2024
RPPA.ru
февраль **2024**

Правила сертификации

PPCP

УТВЕРЖДЕНО: АЛЕКСАНДР ПАРТИН, АЛЕКСЕЙ МУНТЯН, ИЛЬЯ ШАЛЕНКОВ, НИКОЛАЙ ДМИТРИК, КРИСТИНА БОРОВИКОВА

Содержание

1. Понятия

1.1. Сертификация - **PRIVACY PROFESSIONALS CERTIFICATION PROGRAM** (программа сертификации профессионалов в области приватности), представляющая собой процесс подтверждения Сообществом знаний и навыков физического лица (Специалиста) в сфере защиты частной жизни и персональных данных. Сайт Сертификации находится по адресу **ppcp.pro**.

1.2. Сообщество – Общественное учреждение «Сообщество профессионалов в области приватности» (**rppa.ru**).

1.3. Перечень компетенций - перечень компетенций ответственных за обработку и защиту персональных данных в организации, а равно другие перечни компетенций, принятые Сообществом.

1.4. Сертификационные испытания – проверка представителями Сообщества знаний и навыков Специалиста, заявленных им для целей Сертификации.

1. Понятия

1.5. Независимый совет органа по сертификации (Совет) - представители Сообщества, проводящие Сертификационные испытания.

1.6. Профиль специалиста – персональные данные Специалиста, обрабатываемые Офисом.

1.7. Офис – Общество с ограниченной ответственностью «РППА.ОФИС», обеспечивающее организационную и техническую поддержку Сертификации.

1.8. Ментор - участник Сообщества, имеющий знания, навыки и опыт деятельности в соответствующей области и привлекаемый Специалистом для помощи в подготовки к Сертификационным испытаниям.

2. Цели сертификации

2.1. Целями Сертификации являются:

2.1.1. сопоставление фактически имеющихся у Специалиста знаний и навыков с Перечнем компетенций;

2.1.2. создание условий для участия каждого Специалиста в развитии Сообщества;

2.1.3. обеспечение доверия участников Сообщества и третьих лиц, с которыми они взаимодействуют, к знаниям и навыкам Специалистов, прошедших сертификацию;

2.1.4. поддержание Перечня компетенций в актуальном состоянии.

2.2. Цели Сертификации достигаются путем проведения Сертификационных испытаний, создания Профилей специалистов и поддержания сведений в Профилях в актуальном состоянии.

3. Порядок проведения Сертификационных испытаний

3.1. Сертификационные испытания проводятся Советом.

3.2. Совет формируется Офисом из участников Сообщества, соответствующие компетенции которых были подтверждены ранее (о чем имеются данные в их Профилях) и которые заявили Офису о своем желании принимать Сертификационные испытания. При отсутствии участников Сообщества с соответствующими подтвержденными знаниями и навыками Офис формирует Совет из участников Сообщества, которые имеют опыт деятельности в соответствующей области.

3.3. Специалист вправе подготовиться к Сертификационным испытаниям самостоятельно либо согласовать с Советом Ментора для подготовки к Сертификационным испытаниям.

3.4. Для целей проведения Сертификационных испытаний Специалист согласует с Офисом:

3.4.1. компетенции из Перечня компетенций, заявляемые для подтверждения;

3.4.2. сроки проведения Сертификационных испытаний;

3.4.3. форму проведения Сертификационных испытаний;

3.4.4. необходимость Ментора.

3. Порядок проведения Сертификационных испытаний

3.5. Сертификационные испытания, в зависимости от заявленных компетенций, проводятся в одной из следующих форм:

3.5.1. устного экзамена;

3.5.2. защиты проекта;

3.5.3. деловой игры.

3.6. Взаимодействие Совета со Специалистом в ходе Сертификационных испытаний осуществляется в три этапа:

3.6.1. собеседование со Специалистом, в рамках которого обсуждаются материалы для проведения Сертификационных испытаний (вопросы на экзамен, возможный проект и т.п.);

3.6.2. консультация перед Сертификационным испытанием, в рамках которой оценивается готовность Специалиста к Сертификационному испытанию;

3.6.3. проведение Сертификационного испытания в форме, согласованной Специалистом с Советом. По результатам проведения Сертификационного испытания Совет делает заключение о подтверждении Специалистом заявленных компетенций, которое является основанием для внесения изменений и дополнений в Профиль этого Специалиста.

