Система менеджмента качества группы компаний ИнфоВотч

УТВЕРЖДАЮ
Генеральный директор
ООО «Лаборатория ИнфоВотч»
/ Н.И. Касперская /
«23» декабря 2021 г.

ООО «Лаборатория ИнфоВотч»

Стандарт организации

Защита информации. Процессы контроля обработки смысловой компьютерной информации. Автоматизированные системы контроля процессов обработки смысловой компьютерной информации. Термины и определения

СК СТ 01-1

Москва
2021

Бизнес-центр «Верейская плаза III»
121357, Москва, ул. Верейская, д. 29, стр. 134
+7 495 22 900 22, +7 499 37 251 74
sales@infowatch.ru
infowatch.ru

Предисловие

Цели и принципы стандартизации в Российской Федерации установлены Федеральным законом от 29 июня 2015 года N 162-ФЗ «О стандартизации в Российской Федерации».

Отношения, возникающие при разработке, принятии, применении и исполнении обязательных требований к продукции, применении и исполнении на добровольной основе требований к продукции, процессам проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, а также к выполнению работ или оказанию услуг в целях добровольного подтверждения соответствия; оценке соответствия установлены Федеральным законом от 27 декабря 2002 г. N 184-ФЗ "О техническом регулировании".

Сведения о стандарте

1 РАЗРАБОТАН ООО «Лаборатория ИнфоВотч»

2 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ «23» декабря 2021 г.
приказом генерального директора ООО «Лаборатория ИнфоВотч» Касперской Н.И. от «23» декабря 2021 г. № 2-СМК/ЛИ-21.

3 ВВЕДЕН ВПЕРВЫЕ

4 В настоящем стандарте реализованы нормы Федеральных законов от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации", от 27.07.2006 N 152-ФЗ "О персональных данных", от 29 июля 2004 г. N 98-ФЗ "О коммерческой тайне".

5 РАЗРАБОТАЛ _____ А.С. Арефьев _____ М.Б. Смирнов

6 ПРОВЕРИЛ В.А. Иванов

7 ЗАРЕГИСТРИРОВАЛ Е.П. Наумова

Номер СК СТ 01-1

Инв. номер 2101 от « 23 » декабря 2021 г.

Бизнес-центр «Верейская плаза III»
121357, Москва, ул. Верейская, д. 29, стр. 134
+7 495 22 900 22, +7 499 37 251 74
sales@infowatch.ru
infowatch.ru

Содержание

Введение

Установленные настоящим стандартом термины расположены в систематизированном порядке, отражающем систему понятий в данной области знания.

Для каждого понятия установлен один стандартизованный термин.

Заключенная в круглые скобки часть термина образует его краткую форму.

Цифра, заключенная в квадратные скобки, означает ссылку на документ, приведенный в структурном элементе "Библиография".

Приведенные определения можно при необходимости изменять, вводя в них производные признаки, раскрывая значения используемых в них терминов, указывая объекты, входящие в объем определяемого понятия.

Изменения не должны нарушать объем и содержание понятий, определенных в настоящем стандарте.

Стандартизованные термины набраны полужирным шрифтом, их краткие формы, представленные аббревиатурой, - светлым, а синонимы - курсивом.

Термины и определения общетехнических понятий, которые необходимы для понимания текста основной части настоящего стандарта, приведены в приложении А.

1 Необходимость создания стандарта

В настоящее время основной массив информации (данных), необходимой для государственного и муниципального управления, обеспечения функционирования умных городов, функционирования и развития бизнеса представлен в виде компьютерной информации и содержится в корпоративных информационных системах, локальных системах, в виде файлов на рабочих станциях и общих ресурсах пользователей. Кроме того, управление производством и технологическими процессами также переместилось в сектор информационных технологий (АСУ, Интернет вещей (IoT, IIoT), цифровые платформы), в которых содержится компьютерная информация различных видов, в т.ч. та, которая не может быть интерпретирована, воспринята человеком даже после представления в печатном, графическом, акустическом виде, и та, которую человек воспринимает после обработки, например, в ходе реализации процедур диспетчерского управления (далее – компьютерная смысловая информация).

