Для каждого из этих активов можно идентифицировать определенные угрозы. В связи с этим, экспертная группа разрабатывает подробный реестр уязвимостей и связанных с ними угроз. Сопоставление упомянутых уязвимостей и угроз интеграции программного скрипта в рабочие процессы представлено в таблице 2 (в данной статье экспертом выступает автор).

Таблица 2 – Уязвимости и угрозы внедрения автоматизации

Уязвимость	Угроза
Ошибки в коде, неправильная конфигурация систем	Вредоносные атаки (например, эксплойты) или сбои в работе системы
Недостаточная подготовка сотрудников к новым системам	Сопротивление изменениям и ошибки при использовании новых технологий
Отсутствие четких инструкций использования нововведений	Неправильное выполнение операций из-за недостатка контроля
Отсутствие шифрования или слабые механизмы аутентификации	Компрометация данных
Неправильная оценка затрат или недостаточный анализ ROI	Превышение бюджета или скрытые расходы на поддержку систем
Несовместимость программного обеспечения или протоколов	Сбой интеграции или потеря функциональности существующих решений

На основе этого выявляются риски, и для каждого риска экспертная группа определяет показатели ущерба и вероятности возникновения риска. По таблице 2 можно выделить основные виды рисков, связанных с интеграцией автоматизированных систем в работу специалистов по ИБ. Эти риски можно классифицировать по нескольким категориям, представленным на рисунке 2: технические, организационные,

процессные, риски безопасности данных, правовые, финансовые, интеграционные.

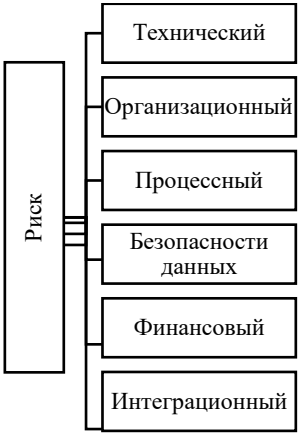

Рисунок 2 – Виды рисков внедрения автоматизации в рабочие процессы

Для каждого выделенного риска эксперты проводят оценку ущерба, вероятности его наступления и уровня риска. На основе этих данных определяется категория риска в соответствии с градацией, установленной в конкретной организации. И после этого принимается решение о том, как поступить с риском: его необходимо снизить, перенести, принять или избежать.

Крайне важно отметить, что в информационной безопасности не существует низкого уровня риска, который был бы приемлемым для организации. Все обозначенные риски требуют внимания и усилий для их снижения. Оценка рисков внедрения автоматизации в рабочие процессы представлена в таблице 3.

Градация уровня риска:

- 0–20: Низкий;
- 20–70: Средний;
- 70–100: Высокий.

Таблица 3 – Риски внедрения автоматизации в рабочие процессы

Риск	Ущерб	Вероятность наступления (%)	Уровень риска	Мера
Ошибки ПО, неправильная конфигурация	Высокий (может достигать сотен тысяч долларов из-за простоя и восстановления)	40-60%	Средний	Снижение

Неготовность к изменениям	Средний (может привести к задержкам в проектах, снижению производительности)	20-40%	Средний	Снижение
Некорректное выполнение операций скриптом	Средний (может привести к неэффективности процессов и потерям)	60-80%	Высокий	Снижение
Компрометация данных пользователей	Высокий (может включать штрафы, репутационные потери и судебные разбирательства)	60-80%	Высокий	Снижение
Потеря финансов	Высокий (может привести к финансовым затруднениям и необходимости сокращения других расходов)	40-60%	Средний	Снижение
Несовместимость с существующими решениями	Средний (может вызвать дополнительные затраты)	40-60%	Средний	Снижение

Первый вид риска — технический, связанный с возможными ошибками в программном обеспечении и неправильной конфигурацией. Для его минимизации необходимо регулярно обновлять программное обеспечение, проводить тестирование и аудит безопасности перед запуском системы, а также использовать надежные решения от известных поставщиков. Второй вид риска — организационный, возникает из-за недостатка квалификации сотрудников и сопротивления изменениям. Для его снижения важно обучать сотрудников работе с новыми системами, создавать культуру открытости к изменениям через вовлечение персонала в процесс внедрения и проводить регулярные тренинги по реагированию на инциденты. Далее — процессный риск, который может проявляться в зависимости от технологий и устаревании процессов. Чтобы минимизировать этот риск, следует разработать четкие процедуры для работы с автоматизированными системами, поддерживать баланс между автоматизацией и ручным контролем в критических процессах, а также периодически пересматривать и обновлять процессы в соответствии с изменениями в технологии. Риск безопасности данных связан с возможными утечками информации. Для его минимизации необходимо шифровать данные как при передаче, так и при хранении, регулярно проверять системы на наличие уязвимостей и внедрять многофакторную аутентификацию для доступа к чувствительной информации. Немаловажен и финансовый риск, связанный с высокими

затратами на внедрение и обслуживание систем. Чтобы минимизировать этот риск, следует проводить детальный анализ затрат до начала проекта, оценивать возврат инвестиций (ROI) перед принятием решения о внедрении и постоянно отслеживать расходы на поддержку системы. Интеграционный риск возникает при несовместимости новых систем с существующими решениями. Для его снижения необходимо проводить предварительный анализ совместимости новых технологий, осуществлять поэтапную интеграцию с возможностью тестирования на каждом этапе и использовать стандарты и протоколы для обеспечения лучшей совместимости между системами.

