

Отчет о проверке

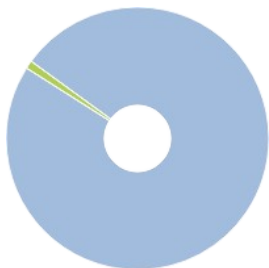
Автор: _____

Проверяющий: _____

Название документа: 95 _ ии_natural_academic_rewrite_HS3_OCR1-FOCUS-B58-M (8).docx

Организация: _____

РЕЗУЛЬТАТЫ ПРОВЕРКИ



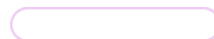
Совпадения:
0%



Оригинальность:
99,48%



ИИ-контент:
0%



Цитирования:
0,52%



Самоцитирования:
0%



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

- **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: 166464

Тип документа: Не указано

Дата проверки: 15.09.2026 13:49:26

Дата корректировки: Нет

Количество страниц: 13

Символов в тексте: 31037

Слов в тексте: 3954

Число предложений: 229

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

ИСТОЧНИКИ

№	Доля в тексте	Доля в отчете	Источник	Актуален на	Модуль поиска	Комментарий
[01]	0,52%	0,52%	Постановление Администрации ... http://ivo.garant.ru	07 Фев 2025	СПС ГАРАНТ: нормативно-правовая документация	
[02]	0,47%	0%	не указано	17 Сен 2025	Шаблонные фразы	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 образовательное учреждение, которое работает в сфере высшего образования и научных исследований. Его деятельность регулируется законодательством Российской Федерации, а по своему статусу университет относится к некоммерческим организациям. Здесь реализуют образовательные программы, готовят специалистов, выполняют научные и аналитические задачи. Подготовка ведётся по разным направлениям, поэтому университету приходится работать с большим объёмом информации. В учебной работе всё заметнее становится и роль цифровых технологий: они входят не только в отдельные занятия, но и в повседневную организацию образовательного процесса.

Статус федерального государственного бюджетного учреждения задаёт и порядок финансирования университета: средства поступают из федерального бюджета, а организация выполняет государственные задания в области образования и науки. Российская Федерация выступает учредителем, а от её имени соответствующие функции в пределах компетенции выполняет Министерство науки и высшего образования Российской Федерации, которое руководит учреждением и контролирует его работу. В центре деятельности остаются образовательные программы высшего образования и подготовка специалистов, которым предстоит работать в цифровой среде. Обучение при этом не сводится к передаче теории. Студентам нужны и практические навыки, необходимые для дальнейшей профессиональной деятельности. Научная работа идёт параллельно: университет проводит исследования, а их результаты используют в учебном процессе и при подготовке методических материалов. Так научные задачи связаны с обучением не только по названию, но и через конкретное использование полученных результатов.

У университета сразу несколько направлений работы - образовательное, научно-исследовательское и организационное, хотя главным из них остаётся обучение по разным специальностям. Научно-исследовательская работа поддерживает развитие научного

потенциала, а полученные результаты находят применение в деятельности университета. Информационные и цифровые технологии здесь нужны для хранения, обработки и передачи данных, то есть сопровождают и учебную, и исследовательскую работу. Кроме того, университет работает с государственными органами и коммерческими организациями, вместе с ними реализует проекты и организует практическую подготовку студентов. Управление построено по нескольким уровням. Ректор и проректоры ведут общее руководство, каждый в пределах своего направления; образовательные программы реализуют факультеты и институты, а кафедры внутри них ведут учебную и научную работу. В структуре предусмотрены также научные подразделения, учебно-методические и административные службы - они обеспечивают отдельные стороны общей работы университета.

