ОТРАСЛЕВОЙ СТАНДАРТ ЗАЩИТЫ ДАННЫХ

(с изм. в соответствии с протоколом Совета
по совершенствованию практик N25 от 30.07.2026)

г. Москва

АССОЦИАЦИЯ УЧАСТНИКОВ РЫНКА БОЛЬШИХ ДАННЫХ

Оглавление

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Отраслевой стандарт защиты данных (далее – Стандарт) разработан с учетом положений статьи 19 Закона «О персональных данных» от 27.07.2006 № 152-ФЗ и представляет собой свод оценочных критериев и метрик, позволяющих сделать вывод об зрелости организационных и управленческих процессов обеспечения защиты информации операторов персональных данных (далее по тексту Стандарта термин «информация» включает в себя персональные данные).

1.2. Стандарт определяет порядок осуществления оценки уровня зрелости организации процессов в области защиты информации, а также способов валидации результатов проведенной оценки.

1.3. Согласно настоящему Стандарту, оценка зрелости в области защиты информации проводится организациями, осуществляющими обработку персональных данных (далее – организации/операторы персональных данных), на добровольной основе.

1.4. Актом официального подтверждения, направляемым в Ассоциацию участников рынка больших данных, организации признают и обязуются применять настоящий Стандарт.

1.5. Оценка эффективности организационных и управленческих процессов обеспечения защиты информации операторов персональных данных проводится в ходе внутренней оценки, а также последующей валидации результатов внутренней оценки, с привлечением внешних независимых экспертов. Требования к внешним независимым экспертам приведены в пункте 2.2.5 настоящего Стандарта.

2. ОЦЕНКА СООТВЕТСТВИЯ КРИТЕРИЯМ/МЕТРИКАМ НАСТОЯЩЕГО СТАНДАРТА

2.1. Внутренняя оценка соответствия организационных и управленческих процессов обеспечения защиты персональных данных, критериям и метрикам настоящего Стандарта.

2.1.1. Для проведения внутренней оценки оператор персональных данных формирует экспертную группу из сотрудников подразделений (при наличии), в задачи которых входит защита информации, обеспечение информационных технологий и непосредственная обработка персональных данных.

2.1.2. По усмотрению оператора персональных данных в состав экспертной группы могут быть включены сотрудники других подразделений и эксперты сторонних организаций.

2.1.3. В ходе внутренней оценки соответствия:

- *осуществляется сбор информации о процессах, реализуемых в рамках жизненного цикла обработки персональных данных, и об информационной инфраструктуре оператора персональных данных;*

- *оценивается эффективность организационных и управленческих процессов обеспечения защиты информации.*

2.1.4. По результатам внутренней оценки, в случае достижения максимального показателя, предусмотренного пунктом 4.1 настоящего Стандарта, экспертная группа утверждает протокол оценки. В случае недостижения максимального показателя зрелости, предусмотренного пунктом 4.1, оператор персональных данных должен сформировать план-проспект комплекса мероприятий по повышению зрелости организационных и управленческих мер обеспечения защиты информации.

2.1.5. При проведении последующей оценки соответствия критериям/метрикам оценки зрелости организационных и управленческих процессов обеспечения защиты информации осуществляется анализ результатов реализации план-проспекта

комплекса мероприятий по повышению зрелости организационных и управленческих процессов обеспечения защиты информации, принятого в рамках проведенной ранее оценки.

2.1.6. В рамках сбора информации о процессах, реализуемых в рамках жизненного цикла обработки персональных данных, и об информационной инфраструктуре оператора персональных данных, осуществляется сбор и анализ организационно-распорядительных документов по защите информации объекта информатизации и информационной инфраструктуре в целом (регламентирующих вопросы защиты информации, мероприятия по защите информации, оценку угроз безопасности информации, управления системой защиты информации, реагирования на инциденты, обучения персонала, мониторинга уровня защищенности), а также документов и любой другой информации, подтверждающих реализацию процессов (свидетельства, отчеты, журналы регистраций, сообщения, передаваемые в НКЦКИ и др.).

2.2. Валидация результатов внутренней оценки зрелости организационных и управленческих процессов обеспечения защиты информации.

2.2.1. Оператор персональных данных начинает валидацию результатов внутренней оценки зрелости организационных и управленческих процессов обеспечения защиты информации не позднее двух месяцев с момента завершения проведения внутренней оценки.

2.2.2. Валидация результатов проводится в форме внешней оценки, которую возможно комбинировать с:

- *внешним и (или) внутренним анализом защищенности (в том числе инструментальный анализ);*
- *социотехническим тестированием для оценки осведомленности;*
- *киберучениями;*
- *программами БагБаунти.*

2.2.3. Целью валидации результатов внутренней оценки является оценка объективности сделанных экспертной группой выводов, а также планирование работ по повышению зрелости организационных и управленческих процессов обеспечения защиты информации.

