

Отчет о проверке

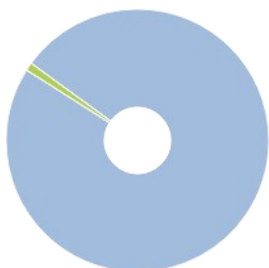
Автор: _____

Проверяющий: _____

Название документа: 95 _ ии_natural_academic_rewrite (2).docx

Организация: _____

РЕЗУЛЬТАТЫ ПРОВЕРКИ



Совпадения:
0%



Оригинальность:
98,89%



ИИ-контент:
90,07%



Цитирования:
1,11%



Самоцитирования:
0%



«Совпадения», «Цитирования», «Самоцитирования», «Оригинальность» являются отдельными показателями, отображаются в процентах и в сумме дают 100%, что соответствует проверенному тексту документа.



Есть подозрения на следующие группы маскировки заимствований: Сгенерированный текст на страницах: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10... еще на 1 стр.

- **Совпадения** — фрагменты проверяемого текста, полностью или частично сходные с найденными источниками, за исключением фрагментов, которые система отнесла к цитированию или самоцитированию. Показатель «Совпадения» — это доля фрагментов проверяемого текста, отнесенных к совпадениям, в общем объеме текста.
- **Самоцитирования** — фрагменты проверяемого текста, совпадающие или почти совпадающие с фрагментом текста источника, автором или соавтором которого является автор проверяемого документа. Показатель «Самоцитирования» — это доля фрагментов текста, отнесенных к самоцитированию, в общем объеме текста.
- **Цитирования** — фрагменты проверяемого текста, которые не являются авторскими, но которые система отнесла к корректно оформленным. К цитированиям относятся также шаблонные фразы; библиография; фрагменты текста, найденные модулем поиска «СПС Гарант: нормативно-правовая документация». Показатель «Цитирования» — это доля фрагментов проверяемого текста, отнесенных к цитированию, в общем объеме текста.
- **Текстовое пересечение** — фрагмент текста проверяемого документа, совпадающий или почти совпадающий с фрагментом текста источника.
- **Источник** — документ, проиндексированный в системе и содержащийся в модуле поиска, по которому проводится проверка.
- **Оригинальный текст** — фрагменты проверяемого текста, не обнаруженные ни в одном источнике и не отмеченные ни одним из модулей поиска. Показатель «Оригинальность» — это доля фрагментов проверяемого текста, отнесенных к оригинальному тексту, в общем объеме текста.

Обращаем Ваше внимание, что система находит текстовые совпадения проверяемого документа с проиндексированными в системе источниками. При этом система является вспомогательным инструментом, определение корректности и правомерности совпадений или цитирований, а также авторства текстовых фрагментов проверяемого документа остается в компетенции проверяющего.

ИНФОРМАЦИЯ О ДОКУМЕНТЕ

Номер документа: 162272

Тип документа: Не указано

Дата проверки: 30.08.2026 13:55:44

Дата корректировки: Нет

Количество страниц: 11

Символов в тексте: 24972

Слов в тексте: 2889

Число предложений: 176

Комментарий: не указано

ПАРАМЕТРЫ ПРОВЕРКИ

Выполнена проверка с учетом редактирования: Да

Исключение элементов документа из проверки: Да

Выполнено распознавание текста (OCR): Нет

Выполнена проверка с учетом структуры: Да

Разделы и элементы, отключенные пользователем: Библиография, Таблицы

Модули поиска: Патенты СССР, РФ, СНГ, Публикации eLIBRARY, Издательство Wiley, ИПС Адилет, Публикации РГБ (переводы и перефразирования), Медицина, Учебные работы (переводы и перефразирования), СПС ГАРАНТ: аналитика, СМИ России и СНГ, Перефразированные заимствования по коллекции Интернет в русском сегменте, СПС ГАРАНТ: нормативно-правовая документация, Шаблонные фразы, Цитирование, Перефразирования по коллекции издательства Wiley, Коллекция НБУ, Диссертации НББ, Сводная коллекция ЭБС, IEEE, Публикации РГБ, Учебные работы* (переводы и перефразирования), Интернет Плюс, Издательство Springer Nature, Переводные заимствования издательства Wiley, Публикации eLIBRARY (переводы и перефразирования), Перефразированные заимствования по коллекции Интернет в английском сегменте, Переводные заимствования IEEE, Перефразирования по коллекции IEEE, Учебные работы, Переводные заимствования по коллекции Гарант: аналитика, Учебные работы*, Переводные заимствования по коллекции Интернет в английском сегменте, Перефразирования по СПС ГАРАНТ: аналитика, Переводные заимствования по коллекции Интернет в русском сегменте

