GLOSSARY

Category [Категория] — A general concept for describing and grouping certain types of information. In the context of Perimetrix SafeSpace, a category is a specific point along a given *dimension*. Each dimension can contain several categories. To simplify the process of *classification* and defining access rights, the categories are organized in a tree-like structure. For example, the "Confidentiality" dimension may contain the categories "Top secret", "Secret", and "For internal use only", while the "Department" dimension may contain the categories "HR", "Finance", "R&D", "Sales", and "Legal".

RU Объяснительная модель, используемая в Perimetrix SafeSpace для выделения сутевого подмножества информационных объектов в рамках одного *измерения*. Категории применяются для упрощения процесса *классификации* и определения прав доступа. Каждое *измерение* может содержать неограниченное число категорий, которые организованы в древовидную структуру. Например, измерение «Конфиденциальность» может содержать категории «Совершенно секретно», «Секретно» и «ДСП», а измерение «Отдел» может содержать категории «Кадры», «Финансы», «НИиОКР», «Продажи» «Юридический отдел».

Certificate Authority *or* **Certification Authority [Удостоверяющий центр]** — A trusted entity that issues digital certificates.

RU Корневой центр сертификации, отвечающий за выдачу цифровых сертификатов.

Certificate Owner [Владельцы сертификатов] — In the context of SafeSpace, any service that has a digital certificate assigned.

RU Сервисы SafeSpace, к которым привязан цифровой сертификат.

Classification (Data Classification) [Классификация] — A systematic arrangement of objects into groups or *categories* based on established criteria. In the context of SafeSpace, this is the process by which a *level of confidentiality* is assigned to an object.

RU Процесс отнесения информационных объектов к определенным *категориям* в соответствии с некоторыми формализованными критериями. В нотации SafeSpace классификация предполагает присвоение *уровня конфиденциальности (уровня)* любому информационному объекту, находящемуся под защитой системы.

Classification Tag [Метка конфиденциальности] — In the context of SafeSpace, an element of information attached to a data object that characterizes the confidentiality of information contained in that object.

RU Метка, прикрепленная к классифицированному объекту, характеризующая конфиденциальность содержащейся в нем информации.

Classified [Классифицированный] — Describes a data object (file, data, etc.) that has received a *classification tag*.

RU Состояние информационного объекта, отнесенного к определенной *категории* и имеющего (получившего) определённый *уровень* конфиденциальности, с присвоением *метки конфиденциальности*.

Confidential [Конфиденциальный] — Often used in business to describe information (such as trade secrets, personal data, etc.) that should not be shared with those not having appropriate authorization.

RU Обобщенное определение любой информации, содержащей закрытые сведения, имеющие ограниченное обращение и/или доступ (например, информации содержащей коммерческую тайну, персональные данные и т.п.).

Confidentiality [Конфиденциальность] — A mandatory requirement that a person who has access to certain information must not transfer such information to others without the consent of its owner. Transferring information without the approval of its owner is considered "a leak".

RU Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не переда-

вать такую информацию третьим лицам без согласия ее владельца. Нарушением конфиденциальности является «утечка данных».

Configuration [Конфигурация] — A snapshot of the SafeSpace configuration parameters. Each parameter is treated as a single data block. For SafeSpace to work correctly, it must always have an applied (effective) configuration which defines how classified data is handled. How confidential data can be handled is based on corporate security policies.

RU Последовательность цифровых слепков параметров настройки системы, каждый из которых рассматривается в виде единого блока данных. Для правильной работы SafeSpace всегда должна быть применена эффективная конфигурация, которая на основе политик безопасности определяет, как обрабатываются защищённые данные.

Container [Контейнер] — One of the elements of the *Universal Event Model (UEM)* that defines the location of an information object in order to analyze its movement.

RU Один из элементов *универсальной модели событий* Perimetrix, который определяет местоположение информационного объекта для анализа его *перемещения*.