2.2.4. Основой проведения валидации результатов внутренней оценки зрелости организационных и управленческих процессов обеспечения защиты информации являются критерии и метрики, определенные настоящим Стандартом.

2.2.5. С целью обеспечения качества и доверия к результатам внешней оценки, данные работы должны проводиться с привлечением организаций, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Не допускается привлечение организаций, являющихся дочерними или зависимыми обществами по отношению к оператору персональных данных в отношении, которого, проводится внешняя оценка.

3. ПЕРИОДИЧНОСТЬ ПРОВЕДЕНИЯ ОЦЕНКИ ЗРЕЛОСТИ ОРГАНИЗАЦИОННЫХ И УПРАВЛЕНЧЕСКИХ ПРОЦЕССОВ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ

3.1. Плановая оценка зрелости организационных и управленческих процессов обеспечения защиты информации проводится оператором персональных данных не реже одного раза в три года.

3.2. Значения оценки, определенные пунктом 4.1. настоящего Стандарта, применяются при проведении оценки зрелости организационных и управленческих процессов обеспечения защиты информации в значениях, установленных в соответствии с годом ее проведения.

3.3. Изменение значений оценки, определенных пунктом 4.1. настоящего Стандарта не являются основанием для проведения внеплановой (внеочередной) оценки зрелости организационных и управленческих процессов обеспечения защиты информации в течение срока ее действия, определенного в пункте 3.1.

3.4. Случаями, при наступлении которых целесообразно проведение внеочередной оценки зрелости организационных и управленческих процессов обеспечения защиты информации, являются:

- *реализация значимого инцидента безопасности информации, связанного с персональными данными;*
- *развитие и (или) модернизация информационной инфраструктуры и объектов информатизации, вызванной слиянием или поглощением юридического лица и (или) повлекшее изменение категории оператора.*

Значения оценки, определенные пунктом 4.1. настоящего Стандарта, применяются при проведении внеочередной оценки зрелости организационных и управленческих процессов обеспечения защиты информации в значениях, установленных в соответствии с годом её проведения.

4. КРИТЕРИИ И МЕТРИКИ, ПОЗВОЛЯЮЩИЕ СДЕЛАТЬ ВЫВОД ОБ ЗРЕЛОСТИ ОРГАНИЗАЦИОННЫХ И УПРАВЛЕНЧЕСКИХ ПРОЦЕССОВ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ ОПЕРАТОРОВ

<table>
<tr><th></th><th colspan="2">КРИТЕРИЙ/МЕТРИКА</th><th>ОЦЕНКА</th></tr>
<tr><td colspan="4">1.ОРГАНИЗАЦИЯ И УПРАВЛЕНИЕ ЗАЩИТОЙ ИНФОРМАЦИИ</td></tr>
<tr><td>1.1.</td><td colspan="3">Руководство системой организации защиты информации</td></tr>
<tr><td>1.1.1</td><td colspan="2">Вопросы защиты информации решаются по мере возникновения проблем, функция по организации защиты не возложена на руководителя организации или одного из его заместителей</td><td>0</td></tr>
<tr><td>1.1.2</td><td rowspan="5">Функции по организации защиты информации возложены на одного из заместителей генерального директора (или иного уполномоченного Заместителя единоличного исполнительного органа, в соответствии с учредительными документами)</td><td>наряду с иными функциями.</td><td>0,2</td></tr>
<tr><td>1.1.3</td><td>ответственного за цифровую трансформацию</td><td>0,4</td></tr>
<tr><td>1.1.4</td><td>ответственного за общую безопасность в организации или руководителя организации</td><td>0,6</td></tr>
<tr><td>1.1.5</td><td>ответственного только за защиту информации</td><td>1</td></tr>
<tr><td>1.1.6</td><td>головной компании</td><td>1</td></tr>
<tr><td>1.2</td><td colspan="3">Подразделение по защите информации</td></tr>
<tr><td>1.2.1</td><td colspan="2">Подразделение не создано</td><td>0</td></tr>
<tr><td>1.2.2.</td><td colspan="2">Функции по защите информации возложены на отдельных специалистов. Специалисты по защите информации имеют непрофильное образование</td><td>0,2</td></tr>
<tr><td>1.2.3</td><td rowspan="3">Функции по защите информации возложены на непрофильное подразделение. Специалисты по защите информации</td><td>имеют непрофильное образование</td><td>0,2</td></tr>
<tr><td>1.2.4.</td><td>непрофильное образование и проходят курсы повышения квалификации в области защиты информации</td><td>0,3</td></tr>
<tr><td>1.2.5</td><td>имеют базовое образование в области защиты информации (информационной безопасности) и проходят периодическое повышение квалификации</td><td>0,4</td></tr>
<tr><td>1.2.6</td><td>Функции по защите информации возложены</td><td>имеют непрофильное образование</td><td>0,3</td></tr>
</table>