ИСТОЧНИКИ

№	Доля в тексте	Доля в отчете	Источник	Актуален на	Модуль поиска	Комментарий
[01]	1,11%	1,11%	не указано	17 Сен 2025	Шаблонные фразы	
[02]	0,85%	0%	Введен институт независимой о...	07 Фев 2025	Переводные заимствования по коллекции Гарант: аналитика	Источник исключен. Причина: Маленький процент пересечения.
[03]	0,58%	0%	Апелляционное определение СК... http://ivo.garant.ru	25 Ноя 2023	СПС ГАРАНТ: нормативно-правовая документация	Источник исключен. Причина: Маленький процент пересечения.
[04]	0,58%	0%	Разработка курса в системе дист... http://biblioclub.ru	21 Янв 2020	Сводная коллекция ЭБС	Источник исключен. Причина: Маленький процент пересечения.
[05]	0,58%	0%	420278226 https://docs.cntd.ru	17 Авг 2026	Интернет Плюс	Источник исключен. Причина: Маленький процент пересечения.
[06]	0,58%	0%	ВКР Калова	12 Янв 2024	Учебные работы	Источник исключен. Причина: Маленький процент пересечения.
[07]	0,58%	0%	Комментарий к Федеральному з... http://ivo.garant.ru	01 Апр 2023	СПС ГАРАНТ: аналитика	Источник исключен. Причина: Маленький процент пересечения.
[08]	0,58%	0%	otchet_po_samoobsledovaniyu_18... https://stu.lipetsk.ru	09 Апр 2026	Интернет Плюс	Источник исключен. Причина: Маленький процент пересечения.
[09]	0,54%	0%	ВКР Борисов ИСТ-341	12 Янв 2024	Учебные работы	Источник исключен. Причина: Маленький процент пересечения.
[10]	0,54%	0%	РАЗРАБОТКА WEB-РЕСУРСА ДЛЯ ...	12 Янв 2024	Учебные работы	Источник исключен. Причина: Маленький процент пересечения.
[11]	0,54%	0%	ВКР Цайзер	12 Янв 2024	Учебные работы	Источник исключен. Причина: Маленький процент пересечения.
[12]	0,54%	0%	«РАЗРАБОТКА WEB-РЕСУРСА ДЛЯ...	12 Янв 2024	Учебные работы	Источник исключен. Причина: Маленький процент пересечения.
[13]	0,44%	0%	Методологическая основа образ...	20 Мар 2025	СПС ГАРАНТ: аналитика	Источник исключен. Причина: Маленький процент пересечения.
[14]	0,44%	0%	Эвенки дисс правка итог	13 Дек 2025	Учебные работы*	Источник исключен. Причина: Маленький процент пересечения.
[15]	0,44%	0%	Эвенки дисс правка итог (1)	18 Авг 2025	Учебные работы*	Источник исключен. Причина: Маленький процент пересечения.

1. АНАЛИЗ ДЕЯТЕЛЬНОСТИ ОРГАНИЗАЦИИ И ЕЁ ИНФОРМАЦИОННОЙ СРЕДЫ

1.1. Общая характеристика организации, структура и направления деятельности

Ростовский государственный экономический университет (РИНХ) — федеральное государственное бюджетное образовательное учреждение высшего образования, совмещающее образовательную и научно-исследовательскую деятельность. Университет действует в соответствии с законодательством Российской Федерации и имеет статус некоммерческой организации. Он реализует образовательные программы, готовит специалистов, проводит научные исследования и выполняет аналитические задачи. Обучение ведётся по нескольким направлениям, причём всё более существенное место в нём занимают работа с информацией и цифровые технологии.