Cryptex [Криптекс] — See *cryptographic container*.

RU См. *криптографический архив*.

Cryptex Manager [Криптекс-менеджер] — A SafeSpace tool that is used for creating Cryptex (cryptographic *containers*).

RU Средство SafeSpace для создания криптографического *контейнера*.

Cryptographic Container [Криптографический архив]— An encrypted archive that may contain both classified and non-classified information. Cryptographic containers (Cryptex) can be used to store data in an unsecured environment and/or transmit it over unsecured channels. Any environment that is not protected by the SafeUse agent is unsecure. Therefore, storing classified data in such an environment requires protection through encryption.

RU Зашифрованный архив, который может содержать как *классифицированную*, так и *неклассифицированную* информацию. Может использоваться для хранения данных в незащищённой среде и/или передачи по недоверенным каналам связи. Любая среда, не защищаемая *драйвером*, является для Perimetrix недоверенной. Для хранения классифицированных данных в такой среде требуется защита средствами криптографии.

Cryptography Parameters [Параметры криптографии] — The parameters that the SafeSpace system uses to encrypt data when files are saved in a Cryptex.

RU Параметры, которые использует SafeSpace для шифрования данных при сохранении файлов в *криптографическом архиве*.

Data Centric Security Model, DCSM [Информационно-центричная модель безопасности] — An approach to security that emphasizes the dependability of the data itself rather than the security of networks, servers, or applications. Data-centric security also allows organizations to overcome the disconnect between IT security technologies and the objectives of business strategy by relating security services directly to the data they implicitly protect. ➔ Please refer to perimetrix.com for more highlights on DCSM.

RU Модель безопасности с акцентом на необходимости непрерывной *классификации* данных для их корректного отнесения к сведениям, содержащим тайну той или иной *категории, и принятия исходя из этого надлежащих мер по их защите*. Такая модель, ориентированная на данные, а не на ИТ-инфраструктуру, позволяет увязать информационную безопасность и цели бизнеса. ➔ См. подробнее раздел DCSM на сайте perimetrix.com.

Data Governance [Модель корпоративного управления данными] — A data management concept that concerns the ability of an organization to ensure that it maintains a very high level of data quality throughout the data's lifecycle. Moreover, controls are implemented that ensure the data supports business objectives. Data governance focuses on availability, usability, consistency, integrity and security.

RU Один из концептов управления данными, подразумевающий способность компании гарантировать высокий уровень качества корпоративных данных на всем протяжении их жизненного цикла. Каждый этап такого управления подразумевает наличие измеряемых метрик, гарантирующих эффективность поддержки бизнеса. Фокус при этом делается на доступности, непротиворечивости, целостности и безопасности самих данных.

Data Governance Policies [Политики управления данными] — Policies which apply to an organization's people, processes, and technology. Data governance policies are designed to ensure the consistent and proper handling of data within the organization. In effect, data governance policies determine what can be done with data, who can do it, when they can do it, with what they can do it, and under which circumstances they can do it.

RU Политики, применяемые в организации к сотрудникам, процессам и технологиям и определяющие варианты оптимальных действий, их исполнителей, время, возможности и обстоятельства исполнения.

Data Management Model [Модель управления данными]— A model defining the customer-specific requirements in terms of data classification, storage locations, permitted applications, authorized users, etc.

RU Модель, определяющая специфические требования заказчика с точки зрения классификации данных, мест хранения, разрешённых приложений, авторизованных пользователей и т. д.

Data Movement [Перемещение данных] — In the context of SafeSpace, the transfer of data from one location (source container) to another location (destination container). During any given operation, data may be transferred between two or more different containers.

RU В нотации SafeSpace любая манипуляция с данными трактуется как перемещение данных из «источника» (контейнер-источник) к «получателю» (контейнер-получатель). При перемещении могут быть задействованы сразу несколько *контейнеров*.