1.2.7	на подразделение по информационным технологиям. Специалисты по защите информации	имеют непрофильное образование и проходят курсы повышения квалификации в области защиты информации	0,4
1.2.8		имеют базовое образование в области защиты информации (информационной безопасности) и проходят периодическое повышение квалификации	0,5
1.2.10	Создано отдельное подразделение по защите информации. Специалисты по защите информации	имеют непрофильное образование	0,5
1.2.11		имеют непрофильное образование и проходят курсы повышения квалификации в области защиты информации	1
1.2.13		имеют базовое образование в области защиты информации (информационной безопасности) и проходят периодическое повышение квалификации	1
1.2.14	Функции по защите информации переданы по договору оказания услуг другому юридическому лицу, имеющему соответствующую лицензию.		1
1.3.	**Положение об организации защиты информации (политика)**		
1.3.1	Не разработано		0
1.3.2	Отдельные положения включены	в положение об организации (или) документы организации	0,2
1.3.3		в положение (концепцию) по цифровой трансформации	0,5
1.3.4	Разработано положение об организации защиты информации (политика)		0,8
1.3.5	Разработано положение об организации защиты информации (политика). С положением ознакомлены руководитель организации и его подразделения. Положение об организации защиты информации (политика) обновляется ежегодно		1
1.4	**Планирование мероприятий по защите информации (стратегия)**		
1.4.1	Планирование мероприятий по защите информации не осуществляется		0
1.4.2	План мероприятий по защите информации разработан и утвержден руководством организации		0,3

1.4.3	План мероприятий по защите информации разработан и утвержден руководством организации. Определены лица, ответственные за реализацию плана мероприятий	0,4
1.4.4	План мероприятий по защите информации разработан и утвержден руководством организации. Определены лица, ответственные за реализацию плана мероприятий. План мероприятий по защите информации доведен до ответственных лиц	0,6
1.4.5	План мероприятий по защите информации разработан и утвержден руководством организации. Определены лица, ответственные за реализацию плана мероприятий. План мероприятий по защите информации доведен до ответственных лиц. Определены лица, ответственные за контроль реализации плана мероприятий по защите информации	0,8
1.4.6	План мероприятий по защите информации разработан и утвержден руководством организации. Определены лица, ответственные за реализацию плана мероприятий. План мероприятий по защите информации доведен до ответственных лиц. Определены лица, ответственные за контроль реализации плана мероприятий по защите информации. Проводятся работы по актуализации плана мероприятий по защите информации	1
1.5	**Определение негативных последствий от реализации угроз безопасности информации**	
1.5.1	В организации не определены негативные последствия	0
1.5.2	В организации определен перечень негативных последствий	0,3
1.5.3	В организации определен перечень негативных последствий. Перечень негативных последствий доведен до руководства организации и профильных подразделений	0,6
1.5.4	В организации определен перечень негативных последствий. Перечень негативных последствий доведен до руководства организации и профильных подразделений. Перечень негативных последствий используется для построения процессов защиты информации и применения технологий безопасности информации	0,8
1.5.5	В организации определен перечень негативных последствий. Перечень негативных последствий доведен до руководства организации и профильных подразделений. Перечень негативных последствий используется для построения процессов защиты информации и применения технологий безопасности	1

	информации. Перечень негативных последствий регулярно актуализируется	
1.6	**Моделирование угроз безопасности информации**	
1.6.1	Моделирование угроз безопасности информации не осуществляется	0
1.6.2	Разработана и утверждена руководством организации модель угроз безопасности информации, или моделирование угроз безопасности информации для информационных систем и данных реализуется иным утвержденным руководством способом.	0,3
1.6.3	Разработана и утверждена руководством организации модель угроз безопасности информации, или моделирование угроз безопасности информации для информационных систем и данных реализуется иным утвержденным руководством способом. Модель угроз безопасности информации доведена до заинтересованных подразделений.	0,6
1.6.4	Разработана и утверждена руководством организации модель угроз безопасности информации, или моделирование угроз безопасности информации для информационных систем и данных реализуется иным утвержденным руководством способом. Модель угроз безопасности информации доведена до заинтересованных подразделений. Модель угроз безопасности информации регулярно актуализируется.	0,8
1.6.5	Разработана и утверждена руководством организации модель угроз безопасности информации, или моделирование угроз безопасности информации для информационных систем и данных реализуется иным утвержденным руководством способом. Модель угроз безопасности информации доведена до заинтересованных подразделений. Модель угроз безопасности информации регулярно актуализируется. Модель угроз безопасности информации используется при проведении работ по контролю (анализу) защищенности	1
1.7	**Контроль услуг контрагентов, имеющих доступ к ИСПДн, или организаций, которым поручена обработка персональных данных**	
1.7.1	В договоры с такими контрагентами не включены требования по информированию оператора персональных данных об инциденте информационной безопасности	0
1.7.2	В договоры с таким контрагентом включены требования по обеспечению мер информационной безопасности и защиты данных, а также информированию оператора персональных данных об инциденте информационной безопасности	0,5