3. Порядок проведения Сертификационных испытаний

3.7. Выводы Совета по результатам Сертификационных испытаний являются окончательными и не подлежат пересмотру. Специалист вправе пройти Сертификационные испытания повторно по любой неподтвержденной компетенции. Повторные Сертификационные испытания назначаются и проводятся в том же порядке, что и первоначальные Сертификационные испытания.

3.8. Если иное не согласовано Специалистом с Офисом, все материалы, созданные Специалистом для целей прохождения Сертификационных испытаний, являются общедоступной информацией, и Специалист разрешает их использование любым участником Сообщества на условиях неисключительной лицензии **CC BY 4.0.** Перечень материалов, представляемых Специалистом на Сертификационные испытания, которые не относятся к общедоступной информацией и в отношении которых не предоставляется право на использование, согласуется Специалистом с Офисом до проведения соответствующего Сертификационного испытания.

4. Порядок ведения Профилей специалиста

4.1. Профиль специалиста создается и ведется для целей подтверждения компетенций Специалиста и включает в себя следующие персональные данные Специалиста:

4.1.1. имя, фамилия

4.1.2. уникальный номер Профиля

4.1.3. записи Сертификационных испытаний с участием Специалиста

4.1.4. сведения о подтвержденных по результатам Сертификационных испытаниях компетенциях Специалиста

4.1.5. отзывы и рекомендации, полученные Офисом в отношении Специалиста, в отношении которых Советом принято решение о включении их в Профиль специалиста;

4.1.6. сведения об участии Специалиста в конференциях и других мероприятиях Сообщества.

4.2. Создание Профиля Специалиста и внесение в него изменений осуществляется только Офисом, от имени и в интересах Сообщества.

4.3. Основанием для создания и ведения Профиля Специалиста является договор между Специалистом и Офисом на проведение Сертификационных испытаний.

4. Порядок ведения Профилей специалиста

4.4. Доступ к Профилю специалиста (за исключением записей Сертификационных испытаний с участием Специалиста) осуществляется на сайте Сертификации при условии указания имени и фамилии Специалиста, соответствующих уникальному номеру Профиля. Доступ к записям Сертификационных испытаний с участием Специалиста осуществляется только Офисом и Советом при возникновении спорных ситуаций, касающихся прохождения Специалистом Сертификационных испытаний.

4.5. Внесение изменений в Профиль специалиста осуществляется Офисом в следующих случаях:

4.5.1. по результатам проведенных Сертификационных испытаний

4.5.2. получение в отношении Специалиста отзывов и рекомендаций или сведений об участии в мероприятиях Сообщества;

4.5.3. получение запроса Специалиста на актуализацию или удаление сведений о нем.

5. Утверждение и изменение Правил сертификации

5.1. Настоящие Правила сертификации PPCP (далее – “Правила сертификации”) были утверждены решением собрания учредителей Сообщества **1** ноября **2023** года и действуют с этого дня.

5.2. Действующая редакция Правил на бумажном носителе хранится в месте нахождения исполнительного органа Офиса.

5.3. Электронная версия действующей редакции Правил сертификации опубликована на сайте Сертификации.

5.4. Правила сертификации утверждаются и вводятся в действие решением собрания учредителей Сообщества и действуют до их отмены.

5.5. Собрание учредителей Сообщества имеет право по мере необходимости вносить изменения в Правила сертификации (далее – “Изменения”). Изменения утверждаются решением собрания учредителей Сообщества. В таком случае измененная редакция Правил сертификации публикуется на сайте Сертификации с указанием срока начала ее действия.

Приложение 1.
Критерии сертификации.
Блок A.