Статус федерального государственного бюджетного учреждения означает, что университет финансируется из федерального бюджета и выполняет государственные задания в области образования и науки. Учредителем организации является Российская Федерация, а соответствующие функции в пределах компетенции осуществляет Министерство науки и высшего образования Российской Федерации, обеспечивающее общее руководство и контроль. Университет готовит специалистов, способных работать в современной цифровой среде, и реализует программы высшего образования. Обучение сочетает освоение теоретических знаний с развитием практических навыков, необходимых для дальнейшей профессиональной деятельности. Одновременно университет проводит научные исследования, результаты которых используют в образовательном процессе и при подготовке методических материалов.

Университет одновременно решает образовательные, научно-исследовательские и организационные задачи. Основное место среди них занимает подготовка обучающихся по различным специальностям. Научная работа направлена на развитие научного потенциала и практическое применение полученных результатов. Для хранения, обработки и передачи данных университет использует информационные и цифровые технологии. Партнёрство с государственными органами и коммерческими организациями создаёт условия для совместных проектов и практической подготовки обучающихся. Система управления построена на нескольких уровнях: общее руководство

осуществляют ректор и проректоры, каждый из которых курирует отдельные направления. Образовательные программы реализуют факультеты и институты, в состав которых входят кафедры, обеспечивающие учебный процесс и научную работу. Кроме того, университет располагает научными подразделениями, учебно-методическими и административными службами.

Университет работает не только в Ростове-на-Дону, где расположена его основная территория, но и через филиалы в Гуково, Таганроге, Ейске, Кисловодске, Миллерово и Черкесске. Филиальная сеть расширяет доступ к образовательным программам в разных регионах, однако все подразделения подчиняются единой системе управления и соблюдают установленные требования. Информационные технологии поддерживают учебный процесс и организационную работу: университет ведёт документацию, хранит и обрабатывает данные, а также обеспечивает информационное сопровождение деятельности с помощью информационных систем и телекоммуникационных сетей. Часть учебных и методических материалов размещается в электронном виде на информационных ресурсах, доступных через Интернет. Участники образовательного процесса используют электронную почту и другие цифровые сервисы, благодаря чему обмен информацией становится быстрее, а рабочие процессы — эффективнее. Такая цифровая среда требует также обеспечить безопасность обрабатываемых данных; этому вопросу посвящён следующий раздел.

1.2. Информационная инфраструктура и используемые цифровые коммуникации организации

Университет опирается на информационную инфраструктуру, которая поддерживает учебную, научную и административную деятельность. Её основу составляют информационные системы, локальная сеть, доступ к Интернету, электронная почта и внутренние цифровые сервисы. С их помощью университет ведёт базы данных и электронный документооборот, составляет расписание занятий, учитывает обучающихся и сотрудников, хранит учебные материалы и передаёт служебную информацию. В образовательной деятельности также задействованы системы дистанционного обучения и внутренние ресурсы, где студенты получают материалы, задания и уведомления.

Телекоммуникационная сеть связывает перечисленные системы и обеспечивает их повседневную работу. Она предоставляет доступ к внутренним ресурсам университета и к Интернету, который необходим для использования учебных материалов и

взаимодействия сотрудников с обучающимися. Данные передаются как внутри локальной сети, так и между университетом и внешними системами, включая государственные и образовательные ресурсы. Сеть поддерживает обмен информацией между подразделениями, удалённое подключение к сервисам, услуги связи и другие цифровые коммуникации. Поэтому сотрудники и обучающиеся могут постоянно пользоваться электронной почтой, порталами, учебными платформами и иными информационными ресурсами.

Участники образовательного процесса взаимодействуют через электронную почту, университетские информационные системы и сетевые сервисы, предназначенные для обмена сообщениями и передачи данных. Эти каналы сопровождают учебную и организационную работу, а также служебное общение между сотрудниками и обучающимися. Основной массив передаваемой информации составляют текстовые данные: служебные сообщения, учебные материалы, уведомления и другие тексты, используемые в деятельности университета. Рост объёма коммуникаций одновременно усложняет контроль за всем потоком сообщений. Значительную часть писем пользователи проверяют самостоятельно, без автоматического анализа содержания, поэтому потенциально опасное сообщение может выглядеть как обычное служебное письмо. В таких условиях повышается вероятность распространения через цифровые каналы недостоверной или вредоносной информации. При отсутствии средств, способных анализировать текст, ссылки и признаки подмены отправителя, возрастает и риск фишинга. Это определяет необходимость разрабатывать методы выявления подобных воздействий, в частности подходы к распознаванию признаков фишинговых атак в передаваемых текстовых данных.

