ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 29100— 2013

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Основы обеспечения приватности

ISO/IEC 29100:2011
Information technology – Security techniques – Privacy framework
(IDT)

Издание официальное

Москва
Стандартинформ
2014

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН Обществом с ограниченной ответственностью «Научно-производственная фирма «Кристалл» (ООО «НПФ «Кристалл») и Обществом с ограниченной ответственностью «Информационный аналитический вычислительный центр» (ООО «ИАВЦ») на основе собственного аутентичного перевода на русский язык стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 22 «Информационные технологии»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ приказом Федерального агентства по техническому регулированию и метрологии от « 08» ноября 2013 № 1539-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 29100:2011 «Информационная технология. Методы и средства обеспечения безопасности. Основы обеспечения приватности» (ISO/IEC 29100:2011 «Information technology – Security techniques – Privacy framework»)

Наименование настоящего стандарта изменено относительно наименования указанного международного стандарта для приведения в соответствие с ГОСТ Р 1.5 (пункт 3.5).

5 ВВЕДЕН ВПЕРВЫЕ

Правила применения настоящего стандарта установлены в ГОСТ Р 1.0—2012 (раздел 8). Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок – в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования – на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (gost.ru)

© Стандартинформ, 2014

Настоящий стандарт не может быть воспроизведен, тиражирован и распространен в качестве официального издания без разрешения национального органа Российской Федерации по стандартизации.

Введение

Настоящий стандарт предоставляет высокоуровневую структуру для защиты персональной идентификационной информации (ПИИ) в пределах системы информационно-коммуникационной технологии (ИКТ). Он является общим по своему характеру, определяет место организационных, технических и процедурных аспектов в общей структуре обеспечения приватности.

Структура обеспечения приватности предназначена для содействия организациям в определении требований к связанным с ПИИ мерам защиты приватности в среде ИКТ посредством:

- продвижения общей терминологии, связанной с обеспечением приватности;
- определения субъектов и их ролей при обработке ПИИ;
- описания требований к мерам защиты приватности;
- ссылки на известные принципы обеспечения приватности.

В некоторых странах ссылки настоящего стандарта на требования к мерам защиты приватности могут расцениваться как дополнение к законодательным требованиям защиты ПИИ. Из-за растущего ИКТ числа информационно-коммуникационных технологий, которые обрабатывают ПИИ, важно применять международные стандарты по информационной безопасности, которые обеспечивают общее понимание защиты ПИИ. Настоящий стандарт предназначен для улучшения существующих стандартов безопасности посредством сосредоточения значительного внимания на обработке ПИИ.

Увеличение коммерческого использования и ценности ПИИ, совместного использования ПИИ разными странами, а также растущая сложность систем ИКТ могут усложнить для организации обеспечение приватности и достижение соответствия различным законам. Лица, заинтересованные в обеспечении приватности, могут предотвратить возникновение неуверенности и недоверия посредством надлежащего обращения с приватной информацией, а также избегая случаев неправильного использования ПИИ.

Использование настоящего стандарта призвано:

- содействовать проектированию, реализации, эксплуатации и поддержке систем ИКТ, которые обрабатывают ПИИ и обеспечивают её защиту;
- стимулировать инновационные решения, позволяющие обеспечивать защиту ПИИ в системах ИКТ;
- совершенствовать корпоративные программы обеспечения приватности благодаря использованию лучших практических приемов.

Структура обеспечения приватности, представленная в настоящем стандарте, может служить основой для дополнительных инициатив по стандартизации обеспечения приватности, таких как:

- техническая эталонная архитектура;
- реализация и использование конкретных технологий обеспечения приватности и общего менеджмента приватности;
- меры и средства контроля и управления приватностью для процессов обработки данных в рамках аутсорсинга;
- оценка рисков приватности;
- определенные технические спецификации.

Некоторые страны могут потребовать соответствия с одним или более документами, на которые имеются ссылки в постоянно действующем документе 2 РГ 5 ИСО/МЭК СТК 1/ПК 27 Библиографический список официальных документов по приватности (ISO/IEC JTC 1/SC 27 WG 5 Standing Document 2 (WG 5 SD2) – Official Privacy Documents References) [3], или с другими соответствующими законами и нормативными документами, но настоящий стандарт не предназначен служить примером ни глобальной модели стратегии, ни законодательной основы.

ИСО/МЭК 29100 подготовлен совместным техническим комитетом ИСО/МЭК СТК 1 «Информационная технология», Подкомитетом ПК 27 «Методы и средства обеспечения безопасности».

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационная технология
МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ
Основы обеспечения приватности

Information technology – Security techniques – Privacy framework

Дата введения — 2015—01—01

1 Область применения

В настоящем стандарте представлена структура обеспечения приватности, которая:

- устанавливает общую терминологию приватности;
- определяет субъектов и их роли в обработке персональной идентификационной информации (ПИИ);
- описывает соображения, касающиеся мер защиты приватности;
- предоставляет ссылки на известные принципы обеспечения приватности.

Настоящий стандарт предназначен для физических лиц и организаций, вовлеченных в определение особенностей, приобретение, моделирование, проектирование, создание, тестирование, обслуживание, управление и функционирование системы информационно-коммуникационных технологий (ИКТ)или услуги, где для обработки ПИИ требуются меры и средства контроля и управления приватностью.

2 Термины и определения

Для целей данного документа применяются следующие термины и определения:

Примечание – В целях упрощения использования семейства международных стандартов ИСО/МЭК 27000 в специфическом контексте приватности и интеграции понятий приватности в контексте ИСО/МЭК 27000, в таблице, приведенной в Приложении А, представлены понятия ИСО/МЭК 27000, соответствующие понятиям ИСО/МЭК 29100, используемым в настоящем стандарте.

2.1 **анонимность** (anonymity): Свойство информации, не позволяющее прямо или косвенно определить обладателя ПИИ.

2.2 **обезличивание** (anonymization): Процесс, посредством которого ПИИ изменяется так, что обладатель ПИИ не может быть опознан прямо или косвенно ни самим оператором ПИИ, ни в сотрудничестве с любой другой стороной.

2.3 **обезличенные данные** (anonymized data): Данные, которые были получены в результате процесса обезличивания ПИИ.

2.4 **согласие** (consent): Добровольное, конкретное и осознанное разрешение, данное обладателем ПИИ на обработку его ПИИ.

2.5 **идентифицируемость** (identifiability): Условие, результатом которого является прямая или косвенная идентификация обладателя ПИИ на основе данного набора ПИИ.

2.6 **идентифицировать** (identify): Устанавливать связь между обладателем ПИИ и ПИИ или набором ПИИ.

2.7 **идентификационные данные** (identity data): Набор атрибутов, которые позволяют идентифицировать обладателя ПИИ.

2.8 **согласие на обработку** (opt-in): Процесс или тип политики, посредством которой обладатель ПИИ обязан предпринять действие, чтобы выразить определенное, ясное и заблаговременное согласие на обработку его ПИИ для конкретной цели.

Примечание – Другим термином, часто используемым в отношении принципа приватности «согласие и выбор», является термин «запрет на обработку». С его помощью описывается процесс или тип политики, посредством которой обладатель ПИИ обязан предпринять отдельное действие, чтобы отказать или отозвать согласие либо воспрепятствовать осуществлению определенного вида обработки его ПИИ. Использование политики отказа от обработки предполагает, что оператор ПИИ обладает правом обработки ПИИ назначенным

Издание официальное

образом. Под этим правом может подразумеваться некое действие обладателя ПИИ, отличающееся от согласия (Например, размещение заказа в онлайновом магазине).

2.9 **персональная идентификационная информация; ПИИ** (personally identifiable information, PII): Любая информация: (a) которая может использоваться для идентификации обладателя ПИИ, которому такая информация принадлежит; (b) которая прямо или косвенно уже связана или может быть связана с обладателем ПИИ.

Примечание – Для того чтобы определить, является ли обладатель ПИИ идентифицируемым, следует учесть все средства, которые могут быть корректно использованы лицом, заинтересованным в обеспечении приватности, владеющим данными, или любой другой стороной для идентификации этого физического лица.