DataSure [DataSure] — An auxiliary software component of the SafeSpace solution for recognizing unclassified data. It is based on content filtering technology and supports technologies of morphological analysis, semantic analysis, and analysis based on digital fingerprints. Designed to automate the process of initial classification of data.

RU Вспомогательный программный компонент Perimetrix SafeSpace. Основан на технологии контентной фильтрации и поддерживает технологии цифровых отпечатков. Предназначен для автоматизации процесса первоначальной классификации данных в местах хранения.

Declassified [Деклассификация] — An object that has had its *classification* removed and is no longer required to be kept confidential (i.e., the information has little to no sensitivity and can be made public).

RU Процесс снятия *уровня* классификации с документа, который более не содержит сведений, составляющих ту или иную категорию тайны, и в дальнейшем может стать публичным, выведенным из защищенного оборота.

Digital Certificate [Цифровой сертификат] — A digital certificate that confirms the ownership of a public key by the subject named on the certificate.

RU Электронный документ, который удостоверяет право собственности его владельца на открытый ключ .

Digital Fingerprint [Цифровые отпечатки] — The elements of a file that help to identify whether it contains potentially confidential information (the number of and occurrences of key words in a document, etc.).

RU Технология цифровых отпечатков, обеспечивающая классификацию на основании анализа сходства документов и/или их частей.

Digital Fingerprint Level [Уровень цифрового отпечатка] — A classification level that is assigned to an object based on the existing classification of reference objects. If the analyzed object is similar to the referenced documents, it will be automatically assigned the corresponding *classification level*.

RU Определённый уровень, присваиваемый анализируемому объекту по аналогии с документами, уровень классификации которых уже известен, в этом случае объекту автоматически будет присвоен соответствующий *уровень конфиденциальности*.

Digital Fingerprinting [Снятие цифровых отпечатков] — The process of searching for and calculating digital fingerprints using location and mask information which are defined in the digital fingerprinting parameters. The parameters are based on reference data (e.g., sample documents), whose classification level was determined based on an expert assessment.

RU Процесс поиска и вычисления цифровых отпечатков в файлах с использованием информации о местоположении документа, на основе референсных экспертных образцов (примеров документов, содержащих искомые сведения).

Dimension [Измерение] — An axis containing at least two hierarchically related *categories* which are used to classify data. Defining two or more dimensions for data classification is called a *multidimensional* matrix and provides more exact classifications and greater flexibility when assigning permissions to confidential data. . For example, combing the dimensions "confidentiality" and "line of business" produces a simple yet powerful two-dimensional matrix.

RU Объяснительная модель для набора из двух и более *категорий*. С помощью нескольких измерений можно создавать *многомерные* модели классификации — для более точного отнесения информации к сведениям того или иного уровня секретности и управления доступом. Например, используя измерения «чувствительность данных» и «функциональность можно получить простейшую двухмерную модель классификации.

Event [Событие] — A user action that was intercepted by the SafeSpace system. The term intercepted does not suggest that the event was blocked but that it was identified as *movement* from one container to another. The action will be allowed or disallowed depending on the security policies defined in the system and the classification of the data.

RU Действие пользователя, перехваченное системой SafeSpace. Термин «перехваченный» не означает, что событие было заблокировано, а значит, что оно было идентифицировано как *перемещение* из одного контейнера в другой. Действие будет разрешено или запрещено в зависимости от конфигурации системы и классификации данных.

Event Category [Категория события] — A classification *tag* assigned to an event.

RU *Метка* классификации, присвоенная событию.

Inventory [Инвентаризация] — A centralized procedure for detecting files on protected workstations, analyzing detected files to determine their classification levels and, if necessary, adjust existing levels.

RU Централизованная процедура поиска файлов в местах хранения, анализ их содержимого и классификация на основе содержащихся в них сведений.