Основная площадка университета находится в г. Ростове-на-Дону, но работа организована и через филиалы - они действуют в г. Гуково, г. Таганроге, г. Ейске, г. Кисловодске, г. Миллерово и г. Черкесске. Такая сеть расширяет охват образовательных программ и даёт возможность учиться в разных регионах. При этом филиалы не образуют отдельные системы: ими управляют в общем контуре, и они соблюдают установленные требования. Учебная и организационная работа опирается на информационные технологии, информационные системы и телекоммуникационные сети. В них ведут документацию, хранят и обрабатывают данные, обеспечивают информационную работу университета. Часть учебных и методических материалов уже размещена в электронных ресурсах, доступных через сеть Интернет. Электронная почта и другие цифровые сервисы связывают участников учебного процесса, ускоряют обмен сведениями и делают взаимодействие сотрудников и обучающихся оперативнее. Через эти решения организуется и текущая работа, и доступ к материалам, которые используются в обучении. Одновременно такая цифровая среда требует защищать обрабатываемые данные, что важно для дальнейшего рассмотрения вопросов безопасности.

1.2. Информационная инфраструктура и используемые цифровые коммуникации организации

Учебные, научные и организационные задачи университета держатся на общей информационной инфраструктуре. В неё входят информационные системы, локальная сеть, доступ в Интернет, электронная почта и внутренние сервисы. Через них ведутся базы данных и документооборот, составляются расписания, учитываются обучающиеся и

сотрудники, хранятся учебные материалы и передаются служебные сообщения. Эти же ресурсы поддерживают обмен информацией внутри повседневной работы университета. Для занятий есть и отдельный контур - системы дистанционного обучения и внутренние ресурсы, где студенты получают материалы, задания и уведомления. Так учебная информация поступает к ним через те сервисы, которыми университет пользуется в своей общей работе. Внутренние ресурсы объединяют материалы, задания и уведомления в одном учебном контуре, не отделяя их от общей информационной работы университета.

Без телекоммуникационной сети эта инфраструктура работать не может. Она соединяет пользователей с внутренними ресурсами и даёт выход в Интернет, который нужен для учебных материалов и общения сотрудников с обучающимися. Данные передаются и внутри локальной сети, и во внешние системы, в том числе государственные и образовательные ресурсы. Между подразделениями идут информационные обмены, а к сервисам можно подключаться удалённо. Сеть нужна не только для доступа к ресурсам: через неё университет предоставляет услуги связи и поддерживает цифровые коммуникации. Поэтому сотрудники и обучающиеся постоянно пользуются электронной почтой, порталами, учебными платформами и другими сервисами. Через эти каналы они получают доступ к материалам и поддерживают рабочее взаимодействие, даже когда обращаются не к одному внутреннему ресурсу, а к нескольким связанным системам.

Сотрудники и обучающиеся общаются через электронную почту, университетские информационные системы и сетевые сервисы, где можно отправлять сообщения, передавать данные и получать уведомления. Эти каналы входят в учебную работу, служебную переписку и повседневное взаимодействие внутри университета, поэтому через них проходят не только отдельные письма, но и значительная часть текущих организационных действий. В основном по ним передаются тексты, причём содержание таких сообщений может быть связано и с учёбой, и с организационной работой, в том числе служебные сообщения, учебные материалы, уведомления и другие текстовые данные, которые сопровождают образовательную и административную деятельность, передаются между сотрудниками и обучающимися и используются в текущей работе. Чем плотнее такой обмен и чем больше каналов используется одновременно, тем труднее увидеть весь поток целиком. Передаваемые сведения активно включены в ежедневную работу университета, однако значительную часть писем проверяет сам пользователь, без

автоматической оценки содержания. Из-за этого своевременно заметить опасное сообщение бывает трудно - письмо с подозрительными признаками может выглядеть как обычное служебное, а решение о том, открывать его или нет, принимается без автоматической проверки и нередко без дополнительного внимания. Через цифровые каналы тогда распространяются недостоверные и вредоносные сведения. Особенно возрастает риск фишинга, если система не проверяет текст, ссылки и признаки подмены отправителя. Поэтому нужны подходы, которые помогают находить такие воздействия по признакам фишинговой атаки, сохранившимся в передаваемых текстовых данных, которые пользователь получает по этим каналам.