1.3. Потенциальные информационные угрозы организации в открытой цифровой среде

Университет сталкивается с информационными угрозами не только при технических сбоях и атаках на системы: существенная часть рисков возникает в повседневной работе с электронной почтой, сайтами, документами и сообщениями. Информационной угрозой следует считать ситуацию, создающую возможность нарушения конфиденциальности, целостности или доступности информации. В нормативном смысле угроза обозначает именно вероятность инцидента, а не уже

совершившееся нарушение. Её объектами выступают данные, информационные системы, технические средства обработки и пользователи, взаимодействующие с информацией. Угрозу могут реализовать нарушители, однако не меньшую роль играют пользовательские ошибки и недостатки конфигурации систем. Сетевые технологии, удалённый доступ и электронные коммуникации расширяют число точек, через которые можно воздействовать на данные и системы. Одновременно интенсивный поток сообщений побуждает пользователей действовать автоматически, из-за чего подозрительные признаки часто остаются без внимания. По мере развития технологий меняются и способы воздействия на информационные ресурсы, поэтому защитные меры необходимо регулярно пересматривать. В связи с этим важно определить основные причины возникновения таких угроз и объяснить, почему текстовые сообщения становятся удобным каналом их распространения.

Причины информационных угроз во многом определяются тем, как организация выстраивает работу с информацией и какие технологии использует. Рост объёма данных и скорости их передачи приводит к тому, что пользователи не успевают полноценно проверять весь входящий поток. Особенно уязвимой в этом отношении оказывается переписка: письмо, оформленное от имени преподавателя, деканата или технической поддержки, могут открыть без дополнительной проверки, если его содержание и внешний вид кажутся привычными. При большом количестве сообщений такая практика повышает вероятность ошибки. Цифровые коммуникации дополнительно усиливают зависимость от пользовательских решений, поскольку значительная часть передаваемой информации имеет текстовую форму, а автоматизированные средства анализа используются не всегда. В результате пользователь самостоятельно оценивает достоверность сообщения, хотя высокая нагрузка существенно затрудняет такую проверку. Сказывается и человеческий фактор: при обработке больших объёмов данных снижается внимательность, а решения принимаются быстрее и без обращения к дополнительным источникам. Доверие к привычному каналу связи также уменьшает настороженность — сообщение воспринимается как безопасное уже потому, что поступило обычным способом.

Техническая уязвимость информационных систем может быть связана с необновлённым программным обеспечением, ошибками конфигурации, избыточными правами доступа и слабым разграничением полномочий пользователей. Устойчивость системы к несанкционированному доступу существенно снижают простые или повторно

используемые пароли, а также отсутствие многофакторной аутентификации. При этом организация не всегда полностью контролирует действия пользователей. На уровень угроз влияет и сетевая инфраструктура: без сегментации сети и контроля трафика выявлять подозрительную активность сложнее, а незащищённые каналы передачи данных повышают вероятность перехвата информации. Если средства мониторинга и журналирования отсутствуют либо используются формально, опасные действия могут остаться незамеченными; недостаточный анализ событий усиливает этот риск. Дополнительные точки уязвимости появляются при интеграции платформ, обмене данными между ними, подключении сторонних решений и работе через API, поскольку связанные компоненты могут иметь неодинаковый уровень защиты. Сходная проблема возникает при использовании пользовательских устройств, безопасность которых не всегда соответствует организационным требованиям. В совокупности эти факторы делают угрозы постоянным элементом цифровой среды. Особенно явно это проявляется при передаче текстовой информации по электронным каналам связи, когда решение о её достоверности пользователь часто принимает самостоятельно, без автоматизированной поддержки. Поэтому необходимо рассмотреть, каким образом цифровая среда способствует распространению таких угроз.