Level of Confidentiality (Classification Level) [Уровень конфиденциальности] — A combination of categories from all dimensions. In the process of analyzing an information object, it can be assigned various classification levels. For elements in the Universal Event Model to gain access to a classified object, they must have appropriate permissions. These permissions are determined by the acceptable level of the Universal Event Model element. The current level can include only one category from each dimension, the so-called point level. While acceptable levels can include several categories from the same dimension, in this case they are called multi-level.

RU Набор *категорий* классифицированного объекта, который может меняться в процессе жизненного цикла. Для получения доступа к классифицированному объекту в *универсальной модели событий* у процесса (приложения) или субъекта должны быть соответствующие права. Текущий уровень может включать только одну категорию из каждого *измерения*, тогда как допустимые уровни могут включать несколько категорий из одного измерения, и в этом случае они называются многоуровневыми.

Management Console [Консоль управления]— A web-based graphical user interface that is used to configure and maintain the SafeSpace solution.

RU Рабочее место администратора, которое используется для настройки и обслуживания программного обеспечения SafeSpace.

Multidimensional Matrix [Многомерная матрица] — Two or more *dimensions* which are used to *classify* data. Using more than one dimension can improve the accuracy of data classification and enable more flexible configuration of access rights to various objects and types of information.

RU *Классификация* с использованием 2-х и более *измерений*. Применяется для гранулярной сегментации данных — по уровню доступа и отнесения информации к классифицируемым сведениям.

Responsibility Zone [Зона ответственности] — Each event, during processing, is assigned a specific area of responsibility identifying the executor of the action which triggered the event. All users who have access to the management console must be associated with at least one area of responsibility. While working on the management console, the user is permitted access only to those events that relate to their responsibility zone. In addition to restricting access to dynamic data, responsibility zones can be used to restrict access to specific forms in the *management console*.

RU Зона ответственности определяет, кто из участников процесса является исполнителем задач. Все пользователи, имеющие доступ, должны быть связаны с зонами ответственности. При работе пользователю разрешается доступ только к тем событиям, которые относятся к его зоне ответственности. Помимо ограничения доступа к динамическим данным, зоны ответственности можно использовать для ограничения доступа к определённым формам *консоли управления*.

SafePrint [SafePrint]— A Perimetrix SafeSpace module that manages where classified files can be printed, including automatically adding appropriate watermarks and other identifying data to the printed material.

RU Компонент Perimetrix SafeSpace, обеспечивающий печать «водяных знаков» и других атрибутов на бумажные копии классифицированных данных.

SafeResource [SafeResource] — A Perimetrix SafeSpace module (implemented as a processing node or separate server) that manages access to classified files on remote resources (portals, databases, etc.).

RU Компонент Perimetrix SafeSpace, обеспечивающий доступ у удаленным классифицированным ресурсам (портал, база данных и т.д.) только с рабочей станции с установленным и запущенным сервисом SafeUse.

SafeSpace [SafeSpace] — Refers to the entire Perimetrix SafeSpace solution including SafeSpace servers, databases, and related modules.

RU Полный набор всех модулей Perimetrix, поставляемый в актуальной версии программного продукта.

SafeSpace server [Сервер SafeSpace] — The core server in a SafeSpace system which is supported by a database containing all of the *configuration* parameters for the system.

RU Центральный сервер SafeSpace, который содержит базу данных и все параметры *конфигурации* системы.

SafeStore [SafeStore] — A Perimetrix SafeSpace component designed for storing and exchanging (transmitting) encrypted documents with the help of Cryptex. SafeStore prevents data from being compromised in the event of physical theft of the media or the leakage electronic copies of the data (from backups, etc.).

RU Компонент Perimetrix SafeSpace, предназначенный для хранения и обмена (передачи) зашифрованных документов, предназначенный для хранения и передачи зашифрованных документов с помощью криптографического архива. Предотвращает компрометацию данных в случае физической кражи или копирования данных.

SafeUse [SafeUse] — A Perimetrix SafeSpace component designed for classifying and managing confidential data. SafeUse implements and enforces company security policies by applying restrictions to the creation, storage, processing, and transmission of classified data.