1. Понимание системы законодательства приватности в России и обобщенно в мире	
1.1 Понимает причины появления и историю развития права на неприкосновенность частной жизни.	**1.** Знает основные этапы появления права на неприкосновенность частной жизни (в США, Европе и в целом в мире) **2.** Может назвать факторы, которые на каждом этапе повлияли на содержание права на неприкосновенность частной жизни
1.2 Знает причины появления института защиты персональных данных как отдельного правового института, основные этапы его развития.	**1.** Понимает отличия институтов неприкосновенности частной жизни и защиты персональных данных **2.** Знает акты зарубежных стран и международные договоры, в которых были изначально закреплены подходы, формирующие регулирование персональных данных в настоящее время **3.** Может назвать цели, стоявшие перед ключевыми актами, исторически приведшими к формированию института защиты персональных данных в Европе
1.3 Знает существующие общие подходы к приватности в мире. (Американский, Европейский и Южно-Азиатский)	**1.** Может указать основные источники права на неприкосновенность частной жизни и на защиту персональных данных в США, Канаде, странах ЕАЭС, КНР и Японии **2.** Понимает ключевые отличия основных подходов к приватности в Северной Америке, странах-участницах Конвенции Совета Европы и в странах Юго-Восточной Азии
2. Понимает правовые основы регулирования приватности в России.	**1.1.** Может назвать отрасли и институты законодательства, регламентирующие обработку разных видов информации о человеке в России **2.2.** Знает основные критерии применения мер гражданской, административной, уголовной ответственности в случае нарушения прав человека на информацию о себе

Приложение 1.
Критерии сертификации.
Блок A.

3. Понимает систему законодательства в сфере приватности в России и обобщенно в мире:	
3.1 Знает критерии применимости российского законодательства в области приватности, а также законодательства в области приватности других стран мира, которое может влиять на российский бизнес.	**1.** Может назвать критерии применимости Российского законодательства к процессам обработки ПД с указанием примеров **2.** Выделены / сгруппированы критерии применимости иностранного права в сфере приватности к компаниям, учреждениям на территории РФ с указанием конкретных примеров - более **3**х: например, локализация, экстерриториальность, косвенная применимость
3.2 Понимает соотношение иных норм права с регулированием обработки и защиты ПД.	**1.** Понимает соотношение правовых норм в области персональных данных с нормами - о свободе слова; - о труде; - об интеллектуальной собственности; - об информации и информационных технологиях **2.** Может аргументированно разграничивать применение норм разных отраслей в конкретных кейсах
3.3 Знает полномочия надзорных органов в области обработки и защиты ПД. Понимает основные правоотношения, возникающие при взаимодействии с надзорными органами.	**1.** Знает систему надзорных органов в сфере ПД **2.** Знает полномочия каждого из органов в отношении операторов **3.** Знает правовые акты, регламентирующие порядок взаимоотношения надзорных органов с операторами и субъектами
4 Знает основные характеристики объектов регулирования: Персональные данные, Особые категории персональных данных, Источники персональных данных, Средства обработки персональных данных.	**1.** Знает критерии выявления ПД из массива разнородной информации и может обосновать их применение **2.** Умеет строить модели категорирования ПД на основе категорий ПД, определенных в законе, а также дополнительных категорий, самостоятельно выделенных (не менее **2**х) **3.** Знает виды источников ПД (не менее **3**х), может привести примеры **4.** Знает средства обработки ПД, может привести примеры

Приложение 1.
Критерии сертификации.
Блок A.

5. Понимает и различает роли основных участников отношений по обработке персональных данных: Субъект, Оператор (контролер), Обработчик (процессор, суб-процессор), Совместные операторы (совместные контролеры), Независимые операторы (независимые контролеры)	**1.** Знает критерии, по которым данные связываются с субъектами, а также критерии отделения субъекта от иных схожих ролей (организации, группы лиц и т.п.) **2.** Знает признаки оператора персональных данных и виды операторов **3.** Знает иные роли, встречающиеся во взаимоотношениях между участниками обработки
6. Осознает и умеет применять основания обработки персональных данных, определенные применимым законодательством в области приватности.	**1.** Знает предусмотренные законом основания обработки ПД и критерии их выбора **2.** Умеет выбирать правовое основание обработки в предложенной ситуации
7. Понимает принципы обработки и защиты персональных данных, определенные применимым законодательством в области приватности.	**1.** Знает предусмотренные законом принципы обработки ПД **2.** Умеет демонстрировать применение принципов обработки ПД в предложенной конкретной ситуации
9. Обладает знаниями в сфере регулирования персональных данных с учетом требований по локализации и трансграничной передачи.	**1.** Понимает причины ограничений на трансграничную передачу или запрета таких ограничений **2.** Понимает критерии локализации ПД **3.** Умеет выстраивать систему мероприятий для локализации ПД и трансграничной передачи

Приложение 2. Критерии сертификации. Блок B.