2.10 **оператор ПИИ** (PII controller): Лицо, заинтересованное в обеспечении приватности (или лица, заинтересованные в обеспечении приватности), которое определяет цели и способы обработки ПИИ, в отличие от физических лиц, использующих данные в личных целях.

Примечание – Оператор ПИИ может давать указания другим (например, третьей стороне) по обработке ПИИ от своего лица, в то время как ответственность за обработку остается на операторе ПИИ.

2.11 **обладатель ПИИ** (PII principal): Физическое лицо, к которому относится ПИИ.

Примечание – В зависимости от страны и конкретного закона в области защиты данных и обеспечения приватности синоним «субъект данных» может быть также использован вместо термина «обладатель ПИИ».

2.12 **обработчик ПИИ** (PII processor): Лицо, заинтересованное в обеспечении приватности, которое обрабатывает ПИИ от имени и в соответствии с инструкциями оператора ПИИ.

2.13 **нарушение приватности** (privacy breach): Ситуация, когда ПИИ обрабатывается в нарушение одного или более соответствующих требований защиты приватности.

2.14 **меры и средства контроля и управления приватностью** (privacy controls): Меры, которые обрабатывают риски путем снижения их вероятности или их последствий.

Примечания

1 Меры и средства контроля и управления приватностью включают организационные, физические и технические меры, например, политики, процедуры, рекомендации, законные контракты, практики менеджмента или организационные структуры.

2 Мера и средство контроля и управления приватностью также применяется как синоним защитных мер или контрмер.

2.15 **технология, улучшающая обеспечение приватности** (privacy enhancing technology, PET): Мера и средство контроля и управления приватностью, состоящая из мер, продуктов или сервисов системы ИКТ, которые обеспечивают защиту приватности путем уничтожения или сокращения объема ПИИ или предотвращения ненужной и (или) нежелательной обработки ПИИ без потери функциональности системы ИКТ.

Примечания

1 Примерами использования технологии, улучшающей обеспечение приватности, являются средства обезличивания и псевдонимизации, которые устраняют, уменьшают, маскируют или обезличивают ПИИ либо предотвращают ненужную, несанкционированную и (или) нежелательную обработку ПИИ, но не ограничиваются ими.

2 Маскирование является процессом, результатом которого является затруднение понимания ПИИ.

2.16 **политика приватности** (privacy policy): Общее намерение и направление деятельности, правила и обязательства, формально выраженные оператором ПИИ, касающиеся обработки ПИИ в определенной области.

2.17 **предпочтительные способы обеспечения приватности** (privacy preferences): Конкретный выбор, сделанный обладателем ПИИ в отношении того, как должна быть обработана для определенной цели его ПИИ.

2.18 **принципы обеспечения приватности** (privacy principles): Совокупность утверждений, направленных на управление обеспечением приватности ПИИ при ее обработке в системах ИКТ.

2.19 **риск обеспечения приватности** (privacy risk): Влияние неопределенности на приватность.

Примечания

1 В Руководстве 73 ИСО и ИСО 31000 риск определяется как «влияние неопределенности на цели».

2 Неопределенность – это состояние, даже частичное, отсутствия информации, касающейся понимания или знания о событии, его последствиях или вероятности.

2.20 **оценка риска обеспечения приватности** (privacy risk assessment): Общий процесс идентификации, анализа и оценивания риска в отношении обработки ПИИ.

Примечание – Этот процесс известен также как оценка влияния на приватность.

2.21 **требования к мерам защиты приватности** (privacy safeguarding requirements): Набор требований, которые организация должна учитывать при обработке ПИИ в части защиты приватности ПИИ.

2.22 **лицо, заинтересованное в обеспечении приватности** (privacy stakeholder): Физическое или юридическое лицо, орган государственной власти, агентство или какая-либо другая организация, которые могут влиять, подвергаться влиянию или испытывать на себе влияние решения или деятельности, связанной с обработкой ПИИ.

2.23 **обработка ПИИ** (processing of PII): Любая операция или совокупность операций, выполняемых в отношении ПИИ.

Примечание – Примеры операций включают (но не ограничиваются этим) сбор, хранение, изменение, восстановление, опрос, разглашение, обезличивание, псевдонимизацию, распространение или иное предоставление, удаление или уничтожение ПИИ.

2.24 **псевдонимизация** (pseudonymization): Процесс, относящийся к ПИИ, который заменяет идентификационную информацию псевдонимом.

Примечания

1 Псевдонимизация может выполняться либо самими обладателями ПИИ, либо операторами ПИИ. Псевдонимизация может использоваться обладателями ПИИ для последовательного использования ресурса или сервиса без раскрытия своей идентификационной информации в отношении данного ресурса или сервиса (или между сервисами), оставаясь в то же время ответственными за это использование.

2 Псевдонимизация не исключает возможность существования ограниченного числа лиц, заинтересованных в обеспечении приватности, не являющихся операторами ПИИ псевдонимизированных данных, которые способны определять идентификационную информацию об обладателях ПИИ, основываясь на псевдонимах и связанных с ними данных.

2.25 **вторичное использование** (secondary use): Обработка ПИИ в условиях, отличающихся от начальных условий.

Примечание – Условия, отличающиеся от начальных условий, могут включать, например, новую цель обработки ПИИ, нового получателя ПИИ и т. п.

2.26 **чувствительная ПИИ** (sensitive PII): Категория ПИИ, которая либо является по своей природе чувствительной, например, затрагивает наиболее личную сферу обладателя ПИИ, либо может оказывать значительное влияние на обладателя ПИИ.

Примечание – В некоторых странах или при определенных обстоятельствах чувствительная ПИИ определяется относительно типа ПИИ и может состоять из ПИИ, раскрывающей расовую принадлежность, политические убеждения или религиозные либо другие верования, персональные данные о здоровье, сексуальной жизни или преступлениях, и другой ПИИ, которая может быть определена как чувствительная.

2.27 **третья сторона** (third party): Лицо, заинтересованное в обеспечении приватности, не являющееся обладателем ПИИ, оператором ПИИ или обработчиком ПИИ, а также физические лица, уполномоченные обрабатывать данные под непосредственным руководством оператора ПИИ или обработчика ПИИ.

3 Обозначения и аббревиатуры

Приведенные далее аббревиатуры являются общими для ИСО/МЭК 29100:

PET – технология, улучшающая обеспечение приватности (Privacy Enhancing Technology);

ИКТ – информационно-коммуникационные технологии;

ПИИ – персональная идентификационная информация.

4 Основные элементы структуры обеспечения приватности

4.1 Общий обзор структуры обеспечения приватности

Следующие компоненты связаны с обеспечением приватности и обработкой ПИИ в системах ИКТ и составляют структуру обеспечения приватности, описанную в настоящем стандарте:

- субъекты и роли;
- взаимодействие;
- распознавание ПИИ;
- требования к мерам защиты приватности;
- политики обеспечения приватности;
- меры и средства контроля и управления приватностью.

Для разработки данной структуры обеспечения приватности учитывались понятия, определения и рекомендации из других официальных источников. Данный источник может быть найден в постоянно действующем документе 2 РГ 5 ИСО/МЭК СТК 1/ПК 27 «Библиографический список официальных документов по приватности» (ISO/IEC JTC 1/SC 27 WG 5 Standing Document 2 – «Official Privacy Documents References») [3].

4.2 Субъекты и роли

Для целей данного стандарта важно идентифицировать субъектов, вовлеченных в обработку ПИИ. Существуют четыре типа субъектов, которые могут быть вовлечены в обработку ПИИ: обладатели ПИИ, операторы ПИИ, обработчики ПИИ и третьи стороны.

4.2.1 Обладатели ПИИ

Обладатели ПИИ предоставляют свою ПИИ для обработки операторам ПИИ и обработчикам ПИИ и, если обратное не установлено применимым законом, они дают согласие и определяют свои предпочтения в отношении способов обработки их ПИИ. Например, обладателем ПИИ может быть: работник, включенный в штатное расписание компании, потребитель, упомянутый в отчете о кредитных операциях, и пациент, запись о здоровье которого внесена в электронную базу. Чтобы считаться обладателем ПИИ, соответствующее физическое лицо необязательно должно быть идентифицировано по его имени. Если физическое лицо, к которому относится ПИИ, может быть идентифицировано косвенно (например, через идентификатор счета, номер полиса социального страхования или даже через комбинацию доступных признаков), он или она также являются обладателем ПИИ для данного набора ПИИ.

