Отраслевой стандарт защиты данных

г. Москва

АССОЦИАЦИЯ УЧАСТНИКОВ РЫНКА БОЛЬШИХ ДАННЫХ

Оглавление

1. Общие положения

1.1. Отраслевой стандарт защиты данных (далее – Стандарт) разработано с учетом положений статьи 19 Закона «О персональных данных» от 27.07.2006 N 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 Положению, 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 настоящее Стандарт.

1.5. Оценка зрелости 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.

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 зрелость организационных и управленческих процессов обеспечения защиты информации.

2.1.4. По результатам внутренней оценки, в случае достижения максимального показателя, предусмотренного пунктом 4.1, 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 оценке 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 на ежегодной основе.

3.2. 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.

4. Критерии и метрики, позволяющие сделать вывод об зрелости организационных и управленческих процессов обеспечения защиты информации операторов персональных данных

	Критерий/Метрика	Оценка
1.Организация и управление защитой информации		
1.1.	**Руководство системой организации защиты информации**	
1.1.1	Вопросы защиты информации решаются по мере возникновения проблем, функция по организации защиты не возложена на руководителя организации или одного из его заместителей	0
1.1.2	Функции по организации защиты информации возложены на одного из заместителей генерального директора (или иного уполномоченного заместителя единоличного исполнительного органа, в соответствии с учредительными документами) наряду с иными функциями.	0,2
1.1.3	Функции по организации защиты информации возложены на заместителя генерального директора (или иного уполномоченного заместителя единоличного исполнительного органа, в соответствии с учредительными документами), ответственного за цифровую трансформацию	0,4
1.1.4	Функции по организации защиты информации возложены на заместителя генерального директора (или иного уполномоченного заместителя единоличного исполнительного органа, в соответствии с учредительными документами),	0,6

	ответственного за общую безопасность в организации или руководителя организации	
1.1.5	Функции по организации защиты информации возложены на заместителя генерального директора (или иного уполномоченного заместителя единоличного исполнительного органа, в соответствии с учредительными документами), ответственного только за защиту информации	1
1.1.6	Функции по организации защиты информации в группе компаний возложены на заместителя генерального директора (или иного уполномоченного заместителя единоличного исполнительного органа, в соответствии с учредительными документами) головной компании	1
1.2	**Подразделение по защите информации**	
1.2.1	Подразделение не создано	0
1.2.2.	Функции по защите информации возложены на отдельных специалистов. Специалисты по защите информации имеют непрофильное образование	0,2
1.2.3	Функции по защите информации возложены на непрофильное подразделение. Специалисты по защите информации имеют непрофильное образование	0,2
1.2.4.	Функции по защите информации возложены на непрофильное подразделение. Специалисты по защите информации имеют непрофильное образование и проходят курсы повышения квалификации в области защиты информации	0,3
1.2.5	Функции по защите информации возложены на непрофильное подразделение. Специалисты по защите информации имеют базовое образование в области защиты информации (информационной безопасности) и проходят периодическое повышение квалификации	0,4
1.2.6	Функции по защите информации возложены на подразделение по информационным технологиям. Специалисты по защите информации имеют непрофильное образование	0,3
1.2.7	Функции по защите информации возложены 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	Функции по защите информации возложены на подразделение по информационным технологиям. Специалисты по защите информации 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	Создано отдельное подразделение по защите информации.	1

	Специалисты по защите информации имеют непрофильное образование и проходят курсы повышения квалификации в области защиты информации	
1.2.13	Создано отдельное подразделение по защите информации. Специалисты по защите информации 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, стратегия)**	
1.3.1	Не разработано	0
1.3.2	Отдельные положения включены в положение об организации (или) документы организации	0,2
1.3.3	Отдельные положения включены в положение (концепцию) по цифровой трансформации	0,5
1.3.4	Разработано положение об организации защиты информации (политика, стратегия)	0,8
1.3.5	Разработано положение об организации защиты информации (политика, стратегия). С положением ознакомлены руководитель организации и его подразделения. Положение об организации защиты информации (политика, стратегия) обновляется ежегодно	1
1.4	**Планирование мероприятий по защите информации**	
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	1

	лиц. Определены лица, ответственные за контроль реализации плана мероприятий по защите информации. Проводятся работы по актуализации плана мероприятий по защите информации	
1.5	**Определение негативных последствий**	
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 информации. Перечень негативных последствий регулярно актуализируется	1
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	0,3
1.6.3	Разработана и утверждена руководством организации модель угроз безопасности информации. Модель угроз безопасности информации доведена до заинтересованных подразделений.	0,6
1.6.4	Разработана и утверждена руководством организации модель угроз безопасности информации. 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. 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	0

	информационной безопасности	
1.7.2	В договора с таким контрагентом включены требования по информированию оператора персональных данных об инциденте информационной безопасности	0,7
1.7.3	В договора с таким контрагентом включены требования по информированию оператора персональных данных об инциденте информационной безопасности и определены лица такого контрагента, ответственные за информирование оператора персональных данных об инциденте информационной безопасности	1
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 регламентирован и утвержден	0,3
2.1.3	Процесс управления доступом регламентирован и утвержден. Разделение полномочий (ролей) пользователей осуществляется в соответствии с процессом	0,6
2.1.4	Процесс управления доступом 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 двухфакторной аутентификации.	1
2.3	**Управление учетными записями**	
2.3.1	Управление учетными записями не осуществляется	0
2.3.2	Управление учетными записями регламентировано (в руководстве, политике, инструкции и др.)	0,3
2.3.3	Управление учетными записями регламентировано (в руководстве, политике, инструкции и др.). Пользователям назначены минимальные права.	0,5
2.3.4	Управление учетными записями регламентировано (в руководстве, политике, инструкции и др.). Пользователям назначены минимальные права. Обеспечивается блокировка доступа к ресурсам в течении суток с момента потери прав пользователя на использование ресурсов.	0,6
2.3.5	Управление учетными записями регламентировано (в руководстве, политике, инструкции и др.). Пользователям	1