1.7.3	В договоры с таким контрагентом включены требования по обеспечению мер информационной безопасности и защиты данных, а также информированию оператора персональных данных об инциденте информационной безопасности и определены лица такого контрагента, ответственные за информирование оператора персональных данных об инциденте информационной безопасности	0,7
1.7.4	В организации внедрены внутренние регламенты, организационные и технические меры по безопасному взаимодействию с такими контрагентами. В договоры с ними включены требования по обеспечению мер информационной безопасности и защиты данных (в том числе в части уничтожения персональных данных), возможность привлечения субподрядчиков (при условии выполнения ими требований по обеспечению мер информационной безопасности и защиты данных, в том числе в части уничтожения персональных данных), а также информированию оператора персональных данных об инциденте информационной безопасности, определены лица такого контрагента, ответственные за информирование оператора персональных данных об инциденте информационной безопасности, определены сроки информирования оператора персональных данных об инциденте, определены каналы коммуникации, в том числе резервные.	1
2. РЕАЛИЗАЦИЯ ПРОЦЕССОВ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ		
2.1.	**Регламент правил управления доступом**	
2.1.1	Управление учетными данными не регламентировано	0
2.1.2	Процесс управления доступом внедрен, регламентирован и утвержден	0,3
2.1.3	Процесс управления доступом внедрен, регламентирован и утвержден. Разделение полномочий (ролей) пользователей осуществляется в соответствии с процессом	0,6
2.1.4	Процесс управления доступом внедрен, регламентирован и утвержден. Разделение полномочий (ролей) пользователей осуществляется в соответствии с процессом. Регламентированы правила удаленного доступа	1
2.2.	**Аутентификация доступа к информационным системам организации и их ресурсам с применением однофакторной и двухфакторной аутентификации**	
2.2.1	Доступ к информационным системам организации и их ресурсам осуществляется без применения аутентификации	0

2.2.2	Доступ к информационным системам организации и их ресурсам осуществляется с применением однофакторной аутентификации.	0,6
2.2.3	Доступ к информационным системам организации и их ресурсам осуществляется с применением многофакторной аутентификации.	1
2.3	**Управление учетными записями**	
2.3.1	Управление учетными записями не осуществляется, парольная политика отсутствует	0
2.3.2	Управление учетными записями и парольной защитой внедрено, регламентировано (в руководстве, политике, инструкции и др.)	0,3
2.3.3	Управление учетными записями и парольной защитой внедрено, регламентировано (в руководстве, политике, инструкции и др.). Пользователям назначены минимальные права. Установлены требования к паролям и частоте их смены.	0,5
2.3.4	Управление учетными записями и парольной защитой внедрено, регламентировано (в руководстве, политике, инструкции и др.). Пользователям назначены минимальные права. Установлены требования к паролям и частоте их смены. Обеспечивается блокировка доступа к ресурсам в течение суток с момента потери прав пользователя на использование ресурсов.	0,6
2.3.5	Управление учетными записями и парольной защитой внедрено, регламентировано (в руководстве, политике, инструкции и др.). Пользователям назначены минимальные права. Обеспечивается блокировка доступа к ресурсам в течение суток с момента потери прав пользователя на использование ресурсов. Осуществляется ежегодная инвентаризация учетных записей пользователей на основании данных из кадровой службы. Установлены требования к паролям и частоте их смены. Контроль соблюдения требований к паролям и процессу регулярной проверки своевременной смены паролей автоматизирован.	1
2.4	**Выявление и оценка уязвимостей**	
2.4.1	Выявление и оценка уязвимостей не осуществляются	0
2.4.2	Порядок выявления, оценки и устранения уязвимостей внедрен и регламентирован (в руководстве, политике, инструкции и др.)	0,2
2.4.3	Порядок выявления, оценки и устранения уязвимостей внедрен и регламентирован (в руководстве, политике, инструкции и др.). Определены работники, ответственные за выявление и оценку уязвимостей	0,3