Для работы с компьютерной смысловой информацией параллельно с существующими основными и вспомогательными процессами, управленческими, производственными и технологическими сформировались специфические процессы управления доступом и контроля того, как информация фактически используется:

1. Контроль использования информации человеком.
2. Анализ информационных потоков с точки зрения контента и связей.
3. Построение карты коммуникаций между сотрудниками и физической топологии коммуникаций. Оценка эффективности коммуникаций.
4. Анализ доступности информационных ресурсов с точки зрения расположения и прав доступа (расположения файлов, наличие ненужных прав и т.д.)
5. Прогнозирование вхождения сотрудника в группу риска.

Таким образом, возможно говорить о новой сфере управления и контроля за информацией, за контролем того как используется информация, к которой сотрудники получили правомерный (легитимный) доступ, а также как и в каких целях они используют информационные (телекоммуникационные) каналы, предоставленные им организацией, создают ли риски для организации, связанные с их деятельностью (группы риска).

Кроме того, на данный момент существуют программные продукты, на базе которого возможно создание автоматизированных систем (АС), используемых для контроля обработки информации, но применение таких продуктов ограничено функциями выявления и, для некоторых решений, предотвращения утечек информации, к которой у пользователя есть легитимный доступ, а также к выявлению групп риска среди сотрудников.

Существует большое количество программных продуктов, использующих различные подходы и технологии для решения указанных задач / проблем. В силу их

разнообразия невозможно объективно измерить качество решения задачи контроля обработки смысловой информации.

Таким образом, необходимо разработать требования к системам, контролирующим процессы обработки смысловой информацией (информации, используемой и воспринимаемой человеком).

2 Область применения

Настоящий стандарт устанавливает основные термины с соответствующими определениями, применяемые при проведении работ по стандартизации в области защиты информации.

Термины, установленные настоящим стандартом, рекомендуется использовать для разработки документов системы менеджмента качества, системы менеджмента информационной безопасности, а также документов на продукты (продукцию), разрабатываемую и выпускаемую компаниями, входящими в группу ИнфоВотч.

Настоящий стандарт предназначен для оценки качества процессов контроля обработки смысловой информации и АС, осуществляющих такой контроль.

Настоящий стандарт распространяется на

- процессы контроля обработки смысловой компьютерной информации
- автоматизированные системы контроля процессов обработки смысловой компьютерной информации, в т.ч. на автоматизированные системы, предназначенные для выявления и предотвращения утечек информации,
- прикладное программное обеспечение, используемое для создания автоматизированных систем контроля процессов обработки смысловой компьютерной информации, в т.ч. программного обеспечения для выявления и предотвращения утечек компьютерной информации.

Настоящий стандарт устанавливает основные термины и определения в данной области, вводит понятия смысловой компьютерной информации, модели зрелости процессов контроля обработки смысловой компьютерной информации, модели зрелости автоматизированных систем, создаваемых для контроля этих процессов, в т.ч. предназначенных для выявления и предотвращения утечек информации.

В настоящем стандарте общие технические условия или технические условия не устанавливаются.

Стандарт не распространяется на системы и процессы:

- обработки информации на бумажных носителях или существующей в виде акустических, виброакустических колебаний, за исключением событий преобразования компьютерной информации в другую форму (распечатка, сканирование, озвучание, запись звука на машинный носитель в машиночитаемом виде);

- обработки и реагирования на компьютерные инциденты (инциденты ИБ) в терминологии ГОСТ Р ИСО/МЭК ТО 18044-2007, «новые стандарты КИИ» и нормативно-правовых, организационных и методических документов по обеспечению безопасности критической информационной инфраструктуры РФ.