1.3. Потенциальные информационные угрозы организации в открытой цифровой среде

Университет сталкивается с информационными угрозами не только тогда, когда отказывает техника или происходит атака на систему, - значительная часть рисков появляется в привычных операциях с данными. Риск возникает и в обычной работе с электронной почтой, сайтами, документами и сообщениями, то есть там, где пользователь ежедневно получает, открывает и передаёт информацию. Угрозой здесь можно считать ситуацию, в которой появляется возможность нарушить конфиденциальность, целостность либо доступность информации; сам инцидент ещё не произошёл, речь идёт именно о предпосылке к нему, а не о завершённом событии. Под ударом оказываются не только данные. В ту же среду входят информационные системы, технические средства их обработки и люди, которые с этой информацией работают. Источником воздействия может стать нарушитель, но не исключены пользовательская ошибка, недостаточная внимательность или слабая настройка системы. Сетевые технологии, удалённый доступ и электронная связь расширяют число мест, через которые можно воздействовать на данные или системы, а значит, увеличивают количество точек взаимодействия с информацией. При большом потоке сообщений человек действует быстрее и чаще пропускает подозрительные признаки, особенно когда содержание похоже на привычную переписку и не требует от пользователя немедленной реакции. Угрозы при этом меняются вместе с технологиями и способом работы с информацией, поэтому меры защиты и подходы к обеспечению безопасности нельзя пересматривать один раз и навсегда. Нужно понять, какие условия поддерживают их возникновение и почему именно текстовые сообщения

так часто становятся удобным каналом воздействия, когда пользователь работает с ними в условиях высокой нагрузки и постоянного обмена сообщениями.

То, насколько часто возникают информационные угрозы, зависит и от внутренней организации работы с данными, и от применяемых технологий. Данных стало больше, передаются они быстрее, а полноценная проверка уже не охватывает всё, что приходит пользователю через разные каналы и в разное время. В переписке это видно особенно хорошо - письмо от преподавателя, деканата или технической поддержки открывают почти автоматически, если оно похоже на привычное сообщение от знакомого отправителя. Проверять каждое письмо при таком потоке невозможно, поэтому часть решений принимается по внешнему виду сообщения, знакомости отправителя и привычности канала, а вероятность ошибки растёт. Текст остаётся основной формой цифрового обмена, поэтому решение о его достоверности во многом принимает сам пользователь, а не автоматизированное средство, способное проверить весь поток сообщений. Когда автоматического анализа нет, эта задача фактически ложится на него целиком и при высокой нагрузке становится трудной и менее надёжной. Усталость тоже меняет поведение - внимание снижается, решения принимаются быстрее, без дополнительной проверки, а знакомому каналу связи доверяют даже тогда, когда сообщение содержит признаки потенциальной угрозы.

Уязвимость информационной среды складывается из нескольких технических обстоятельств. Необновлённое программное обеспечение может сохранять уязвимости, а ошибки в настройках, лишние права и слабое разграничение пользователей расширяют пространство для воздействия. Отдельная проблема - доступ к системе, где простые или повторно используемые пароли и отсутствие многофакторной аутентификации заметно облегчают несанкционированный вход, тогда как права пользователей могут быть избыточными, а их действия контролируются не всегда и не во всех случаях фиксируются. Сеть тоже может скрывать подозрительную активность, если она не разделена на сегменты и трафик не проверяется. Когда каналы передачи не защищены шифрованием, возрастает вероятность перехвата информации, особенно если данные проходят через несколько участков сетевой инфраструктуры. Не хватает и наблюдений за событиями - без журналирования либо при его формальном использовании опасные действия могут остаться незамеченными в общем потоке событий, а отсутствие регулярного анализа событий только закрепляет эту проблему. Дополнительные точки

риска появляются там, где системы соединяются между собой, подключаются сторонние решения или используется API - данные проходят через разные платформы, а требования и уровень защиты у них могут различаться, поэтому уязвимость появляется уже на стыке систем, через который проходит обмен данными. То же относится к пользовательским устройствам, поскольку их защита не всегда соответствует требованиям организации. Все эти обстоятельства действуют одновременно и делают угрозы постоянной частью цифровой среды. Особенно заметно это при работе с текстовой информацией, которая приходит по электронным каналам, тогда как решение о её безопасности пользователь нередко принимает сам, без автоматизированной поддержки. Здесь возникает вопрос о том, как такие угрозы распространяются в цифровой среде.