2.4.4	Порядок выявления, оценки и устранения уязвимостей внедрен и регламентирован (в руководстве, политике, инструкции и др.). Определены работники, ответственные за выявление и оценку уязвимостей. Поиск уязвимостей осуществляется не регулярно.	0,4
2.4.5	Порядок выявления, оценки и устранения уязвимостей внедрен и регламентирован (в руководстве, политике, инструкции и др.). Определены работники, ответственные за выявление и оценку уязвимостей. Осуществляется выявление уязвимостей на регулярной основе, но не реже чем раз в квартал.	0,6
2.4.6	Порядок выявления, оценки и устранения уязвимостей внедрен и регламентирован (в руководстве, политике, инструкции и др.). Определены работники, ответственные за выявление и оценку уязвимостей. Осуществляется выявление уязвимостей на регулярной основе, не реже чем раз в квартал. Процесс выявления уязвимостей автоматизирован.	0,7
2.4.7	Порядок выявления, оценки и устранения уязвимостей внедрен и регламентирован (в руководстве, политике, инструкции и др.). Определены работники, ответственные за выявление и оценку уязвимостей. Осуществляется выявление уязвимостей на регулярной основе, не реже чем раз в месяц. Проводится классификация выявленных уязвимостей по степени критичности. Организованы работы по устранению уязвимостей.	0,8
2.4.8	Порядок выявления, оценки и устранения уязвимостей внедрен и регламентирован (в руководстве, политике, инструкции и др.). Определены работники, ответственные за выявление и оценку уязвимостей. Осуществляется выявление уязвимостей на регулярной основе, не реже чем раз в месяц. Проводится классификация выявленных уязвимостей по степени критичности. Процесс выявления уязвимостей автоматизирован. Организованы работы по устранению уязвимостей. Определены время реакций на выявленные уязвимости с уровнем «критично»/«высокий».	1
2.5.	**Управление обновлениями безопасности**	
2.5.1	Управление обновлениями безопасности не осуществляется	0
2.5.2	Правила установки обновлений выполняются и регламентированы (в руководстве, политике, инструкции и др.)	0,3
2.5.3	Правила установки обновлений выполняются и регламентированы (в руководстве, политике, инструкции	0,5

	и др.). Определены лица, ответственные за установку обновлений.	
2.5.4	Правила установки обновлений выполняются и регламентированы (в руководстве, политике, инструкции и др.). Определены лица, ответственные за установку обновлений. Реализовано тестирование обновлений.	1
2.6	**Инвентаризация информационных ресурсов**	
2.6.1	Инвентаризация информационных ресурсов не проводится	0
2.6.2	Порядок инвентаризации информационных ресурсов внедрен и регламентирован (в руководстве, политике, инструкции и др.).	0,3
2.6.3	Порядок инвентаризации информационных ресурсов внедрен и регламентирован (в руководстве, политике, инструкции и др.). Также ведётся реестр информационных ресурсов (информационные системы, базы данных, средства защиты информации и др.). Определены лица, ответственные за актуализацию реестра.	0,5
2.6.4	Порядок инвентаризации информационных ресурсов внедрен и регламентирован (в руководстве, политике, инструкции и др.). Определены лица, ответственные за актуализацию реестра. Определен перечень пользователей, осуществляющих обработку конфиденциальной информации. Реестр информационных ресурсов (информационные системы, базы данных, средства защиты информации и др.) ведется с использованием средств автоматизации.	0,7
2.6.5	Порядок инвентаризации информационных ресурсов внедрен и регламентирован (в руководстве, политике, инструкции и др.). Определены лица, ответственные за актуализацию реестра. Определен перечень пользователей, осуществляющих обработку конфиденциальной информации. Определен перечень конфиденциальной информации и места их обработки и хранения в информационной системе. Инвентаризация и ведение реестра информационных ресурсов (информационных систем, базы данных, средства защиты информации и др.) проводится с использованием средств автоматизации.	1
2.7.	**Управление изменениями конфигурации**	
2.7.1	Управление изменениями конфигурации не осуществляется.	0
2.7.2	Определены разрешенные или запрещенные к использованию программные и программно-аппаратные средства, средства защиты информации.	0,3