	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.	
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 регламентирован (в руководстве, политике, инструкции и др.)	0,2
2.4.3	Порядок выявления, оценки и устранения уязвимостей 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 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 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 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 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. Организованы работы по устранению уязвимостей	0,8
2.4.8	Порядок выявления, оценки и устранения уязвимостей 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. Процесс выявления уязвимостей автоматизирован. Организованы работы по устранению уязвимостей.	1
2.5.	**Управление обновлениями безопасности**	
2.5.1	Управление обновлениями безопасности не осуществляется	0
2.5.2	Правила установки обновлений регламентированы (в руководстве, политике, инструкции и др.)	0,3

2.5.3	Правила установки обновлений регламентированы (в руководстве, политике, инструкции и др.). Определены лица, ответственные за установку обновлений.	0,5
2.5.4	Правила установки обновлений 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 регламентирован (в руководстве, политике, инструкции и др.)	0,3
2.6.3	Порядок инвентаризации информационных ресурсов регламентирован (в руководстве, политике, инструкции и др.). Ведётся реестр активов (информационные системы, базы данных, средства защиты информации и др.)	0,5
2.6.4	Порядок инвентаризации информационных ресурсов регламентирован (в руководстве, политике, инструкции и др.). Определен перечень пользователей, осуществляющих обработку конфиденциальной информации. Реестр активов (информационные системы, базы данных, средства защиты информации и др.) ведется с использованием средств автоматизации	0,7
2.6.5	Порядок инвентаризации информационных ресурсов регламентирован (в руководстве, политике, инструкции и др.). Определен перечень пользователей, осуществляющих обработку конфиденциальной информации. Определен перечень конфиденциальной информации и места их обработки и хранения в информационной системе. Инвентаризация и ведение реестра активов (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.	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 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 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 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 перечень событий, подлежащих регистрации. Определены лица, ответственные за мониторинг событий безопасности. Регламентированы правила реагирования на события безопасности информации. Реализовано реагирование на сбои при регистрации событий безопасности	1
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 безопасности. Осуществляется информирование о компьютерных инцидентах. Проводится анализ компьютерных инцидентов. Проводится устранение последствий компьютерных инцидентов. Принимаются меры по предотвращению повторного возникновения компьютерных инцидентов.	0,9
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. 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 регламентированы (в руководстве, политике, инструкции и др.)	0,3
2.11.3	Правила и процедуры информирования, обучения и повышения осведомленности персонала 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 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	0.9

	персонала 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	
2.11.6	Правила и процедуры информирования, обучения информирования, обучения и повышения осведомленности персонала 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 статистический анализ программного кода	0,6
2.12.3	Реализован динамический анализ программного кода	0,7
2.12.4	Реализован статистический 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	**На периметре информационной инфраструктуры установлены межсетевые экраны**	**0/1**
2.14	**На периметре информационной инфраструктуры отсутствуют уязвимости критического или высокого уровня (с датой публикации обновления более 30 дней)**	**0/1**
2.15	**На аппаратных и программно-аппаратных средствах отсутствуют уязвимости критического уровня (с датой публикации обновления более 60 дней)**	**0/1**
2.16	**Реализована очистка входящего сетевого трафика от аномалий на сетевом уровне**	**0/1**
2.17	**Обеспечена проверка вложений в электронные письма (более**	**0/1**

	90% пользователям осуществляется проверка)	
2.18	**Установлены средства антивирусной защиты с централизованным управлением (или автономные средства защиты) или иные системы, обеспечивающие защиту от вредоносного кода**	**0/1**
2.19	**Проводится (не реже чем раз в полгода) тестирование на проникновение внешнего периметра**	**0/1**
2.20	**Внедрена политика разглашения уязвимостей**	**0/1**
2.21	**Внедрена программа по поиску уязвимостей (БагБаунти)**	**0/1**
2.22.	**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		
	2024 г.	2025	2026
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 6 и более баллах	При 7 и более баллах	При 9 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 10 и более баллах	При 11 и более баллах	При 14 и более баллах
Категория 3. Наличие специальных категорий ПДн; либо есть ИСПДн не ниже 2УЗ;	При 14 и более баллах	При 15 и более баллах	При 17 и более баллах
Категория 4. Более 500.000 персональных данных в ИСПДн; либо критический профиль рисков (Обработка данных может привести к критичным для государства последствиям. За основу взят фактор дизайна из COBIT 2019 «Оценка ландшафта угроз» (DF5), согласно которому в силу своего геополитического положения, отраслевого сектора или конкретного профиля предприятие работает в условиях повышенного уровня угроз).	При 18 и более баллах	При 19 и более баллах	При 21 и более баллах

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

4.2. Организационные и управленческие процессы обеспечения защиты информации оператора персональных данных признаются незрелыми 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 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 и обозначенных критериев/метрик равное «0»
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 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 и обозначенных критериев/метрик равное «0»
Категория 3. Наличие специальных категорий ПДн; либо есть ИСПДн не ниже 2УЗ;	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; 2.14-2.15 получено значение по одному и обозначенных критериев/метрик равное «0»
Категория 4. Более 500.000 персональных данных в ИСПДН; либо критический профиль рисков (Обработка данных может привести к критичным для государства последствиям. За основу взят фактор дизайна из COBIT 2019 «Оценка ландшафта угроз» (DF5), согласно которому в силу своего геополитического положения, отраслевого сектора или конкретного профиля предприятие работает в условиях повышенного уровня угроз).	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 и обозначенных критериев/метрик равное «0»