Распространению информационных угроз способствует сама организация современных цифровых сервисов. Большинство платформ рассчитано на одновременное обслуживание большого числа пользователей, поэтому данные можно быстро передать широкой аудитории практически без ограничений. Интернет обеспечивает доступ к системам независимо от местоположения, а мобильные устройства делают этот доступ постоянным. Облачные технологии и централизованные сервисы упрощают обмен между пользователями и системами и позволяют распространять один и тот же контент из единой точки сразу на несколько платформ. При интеграции сервисов и взаимодействии через API материал последовательно проходит через связанные системы, не ограничиваясь одним каналом. Автоматизация, в свою очередь, даёт возможность создавать значительные объёмы сообщений без непосредственного участия пользователя. Алгоритмы генерации, включая технологии искусственного интеллекта, позволяют быстро подготавливать однотипные или адаптированные тексты. Унифицированные интерфейсы и сходные формы уведомлений облегчают имитацию официальных источников: визуально похожие ресурсы, поддельные доменные имена и стандартные

шаблоны затрудняют различение подлинных и поддельных сообщений. Ссылки и вложения также расширяют возможности воздействия. Сокращённые ссылки, перенаправления и различные форматы файлов могут скрывать фактическое содержание данных и затруднять определение конечного адреса перехода. Поскольку такие элементы естественно включаются в текст сообщения, пользователь может воспринимать их как обычную часть цифрового взаимодействия.

Цифровой контент легко изменять, копировать и повторно использовать без заметной потери качества, а затем передавать новым пользователям. Социальные сети ускоряют этот процесс благодаря репостам и пересылке, позволяя быстро распространять данные внутри пользовательских сообществ. При этом адресат не всегда способен установить, кто сформировал сообщение и насколько оно достоверно: происхождение данных трудно отследить, а фильтры не во всех случаях своевременно обнаруживают потенциально опасные элементы. Современные инструменты создания контента дополнительно расширяют круг возможных источников, поскольку позволяют подготавливать сообщения, страницы и другие материалы без специальной подготовки. В результате цифровая среда поддерживает быстрое изменение и многократное воспроизведение данных. Особенно характерно это для текстовых материалов, которые пользователи воспринимают и передают быстрее, чем многие другие формы информации. На практике подобные условия возникают при работе через Интернет и внешние цифровые ресурсы.

Организация регулярно использует Интернет и внешние цифровые ресурсы: веб-сайты, облачные сервисы, образовательные платформы и другие системы. Это расширяет возможности работы с данными, однако одновременно увеличивает число внешних точек взаимодействия. Часть операций при обращении к таким ресурсам выполняется за пределами внутренней инфраструктуры, поэтому проверить надёжность поступающей информации удаётся не всегда. Кроме того, внешние сервисы отличаются по уровню защищённости, поскольку работают на основе неодинаковых правил и стандартов, что относится как к их технической реализации, так и к содержанию. Пользователь может получить недостоверные либо потенциально опасные данные, в том числе перейти на поддельный ресурс, имитирующий официальный сайт. Риски повышаются и при передаче информации через веб-интерфейсы, формы ввода и механизмы загрузки файлов. Ссылки и перенаправления затрудняют определение конечного ресурса, тогда как

динамичное содержимое позволяет изменять информацию без уведомления пользователей. Открытость цифровой среды, отсутствие централизованного контроля за размещаемыми сведениями и возможность их распространения неограниченным кругом лиц создают условия, при которых данные могут передаваться независимо от достоверности и происхождения. Информация в такой среде не только поступает извне, но и активно циркулирует между пользователями внутри организации. Поэтому цифровые коммуникации становятся ключевым каналом информационного взаимодействия и обеспечивают распространение значительной части данных.