То, как устроены современные информационные сервисы, во многом определяет скорость распространения угроз. Платформы рассчитаны на одновременную работу множества пользователей, поэтому данные быстро доходят до большой аудитории и почти не встречают технических ограничений. Через Интернет к системам обращаются из разных мест, независимо от того, где находится пользователь, а мобильные устройства усиливают этот эффект, делая доступ к сервисам и каналам связи постоянным, в том числе вне рабочего места. Важен и способ работы с данными. Облачное хранение и централизованная обработка упрощают обмен между пользователями и сервисами; кроме того, контент может выйти из одной точки сразу на несколько платформ и одновременно стать доступным разным группам пользователей. При связке систем через API один и тот же материал проходит по нескольким каналам и связанным платформам, не ограничиваясь одним сервисом и не оставаясь в пределах одной точки хранения или одного интерфейса, которым пользуется сотрудник. Автоматизация расширяет эту возможность - программные инструменты создают большое число сообщений без непосредственного участия пользователя, а алгоритмы генерации, в том числе технологии искусственного интеллекта, быстро готовят однотипные или специально адаптированные тексты. Похожесть интерфейсов цифровых сервисов и уведомлений помогает имитировать официальный источник. Если к этому добавить визуально сходные сайты, поддельные доменные имена и стандартные шаблоны, различить настоящее сообщение и подделку становится труднее. Дополнительная неопределённость появляется при использовании ссылок и вложений, когда сокращённый адрес, перенаправление или файл могут скрывать фактическое содержание передаваемых

данных и конечный адрес перехода. В обычном тексте такие элементы выглядят вполне уместно и потому не обязательно воспринимаются как отдельный признак опасности.

Цифровой контент можно менять и использовать повторно почти без потери качества. Текст легко копируют и редактируют без потери качества, а затем отправляют дальше, сохраняя исходный вид или меняя отдельные элементы; в социальных сетях к этому добавляются репосты и пересылка, из-за чего данные быстро расходятся по пользовательским сообществам и могут переходить от одного участника к другому. Источник сообщения при этом не всегда удаётся установить - пользователь может не понимать, кто его подготовил, откуда оно было получено и насколько ему можно доверять. Происхождение данных отслеживается трудно, поскольку между исходным сообщением и его очередной копией может быть несколько промежуточных пересылок, а существующие фильтры не во всех случаях вовремя замечают потенциально опасные элементы. Создавать контент тоже стало проще - сообщения, страницы и другие материалы можно подготовить без специальной подготовки, поэтому круг возможных источников расширяется. Цифровая среда допускает, что один и тот же материал будет быстро изменён, снова скопирован и многократно воспроизведён, причём новые версии могут распространяться уже по другим каналам и в изменённом виде, с сохранением отдельных узнаваемых элементов. Для текстов это особенно характерно - их читают, редактируют и передают быстрее, чем многие другие виды представления информации. На практике такая динамика проявляется при работе с сетью Интернет и внешними цифровыми ресурсами.

Организация ежедневно работает не только во внутренней инфраструктуре: сотрудникам и обучающимся приходится обращаться к веб-сайтам, облачным сервисам, образовательным платформам и другим внешним системам. Это расширяет доступ к данным, но одновременно добавляет новые точки взаимодействия, причём часть операций проходит уже за пределами контролируемой среды. Здесь сложнее понять, насколько надёжна поступившая информация, поскольку проверить её исходный источник удаётся не всегда. Внешние сервисы тоже нельзя считать одинаково защищёнными: они устроены по разным техническим правилам и работают с разным содержанием. Пользователь может встретить недостоверные либо опасные данные, в том числе поддельную страницу, которая выглядит как официальный сайт. Риск появляется и в более обычных действиях - при вводе сведений в веб-форму, загрузке файла или

передаче информации через интерфейс. Ссылка не всегда сразу показывает, куда приведёт переход: перенаправление может скрыть конечный ресурс. Внешне действие остаётся обычным, но пользователь не видит всю цепочку до того, как окажется на конечной странице. К тому же содержимое интернет-ресурса меняется без обязательного уведомления, поэтому одна и та же страница в разные моменты может содержать разные сведения. Открытая цифровая среда не имеет единого центра, который проверял бы всё размещаемое в ней, а распространять информацию можно среди неограниченного круга пользователей. Из-за этого данные продолжают передаваться даже тогда, когда их источник и достоверность не установлены. Они приходят извне, но на этом движение не заканчивается - внутри организации пользователи пересылают их друг другу. Через такие цифровые коммуникации проходит значительная часть информационного взаимодействия организации: внешняя информация сначала входит в рабочую среду, а затем может перемещаться между её участниками по тем же каналам.