2.7.3	Определены разрешенные или запрещенные к использованию программные и программно-аппаратные средства, средства защиты информации. Регламентировано резервное копирование конфигурации.	0,6
2.7.4	Определены разрешенные или запрещенные к использованию программные и программно-аппаратные средства, средства защиты информации. Регламентировано резервное копирование конфигурации. Реализован контроль действий по внесению изменений. Определены правила (стандарт) конфигурирования активов (эталонные настройки , харденинг).	1
2.8.	**Мониторинг информационной безопасности**	
2.8.1	Мониторинг информационной безопасности не осуществляется.	0
2.8.2	Определен состав программных и программно-аппаратных средств, средств защиты информации, в которых осуществляется регистрация событий безопасности информации.	0,3
2.8.3	Определен состав программных и программно-аппаратных средств, средств защиты информации, в которых осуществляется регистрация событий безопасности информации. Определен и установлен перечень событий или типов событий, подлежащих регистрации.	0,4
2.8.4	Определен состав программных и программно-аппаратных средств, средств защиты информации, в которых осуществляется регистрация событий безопасности информации. Определен и установлен перечень событий, подлежащих регистрации. Определены лица, ответственные за мониторинг событий безопасности.	0,6
2.8.5	Определен состав программных и программно-аппаратных средств, средств защиты информации, в которых осуществляется регистрация событий безопасности информации. Определен и установлен перечень событий, подлежащих регистрации. Определены лица, ответственные за мониторинг событий безопасности. Регламентированы правила реагирования на события безопасности информации.	0,8
2.8.6	Определен состав программных и программно-аппаратных средств, средств защиты информации, в которых осуществляется регистрация событий безопасности информации. Определен и установлен перечень событий, подлежащих регистрации. Определены лица, ответственные за мониторинг событий безопасности. Регламентированы правила реагирования на события	1

	безопасности информации. Реализовано реагирование на сбои при регистрации событий безопасности.	
2.9.	**Реагирование на инциденты безопасности информации**	
2.9.1	Реагирование на инциденты безопасности информации не осуществляется.	0
2.9.2	Правила и процедуры реагирования на компьютерные инциденты регламентированы (в руководстве, политике, инструкции и др.). Определены временные интервалы начала процедур реагирования на инциденты информационной безопасности, не превышающие 36 часов с момента выявления события информационной безопасности.	0,3
2.9.3	Правила и процедуры реагирования на компьютерные инциденты регламентированы (в руководстве, политике, инструкции и др.). Определены временные интервалы начала процедур реагирования на инциденты информационной безопасности, не превышающие 36 часов с момента выявления события информационной безопасности. Осуществляется информирование о компьютерных инцидентах.	0,6
2.9.4	Правила и процедуры реагирования на компьютерные инциденты регламентированы (в руководстве, политике, инструкции и др.). Определены временные интервалы начала процедур реагирования на инциденты информационной безопасности, не превышающие 36 часов с момента выявления события информационной безопасности. Осуществляется информирование о компьютерных инцидентах. Проводится анализ компьютерных инцидентов.	0,7
2.9.5	Правила и процедуры реагирования на компьютерные инциденты регламентированы (в руководстве, политике, инструкции и др.). Определены временные интервалы начала процедур реагирования на инциденты информационной безопасности, не превышающие 4 часов с момента выявления события информационной безопасности. Осуществляется информирование о компьютерных инцидентах. Проводится анализ компьютерных инцидентов. Проводится устранение последствий компьютерных инцидентов.	0,8
2.9.6	Правила и процедуры реагирования на компьютерные инциденты регламентированы (в руководстве, политике, инструкции и др.). Определены временные интервалы начала процедур реагирования на инциденты информационной безопасности, не превышающие 4 часов с момента выявления события информационной	0,9

	безопасности. Осуществляется информирование о компьютерных инцидентах. Проводится анализ компьютерных инцидентов. Проводится устранение последствий компьютерных инцидентов. Принимаются меры по предотвращению повторного возникновения компьютерных инцидентов.	
2.9.7	Правила и процедуры реагирования на компьютерные инциденты регламентированы (в руководстве, политике, инструкции и др.). Определены временные интервалы начала процедур реагирования на инциденты информационной безопасности, не превышающие 4 часов с момента выявления события информационной безопасности. Осуществляется информирование о компьютерных инцидентах. Проводится анализ компьютерных инцидентов. Проводится устранение последствий компьютерных инцидентов. Принимаются меры по предотвращению повторного возникновения компьютерных инцидентов. Проводится периодический проактивный поиск следов компрометации организации – не реже, чем раз в год. Проводятся киберучения не реже раза в год.	1
2.10	**Действия в нештатных ситуациях**	
2.10.1	Действия при возникновении отказов (сбоев) функционирования программных и программно-аппаратных средств, средств защиты информации, не регламентированы.	0
2.10.2	Разработан план действий при возникновении отказов (сбоев) функционирования программных и программно-аппаратных средств, средств защиты информации.	0,3
2.10.3	Разработан план действий при возникновении отказов (сбоев) функционирования программных и программно-аппаратных средств, средств защиты информации. Проведено обучение и отработка действий персонала при возникновении отказов (сбоев) функционирования программных и программно-аппаратных средств, средств защиты информации.	0,6
2.10.4	Разработан план действий при возникновении отказов (сбоев) функционирования программных и программно-аппаратных средств, средств защиты информации. Проведено обучение и отработка действий персонала при возникновении отказов (сбоев) функционирования программных и программно-аппаратных средств, средств защиты информации. Проводится анализ возникших нештатных ситуаций и принятие мер по недопущению их повторного возникновения.	0,8