Компетенция	Критерии для подтверждения компетенции	Сценарий сертификации
1.1 Обладает знанием и пониманием основных фреймворков в области приватности от ведущих институтов и ассоциаций мира.	**1.**Имеет представление о выбранном фреймворке: структуре, области и специфике применения **2.**Понимает порядок внедрения фреймворка в процессы компании **3.**Знает методы поддержания соответствия процессов компании рекомендациям выбранного фреймворка	**1.**Описание методологии внедрения фреймворка в процессы компании **2.**Для самостоятельно выбранных контролей – презентация проекта **3.**Ответы на дополнительные вопросы по иным контролям
1.2 Обладает умением построения контрольной среды в области приватности.	**1.**Понимает порядок формирования и проверки контролей, применимых к процессам компании **2.**Знает методы поддержания соответствия процессов компании сформированным контролям	**1.**Описание подхода по формированию и проверке контролей **2.**Для самостоятельно выбранных контролей – презентация проекта **3.**Ответы на дополнительные вопросы по иным контролям
2.2 Умеет определять применимое к отношениям право, помимо базового для компании.	**1.**Знает основные подходы по выявлению применимого к процессам компании иностранного законодательства в сфере приватности **2.**Понимает порядок формирования перечня применимого права **3.**Знает инструменты для выполнения мониторинга изменений в выявленном перечне	**1.**Описание порядка и методологии выявления и мониторинга применимого к процессам компании иностранного законодательства в сфере приватности **2.**Презентация проекта по выявлению и мониторингу применимого к процессам компании иностранного законодательства в сфере приватности **3.**Ответы на дополнительные вопросы по порядку

Приложение 2.
Критерии сертификации.
Блок B.

2.3 Знает подходы и умеет проводить аудиты в области приватности (планирование – проведение – оценка – распределение задач – контроль).	**1.**Знает основные этапы проведения аудита процессов обработки ПД **2.**Понимает порядок проверки функции приватности **3.**Знает инструменты, используемые в аудитах и проверках	**1.**Описание порядка проведения аудита процессов обработки ПД / функции приватности в компании **2.**Презентация проекта по проведенному аудиту процессов обработки ПД / функции приватности **3.**Ответы на дополнительные вопросы по порядку аудита
3.1 Умеет проводить моделирование угроз безопасности ПД.	**1.** Знает основные требования применимого законодательства и лучшие практики в части моделирования угроз безопасности ПД **2.**Понимает порядок моделирования угроз безопасности ИБ	**1.**Описание требований и порядка моделирования угроз безопасности ИБ **2.**Презентация проекта по проведенному моделированию угроз безопасности ИБ для самостоятельно выбранного процесса **3.**Ответы на дополнительные вопросы по порядку моделирования угроз безопасности ИБ
3.2 Умеет проводить оценку вреда субъектам ПД.	**1.**Знает современные методологии оценки вреда субъектам **2.**Умеет идентифицировать вред, потенциально наносимый субъекту вследствие обработки ПД, а также рассчитывать вероятность наступления такого события **3.**Понимает и умеет выявлять инструменты, необходимые для снижения потенциального вреда субъекту при обработке ПД	**1.**Описание выбранной методологии оценки вреда субъектам **2.**Презентация проекта по оценке вреда субъектам для самостоятельно выбранного процесса **3.**Ответы на дополнительные вопросы по порядку оценки

Приложение 2.
Критерии сертификации.
Блок B.