Сотрудники и обучающиеся в современной организации общаются главным образом через цифровые каналы. Для этого они используют электронную почту, корпоративные информационные системы и мессенджеры, где быстро отправляют сообщения. По ним идут служебные уведомления, задания, документы и другие сведения, без которых не обходится повседневная работа. Сообщения поступают непрерывно и почти без задержки, поэтому за короткое время пользователь сталкивается с большим их количеством. Внимание расплывается, отдельное сообщение приходится обрабатывать быстрее, а его содержание не всегда получает полноценную оценку. Основной поток при этом текстовый. Пользователь быстро читает сообщение, не переводя его в другой формат, и потому может сразу перейти к ответу, пересылке или работе с приложенным материалом. Такой формат легко прочитать и не нужно дополнительно преобразовывать, но решать, что именно означает сообщение и насколько ему можно доверять, в основном приходится самому получателю: автоматический анализ текста применяется ограниченно. Создать и отправить сообщение тоже нетрудно - его можно направить одному адресату или сразу нескольким, почти не встречая технических ограничений. Скорость здесь сочетается с ослаблением контроля над тем, что именно передаётся. Ограничений для самого отправителя немного, поэтому один и тот же материал быстро уходит нескольким адресатам и дальше может обрабатываться уже без участия исходного автора. Доверие усиливает привычность канала: уведомление, оформленное как

служебное, или сообщение от знакомого отправителя нередко принимают за достоверное ещё до проверки. Так официальную коммуникацию можно имитировать. Ссылки и вложения этому не мешают, поскольку в цифровой переписке они выглядят обычной частью сообщения и часто не вызывают настороженности. Пользователь открывает файл или переходит по ссылке до того, как оценивает их безопасность. Поэтому именно от его решения зависит, как будет обработана информация и сохранится ли безопасность данных. На это решение влияют не только особенности восприятия, но и повседневный режим работы, а также подготовка в области информационной безопасности. В итоге уязвимость пользователя в цифровой среде требует отдельного внимания. Его решение становится частью всей цепочки обработки данных, хотя сам обмен выглядит привычным и не всегда воспринимается как действие, связанное с безопасностью.

Техническая сторона цифровой среды объясняет лишь часть рисков. Другая их часть возникает там, где с информацией работает человек, и именно он обычно оказывается последней точкой перед её использованием. Когда сообщения идут непрерывно, а данных становится много, сосредоточиться на каждом элементе труднее. Пользователь начинает быстрее просматривать материал и чаще замечает общий вид сообщения, чем его отдельные детали; несоответствия и признаки угрозы при этом легко пропустить. Внешний вид оказывается ориентиром, тогда как содержание и детали требуют времени, которого при постоянном потоке сообщений уже не хватает. Повторяющиеся операции закрепляют ещё одну привычку - действовать сразу, не проверяя каждый шаг. Особенно сильно это проявляется в сообщениях, где есть требование срочного ответа или немедленного действия: времени на дополнительную оценку будто бы уже нет. Доверие повышается и тогда, когда отправителем называют преподавателя, администрацию или техническую службу. Такой статус подменяет самостоятельную проверку: знакомое имя или привычная роль воспринимаются как достаточное подтверждение сообщения. Эмоциональная реакция работает сходным образом и отодвигает критическую проверку содержания. Если сообщение вызывает тревогу или заставляет немедленно отвечать, пользователь сначала реагирует на это впечатление, а уже потом мог бы оценить достоверность сведений. Без регулярного обучения и понятных инструкций пользователю трудно оценить достоверность сведений, распознать современные способы воздействия и выстроить безопасную работу с данными. Неосведомлённость оставляет потенциальные угрозы незамеченными.