2.10.4.	Разработан план действий при возникновении отказов (сбоев) функционирования программных и программно-аппаратных средств, средств защиты информации. Проведено обучение и отработка действий персонала при возникновении отказов (сбоев) функционирования программных и программно-аппаратных средств, средств защиты информации. Проводится анализ возникших нештатных ситуаций и принятие мер по недопущению их повторного возникновения. В соответствии с планом действий сформирована команда управления кризисными ситуациями, в которую входит руководитель организации или уполномоченное им лицо. Проводятся киберучения не реже раза в год.	1
2.11	**Информирование и обучение персонала**	
2.11.1	Информирование и обучение персонала не осуществляется.	0
2.11.2	Правила и процедуры информирования, обучения и повышения осведомленности персонала внедрены и регламентированы (в руководстве, политике, инструкции и др.)	0,3
2.11.3	Правила и процедуры информирования, обучения и повышения осведомленности персонала внедрены и регламентированы (в руководстве, политике, инструкции и др.). Определены лица, ответственные за информирование персонала.	0,6
2.11.4	Правила и процедуры информирования, обучения и повышения осведомленности персонала внедрены и регламентированы (в руководстве, политике, инструкции и др.). Определены лица, ответственные за информирование персонала. Осуществляется периодическое (не реже одного раза в год) информирование персонала об угрозах безопасности информации и о правилах безопасной работы.	0,8
2.11.5	Правила и процедуры информирования, обучения информирования, обучения и повышения осведомленности персонала внедрены и регламентированы (в руководстве, политике, инструкции и др.). Определены лица, ответственные за повышение осведомленности персонала. Осуществляется периодическое (не реже одного раза в полугодие) информирование персонала об угрозах безопасности информации и о правилах безопасной работы. Проводится периодический (не реже одного раза в год) контроль осведомленности персонала об угрозах безопасности информации и о правилах безопасной работы.	0.9

2.11.6	Правила и процедуры информирования, обучения информирования, обучения и повышения осведомленности персонала внедрены и регламентированы (в руководстве, политике, инструкции и др.). Определены лица, ответственные за повышение осведомленности персонала. Осуществляется периодическое (не реже одного раза в полугодие) информирование персонала об угрозах безопасности информации и о правилах безопасной работы. Проводится периодический (не реже одного раза в год) контроль осведомленности персонала об угрозах безопасности информации и о правилах безопасной работы. Периодически (не реже одного раза в год) проводятся практические занятия с персоналом о правилах безопасной работы. Периодически (не реже одного раза в год) проводятся штабные тренировки (учения).	1
2.12	**Безопасность приложений и программного обеспечения**	
2.12.1	Оценка безопасности приложений и программного обеспечения, а также их обновлений не осуществляется.	0
2.12.2	Реализован статический анализ программного кода.	0,6
2.12.3	Реализован динамический анализ программного кода.	0,7
2.12.4	Реализован статический и динамический анализ программного кода.	0,8
2.12.5	В организации внедрены процедуры безопасной разработки в соответствии с международными стандартами.	0,9
2.12.6	В организации внедрены процедуры безопасной разработки с учетом требований применимых национальных стандартов.	1
2.13	**Безопасное использование искусственного интеллекта**	
2.13.1	Управление безопасностью данных при использовании искусственного интеллекта отсутствует.	0
2.13.2	В организации внедрен регламент безопасности данных при использовании искусственного интеллекта.	0,3
2.13.3	В организации внедрен регламент безопасности данных при использовании искусственного интеллекта, проводятся регулярные мероприятия по обучению сотрудников правилам использования ИИ-агентов.	0,5
2.13.4	В организации внедрен регламент безопасности данных при использовании искусственного интеллекта, проводятся регулярные мероприятия по обучению сотрудников правилам использования ИИ-агентов, сопровождающиеся контролем полученных знаний и навыков.	1
2.14	**На периметре ИСПДн установлены межсетевые экраны, правила фильтрации и маршрутизации**	**0/1**