Современная организация поддерживает взаимодействие сотрудников и обучающихся главным образом через цифровые каналы связи. Для этого применяются электронная почта, корпоративные информационные системы и мессенджеры, позволяющие оперативно обмениваться сообщениями. По этим каналам передают служебные уведомления, задания, документы и другие сведения, необходимые для повседневной работы. Такой обмен отличается непрерывностью и высокой скоростью: сообщения поступают почти без задержек и в короткое время формируют значительный информационный поток. Из-за этого внимание к отдельным сообщениям ослабевает, а их содержание обрабатывается менее тщательно. Большинство передаваемых данных имеет текстовую форму, что облегчает восприятие и не требует дополнительной обработки. Вместе с тем достоверность текста в основном оценивает сам получатель, поскольку автоматизированный анализ такой информации используется ограниченно. Создать и распространить сообщение также несложно: пользователь может быстро направить его одному или нескольким адресатам. Скорость передачи при этом сочетается с недостаточным контролем содержания. На восприятие влияет и привычность канала связи. Сообщение, оформленное как служебное уведомление или отправленное знакомым адресантом, нередко принимают за достоверное, что облегчает имитацию официальной коммуникации. Ссылки и вложения воспринимаются как обычные элементы цифрового взаимодействия, поэтому пользователь может открыть файл или перейти по ссылке, не проверив их безопасность. В результате именно он становится центральным участником обработки информации, а безопасность данных во многом зависит от принимаемых им решений. Способность распознавать угрозы определяется особенностями восприятия, характером повседневной работы и уровнем подготовки в области информационной

безопасности. Эти обстоятельства повышают уязвимость пользователей в цифровой среде и требуют самостоятельного рассмотрения данного аспекта.

Уязвимость информационной среды определяется не только техническими характеристиками цифровых технологий. Во многих случаях существенную роль играет поведение пользователя, который оказывается конечным звеном взаимодействия с информацией и потому относится к наиболее уязвимым элементам системы. Постоянный поток сообщений и большой объём данных рассеивают внимание: пользователь ускоряет обработку информации и может не заметить отдельные детали. Нередко он оценивает сообщение по общему виду, а не по содержанию, из-за чего сложнее выявить несоответствия и признаки угрозы. Повторяющиеся операции постепенно выполняются без проверки. На решения влияют и психологические факторы. Срочность, требование немедленного ответа или необходимости совершить действие побуждают реагировать без дополнительной оценки. Доверие возрастает, если сообщение исходит от преподавателя, администрации или технической службы. Эмоциональная реакция, в свою очередь, снижает критичность восприятия. Существенное значение имеет подготовка в области информационной безопасности. Без регулярного обучения и понятных инструкций пользователю может не хватать навыков, чтобы оценить достоверность сведений. Недостаточное знание современных способов воздействия и отсутствие культуры безопасной работы с данными позволяют потенциальным угрозам оставаться незамеченными. Рабочая нагрузка усиливает этот эффект: одновременное выполнение нескольких задач, переключение между сервисами и необходимость быстро отвечать на сообщения ухудшают качество анализа. В результате многие действия совершаются автоматически. Дополнительные риски возникают при работе с личных устройств, подключении к незащищённым сетям и выполнении операций вне контролируемой инфраструктуры организации. В таких условиях защита ослабевает, а пользователь не всегда оценивает последствия своих действий. Повышенная уязвимость делает внешнее воздействие на информационные ресурсы более результативным. Этим могут воспользоваться источники угроз, находящиеся за пределами организации и способные сочетать особенности цифровой среды с уязвимостями поведения пользователей для достижения своих целей.

К внешним источникам угроз относятся киберпреступники, организованные группы, отдельные злоумышленники, автоматизированные средства, а в некоторых

случаях — сторонние организации. Они стремятся получить учётные данные и конфиденциальную информацию, нарушить работу систем, распространить вредоносное ПО или извлечь финансовую выгоду. Для этого используются массовые рассылки, поддельные веб-ресурсы, имитация официальных сообщений, вредоносные элементы в файлах и ссылках, а также ранее скомпрометированные данные. Такие источники не имеют прямого доступа к инфраструктуре организации и обычно действуют через открытые каналы связи, анонимные или сторонние ресурсы. Это позволяет им масштабировать воздействие на большое количество пользователей. Внутренние источники угроз, напротив, возникают внутри организации и связаны с пользователями, которым предоставлен доступ к информационным ресурсам. К ним относятся сотрудники, обучающиеся и технический персонал, администрирующий информационные системы и обеспечивающий их работу. Эти субъекты взаимодействуют с информацией непосредственно и используют штатные средства доступа. Их роль в информационной среде определяется выполняемыми функциями: одни работают с документами и базами данных, другие администрируют системы, третьи передают и обмениваются информацией. Поэтому характер угроз зависит от уровня доступа и набора доступных операций. Внутренний пользователь может получать, изменять и передавать данные, копировать служебную информацию, выводить её за пределы организации, удалять или искажать сведения, а также вызывать сбои в работе систем. Иногда такие действия совершаются намеренно, но значительная часть инцидентов возникает из-за ошибок. Угрозы реализуются через обычные рабочие операции: доступ к файлам и информационным системам, использование учётных записей, передачу данных по внутренним сервисам и обращение к внешним ресурсам. Причиной нарушения могут стать неправильная работа с документами, некорректная настройка доступа, отправка информации без проверки получателя или применение незащищённых носителей. Особую опасность представляет обращение с учётными данными: пользователи могут повторно использовать пароли, передавать их другим лицам или применять учётные записи вне контролируемой среды. В таком случае несанкционированный доступ возможен без преодоления защитных механизмов. Внутренние угрозы трудно выявлять, поскольку действия совершаются с использованием легитимных прав, корпоративных сетей, сервисов и устройств. В отличие от внешнего источника, внутреннему пользователю не требуется обходить защиту: воздействие достигается за счёт особенностей его работы. Такие угрозы обычно не имеют массового характера, но могут