Настоящий стандарт предназначен для применения

1. Руководителями предприятий, внедривших (планирующих внедрить) процессы обработки и контроля обработки смысловой компьютерной информации, специалистами по безопасности, специалистами по системам менеджмента качества для контроля оценки качества внедрения процессов контроля оборота смысловой информации.
2. Специалистами по безопасности, специалистами по системам менеджмента качества, руководителями предприятий, внедривших (планирующих внедрить) автоматизированные системы контроля процессов оборота смысловой информации, в т.ч. программного обеспечения для выявления и предотвращения утечек компьютерной информации.
3. Специалистами по проектированию и внедрению автоматизированных систем контроля процессов оборота смысловой компьютерной информации, в т.ч. программного обеспечения для выявления и предотвращения утечек компьютерной информации.
4. Разработчиками прикладного программного обеспечения, используемого для создания автоматизированных систем контроля процессов оборота смысловой компьютерной информации, в т.ч. программного обеспечения для выявления и предотвращения утечек компьютерной информации.

3 Нормативные ссылки

ГОСТ Р 1.0-2012 Стандартизация в Российской Федерации. Основные положения

ГОСТ Р 1.4-2004 Стандартизация в Российской Федерации. СТАНДАРТЫ ОРГАНИЗАЦИЙ. Общие положения

Р 50.1.075-2011 Рекомендации по стандартизации. Разработка стандартов на термины и определения

ГОСТ Р 50922-2006 Защита информации. ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ.

Р 50.1.053-2005 РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ. Информационные технологии. ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ В ОБЛАСТИ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения

ГОСТ Р 57580.1-2017 Безопасность финансовых (банковских) операций. ЗАЩИТА ИНФОРМАЦИИ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ. Базовый состав организационных и технических мер

ГОСТ Р ИСО 9000-2017 Системы менеджмента качества. Основные положения и словарь

ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения». Применение ГОСТ 34.003-90 на территории Российской Федерации прекращается с 01.01.2022 в связи с утверждением и введением в действие ГОСТ Р 59853-2021 (приказ Росстандарта от 19.11.2021 N 1520-ст).

4 Термины и определения

3.1 Процесс обработки информации – совокупность взаимосвязанных автоматизированных (компьютерных) и неавтоматизированных операций по обработке информации на всех этапах с целью получения результатов с заданной целью для обеспечения функционирования организации.
Примечание: определение «обработка информации» применяется в соответствии с ГОСТ Р 51583-2014.

3.2 Уровни зрелости процессов обработки информации

Уровень 0: Политики и правила обработки информации в организации отсутствуют

Уровень 1:

1. Политики и правила обработки информации в организации отсутствуют
2. Существуют политики обработки информации, выходящей за пределы организации
3. Существуют политики обработки информации, доступной различным подразделениям организации (при передаче, при совместной обработке и т.д.)
4. Существуют политики обработки информации, доступной сотрудникам одного подразделения (в пределах одного подразделения)

Уровень 2:

1. Политика применяется вне зависимости от контента (содержания документа, файла)
2. Политика применяется в зависимости от принадлежности контента к стандарту (ПДн, PCI DSS и т.д.) – наличия требований регуляторов к обработке данного вида информации
3. Политика применяется в зависимости от наличия требований организации к обработке данного вида информации
4. Политика применяется в зависимости от наличия требований регуляторов или организации к обработке данного вида информации в рамках конкретных процессов (управленческих, производственных)

Уровень 3:

1. Организован процесс (вручную или автомат.) Мониторинг и информирование о нарушении политики, правила
2. Организован процесс (вручную или автомат.) Мониторинг, информирование о нарушении правила и блокирование нарушения (например, попытки передачи)
3. Организован процесс (вручную или автомат.) Мониторинг, информирование о нарушении правила и блокирование нарушения (например, попытки передачи) и Процесс реагирования на нарушения правил и политик
4. Организован процесс (вручную или автомат.) Мониторинг, информирование о нарушении правила, блокирование нарушения (например, попытки передачи) с

возможностью для пользователя (исполнителя) согласовать факт передачи информации

3.3 Процесс контроля обработки информации – сопоставление фактической реализации процесса обработки информации заданным правилам и политикам и оповещение, или прерывание процесса обработки информации.

3.4 Смысловая компьютерная информация – информация которая может быть распечатана из автоматизированной системы или ЭВМ (компьютера) на бумажные носители и передана для прочтения и интерпретации без использования специальных инструментов человеку, либо воспроизведена в виде речи на одном из естественных языков.

