

Отчет о результатах оценки организационных и управленческих процессов обеспечения защиты информации сервиса «Яндекс ID» по Отраслевому стандарту защиты данных на 26 сентября 2025 года

Руководству ООО «Яндекс»

Объем оценки и применяемый стандарт

Отраслевой стандарт защиты данных, разработанный Ассоциацией участников рынка больших данных (далее – Стандарт), устанавливает критерии и метрики для целей оценки зрелости организационных и управленческих процессов обеспечения защиты информации оператора персональных данных (далее – ПДн), а также порядок такой оценки.

Настоящий отчет содержит результаты нашей оценки организационных и управленческих процессов обеспечения защиты информации оператора ПДн ООО «Яндекс» (далее – Компания) по критериям и метрикам Стандарта на 26 сентября 2025 года (далее – период оценки).

В область нашей оценки входили исключительно процессы обеспечения защиты информации информационной системы ПДн (далее – ИСПДн) сервиса «Яндекс ID». Какие-либо иные организационные и управленческие процессы Компании не были предметом нашей оценки.

Результаты оценки

В соответствии с полученной от руководства Компании информацией Компания является оператором ПДн категории 4: в ИСПДн обрабатывается более 500 000 персональных данных. Для данной категории оператора ПДн признаются критичными критерии Стандарта со следующими номерами: 1.1, 1.3, 1.4, 1.5, 1.6, 2.1, 2.3 - 2.6, 2.8 - 2.12, 2.14 - 2.18.

Согласно Стандарту, при достижении значения «0» по одному из признанных критичными критериев Стандарта организационные и управленческие процессы обеспечения защиты информации оператора персональных данных признаются недопустимыми, а оценка должна быть прекращена.

По результатам оценки организационные и управленческие процессы обеспечения защиты информации оператора ПДн согласно Стандарту признаны зрелыми в период оценки.

Детали оценки по рассмотренным организационным и управленческим процессам обеспечения защиты информации Компании с обозначением их критичности для различных категорий операторов персональных данных согласно критериям, установленным в Стандарте, приведены в Приложении 1 к настоящему отчету.

Ограничения

Информация, представленная в настоящем Отчете, актуальна на дату Отчета. После указанной даты в Компании могли произойти изменения, которые не отражены в настоящем Отчете.

Настоящий Отчет был подготовлен согласно Дополнительному соглашению 3 от 09.09.2025 к договору между ООО «Кэпт Налоги и Консультирование» и Компанией от 22.08.2024 г. на определенных договором условиях и для руководства Компании исходя из того, что указанный Отчет будет служить только потребностям и интересам получателей Отчета, указанных в соответствующем договоре. В ходе оказания услуг мы рассматривали только вопросы, которые мы обязались рассмотреть согласно соответствующему договору, и не принимали во внимание потребности и интересы третьих лиц.

Любые третьи лица, использующие данный Отчет (или любую его часть) в своих целях, принимают связанные с таким использованием риски и ответственность на себя. В пределах, допускаемых законом, мы не принимаем на себя ответственность и обязательства в связи с данным Отчетом перед третьими лицами.

Оказанные нами Услуги не являются аудитом, обзорной проверкой, заданием по подтверждению достоверности информации или иным заданием, обеспечивающим уверенность, осуществленными в соответствии с какими-либо общепринятыми стандартами, и отличаются от аудита и аналогичных проверок как по объему работ, так и по задачам. Настоящий Отчет не является аудиторским заключением или иным удостоверением, подтверждением или заверением. Данный Отчет также не должен трактоваться как рекомендации.

В своем анализе мы полагались на документы и информацию, предоставленную нам Компанией, в отношении событий и фактов, имеющих значение для нашей оценки.

Мы не даем никаких заверений или гарантий относительно того, что наша оценка непременно совпадет с оценкой, которую можно было бы получить от других организаций или консультантов, проводящих подобную внешнюю оценку.

ООО «Кэпт Налоги и Консультирование»

Лицензия ФСТЭК Л024-00107-77/01118706 на проведение работ и оказание услуг, предусмотренных подпунктами «б», «д», «е» пункта 4 Положения о лицензировании деятельности по технической защите конфиденциальной информации, утвержденного постановлением Правительства Российской Федерации N 79

26 сентября 2025 года

город Москва

Приложение 1.

Оценка выполнения критериев и метрик организационных и управленческих процессов
обеспечения защиты информации оператора персональных данных

Красными выделены номера критериев Стандарта, признанных критичными для Компании в соответствии с определенной категорией оператора ПДн.

№	Критерий	Оценка
1	Организация и управление защитой информации	
1.1	Руководство системой организации защиты информации	1
1.2	Подразделение по защите информации	1
1.3	Положение об организации защиты информации (политика)	1
1.4	Планирование мероприятий по защите информации (стратегия)	1
1.5	Определение негативных последствий от реализации угроз безопасности информации	1
1.6	Моделирование угроз безопасности информации	1
1.7	Контроль услуг контрагентов, имеющих доступ к ИСПДн, или организаций, которым поручена обработка персональных данных	1
2	Реализация процессов обеспечения защиты информации	
2.1	Регламент правил управления доступом	1
2.2	Аутентификация доступа к информационным системам организации и их ресурсам с применением однофакторной и двухфакторной аутентификации	1
2.3	Управление учетными записями	1
2.4	Выявление и оценка уязвимостей	1
2.5	Управление обновлениями безопасности	1
2.6	Инвентаризация информационных ресурсов	1
2.7	Управление изменениями конфигурации	1
2.8	Мониторинг информационной безопасности	1
2.9	Реагирование на инциденты безопасности информации	0.7
2.10	Действия в нештатных ситуациях	1
2.11	Информирование и обучение персонала	1
2.12	Безопасность приложений и программного обеспечения	1
2.13	На периметре ИСПДн установлены межсетевые экраны, правила фильтрации и маршрутизации сконфигурированы, реализовано прохождение трафика только через межсетевые экраны	1
2.14	На периметре ИСПДн информационной инфраструктуры отсутствуют уязвимости критического или высокого уровня (с датой публикации обновления более 30 дней)	1
2.15	На аппаратных и программно-аппаратных средствах, входящих в периметр ИСПДн, отсутствуют уязвимости критического уровня (с датой публикации обновления более 60 дней)	1
2.16	Реализована очистка входящего сетевого трафика от аномалий	1
2.17	Обеспечена проверка вложений в электронные письма (более 90% пользователям осуществляется проверка)	1
2.18	Установлены средства антивирусной защиты с централизованным управлением (или автономные средства защиты) или иные системы, обеспечивающие защиту от вредоносного кода	1
2.19	Проводится (не реже чем раз в полгода) тестирование на проникновение внешнего периметра	0
2.20	Внедрена политика разглашения уязвимостей, инцидентов информационной безопасности и/или утечек персональных данных	1
2.21	Внедрена программа по поиску уязвимостей (БагБаунти)	1
2.22	Осуществляется внутренний аудит ИБ не реже 1 раза в год	1
Суммарная оценка зрелости процессов защиты информации (баллы):		27.7 / 29