	сконфигурированы, реализовано прохождение трафика только через межсетевые экраны.	
2.15	**На периметре ИСПДн информационной инфраструктуры отсутствуют уязвимости критического или высокого уровня (с датой публикации обновления более 30 дней)**	**0/1**
2.16	**На аппаратных и программно-аппаратных средствах, входящих в периметр ИСПДн, отсутствуют уязвимости критического уровня (с датой публикации обновления более 60 дней).**	**0/1**
2.17	**Реализована очистка входящего сетевого трафика от аномалий.**	**0/1**
2.18	**Обеспечена проверка вложений в электронные письма (более 90% пользователями осуществляется проверка).**	**0/1**
2.19	**Установлены средства антивирусной защиты с централизованным управлением (или автономные средства защиты) или иные системы, обеспечивающие защиту от вредоносного кода.**	**0/1**
2.20	**Проводится (не реже чем раз в полгода) тестирование на проникновение внешнего периметра.**	**0/1**
2.22	**Внедрена политика разглашения уязвимостей, инцидентов информационной безопасности и/или утечек персональных данных.**	**0/1**
2.22	**Внедрена программа по поиску уязвимостей (БагБаунти).**	**0/1**
2.23	**Осуществляется внутренний аудит информационной безопасности не реже 1 раза в год.**	**0/1**

4.1. КАТЕГОРИИ ОПЕРАТОРОВ ПЕРСОНАЛЬНЫХ ДАННЫХ И ПРИМЕНИМЫЕ МЕТРИКИ ОЦЕНКИ:

КАТЕГОРИЯ ОПЕРАТОРА ПЕРСОНАЛЬНЫХ ДАННЫХ	ЗНАЧЕНИЯ ОЦЕНКИ		
	2026 Г.	2027	2028
Категория 1. Все информационные системы персональных данных (ИСПДн) относятся к 4 уровню Защищенности (УЗ) (кроме биометрии и спецкатегории), совокупный объём персональных данных (ПДн) во всех ИСПДн не превышает 100.000;	При 9 и более баллах	При 10 и более баллах	При 11 и более баллах
Категория 2. Есть хотя бы 1 ИСПДн, относящаяся к 3УЗ; либо ИСПДн являются стратегическим направлением развития бизнеса; либо объём базы данных более 100.000 записей;	При 14 и более баллах	При 15 и более баллах	При 16 и более баллах
Категория 3. Наличие специальных категорий ПДн; либо есть ИСПДн не ниже 2УЗ;	При 17 и более баллах	При 18 и более баллах	При 19 и более баллах

Категория 4. Более 500.000 персональных данных в ИСПДн.	При 21 и более баллах	При 22 и более баллах	При 23 и более баллах

Организационные и управленческие процессы обеспечения защиты информации оператора персональных данных являются эффективными при достижении значений, приведенных в настоящем пункте.

4.2. Организационные и управленческие процессы обеспечения защиты информации оператора персональных данных признаются неэффективными при недостижении значений, приведенных в п.4.1.

При достижении следующих частных показателей оценка или валидация результатов прекращается, а организационные и управленческие процессы оператора по обеспечению защиты информации признаются недопустимыми, о чём внешний оценщик уведомляет оператора персональных данных в письменной форме.

КАТЕГОРИЯ ОПЕРАТОРА ПЕРСОНАЛЬНЫХ ДАННЫХ	ЧАСТНЫЙ ПОКАЗАТЕЛЬ
Категория 1. Все информационные системы персональных данных (ИСПДн) относятся к 4 уровню защищенности (УЗ) (кроме биометрии и спецкатегории), совокупный объём субъектов персональных данных (ПДн) во всех ИСПДн не превышает 100.000	При оценке значение критерия/метрики 1.1; 1,3; 1.4;1.5; 1.6; 2.1; 2.3 -2.5; получено значение по одному из обозначенных критериев/метрик равное «0»
Категория 2. Есть хотя бы 1 ИСПДн, относящаяся к 3УЗ; либо ИСПДн являются стратегическим направлением развития бизнеса; либо совокупный объём субъектов ПДн во всех ИСПДн более 100.000;	При оценке значение критерия/метрики 1.1; 1,3; 1.4;1.5; 1.6; 2.1; 2.3 -2.6, 2.8 –2.11; получено значение по одному из обозначенных критериев/метрик равное «0»
Категория 3. Наличие специальных категорий ПДн; либо есть ИСПДн не ниже 2УЗ;	Наличие специальных категорий ПДн; либо есть ИСПДн не ниже 2УЗ;
Категория 4. Совокупный объем субъектов ПДн во всех ИСПДн более 500.000.	При оценке значение критерия/метрики 1.1; 1,3; 1.4;1.5; 1.6; 2.1; 2.3 -2.6, 2.8 – 2.12; 2.14-2.18 получено значение по одному из обозначенных критериев/метрик равное «0»