3.3 Знает общие подходы к проведению **PIA/DPIA, LIA.TIA.**	**1.**Понимает различия между **PIA/DPIA, LIA, TIA,** а также при каких условиях используются указанные инструменты **2.**Понимает порядок проведения **PIA/DPIA, LIA, TIA**	**1.**Описание порядка проведения **PIA/DPIA, LIA, TIA** **2.**Презентация проекта **PIA/DPIA, LIA, TIA** для самостоятельно выбранного процесса **3.**Ответы на дополнительные вопросы по инструментам
4.1 Умеет выделять из бизнес-процессов компании процессы обработки ПД.	**1.**Понимает логику формирования бизнес-процессов в компании **2.**Знает подходы и инструменты формирования бизнес-процессов **3.**Знает критерии выделения процессов обработки ПД из бизнес-процессов компании	**1.**Описание порядка формирования бизнес-процессов в компании **2.**Презентация проекта по выявлению процессов обработки ПД в составе бизнес-процессов компании **3.**Ответы на дополнительные вопросы по порядку
4.2 Знает подходы и умеет проводить инвентаризацию процессов обработки и защиты ПД.	**1.**Понимает порядок проведения инвентаризации процессов ПД **2.**Знает объем информации, необходимый для сбора и последующей фиксации информации в рамках инвентаризации процессов	**1.**Описание порядка инвентаризации процессов **2.**Презентация проекта по инвентаризации для самостоятельно выбранного процесса **3.**Ответы на дополнительные вопросы по порядку инвентаризации

Приложение 2.
Критерии сертификации.
Блок B.

4.3 Умеет выявлять избыточные ПД и минимизировать состав ПД с учетом целей обработки.	**1.**Понимает принцип минимизации ПД **2.**Умеет выявлять избыточные ПД **3.**Понимает порядок минимизации ПД	**1.**Описание порядка минимизации ПД **2.**Презентация проекта по минимизации ПД для выбранного процесса **3.**Ответы на дополнительные вопросы по порядку
4.4 Умеет описывать процессы обработки и защиты ПД в компании понятно, кратко и структурировано.	**1.** Умеет понятно преподносить информацию о процессах обработки ПД **2.**Умеет структурировать информацию о процессах обработки ПД	**1.**Презентация примера подготовленного описания процесса **2.**Ответы на дополнительные вопросы
4.5 Умеет составлять согласия на обработку персональных данных для разных категорий субъектов ПД.	**1.** Понимает различия в типах согласий и условия выбора таких типов **2.**Понимает порядок управления согласиями на всем их жизненном цикле **3.**Умеет составлять согласия и понимает значение информации, указанной в них	**1.**Описание порядка управления согласиями, включая составление согласий разных типов **2.**Презентация проекта по управлению согласиями с указанием этапов жизненного цикла **3.**Ответы на дополнительные вопросы по порядку управления согласиями

Приложение 2.
Критерии сертификации.
Блок B.

5.1 Знает риск-ориентированные подходы по выбору контрагентов.	**1.** Понимает различия в ролях контрагентов, участвующих в обработке ПД **2.**Понимает значимость выбора и проведения мероприятий по первичной проверке контрагентов **3.**Разбирается в риск-ориентированных методологиях по выбору контрагентов	**1.**Описание методологии по выбору контрагентов **2.**Презентация проекта с указанием подхода по выбору контрагента для одной роли **3.**Ответы на дополнительные вопросы по порядку выбора контрагентов
5.2 Умеет определять гарантии безопасности ПД.	**1.**Разбирается в организационных и технических мерах митигации выявленных рисков защиты ПД при взаимодействии с контрагентом **2.**Понимает соотношение выявленных рисков и мер их митигации	**1.**Описание методологии по выбору контрагентов **2.**Презентация проекта с указанием подхода по выбору контрагента для одной роли **3.**Ответы на дополнительные вопросы по порядку выбора контрагентов
5.3 Умеет составлять договоры с получателями ПД в разных ролях получателей и компании в части обработки и защиты ПД.	**1.**Умеет различать типы договоров для разных типов взаимоотношений между компаниями в части обработки ПД **2.**Умеет составлять формулировки в части защиты и обработки ПД для разных типов взаимоотношений	**1.**Описание типов договоров / вордингов в части обработки и защиты ПД **2.** Презентация примеров договоров / вордингов в части обработки и защиты ПД **3.**Ответы на дополнительные вопросы

Приложение 2.
Критерии сертификации.
Блок B.