RU Компонент Perimetrix SafeSpace, предназначенный для классификации электронной информации, и дальнейшего управления классифицированной информацией ограниченного доступа с использованием политик хранения, обработки, пересылки и обмена.

SafeUse Agent [Агент SafeUse] — Software installed on a workstation, which receives and applies security policies from the SafeSpace system and reports on any related security events.

RU Специальное программное обеспечение, устанавливаемое на рабочих местах пользователей для работы с классифицированными данными.

Schedule [Расписание] — In the context of Perimetrix SafeSpace, a function used to determine access to the system based on a set schedule. One of the steps when creating a responsibility zone is to create a list of management console forms that members of the created zone will have access to. Restricting when the forms can be accessed is achieved by specifying a schedule.

RU В нотации Perimetrix SafeSpace это функция, используемая для контроля и определения доступа к системе в зависимости от времени суток, зоны ответственности и управления, к которым будут иметь доступ члены созданной зоны для своевременной работы в консоли. Ограничение доступа к формам достигается путём предоставления определённого расписания.

Sensitive Data [Чувствительные данные] — Any data that should not be disclosed since doing so could potentially cause financial or reputational harm to the organization.

RU Любая информация, содержащая сведения, составляющие коммерческую, служебную или иную тайну, определенную локальными нормативными документами и/или законодательством, раскрытие которой может причинить владельцу данных финансовый и/или репутационный ущерб.

Sensitivity [Чувствительность] — The degree to which the disclosure of sensitive data will result in reputational or financial damage to a company or organization. The higher the sensitivity, the greater the need to keep the information secret. This is often a key metric in risk management.

RU Относительная величина потенциального ущерба нарушения конфиденциальности данных, содержащих закрытые сведения. Чем больше чувствительность данных, тем выше ценность содержащихся в них сведений. Чувствительность нередко используется как мера для оценки и управления рисками ИБ.

Unclassified (British English - nonclassified) [Неклассифицированный] — Information which is not considered confidential (i.e., very low level of sensitivity) and which can generally be made available to the public.

RU Информация, не содержащая сведений ограниченного доступа.

Unclassified Category [Неклассифицированная категория]— A special category that is included in each *dimension*. If this category is assigned to an object, it means that the object is not classified by this dimension. An object whose level consists of unclassified categories from each dimension is called unclassified. Permissions are not required for unclassified objects.

RU Служебная категория, включаемая при настройке системы в каждое *измерение*. Если эта категория присвоена объекту, то объект не классифицируется по этому измерению. Для неклассифицированных объектов разрешения на обработку не требуются.

Unconfigured Workstations [Несконфигурированные рабочие станции] — Workstations where the SafeUse Agent is installed, but which are not yet included in the effective configuration of the SafeSpace system. In order to be able to work with classified information on such workstations, they must be added to the current effective configuration of a SafeSpace server. When adding workstations to the current configuration of a SafeSpace server, an area of responsibility is required.

RU Рабочие станции, на которых установлен SafeUse Agent, но которые ещё не включены в существующую конфигурацию системы SafeSpace. Чтобы иметь возможность хранить и обрабатывать секретную информацию на таких рабочих станциях, они должны быть добавлены в новую конфигурацию сервера с определённой зоной ответственности.

Universal Event Model, UEM [Универсальная модель событий] — A model that allows each intercepted event to be represented as an object moving from a source to a destination. This model enables the use of unified analysis, i.e., a single processing logic and a single security policy for information objects, regardless of their type.

RU Универсальная модель принятия решений о допустимых операциях в системе Perimetrix. Любое действие с защищаемой информацией рассматривается как «перемещение» из контейнера–источника в контейнер–получатель. Система сверяет допуски обоих контейнеров с *классификационной меткой* информационного объекта и либо разрешает, либо блокирует такое перемещение.