4.2.2 Операторы ПИИ

Оператор ПИИ определяет, почему (цель) и как (способы) обрабатывается ПИИ. В данной структуре оператор ПИИ должен обеспечивать уверенность, что соблюдение принципов приватности во время обработки ПИИ осуществляется под его контролем (например, путем реализации необходимых мер и средств контроля и управления приватностью). Может существовать более чем одного оператора ПИИ для одного и того же набора ПИИ или набора операций, выполняемых в отношении ПИИ (для тех же самых или различных легальных целей). В этом случае различные операторы ПИИ должны сотрудничать и обеспечивать выполнение принципов обеспечения приватности во время обработки ПИИ. Оператор ПИИ также может разрешить выполнение всех или части операций по обработке ПИИ другим лицам, заинтересованным в обеспечении приватности, от своего лица. Операторы ПИИ должны тщательно оценивать, обрабатывают они чувствительную или нечувствительную информацию, и реализовывать рациональные и относящиеся к делу меры и средства контроля и управления приватностью и безопасностью на основе требований, установленных в соответствующей стране, а также оценивать любое возможное негативное влияние на обладателей ПИИ в связи с их идентификацией во время оценки риска обеспечения приватности.

4.2.3 Обработчики ПИИ

Обработчик ПИИ выполняет обработку ПИИ от имени оператора ПИИ, действует от имени или в соответствии с инструкциями оператора ПИИ, соблюдает установленные требования обеспечения приватности и реализует соответствующие меры и средства контроля и управления приватностью. В некоторых странах обработчик ПИИ ограничен законным договором.

4.2.4 Третьи стороны

Третья сторона может получать ПИИ от оператора ПИИ или обработчика ПИИ. Третья сторона не обрабатывает ПИИ от имени оператора ПИИ. В основном третья сторона становится самостоятельным оператором ПИИ после получения запрашиваемой ПИИ.

4.3 Взаимодействия

Субъекты, идентифицированные в 4.2, могут взаимодействовать между собой различным образом. Можно идентифицировать следующие сценарии, формирующие потоки ПИИ между обладателем ПИИ, оператором ПИИ и обработчиком ПИИ:

a) обладатель ПИИ предоставляет ПИИ оператору ПИИ (например, регистрация для оказания услуги оператором ПИИ);

b) оператор ПИИ предоставляет ПИИ обработчику ПИИ, который обрабатывает эту ПИИ от имени оператора ПИИ (например, как часть соглашения об аутсорсинге);

c) обладатель ПИИ предоставляет ПИИ обработчику ПИИ, который обрабатывает эту ПИИ от имени оператора ПИИ;

d) оператор ПИИ предоставляет ПИИ обладателю ПИИ, и она относится к обладателю ПИИ (например, в соответствии с запросом, сделанным обладателем ПИИ);

e) обработчик ПИИ предоставляет ПИИ обладателю ПИИ (например, регулирование оператором ПИИ);

f) обработчик ПИИ предоставляет ПИИ оператору ПИИ (например, после обслуживания/выполнения сервиса, для которого она была предназначена).

Роли обладателя ПИИ, оператора ПИИ, обработчика ПИИ и третьей стороны в данных сценариях показаны в таблице 1.

Необходимо различать обработчиков ПИИ и третью сторону, потому что при пересылке ПИИ обработчику ПИИ правовой контроль за ПИИ остается функцией первоначального оператора ПИИ, тогда как третья сторона оправданно может стать самостоятельным оператором ПИИ после получения запрашиваемой ПИИ. Например, когда третья сторона принимает решение о передаче ПИИ, полученной от оператора ПИИ, другой стороне, она будет действовать как оператор ПИИ с ее собственными правами и поэтому больше не будет являться третьей стороной.

Можно идентифицировать следующие сценарии, формирующие потоки ПИИ, между операторами ПИИ и обработчиками ПИИ, с одной стороны, и третьей стороной, с другой стороны:

g) оператор ПИИ предоставляет ПИИ третьей стороне (например, в контексте делового соглашения);

h) обработчик ПИИ предоставляет ПИИ третьей стороне (например, по указанию оператора ПИИ).

Роли оператора ПИИ и третьей стороны в этих сценариях также показаны в таблице 1.

Таблица 1 – Возможные потоки ПИИ между обладателем ПИИ, оператором ПИИ, обработчиком ПИИ и третьими сторонами и их ролями

Сценарий	Обладатель ПИИ	Оператор ПИИ	Обработчик ПИИ	Третья сторона
a)	Поставщик ПИИ	Получатель ПИИ	–	–
b)	–	Поставщик ПИИ	Получатель ПИИ	–
c)	Поставщик ПИИ	–	Получатель ПИИ	–
d)	Получатель ПИИ	Поставщик ПИИ	–	–
e)	Получатель ПИИ	–	Поставщик ПИИ	–
f)	–	Получатель ПИИ	Поставщик ПИИ	–
g)	–	Поставщик ПИИ	–	Получатель ПИИ
h)	–	–	Поставщик ПИИ	Получатель ПИИ

4.4 Распознавание ПИИ

Чтобы определить, считается ли физическое лицо идентифицируемым, должны быть приняты во внимание некоторые факторы. В частности, необходимо учитывать все средства, которые могут оправданно использоваться лицом, заинтересованным в обеспечении приватности, хранящим данные, или любой другой стороной для идентификации этого физического лица. Системы ИКТ должны поддерживать механизмы, информирующие обладателя ПИИ о такой ПИИ и предоставлять физическому лицу соответствующие меры и средства контроля и управления при совместном использовании этой информации. В следующих подпунктах содержится дополнительное разъяснение того, как определить, следует ли рассматривать обладателя ПИИ в качестве идентифицируемого.

4.4.1 Идентификаторы

В определенных случаях идентифицируемость обладателя ПИИ может быть очевидной (например, когда информация содержит или связана с идентификатором, который используется для обращения или связи с обладателем ПИИ). Информация может быть отнесена к ПИИ в следующих случаях:

- если она содержит или связана с идентификатором, который относится к физическому лицу (например, номер социального страхования);
- если она содержит или связана с идентификатором, который может быть легко связан с физическим лицом (например, номер и серия паспорта, номер счета);
- если она содержит или связана с идентификатором, который может использоваться для установления связи с идентифицируемым физическим лицом (например, точное географическое местоположение, номер телефона);
- если она содержит ссылку, которая связывает данные с любым из идентификаторов, приведенных ранее.

4.4.2 Другие отличительные характеристики

Идентифицируемость является способностью определения физического лица, к которому относится данный набор ПИИ. Поэтому информация не обязательно должна быть связана с идентификатором, чтобы считаться ПИИ. Информацию можно считать ПИИ, если она будет содержать или будет связана с характеристикой, которая отличает физическое лицо от других физических лиц (например, биометрические данные).

Любой атрибут, имеющий значение, который уникально опознает обладателя ПИИ, необходимо рассматривать как отличительную характеристику. Необходимо отметить, что не зависимо от того, отличает или не отличает данная характеристика физическое лицо от других физических лиц, она может измениться от контекста использования. Например, фамилии физического лица может быть недостаточно, чтобы опознать его в глобальном масштабе, но будет достаточно, чтобы отличить физическое лицо в масштабе компании.

Кроме того, могут также существовать ситуации, в которых физическое лицо является идентифицируемым, даже если не существует никакого единственного признака, который уникально определяет его или ее. В этом случае комбинация нескольких признаков, взятых вместе, отличает физическое лицо от других физических лиц. Возможность отнесения некоего физического лица к идентифицируемым, исходя из комбинации признаков, может также зависеть от конкретной области. Например, комбинации признаков «женщина», «45» «адвокат» может быть достаточно для идентификации некоего физического лица в пределах определенной компании, но зачастую этих признаков бывает недостаточно для идентификации этого же физического лица за пределами этой же компании.

В таблице 2 приведены некоторые примеры атрибутов, которые могли бы быть ПИИ в зависимости от сферы деятельности. Эти примеры являются информативными.