Понимание этих видов риска позволяет руководству более осознанно подходить к процессу интеграции автоматизированных систем, обеспечивать безопасность информационных ресурсов, помогает определить приоритетные направления для дальнейшего анализа и выработки действий по снижению рисков. Для наглядной оценки этих рисков можно использовать тепловую карту, где различные риски будут представлять собой разные уровни угроз.

Таблица 4 – Тепловая карта рисков (в карте используются порядковые номера рисков, выделенных в таблице 3)

Вероятность	Ущерб		
	Низкий (Незначительные последствия)	Средний (Ощутимые, но не критические последствия для работы)	Высокий (Серьёзные последствия, влияющие на работу)
Низкая (Случайная ситуация, кратковременное воздействие, возникает редко)	-	2	-
Средняя (Регулярная опасная ситуация или воздействие, случаи были)	-	5, 6	1
Высокая (Опасная ситуация, повторяется часто)	-	3	4

Итак, будущее автоматизации в информационной безопасности будет зависеть от способности организаций адаптироваться к новым технологиям и угрозам. Контроль за тенденциями развития технологий, такими как

облачные решения, интернет вещей, а также активное использование ИИ и машинного обучения для повышения уровня защиты станут ключевыми факторами успеха в обеспечении безопасности информации. Важно помнить о необходимости сбалансированного подхода между автоматизацией процессов и человеческим контролем для достижения максимальной эффективности защиты. Автоматизация стала ключевым элементом в обеспечении безопасности ИТ-систем, так как она позволяет улучшать эффективность процессов обнаружения и реагирования на инциденты, а также снижать ежедневную нагрузку на специалистов. Однако использование автоматизированных технологий также влечет за собой новые риски и вызовы, требующие большей осознанности и превентивных мер со стороны руководства.

В заключение, стоит отметить, что автоматизация в области информационной безопасности является важным шагом к достижению идеального баланса между делегированием обязанностей программе и тщательным контролем защищённости IT-систем. Однако для достижения успеха в этой области необходимо сочетание современных технологий, продуманных стратегий безопасности и высокого уровня осведомленности среди сотрудников. Ключевым аспектом этого процесса является регулярная оценка рисков с использованием методов количественного и качественного анализа уязвимостей, что позволяет организациям систематически идентифицировать потенциальные угрозы и оценивать их влияние на критические активы. Применение таких инструментов, как матрицы рисков и модели угроз, способствует более глубокому пониманию текущего состояния безопасности и формирует базу для принятия обоснованных решений по управлению рисками. Организации, которые внедряют комплексный подход к автоматизации, грамотно распределяют ресурсы и учитывают все аспекты безопасности, смогут не только минимизировать риски благодаря проактивному управлению ими, но и существенно улучшить свою сопротивляемость к киберугрозам в будущем.

Список использованных источников:

1. Федеральная служба по техническому и экспортному контролю. Угрозы информационной безопасности. [Электронный ресурс]. URL: https://bdu.fstec.ru/threat/ (дата обращения: 15.02.2025).

2. Data-Sec. Угрозы персональных данных. [Электронный ресурс]. URL: https://data-sec.ru/personal-data/threats-data-bank/ (дата обращения: 2025-02-15).

3. Угрозы для компаний, которые следует учитывать. [Электронный ресурс]. – Режим доступа: https://selectel.ru/blog/security-threats/ (дата обращения: 15.02.2025).

4. Пять способов оптимизации рабочего процесса для максимальной эффективности [Электронный ресурс]. – Режим доступа:

https://experience.dropbox.com/ru-ru/resources/how-to-streamline-workflow (дата обращения: 01.03.2025).

5. Термины и определения в области информационной безопасности. [Электронный ресурс]. – Режим доступа: https://www.securityvision.ru/blog/terminy%20-i-opredeleniya-v-oblasti-informatsionnoy-bezopasnosti/ (дата обращения: 13.03.2025).

6. Автоматизация информационной безопасности. [Электронный ресурс]. – Режим доступа: https://ritg.ru/blog/avtomatizatsiya_informatsionnoy_bezopasnosti/#:~:text=Автоматизация%20информационной%20безопасности%20(ИБ)%20позволяет,и%20обеспечить%20круглосуточный%20мониторинг%20систем (дата обращения: 20.03.2025).

7. Автоматизация ИБ. [Электронный ресурс]. – Режим доступа: https://live.anti-malware.ru/am-live/avtomatizaciya-ib/ (дата обращения: 02.04.2025).

8. Автоматизация процесса управления информационной безопасностью. [Электронный ресурс]. – Режим доступа: https://lib.itsec.ru/articles2/control/avtomatizatsiya-protsessa-upravleniya-informatsionnoy-bezopasnostyu (дата обращения: 02.04.2025).

9. Должностная инструкция специалиста по информационной безопасности. [Электронный ресурс]. – Режим доступа: https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/dokumenty-po-informatsionnoj-bezopasnosti/instruktsii-po-informatsionnoj-bezopasnosti/dolzhnostnaya-instruktsiya-spetsialista-po-informatsionnoy-bezopasnosti/ (дата обращения: 02.04.2025).