Повседневная нагрузка усиливает проблему: приходится одновременно выполнять несколько задач, переходить между сервисами и быстро отвечать на сообщения. В таком режиме действия нередко выполняются автоматически, без дополнительного контроля. Переключение между разными сервисами поддерживает этот режим: окно меняется быстрее, чем успевает сформироваться внимательная проверка операции. Снижается защищённость и тогда, когда человек работает с личного устройства, подключается к незащищённой сети или выполняет операцию вне инфраструктуры, которую организация может контролировать. Возможные последствия при этом учитываются не всегда. Пользователь может выполнить привычное действие, не связывая его с тем, что защита в этот момент обеспечивается слабее, чем внутри контролируемой инфраструктуры. Пользовательская уязвимость делает внешнее воздействие на информационные ресурсы более результативным. Этим и пользуются источники угроз за пределами организации, приспособивая свои действия к цифровой среде и к особенностям поведения пользователей. Внешнее воздействие становится эффективнее не само по себе, а потому, что проходит через уже существующие способы работы с сообщениями, устройствами и сетями.

К внешним источникам угроз относят киберпреступников, организованные группы и отдельных злоумышленников, автоматизированные средства, а иногда и сторонние организации. Их интерес может состоять в краже учётных данных и конфиденциальной информации, нарушении работы систем, распространении вредоносного ПО или получении финансовой выгоды. Для этого используются массовые рассылки, сообщения, похожие на официальные, поддельные сайты, вредоносные элементы в файлах и ссылках, а также данные, которые уже были скомпрометированы. Прямого доступа к инфраструктуре организации у таких субъектов обычно нет, поэтому они опираются на открытые каналы связи, анонимность и чужую инфраструктуру. Одно воздействие при этом можно развернуть сразу на большое число пользователей. Открытые каналы и сторонняя инфраструктура позволяют обращаться к ним без непосредственного присутствия в организации, а анонимность затрудняет установление источника. Внутренние источники складываются иначе: они находятся внутри организации и уже имеют доступ к её информационным ресурсам. К ним относятся сотрудники, обучающиеся и технический персонал, который работает с системами и поддерживает их функционирование. Все они входят в общую информационную среду,

но используют её не одинаково и поэтому соприкасаются с разными ресурсами. Эти пользователи не обходят внешний рубеж, а непосредственно взаимодействуют с информацией через штатные средства. Их роли различаются. Поэтому один и тот же доступ не означает одинаковых возможностей: работа с документом, администрирование системы и передача сведений связаны с разными действиями над информацией. Одни работают с документами и базами данных, другие администрируют системы, третьи передают сведения и обмениваются ими. От уровня доступа и набора операций зависит, какой именно риск возникает. Внутренний пользователь способен получить, изменить или передать данные: скопировать служебные сведения, вывести их за пределы организации, удалить или исказить информацию, вызвать сбой в работе системы. В каждом случае меняется не только состояние данных, но и то, кто ещё сможет ими пользоваться и в каком виде они останутся доступными. Иногда это делается намеренно, но значительная часть инцидентов начинается с ошибки. На практике источник такой ошибки действует через обычные операции - открывает файлы, использует информационную систему и учётную запись, передаёт данные внутренним сервисом либо обращается к внешнему ресурсу. Нарушение появляется, когда документ обрабатывают неправильно, доступ настраивают некорректно, сведения отправляют без проверки получателя или используют незащищённый носитель. Все эти действия выглядят как обычные операции, но в них меняется режим обращения с информацией и границы её доступности. Отдельная проблема связана с паролями и учётными данными. Здесь риск возникает уже в момент обращения с доступом, ещё до того, как пользователь начинает работать с конкретным документом или системой. Их могут повторно использовать, передавать другим лицам или применять вне контролируемой среды, и тогда несанкционированный доступ возникает без прямого преодоления защитных механизмов. Внутренний источник особенно труден для обнаружения именно потому, что действует в пределах легитимных прав, через корпоративные сети, сервисы и устройства. Ему не обязательно обходить защиту. Достаточно особенностей обычной работы пользователя. Именно легитимный доступ связывает внутреннего источника с тем ресурсом, на который он воздействует, и поэтому делает угрозу точечной, а не массовой. Такие угрозы обычно не охватывают массово всю организацию, зато могут точнее попадать в конкретный ресурс и иметь более серьёзные последствия, поскольку доступ к нему уже открыт. Поэтому последствия определяются не числом затронутых

пользователей, а тем, какие данные и операции доступны конкретному внутреннему источнику.