Таблица 2 – Примеры атрибутов, которые могут использоваться для идентификации физических лиц

Примеры
Возраст или особые потребности уязвимых физических лиц
Заявление о криминальном поведении
Любая информация, собранная во время оказания медицинских услуг
Номер банковского счета или кредитной карты
Биометрический идентификатор
Информация о кредитной карте
Осуждение в уголовном порядке или совершенные преступления
Отчеты об уголовном расследовании
Абонентский номер
Дата рождения
Информация о диагностике состояния здоровья
Нетрудоспособность
Документ о нетрудоспособности
Сведения о заработной плате служащих и файлы отдела кадров
Финансовая информация
Пол
Данные GPS о местоположении
Траектории GPS
Домашний адрес
IP-адрес
Информация о местоположении, полученная от телекоммуникационных систем
История болезни
Фамилия
Государственные идентификаторы, например, номер и серия паспорта
Адрес личной электронной почты
Личные идентификационные номера (PIN-коды) или пароли
Личные интересы, полученные из отслеживания Web-сайтов Интернет
Личный или поведенческий стереотип
Номер личного телефона
Фотография или видео, по которым можно идентифицировать человека
Предпочтения, касающиеся продуктов и услуг
Расовое или этническое происхождение
Религиозные или философские убеждения
Сексуальная ориентация
Членство в профсоюзах
Счет за коммунальные услуги

4.4.3 Информация, которая связана или может быть связана с обладателем ПИИ

Если рассматриваемая информация не идентифицирует обладателя ПИИ, то должно быть определено, связана ли информация или может ли она быть связана с идентификационными данными физического лица.

После установления связи с идентифицируемым физическим лицом необходимо решить сообщает ли что-либо информация о данном физическом лице, например, если она связана с его или ее характеристиками либо поведением. Примеры включают истории болезни, финансовую информацию или личные интересы, полученные посредством отслеживания использования Web-сайтов Интернет. Простые сообщения об отличительных чертах физического лица, таких как возраст или пол физического лица, могут также квалифицировать связанную с ним информацию как ПИИ. Независимо от этого, если связь с идентифицируемым физическим лицом может быть установлена, такая информация также должна обрабатываться как ПИИ.

4.4.4 Псевдонимные данные

Чтобы ограничить возможность операторов и обработчиков ПИИ идентифицировать обладателя ПИИ, идентификационная информация может быть заменена псевдонимами. Такая замена обычно выполняется поставщиком ПИИ до передачи ПИИ получателю ПИИ, в частности, как указано в сценариях a, b, c, g, h таблицы 1.

При некоторых процессах бизнеса полагаются на назначенных обработчиков, которые выполняют замену и контролируют таблицу или функцию назначения. Зачастую это бывает тогда,

когда существует необходимость обработки чувствительных данных лицами, заинтересованным в обеспечении приватности, не производившими их сбор.

Замена, рассматриваемая как псеводонимизация, обеспечивает следующее:

a) оставшиеся атрибуты, связанные с псевдонимами, недостаточны для идентификации обладателя ПИИ, к которому они относятся;

b) псевдонимы назначаются так, чтобы их использование для выполнения обратного действия не могло осуществляться даже при затрачивании значительных усилий лицами, заинтересованным в обеспечении приватности, кроме тех лиц, которые уполномочены это делать.

Псевдонимизация сохраняет возможность установления связи. Можно установить связь между различными данными, связанными с одним и тем же псевдонимом. Чем больше объем данных, связанных с данным псевдонимом, тем больше риск того, что свойство (a) будет нарушено. Более того, чем меньше группа физических лиц, к которым относится набор псевдонимных данных, тем больше вероятность того, что обладатель ПИИ станет идентифицируемым. Признаки, содержащиеся непосредственно в информации, о которой идет речь, и признаки, которые могут быть легко связаны с этой информацией (например, посредством использования поисковой системы или перекрестных ссылок с другими базами данных) должны быть приняты во внимание при определении того, относится или не относится информация к идентифицируемому физическому лицу.

Псевдонимизация является действием, противоположным обезличиванию. Процессы обезличивания также обеспечивают свойства (a) и (b), приведенные ранее, но нарушают возможность установления связи. Во время обезличивания идентификационная информация либо удаляется, либо заменяется псевдонимами, для которых функция или таблица назначения уничтожается. Поэтому обезличенные данные больше не являются ПИИ.

4.4.5 Метаданные

ПИИ может храниться в системе ИКТ таким образом, что она не будет являться видимой для пользователя системы (т. е. обладателя ПИИ). Примерами такой информации являются фамилия обладателя ПИИ, хранящаяся как метаданные в свойствах документа, и комментарии или отслеженные изменения, хранящиеся как метаданные в документе по подготовке текстов. Если обладателю ПИИ станет известно о существовании ПИИ или обработке ПИИ для этой цели, то он или она, возможно, предпочтут, чтобы ПИИ не обрабатывалась таким образом или не использовалась совместно.

4.4.6 Незапрашиваемая ПИИ

ПИИ, которая не была запрошена оператором ПИИ или обработчиком ПИИ (т. е. получена непреднамеренно), может также храниться в системе ИКТ. Например, обладатель ПИИ потенциально мог бы предоставить ПИИ оператору ПИИ, которую последний не запрашивал или не отыскивал (например, дополнительная ПИИ, предоставляемая в контексте в форме анонимной обратной связи на Web-сайте). Риск сбора незапрашиваемой ПИИ может быть уменьшен путем рассмотрения мер защиты приватности во время проектирования системы (также известных как понятие «обеспечение приватности через проектирование»).

4.4.7 Чувствительная ПИИ

Чувствительность распространяется на всю ПИИ, из которой может быть получена чувствительная ПИИ. Например, медицинские предписания могут показать подробную информацию о здоровье обладателя ПИИ. Даже если ПИИ не содержит прямую информацию о сексуальной ориентации или здоровье обладателя ПИИ, но может использоваться для получения подобной информации, то такая ПИИ может быть чувствительной. Для целей этого стандарта ПИИ нужно рассматривать как чувствительную там, где это возможно.

В некоторых странах понятие чувствительной ПИИ явно определено в законе. Примером является информация о расовой принадлежности, этническом происхождении, религиозных или философских убеждениях, политических взглядах, членстве в профсоюзах, сексуальной жизни или ориентации, а также о физическом или психическом здоровье обладателя ПИИ. В других странах чувствительная ПИИ может включать информацию, которая могла бы способствовать «краже личности» (идентификационных данных) или иным образом приводить к значительному финансовому ущербу для физического лица (например, номера кредитных карт, информация о банковском счете или государственные идентификаторы, такие как номер и серия паспорта, номера страховых свидетельств, номера водительских удостоверений), и информацию, которая могла бы использоваться для определения местонахождения обладателя ПИИ в реальном масштабе времени.

Обработка чувствительной ПИИ требует применения специальных мер. Во многих странах обработка чувствительной ПИИ может быть запрещена действующим законом, даже если обладатель ПИИ дал согласие на ее обработку. Некоторые страны могут потребовать выполнения определенных мер и средств контроля и управления при обработке определенных типов чувствительной ПИИ (например, требование зашифровать медицинскую ПИИ при передаче ее по общедоступной сети).

4.5 Требования к мерам защиты приватности

Организации заинтересованы защищать ПИИ по разным причинам: чтобы защищать приватность обладателя ПИИ, соответствовать правовым и нормативным требованиям, выполнять обязанности корпорации, повышать доверие клиентов и т. д. Цель 4.5 – дать общее представление о различных факторах, которые могут влиять на требования по защите приватности, являющиеся соответствующими для отдельных организаций или лиц, обрабатывающих ПИИ и заинтересованных в обеспечении приватности.

Требования по защите приватности могут затрагивать многие различные аспекты обработки ПИИ, например, сбор и сохранение ПИИ, передачу ПИИ третьим сторонам, договорные взаимоотношения между операторами ПИИ, обработчиками ПИИ, трансграничная передача ПИИ и т. д. Требования по защите приватности могут также различаться по специфике. Они могут быть общими по характеру, например, состоять из определенного количества высокоуровневых принципов приватности, которые, как ожидается, организация будет принимать во внимание при обработке ПИИ. Однако требования по защите приватности могут также включать очень специфические ограничения на обработку определенных типов ПИИ или предписывать реализацию специфических мер и средств контроля и управления приватностью.