5.4 Знает подходы и умеет проводить аудит уровня безопасности ПД получателей ПД.	**1.**Знает методы аудита получателя ПД в части ИБ **2.**Умеет проводить проверку уровня ИБ получателя ПД	**1.**Описание порядка проведения аудита ИБ получателя ПД **2.**Презентация проекта аудита ИБ для выбранного обезличенного получателя ПД **3.**Ответы на дополнительные вопросы по порядку аудита
5.5 Обладает навыками организации процесса трансграничной передачи данных.	**1.**Знает порядок трансграничной передачи данных в выбранной юрисдикции: определение, ограничения, требования **2.**Умеет выявлять наличие трансграничной передачи ПД в потоках информации **3.**Умеет выбирать и внедрять организационные и технические меры, направленные на обеспечение соответствия процессов с трансграничной передачей ПД требованиям выбранного законодательства, а также на минимизацию выявленных рисков приватности и ИБ	**1.**Описание порядка идентификации трансграничной передачи ПД в процессах компании **2.**Презентация проекта по организации трансграничной передачи для выбранного процесса **3.**Ответы на дополнительные вопросы
6.1 Обладает общими знаниями подходов управления физическим и логическим доступом к данным.	**1.** Знает технологии управления физическим доступом к данным **2.**Знает технологии управления логическим доступом к данным **3.**Умеет выбирать необходимые технологии управления доступом с учетом специфики процесса обработки ПД	**1.**Перечисление и краткое описание доступных на рынке технологий управления физическим и логическим доступом (не менее **3**х) **2.**Презентация проекта или подхода по выбору необходимой технологии управления доступом с учетом специфики процесса обработки ПД **3.**Ответы на дополнительные вопросы по управлению доступом

Приложение 2.
Критерии сертификации.
Блок B.

6.2. Имеет базовое техническое представление о системах защиты конфиденциальной информации, средствах шифрования, алгоритмах анонимизации и псевдонимизации данных.	**1.**Знает технологии защиты конфиденциальной информации **2.**Умеет выбирать необходимые технологии защиты информации с учетом специфики процесса обработки ПД	**1.**Перечисление и краткое описание доступных на рынке технологий защиты информации (не менее одного для каждого выявленного типа) **2.**Презентация проекта или подхода по выбору необходимой технологии защиты информации с учетом специфики процесса обработки ПД **3.**Ответы на дополнительные вопросы по средствам защиты
6.3 Умеет выбирать средства и меры защиты конфиденциальной информации для минимизации выявленных рисков приватности.	**1.**Знает типы организационных и технических мер защиты информации **2.**Понимает порядок минимизации выявленных рисков приватности с применением средств защиты информации	**1.**Презентация проекта по выбору мер защиты информации от выявленных рисков **2.**Ответы на дополнительные вопросы
6.4 Умеет определять критерии хранения данных, формировать процедуры и подходы по хранению ПД в компании.	**1.**Знает критерии, влияющие на порядок хранения данных **2.**Понимает принципы формирования порядка хранения данных **3.**Знает технологии хранения данных **4.** Умеет формировать подходы по хранению данных	**1.**Описание порядка хранения данных с указанием критериев выбора такого порядка и использования технологий **2.**Презентация проекта по организации хранения данных для выбранного процесса **3.**Ответы на дополнительные вопросы по порядку хранения данных

Приложение 2. Критерии сертификации. Блок B.

6.5 Обладает базовыми знаниями технологий удаления и гарантированного уничтожения данных.	**1.**Знает различия между удалением и уничтожением данных **2.**Знает технологии удаления и гарантированного уничтожения данных	**1.**Перечисление и краткое описание доступных на рынке технологий удаления и гарантированного уничтожения данных (не менее одного для каждого выявленного типа) **2.**Презентация проекта или подхода по выбору необходимой технологии удаления и уничтожения данных с учетом специфики процесса обработки ПД **3.**Ответы на дополнительные вопросы по технологиям
6.6 Обладает базовыми знаниями технологий резервного копирования, логирования и мониторинга в разрезе приватности.	**1.** Знает технологии резервного копирования, логирования и мониторинга информации **2.**Умеет выбирать необходимые технологии с учетом специфики процесса обработки ПД	**1.**Перечисление и краткое описание доступных на рынке технологий резервного копирования, логирования и мониторинга информации (не менее одного для каждого выявленного типа) **2.**Презентация проекта или подхода по выбору необходимой технологии учетом специфики процесса обработки ПД **3.**Ответы на дополнительные вопросы по технологиям
7.1 Знает критерии определения инцидентов информационной безопасности, а также механизмы выявления инцидентов.	**1.**Знает различия между событием, инцидентом и утечкой данных **2.**Знает критерии выявления инцидентов информационной безопасности **3.**Понимает механизмы выявления инцидентов информационной безопасности	**1.**Описание порядка выявления инцидентов информационной безопасности с указанием критериев выявления **2.**Презентация проекта по организации порядка управления инцидентами для этапа выявления инцидентов **3.**Ответы на дополнительные вопросы по порядку управления инцидентами