Важно различать не только субъектов, от которых исходит угроза, но и то, как именно она реализуется. По этому признаку выделяются преднамеренные и случайные угрозы. В первом случае человек или группа заранее выбирает цель и способ воздействия - получить доступ к данным, изменить их или использовать дальше. Для этого подбирают учётные данные, применяют ранее скомпрометированную информацию, копируют вид доверенного сообщения либо создают ситуацию, в которой нужное действие выполнит сам пользователь. Способ выбирается не случайно: он должен привести к нужному результату - к доступу, изменению или последующему использованию данных. Воздействие часто подстраивают под контекст: берут привычный формат переписки, знакомую рабочую ситуацию и детали, вызывающие доверие. Чем привычнее выглядит такая форма, тем меньше оснований у пользователя остановиться и проверить, кто именно сформировал сообщение и зачем в нём размещены ссылка или файл. Тогда действия злоумышленника выглядят как обычная работа и не сразу вызывают подозрение. Пользователя могут подталкивать срочностью, ссылкой, вложением, ссылкой на авторитет или игрой на внимании. Внешнее воздействие здесь строится не только на техническом элементе, но и на том, как человек воспринимает обычную рабочую ситуацию. Он сам выполняет шаг, который воспринимает как обычный, хотя через него и проходит реализация угрозы. Случайный вариант возникает по другой причине - намерения причинить ущерб здесь нет. Ошибка появляется в повседневной работе: сведения отправляют не тому адресату, выбирают простой или уже использованный пароль, открывают файл, не проверив его содержимое, либо пропускают системное предупреждение. Такие действия часто совершаются автоматически и не выглядят для пользователя опасными. Их особенность в повторяемости: одни и те же рабочие операции регулярно создают возможность для инцидента. Ошибка возвращается вместе с привычной последовательностью действий, поэтому отдельный случай нельзя рассматривать только как разовый сбой внимания. Поэтому отсутствие умысла само по себе не делает последствия незначительными. Если переданы конфиденциальные сведения или открыт доступ к системе, результат может быть сопоставим с преднамеренным воздействием. Для защищаемой информации важен сам факт передачи или открытия доступа, а не то, хотел ли пользователь причинить ущерб. Различаются

источник и логика двух типов угроз, но место реализации нередко одно и то же. В обоих случаях в нём участвует пользователь. Меняется лишь его роль в этой цепочке: при намеренной атаке на него воздействуют извне, а при случайном нарушении его собственное действие становится непосредственным условием инцидента. При намеренной атаке он становится целью, при ошибке - источником нарушения.

Нарушителем в информационной среде может оказаться не только внешний злоумышленник. Им становится любой пользователь, чьи действия способны нарушить конфиденциальность, целостность или доступность информации, даже если такой результат не был осознанной целью. Разделять таких субъектов удобно прежде всего по тому, к чему именно они имеют доступ. Одни связываются с системой только через внешние каналы, другие работают с данными в пределах должностных обязанностей, а пользователи с расширенными правами могут менять настройки и влиять на работу информационных систем. Разный уровень подготовки тоже меняет картину: где-то достаточно базовых знаний и стандартных средств, а где-то используются специальные инструменты и автоматизация. От этого зависят и масштаб, и характер воздействия. Целью может быть получение информации, изменение данных или нарушение работы системы. При этом сам факт нарушения не указывает на умысел. Пользователь может действовать в рамках своих полномочий, но результат всё равно затронет конфиденциальность, целостность или доступность информации. Часть рисков возникает во время обычной работы, когда пользователь ошибается или неверно выполняет доступную ему операцию. Поэтому в понятие нарушителя входят не только те, кто сознательно воздействует на систему, но и те, чьи действия в пределах доступа приводят к такому результату.