Разработке какой-либо системы ИКТ, включающей обработку ПИИ, должна предшествовать идентификация соответствующих требований по защите приватности. Последствия обеспечения приватности, связанные с новыми или значительно модифицированными системами ИКТ, участвующими в обработке ПИИ, должны быть приняты во внимание (разрешены) до того, как те системы ИКТ будут реализованы. В плановом порядке организации выполняют широкий спектр деятельностей по менеджменту риска и разрабатывают профили риска, относящиеся к их системам ИКТ.

Менеджмент риска определяется как «скоординированные действия по руководству и управлению организацией в отношении риска» (ИСО Руководство 73:2009). Процесс менеджмента риска обеспечения приватности включает следующие процессы:

- установления контекста путем осмысления организации (например, обработка ПИИ, обязанности), технической среды и факторов, влияющих на менеджмент риска обеспечения приватности (т. е. правовые и нормативные факторы, договорные факторы, факторы бизнеса и другие факторы);
- оценки риска путем идентификации, анализа и оценивания рисков для обладателей ПИИ (риски, которые могут повлиять на них неблагоприятным образом);
- обработки риска путем определения требований по защите приватности, идентификации и реализации мер и средств контроля и управления приватностью для предотвращения или уменьшения рисков для обладателей ПИИ;
- коммуникации и консультирование путем получения информации от заинтересованных сторон, достижения согласия по каждому процессу менеджмента риска, а также информирования обладателей ПИИ и сообщения им о рисках и мерах и средствах контроля и управления;
- мониторинга и пересмотра путем отслеживания рисков и мер и средств контроля и управления, а также усовершенствования процесса.

Одним из результатов может быть оценка влияния обеспечения приватности, которая является составной частью менеджмента рисков, направленного на обеспечение соблюдения законодательных требований в части приватности и защиты данных, и оценка последствий обеспечения приватности новых или существенно измененных программ или деятельностей. Оценки влияния обеспечения приватности должны быть оформлены в рамках более широкой структуры менеджмента рисков организации.

Требования к мерам защиты приватности идентифицируются как часть общего процесса менеджмента риска обеспечения приватности, на который оказывают влияние следующие факторы (как показано на рисунке 1 и описано далее):

- правовые и нормативные факторы, направленные на защиту приватности физического лица и защиту его ПИИ;
- договорные факторы, такие как отраслевые нормы, профессиональные стандарты, политики компании;
- факторы бизнеса, предопределенные специфичными бизнес-приложениями или, в отдельных случаях, специфичным контекстом;
- другие факторы, которые могут влиять на проектирование системы ИКТ и связанные с ними требования к мерам защиты приватности.



Рисунок 1 - Факторы, влияющие на менеджмент риска обеспечения приватности

4.5.1 Правовые и нормативные факторы

Требования к мерам защиты приватности часто отражены в (1) международных, национальных и местных законах, (2) постановлениях, (3) судебных решениях или (4) договорных соглашениях с трудовыми советами или другими организациями работников. Некоторые примеры местного и национального законодательства включают законы о защите данных, о защите прав потребителя, законы о предупреждении нарушений, законы о хранении данных и трудовое законодательство. Соответствующие международные законы могут включать правила, затрагивающие трансграничную передачу ПИИ. Операторы ПИИ должны быть осведомлены обо всех соответствующих требованиях к мерам защиты приватности, вытекающих из юридических или нормативных факторов. Для достижения этой цели операторы могут действовать в тесном сотрудничестве с юрисконсультами. В то время как для многих стран ответственность за соблюдение требований, в конечном счете, несет оператор ПИИ, все стороны, участвующие в обработке ПИИ, также должны занять активную позицию в определении соответствующих требований обеспечения приватности, вытекающих из правовых и нормативных факторов.

4.5.2 Договорные факторы

Договорные обязательства также могут влиять на требования к мерам защиты приватности. Эти обязательства могут являться результатом соглашения между несколькими субъектами и соглашений с отдельными субъектами, например, соглашение обработчиков ПИИ, соглашения операторов ПИИ и третьих сторон. Например, лицо, заинтересованное в обеспечении приватности, может потребовать, чтобы третьи стороны использовали определенные меры и средства контроля и управления приватностью и согласовывали требования о распоряжении специфической ПИИ до передачи им ПИИ. Требования к мерам защиты приватности могут также определяться политикой компании и обязательными корпоративными правилами, которые лицо, заинтересованное в обеспечении приватности, определило само для себя, например, для защиты торговой марки от утраты репутации в случае нарушения приватности.

В принципе, любая сторона, имеющая доступ к ПИИ, должна быть официально проинформирована о своих обязательствах соответствующим(и) оператором(ами) ПИИ, например, путем заключения соглашения с третьей стороной. Такие соглашения, вероятно, будут содержать ряд требований к мерам защиты приватности, которые третья сторона (получатель ПИИ) должна принимать во внимание. В некоторых странах национальные и региональные органы могут иметь установленные правовые и договорные документы, делающие возможной передачу ПИИ третьим сторонам.

4.5.3 Факторы бизнеса

На требования к мерам защиты приватности могут также влиять факторы бизнеса, к которым относятся определенные характеристики предполагаемого применения или контекст использования. Факторы бизнеса могут широко варьироваться в зависимости от типа лица, заинтересованного в обеспечении приватности, и вида бизнеса. Например, они могут иметь отношение к сегменту, в котором организация функционирует (например, отраслевые нормы, кодекс поведения, лучшие практики, стандарты) или к характеру ее модели бизнеса (например, онлайновые сервисы в непрерывном режиме, сервисы совместного использования информации, банковские приложения).

Многие факторы бизнеса, как таковые, не оказывают непосредственного влияния на требования к мерам защиты приватности. Предусматриваемое использование ПИИ, вероятно, будет влиять на

реализацию организацией политик обеспечения приватности, а также на выбор мер и средств контроля и управления приватностью, но это не должно влиять на принципы приватности, которые приняты в организации. Например, предложение определенного сервиса может потребовать, чтобы поставщик сервисов собирал дополнительную ПИИ или позволял большинству своих сотрудников осуществлять доступ к определенным видам ПИИ. Однако это не означает, что оператор ПИИ, который обязался соблюдать содержащиеся в этой структуре принципы, больше не должен тщательно оценивать, какие виды ПИИ точно необходимы для предоставления сервиса (принцип ограничения сбора), и не должен ограничивать доступ к ПИИ тем своим служащим, которым это необходимо для выполнения своих обязанностей (принцип обеспечения информационной безопасности).

4.5.4 Другие факторы

Наиболее важный фактор, который должны учитывать организации при идентификации требований к мерам защиты приватности, связан с предпочтениями обладателей ПИИ в сфере приватности. Персональная позиция физического лица по отношению к приватности и что оно вкладывает в понятие «риски», может зависеть от ряда факторов, включающих: понимание физическим лицом используемой технологии, их происхождение, предоставляемую информацию, назначение транзакций, приобретенный опыт, а также социально-психологические факторы.

Проектировщики системы ИКТ должны попытаться понять вероятные проблемы обеспечения приватности обладателей ПИИ и типы ПИИ, которая будет обрабатываться с помощью их системы. И они, так же как разработчик систем или приложения, или поставщик услуг изучают целевую аудиторию клиентов, нуждающихся в обеспечении приватности, для того чтобы понять их ожидания и предпочтения относительно обеспечения приватности. Проектировщики систем ИКТ не всегда могут предоставить обладателю ПИИ выбор, который бы соответствовал их предпочтению по обеспечению приватности.

Примеры предпочтений приватности могут включать предпочтение анонимности или назначения псевдонимов, возможность ограничения доступа к конкретной ПИИ или возможность ограничения цели обработки ПИИ. До определенной степени обладателю ПИИ предоставляется выбор предпочтения обработки его данных, например, использовать ли ПИИ во вторичных целях, таких как маркетинг. Способность выразить предпочтения, не влияющие неблагоприятным образом на приватность, могут быть реализованы с помощью графического интерфейса пользователя системы ИКТ. Это может помочь обладателю ПИИ сделать выбор, представив набор предопределенных вариантов общих предпочтений в части приватности с использованием легко понимаемого языка. Реализация пользовательского интерфейса может быть основана на таких элементах, как поля выбора и выпадающее меню.