Приложение 2. Критерии сертификации. Блок В.

7.2 Знает критерии выявления утечек персональных данных**.**	**1.**Знает различия между инцидентом ИБ и утечкой данных **2.** Знает критерии и механизмы выявления утечек данных **3.**Понимает порядок выявления утечек данных	**1.**Описание порядка выявления утечек данных с указанием критериев и механизмов **2.**Презентация проекта по организации порядка выявления утечек данных **3.**Ответы на дополнительные вопросы по порядку управления инцидентами
7.3 Знает подходы и процедуры реагирования на утечки персональных данных**.**	**1.**Понимает порядок распределения полномочий в части реагирования на утечки данных **2.**Знает порядок информирования сторон в случае утечки данных **3.** Понимает порядок действий по нейтрализации последствий утечки данных	**1.**Описание порядка выявления реагирования на утечки данных **2.**Презентация проекта по организации порядка реагирования на утечки данных **3.**Ответы на дополнительные вопросы по порядку управления инцидентами
8. Обладает навыками построения и реализации порядка исполнения прав субъектов ПД**.**	**1.**Знает перечень прав субъектов в применимой юрисдикции **2.**Понимает значение конкретных прав субъектов в применимой юрисдикции **3.**Понимает порядок действий по исполнению прав субъектов в применимой юрисдикции	**1.** Описание порядка реализации прав субъектов в применимой юрисдикции **2.**Презентация проекта по организации порядка прав субъектов в применимой юрисдикции **3.**Ответы на дополнительные вопросы по порядку

Приложение 2.
Критерии сертификации.
Блок B.

9. Обладает навыками формирования метрик функции приватности.	**1.** Понимает значение метрик функции приватности **2.**Знает порядок формирования метрик функции приватности **3.** Понимает порядок действий по проверки исполнения метрик функции приватности	**1.**Описание подходов по формированию метрик функции приватности **2.**Презентация проекта, в рамках которого были сформированы и проверены метрики функции приватности **3.**Ответы на дополнительные вопросы
10. Обладает навыками контроля и составления метрика автоматизированных процессов приватности: -Полнота данных в процессе обработки ПД, -Обеспечение достоверности данных, -Обеспечение минимизации данных, Локализация данных, -Обязательные аудиты и проверки, форма отчетности по аудитам	**1.**Знает технологии автоматизации процессов приватности, представленные на применимом рынке **2.**Умеет выбирать необходимые технологии автоматизации процессов приватности с учетом сформированных метрик	**1.**Перечисление и краткое описание доступных на рынке технологий автоматизации функции приватности (не менее одного для каждого выявленного типа) **2.**Презентация проекта или подхода по выбору необходимой технологии с учетом сформированных метрик **3.**Ответы на дополнительные вопросы
11. Обладает базовыми знаниями специфики современных средств обработки информации: облачные технологии, ИИ.	**1.**Знает современные средства обработки информации: облачные технологии, ИИ **2.**Умеет выбирать необходимые технологии с учетом специфики процессов обработки ПД	**1.**Перечисление и краткое описание доступных на рынке современные средств обработки информации **2.**Презентация проекта или подхода по участию в выборе современных средств обработки информации с учетом специфики процесса обработки ПД **3.**Ответы на дополнительные вопросы

Контакты

https://rppa.ru | info@rppa.ru
https://ppcp.pro | info@ppcp.pro