быть более точечными и серьёзными по последствиям, поскольку пользователь уже получает прямой доступ к определённым ресурсам.

Информационные угрозы различаются не только по источнику воздействия, но и по характеру действий, посредством которых они возникают. По этому основанию их разделяют на преднамеренные и случайные. Такое разграничение показывает, формируется ли риск в результате осознанного воздействия или возникает из-за особенностей повседневной работы с информацией. Преднамеренная угроза предполагает наличие цели и заранее выбранного способа её достижения. Злоумышленник может стремиться получить доступ к данным, изменить их или использовать в дальнейшем, применяя для этого подбор учётных данных, скомпрометированную информацию, имитацию доверенных сообщений либо такие приёмы, которые побуждают пользователя самостоятельно выполнить нужное действие. Воздействие часто учитывает контекст: в сообщениях используются привычные форматы, знакомые ситуации и элементы, вызывающие доверие. Поэтому действия злоумышленника могут выглядеть как обычная рабочая активность и не вызывать подозрений. Особую группу составляют методы, рассчитанные непосредственно на пользователя. Манипулирование вниманием, фактор срочности и авторитета, а также ссылки и файлы в составе сообщения побуждают его совершать действия, которые кажутся стандартными. Случайные угрозы имеют иную природу: пользователь не стремится причинить ущерб, однако ошибка или невнимательность приводят к опасному результату. К типичным примерам относятся отправка информации не тому получателю, применение простых или повторяющихся паролей, открытие непроверенных файлов и игнорирование системных предупреждений. Такие действия часто выполняются автоматически и потому не воспринимаются как рискованные. Их отличает повторяемость: они регулярно возникают при выполнении типичных рабочих операций. Хотя намерение причинить вред отсутствует, последствия могут быть сопоставимы с результатами преднамеренного воздействия, особенно когда речь идёт о передаче конфиденциальной информации или предоставлении доступа к системам. Таким образом, преднамеренные и случайные угрозы имеют разную природу, но во многих случаях реализуются в одной точке — через действия пользователя или при его участии. В первом случае пользователь становится объектом воздействия, во втором — источником ошибки.

Источником информационной угрозы может стать любой субъект, способный получить доступ к информационной среде, поэтому к нарушителям относятся не только внешние злоумышленники, но и пользователи системы. Нарушителем считают субъекта, чьи действия способны повлечь нарушение конфиденциальности, целостности или доступности информации, даже если такой результат не был осознанной целью. Основным критерием разграничения нарушителей служит объем доступных им полномочий: одни используют лишь внешние каналы взаимодействия с системой, другие обращаются к данным в пределах должностных обязанностей, а пользователи с расширенными правами могут изменять настройки и влиять на работу информационных систем. Существенное значение имеет также уровень подготовки — от применения базовых знаний и стандартных средств до использования специализированных инструментов и средств автоматизации. От него во многом зависят характер воздействия и его масштаб. Цели нарушителя могут состоять в получении информации, изменении данных или дестабилизации работы систем, однако риск возникает не только вследствие преднамеренных действий: во многих случаях его причиной становятся ошибки пользователей в процессе обычной работы.