В дополнение к факторам, перечисленным в предыдущих пунктах, существуют и другие факторы, которые могут влиять на проектирование систем ИКТ и связанные с ними требования к мерам защиты приватности. Например, на требования к мерам защиты приватности могут влиять системы внутреннего контроля или технические стандарты, принятые организацией (например, такой рекомендуемый стандарт как стандарт ИСО).

4.6 Политики приватности

Высшее руководство организации, участвующее в обработке ПИИ, призвано создать политику приватности. Политика приватности должна:

- соответствовать назначению организации;
- предоставлять структуру для установления целей;
- включать обязательство соответствовать применимым требованиям к мерам защиты приватности;
- включать обязательство в части непрерывного совершенствования;
- быть озвучена в пределах организации;
- быть доступной, при необходимости, заинтересованным сторонам.

Организация должна оформлять свою политику приватности в письменной форме. Если организация, обрабатывающая ПИИ, является обработчиком ПИИ, то эти политики могут в значительной степени определяться оператором ПИИ. Политика приватности должна быть дополнена более детализированными правилами и обязательствами различных лиц, заинтересованных в обеспечении приватности, участвующих в обработке ПИИ (например, процедуры для конкретных ведомств или сотрудников). Кроме того, меры и средства контроля и управления, которые используются для проведения в жизнь политики приватности в конкретных условиях (например, контроль доступа, обеспечение уведомлений, аудиты и т. д.), должны документироваться четким образом.

Термин «политика приватности» часто используется для упоминания как о внутренних, так и о внешних политиках приватности. Внутренняя политика приватности документирует цели, правила,

обязательства, ограничения и (или) формирование мер и средств контроля и управления, которые адаптированы организацией к удовлетворению требований к мерам защиты приватности, являющимся важными для обработки ПИИ. Внешние политики приватности предоставляются внешним поставщикам организации с уведомлениями о практиках организации приватности, а также о другой важной информации, как например, идентификационные данные и официальный адрес оператора ПИИ, точки контакта, откуда обладатели ПИИ могли бы получать дополнительную информацию и т. д. В контексте такой структуры термин «политика приватности» используется для ссылки на внутреннюю политику приватности организации. На внешнюю политику приватности ссылаются как на уведомления.

4.7 Меры и средства контроля и управления приватностью

Организации должны идентифицировать и реализовывать меры и средства контроля и управления приватностью, чтобы соответствовать требованиям к мерам защиты приватности, определенным оценкой риска обеспечения приватности и процессом обработки. Кроме того, идентифицированные и реализованные меры и средства контроля и управления приватностью должны быть документально оформлены как часть оценки риска обеспечения приватности организации. Определенные виды обработки ПИИ, возможно, потребуют применения специальных мер и средств контроля и управления, потребность в которых станет очевидной, как только намеченные действия будут тщательно проанализированы. Оценка риска приватности может оказать помощь организациям в идентификации специфических рисков нарушений приватности, включающих рассматриваемую обработку.

Организация должна приложить усилия, чтобы разработать собственные меры и средства контроля и управления приватностью как часть общего подхода «обеспечения приватности при проектировании», т. е. соблюдение приватности должно приниматься в расчет на стадии проектирования систем, обрабатывающих ПИИ, а не сдвигаться на последующий этап.

Поскольку затрагиваются меры и средства контроля и управления информационной безопасностью, важно отметить, что не вся обработка ПИИ требует одного и того же уровня или типа защиты. Организации должны различать операции по обработке ПИИ в соответствии с их специфическими рисками, чтобы помочь определению того, какие меры и средства контроля и управления информационной безопасностью в каких случаях являются соответствующими. Менеджмент риска может рассматриваться как основной метод этого процесса, а идентификация мер и средств контроля и управления приватностью также должна являться неотъемлемой частью структуры менеджмента информационной безопасности организации.

5 Принципы обеспечения приватности ИСО/МЭК 29100

5.1 Общий обзор принципов обеспечения приватности

Описанные в данном стандарте принципы обеспечения приватности выведены из существующих принципов, разработанных рядом государств, стран и международных организаций. Эта структура направлена на реализацию принципов приватности в системах ИКТ и на разработку систем менеджмента приватности, которые должны быть реализованы в рамках систем ИКТ организации. Эти принципы приватности должны использоваться для руководства проектированием, разработкой и реализацией политик приватности и мер и средств контроля и управления приватностью. Кроме того, они могут быть использованы в качестве основы при мониторинге и измерении эффективности, а также сравнительного анализа и аудита аспектов программы менеджмента приватности в организации.

Несмотря на различия в социальных, культурных, правовых и экономических факторах, которые могут ограничивать применение этих принципов в одном и том же контексте, рекомендуется применение любых принципов, изложенных в настоящем стандарте. Любые исключения из этих принципов должны быть ограничены.

Основу настоящего стандарта формируют следующие принципы обеспечения приватности, приведенные в таблице 3.

Таблица 3 - Принципы обеспечения приватности ИСО/МЭК 29100

Принципы обеспечения приватности
1. Согласие и выбор
2. Законность цели и ее спецификация
3. Ограничение на сбор информации
4. Минимизация данных
5. Ограничения в отношении использования, хранения и раскрытия
6. Точность и качество
7. Открытость, прозрачность и уведомление
8. Индивидуальное участие и доступ
9. Ответственность
10 Информационная безопасность
11. Соответствие обеспечения приватности

5.2 Согласие и выбор

Соблюдение принципа согласия означает:

- предоставление обладателю ПИИ выбора между разрешением или недопущением обработки его ПИИ за исключением случаев, когда обладатель ПИИ не может прямо дать согласие или когда соответствующий закон разрешает проведение обработки ПИИ без согласия физического лица. Выбор обладателем ПИИ должен быть сделан свободно и основан на знаниях;
- получение согласия на обработку от обладателя ПИИ для сбора или иной обработки чувствительной ПИИ, за исключением случаев, когда соответствующий закон разрешает обработку чувствительной ПИИ без согласия физического лица;
- информирование обладателя ПИИ (до получения его согласия) о его правах в соответствии с принципом индивидуального участия и доступа;
- предоставление обладателю ПИИ (до получения его согласия) информации, обозначенной принципами открытости, прозрачности и уведомления;
- объяснение обладателю ПИИ последствий предоставления или отказа от согласия.

Необходимо предоставить обладателю ПИИ возможность выбора того, каким образом его ПИИ будет обрабатываться, и разрешить ему отозвать согласие без затруднений и бесплатно. Этот запрос должен рассматриваться в соответствии с политикой приватности. Даже если согласие будет отозвано, оператор ПИИ может потребовать сохранения определенной ПИИ на период времени, необходимый для выполнения правовых или договорных обязательств (например, сохранение данных, ответственность). В случае, когда обработка ПИИ базируется не на согласии, а на другой правовой основе, обладатель ПИИ должен быть уведомлен при любых обстоятельствах. В тех случаях, когда обладатель ПИИ имеет возможность отзыва согласия, но не решается так поступить, эта ПИИ должна быть освобождена от обработки для какой-либо незаконной цели.

Для оператора ПИИ соблюдение принципа выбора означает:

- предоставление обладателю ПИИ четких, известных, доступных, легко понимаемых, по умеренной стоимости механизмов осуществления выбора и предоставления согласия относительно использования и обработки его ПИИ во время сбора, первоначального использования или после, когда это будет целесообразно;
- осуществление предпочтений обладателя ПИИ, которые выражены в его согласии.

Кроме того, соответствующий закон может определить дополнительные условия в отношении согласия, и другие основания для обработки ПИИ, кроме согласия (например, выполнение условий контракта, жизненные интересы обладателя ПИИ или соблюдение закона). Применимый закон в некоторых случаях предусматривает, что согласие обладателя ПИИ не является достаточным юридическим основанием для обработки ПИИ (например, согласие подростка, данное без одобрения родителей или опекуна). Кроме того, следует учитывать дополнительные требования при передаче ПИИ между различными государствами. Ответственность оператора ПИИ заключается в выполнении этих дополнительных условий до обработки и передачи данных.

5.3 Законность цели и ее описание

Соблюдение принципа законности цели и её описания означает:

- обеспечение уверенности в том, что цель (цели) исполняются в соответствии с законом и основываются на других правовых обязательствах;

- информирование обладателя ПИИ о цели (целях) в период, предшествующий сбору информации или ее использованию впервые для реализации новой цели;
- использование для описания цели таких формулировок, которые четко и соответствующим образом адаптированы к специфике реализации цели;
- разъяснение необходимости обработки чувствительной ПИИ, если существует потребность в таком разъяснении.

В отношении чувствительной ПИИ могут применяться более строгие правила, касающиеся цели обработки. Для соблюдения законности цели может потребоваться правовое основание или специальное разрешение службы защиты данных или правительственных структур. Обработка не должна осуществляться, если цели обработки ПИИ не соответствуют применимому закону.

5.4 Ограничение на сбор

Соблюдение принципа ограничения на сбор означает:

- ограничение сбора ПИИ до такой степени, которая определяется рамками применяемого закона и строго необходимой целью (целями).

Организации не должны собирать личную информацию хаотично. Количество и тип собранной информации должны быть ограничены до такой степени, которая является необходимой для осуществления (в рамках закона) реализации цели (целей), точно определенных оператором ПИИ. Организации, прежде чем приступить к сбору ПИИ, должны тщательно рассмотреть ту ПИИ, которая может быть затребована для осуществления особой цели. Организации должны документировать типы накопленной ПИИ, а также ее правомерность для выполнения деятельности, являющейся частью их политик и практик по обработке информации.

Оператор ПИИ может выразить желание собрать дополнительную ПИИ с иной целью, чем предоставление специфической услуги, требуемой обладателю ПИИ (например, в целях прямого маркетинга). В зависимости от полномочий такая дополнительная информация может быть собрана только при согласии обладателя ПИИ. Возможно также, что сбор определенной информации будет разрешен с помощью соответствующего закона. Когда это допустимо, обладателю ПИИ должна быть дана возможность выбора: предоставлять или не предоставлять такую информацию. Обладатель ПИИ также должен быть четко осведомлен о том обстоятельстве, что его ответные действия на такие запросы о дополнительной информации не являются обязательными.

5.5 Минимизация данных

Минимизация данных тесно связана с принципом «ограничение на сбор», но является более широким понятием. В то время как «ограничение на сбор» связано со сбором ограниченных данных по отношению к указанной цели, «минимизация данных» строго минимизирует обработку ПИИ.

Соблюдение принципа минимизации данных означает разработку и реализацию процедур по обработке данных и систем ИКТ такими способами как:

- сведение к минимуму обрабатываемой ПИИ и числа лиц, заинтересованных в обеспечении приватности, а также лиц, которые осведомлены о ПИИ или имеют к ней доступ;
- обеспечение принятия принципа «необходимого знания», т.е. некоему лицу доступ должен предоставляться только к ПИИ, необходимой для выполнения его обязанностей в рамках законной цели обработки ПИИ;
- использование или предложение использования (в качестве опции по умолчанию, по возможности) взаимодействий и транзакций, не использующих идентификацию обладателей ПИИ, и приводящих к снижению наблюдаемости их поведения, и ограничению взаимосвязанности собираемой ПИИ;
- удаление и ликвидация ПИИ всякий раз, когда истекает срок действия цели обработки ПИИ, отсутствуют какие-либо правовые требования, касающиеся хранения ПИИ или когда это целесообразно сделать.

5.6 Ограничения в отношении использования, хранения и раскрытия

Соблюдение принципа ограничения в отношении использования, хранения и раскрытия означает:

- ограничение использования, хранения и раскрытия (включая передачу) ПИИ, которая необходима, чтобы выполнять специфические, определенные и законные цели;
- ограничение использования ПИИ для целей, определенных оператором ПИИ до сбора информации, за исключением особой цели, прямо определенной законом;
- хранение ПИИ в течение такого промежутка времени, который необходим для выполнения заявленных целей, и последующее безопасное уничтожение или обезличивание ПИИ;
- блокирование (т. е. архивирование, обеспечение безопасности и исключение дальнейшей обработки) любой ПИИ, когда заявленные цели достигнуты, но применимый закон требует обеспечения хранения.

Когда осуществляется трансграничная передача ПИИ, оператор ПИИ должен быть осведомлен обо всех дополнительных международных или региональных требованиях, специфичных для международных пересылок.

5.7 Точность и качество

Соблюдение принципа точности и качества означает:

- обеспечение уверенности в том, что обрабатываемая ПИИ является правильной, полной, обновляемой (за исключением случаев, когда имеется законное основание для хранения данных, утративших свою актуальность), адекватной и значимой для цели использования;
- обеспечение уверенности в достоверности ПИИ, полученной от источника, не являющегося обладателем ПИИ, до её обработки;
- подтверждение соответствующими способами юридической силы и корректности претензий от обладателя ПИИ до выполнения любых изменений в ПИИ (чтобы обеспечить уверенность в том, что изменения санкционированы должным образом) там, где это необходимо выполнить;
- установление процедур сбора ПИИ в целях обеспечения точности и качества;
- установление механизмов управления, обеспечивающих периодическую проверку точности и качества собранной и сохраненной ПИИ.

Этот принцип особенно важен в тех случаях, когда данные могут использоваться для предоставления или отказа в праве на получение материальной выгоды для физического лица, или когда неточные данные при других обстоятельствах могут привести к существенному ущербу для физического лица.

5.8 Открытость, прозрачность и уведомление

Соблюдение принципа открытости, прозрачности и уведомления означает:

- предоставление обладателям ПИИ четкой и легкодоступной информации о политиках, процедурах и практических приемах операторов ПИИ, относящихся к обработке ПИИ;
- включение в уведомления факта обработки ПИИ; цели, для которой осуществляется обработка; типов лиц, заинтересованных в обеспечении приватности, которым может быть раскрыта ПИИ, и идентификационных данных оператора ПИИ, включая контактную информацию оператора ПИИ;
- раскрытие вариантов выбора и средств, предлагаемых оператором ПИИ, обладателю ПИИ для целей ограничения использования информации, а также для доступа, корректировки и пересылки его информации;
- уведомление обладателей ПИИ о существенных изменениях в процедурах, выполняемых при обращении с ПИИ.

Может потребоваться обеспечение прозрачности общей информации, логически лежащей в основе обработки ПИИ, особенно если от результатов обработки зависит решение, влияющее на обладателя ПИИ. Лица, заинтересованные в обеспечении приватности, участвующие в обработке ПИИ, должны владеть определенной информацией о своих политиках и практиках, относящихся к менеджменту ПИИ, которая легкодоступна для общественного пользования. Все договорные обязательства, которые влияют на обработку ПИИ, должны быть документированы и утверждены в организации соответствующим образом. О них должно быть также известно за пределами организации до той степени, когда эти обязательства не будут являться конфиденциальными.

Кроме того, цель обработки ПИИ должна быть достаточно детализирована, чтобы дать возможность обладателю ПИИ понять:

- определенную ПИИ, требующуюся для конкретной цели;
- определенную цель для сбора ПИИ;
- определенную обработку (включая механизмы сбора, передачи и хранения);
- типы уполномоченных физических лиц, кто будет осуществлять доступ к ПИИ и кому ПИИ может передаваться;
- определенные требования к сохранению и удалению данных ПИИ.

5.9 Индивидуальное участие и доступ

Соблюдение принципа индивидуального участия и доступа означает:

- предоставление обладателям ПИИ возможности доступа к ПИИ и возможности проверки их ПИИ при условии, что их идентификационные данные сначала аутентифицируются с соответствующим уровнем обеспечения уверенности и такой доступ не запрещен действующим законом;
- наличие у обладателей ПИИ возможности оспорить точность и полноту ПИИ и добиться внесения в нее поправок, исправлений или ее удаления;

- обеспечение возможности внесения любых поправок, исправлений или удаления для обработчиков ПИИ и третьих сторон, которым были раскрыты персональные данные, где они известны;
- установление процедур, позволяющих обладателям ПИИ осуществить эти права простым, быстрым и эффективным способом, который не влечет за собой неуместное промедление или неоправданные затраты.

Оператор ПИИ должен применять соответствующие меры и средства контроля и управления для обеспечения уверенности в том, что обладателям ПИИ доступна строго их собственная ПИИ, а не та, которая доступна другим обладателям ПИИ, за исключением случаев, когда физическое лицо, осуществляющее доступ, действует в рамках полномочий от лица обладателя ПИИ, который неспособен осуществлять свои права доступа. Применимый закон может предоставить физическому лицу право доступа, просмотра и, в определенных случаях, отказа от обработки ПИИ. Если физическое лицо не удовлетворено решением проблемы, то содержание неразрешенной проблемы должно быть зарегистрировано организацией. При необходимости, о существовании неразрешенной проблемы должны быть оповещены третьи стороны, имеющие доступ к рассматриваемой информации.

5.10 Ответственность

Обработка ПИИ влечет за собой обязанность соблюдения осторожности и применения конкретных и целесообразных мер для обеспечения ее защиты. Соблюдение принципа ответственности означает:

- документирование и сообщение обо всех политиках, процедурах и методах, связанных с обеспечением приватности;
- назначение в пределах организации конкретного лица (которое может, в свою очередь, передать полномочия другим) ответственным за осуществление процедур и методов, связанных с политикой обеспечения приватности;
- при передаче ПИИ третьим сторонам обеспечение уверенности в том, что получатель третьей стороны будет обязан обеспечивать равноценный уровень защиты приватности через договорные или другие средства, такие как обязательные внутренние политики (соответствующий закон может содержать дополнительные требования, касающиеся передачи данных в международных масштабах);
- обеспечение соответствующего обучения сотрудников оператора ПИИ, которым будет предоставляться доступ к ПИИ;
- установление эффективных внутренних процедур обработки претензий и возмещения ущерба для их применения обладателями ПИИ;
- информирование обладателей ПИИ о нарушениях приватности, которые могут нанести им существенный ущерб (если это не запрещено, например, при работе, связанной с применением закона), а также о мерах, принятых для устранения этих нарушений;
- уведомление всех лиц, заинтересованных в обеспечении приватности, о нарушениях приватности, как это требуется в некоторых странах (например, службами защиты данных) и в зависимости от уровня риска;
- предоставление доступа пострадавшему обладателю ПИИ к соответствующим и эффективным санкциям и (или) механизмам, таким как исправление, исключение или восстановление, если произошло нарушение приватности;
- рассмотрение процедур для компенсаций в ситуациях, в которых будет трудно или невозможно вернуть приватный статус физического лица в исходное состояние.

Меры, принимаемые для устранения нарушения безопасности, должны быть пропорциональны рискам, связанным с нарушением, но их реализация должна быть неотложной (за исключением ситуаций, когда это запрещено, например, в процессе расследования правонарушения).

Создание процедур возмещения ущерба является важной частью установления ответственности. Возмещение ущерба предоставляет обладателю ПИИ возможность сохранения ответственности оператора ПИИ за ненадлежащее использование ПИИ. Реституция – это форма возмещения, которая предполагает компенсацию пострадавшему обладателю ПИИ. Это важно не только в ситуации кражи идентификационной информации («кражи личности»), вреда репутации или ненадлежащего использования ПИИ, но также и в случае ошибок в модификации или изменении соответствующей ПИИ.

В случае наличия процессов возмещения ущерба обладатели ПИИ более уверенно идут на соглашение, так как принятый риск для физического лица в отношении результата в этом случае снижен. В отношении некоторых услуг возмещение легче определить (например, при финансовой потере), чем для других (например, кража идентификационной информации, ущерб для имиджа или репутации физического лица), в которых трудно определить размер ущерба и предоставить

компенсацию. Возмещение осуществляется лучше всего, когда оно основано на прозрачности и честности. Необходимыми типами мер по возмещению можно управлять согласно закону.

5.11 Информационная безопасность

Соблюдение принципа обеспечения информационной безопасности означает:

- защиту ПИИ в рамках его полномочий соответствующими мерами и средствами контроля и управления на эксплуатационном, функциональном и стратегическом уровне для обеспечения её целостности, конфиденциальности и доступности, а также защиту от рисков, таких как несанкционированный доступ, разрушение, использование, модификация или раскрытие либо потеря в течение всего ее жизненного цикла;
- выбор обработчиков ПИИ, которые предоставляют достаточные гарантии относительно как организационных, физических и технических мер и средств контроля и управления при обработке ПИИ, так и обеспечения соответствия этим мерам и средствам контроля и управления;
- базирование этих мер и средств контроля и управления на требованиях соответствующего законодательства, стандартов безопасности, результатах систематических оценок рисков безопасности, как описано в ИСО 31000, и результатах анализа «затраты/выгода»;
- реализацию мер и средств контроля и управления соразмерно вероятности и серьезности потенциальных последствий, чувствительности ПИИ, числу обладателей ПИИ, которые могут быть затронуты, и контекста, в котором она производится;
- ограничение доступа к ПИИ для тех лиц, кому такой доступ требуется для выполнения своих обязанностей, и ограничение доступа тех лиц, которые имеют доступ только к той ПИИ, доступ к которой им требуется для выполнения своих обязанностей;
- принятие решений относительно рисков и уязвимостей, обнаруженных с помощью оценок риска обеспечения приватности и процессов аудита;
- периодический пересмотр и переоценка мер и средств контроля и управления в процессе постоянного менеджмента рисков безопасности.

5.12 Соответствие приватности

Соблюдение принципа соответствия приватности означает:

- проверку и демонстрирование того, что обработка удовлетворяет требованиям защиты данных и сохранения приватности путем периодического проведения аудитов с использованием внутренних аудиторов или аудиторов доверенной третьей стороны;
- применение соответствующих внутренних мер и средств контроля и управления и механизмов независимого наблюдения, которые обеспечивают уверенность в соответствии применимому закону о приватности, политикам и процедурам обеспечения безопасности, защиты данных и обеспечения приватности;
- разработку и поддержку оценок риска приватности для оценивания того, соответствуют ли инициативы по поставке программы или сервиса, включающие обработку ПИИ, требованиям защиты данных и обеспечения приватности.

Применимый закон может требовать, чтобы один или более наблюдательных органов был ответственным за мониторинг соответствия действующему закону о защите данных. В этих случаях поддержание принципа соответствия приватности также означает сотрудничество с наблюдательными органами и соблюдение их руководящих принципов и требований.

Приложение А
(информационное)

Соответствие между понятиями ИСО/МЭК 29100 и понятиями ИСО/МЭК 27000

Для упрощения использования семейства международных стандартов ИСО/МЭК 27000 в специфическом контексте обеспечения приватности и интеграции понятий обеспечения приватности в контексте ИСО/МЭК 27000 в таблице А.1 представлены взаимосвязи между основными понятиями ИСО/МЭК 29100 и ИСО/МЭК 27000.

Таблица А.1 – Сопоставление понятий ИСО/МЭК 29100 и понятий ИСО/МЭК 27000

Понятия ИСО/МЭК 29100	Соответствие с понятиями ИСО/МЭК 27000
Лицо, заинтересованное в обеспечении приватности	Причастная сторона
ПИИ	Информационный актив
Нарушение приватности	Инцидент информационной безопасности
Мера и средство контроля и управления приватностью	Мера и средство контроля и управления
Риск обеспечения приватности	Риск
Менеджмент риска обеспечения приватности	Менеджмент риска
Требования к мерам защиты приватности	Цели применения мер и средств контроля и управления

Библиография

[1] ИСО Руководство 73, *Управление рисками — Словарь*

[2] ИСО 31000, *Управление рисками — Принципы и руководства*

[3] ИСО/МЭК СТК 1/ПК 27 РГ 5 Основополагающий документ 2 (РГ 5 ОД2) – *ссылки на официальные конфиденциальные документы*, доступные на сайте gost.e-ecolog.ru

УДК: 658:562.014:006.354 ОКС: 35.040

Ключевые слова: Управление рисками, обеспечение приватности

Подписано в печать 01.10.2014. Формат 60x84 1/8.

Усл. печ. л. 2,79. Тираж 40 экз. Зак. 3594.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

ФГУП «СТАНДАРТИНФОРМ»

123995 Москва, Гранатный пер., 4.

www.gostinfo.ru gost.e-ecolog.ru

gost.e-ecolog.ru