3.5 Процесс обработки смысловой компьютерной информации – совокупность взаимосвязанных автоматизированных (компьютерных) и неавтоматизированных операций по обработке смысловой компьютерной информации на всех этапах с целью получения результатов с заданной целью для обеспечения функционирования организации.

3.6 Процесс контроля смысловой компьютерной обработки информации – сопоставление фактической реализации процесса обработки смысловой компьютерной информации заданным правилам и политикам и оповещение, или прерывание процесса обработки смысловой компьютерной информации.

3.7 Модель зрелости процесса контроля обработки смысловой компьютерной информации - модель, используется для оценки соответствия процессов контроля обработки смысловой компьютерной информации, включая в себя процессы:

- определения типов смысловой компьютерной информации
- определения допустимых маршрутов передвижения смысловой компьютерной информации
- утверждения правил обработки смысловой компьютерной информации
- информирования сотрудников о правилах обращения со смысловой компьютерной информацией
- реагирования на нарушение правил обработки смысловой компьютерной информации

Примечание: модель зрелости строится для процесса обработки информации, существующей в любой форме, для первых уровней, далее учитывает особенности создания и реализации процесса обработки (правил, политик) именно компьютерной информации.

Оценки зрелости выставляются от 0 (наименьший уровень зрелости)

3.8 Автоматизированная Система Контроля Обработки Смысловой Компьютерной Информации (АС КОСКИ) – это автоматизированная система (АС), предназначенная для выявления несоответствия или соответствия фактической обработки смысловой компьютерной информации требованиям и правилам в рамках процессов обработки информации в организации, отвечает на вопрос «как пользователь работает со смысловой компьютерной информацией в рамках имеющегося у него легитимного доступа».

Примечания:

1. Внедрённая в организации DLP-система является примером АС КОСКИ.
2. Автоматизированная система(АС) – из ГОСТ 34….

3.9 ПО DLP (Data Loss Prevention, Data Leak Prevention, Data Leakage Protection) – прикладное ПО для внедрения в организации АС КОСКИ, является основным программным средством реализации АС КОСКИ.

3.10 Модель зрелости АС КОСКИ - модель, используемая для оценки соответствия автоматизированной системы контроля процесса обработки смысловой компьютерной информации процессу определённого уровня зрелости контроля обработки смысловой компьютерной информации.

3.11 Критерии зрелости АС КОСКИ:

1. Имеет настраиваемый процесс реакции на инциденты информационной безопасности, включающий в себя следующие действия:
   - выявляет факты утечек информации и оповещает уполномоченных лиц;
   - пресекает (блокирует) утечки информации и оповещает уполномоченных лиц;
   - помещение в карантин и согласование решение об отправке или блокировке.
2. Выявляет несоответствие / соответствие требованиям и правилам обработки информации
3. Прогнозирует риски информационной безопасности в отношении смысловой компьютерной информации.
4. Выявляет группы риска применительно к сотрудникам организации.
5. Контролирует не менее 100/70/50/30% узлов обработки смысловой компьютерной информации (файл-сервер, АРМ) в АС.
6. Контролирует не менее 100/70/50/30% протоколов передачи смысловой компьютерной информации (протоколы мессенджеров, облачных хранилищ и т.д.) в АС.
7. Контролирует не менее 100/70/50/30% используемых сотрудниками облачных сервисов вне зависимости от средств доступа (АРМ, личные устройства и т.п.).

8. Классифицирует не менее 100/70/50/30% контролируемой (хранящейся, передаваемой) информационной безопасности в отношении смысловой компьютерной информации.
9. Автоматически размечает и контролирует не менее 100/70/50/30% от общего объема хранящейся смысловой компьютерной информации.
10. Количество ошибок при автоматической классификации смысловой компьютерной информации по заданным критериям не превышает 5/10/15/20%.
11. Автоматически выставляет приоритеты обработанным событиям в отношении смысловой компьютерной информации.

Бизнес-центр «Верейская плаза III»
121357, Москва, ул. Верейская, д. 29, стр. 134
+7 495 22 900 22, +7 499 37 251 74
sales@infowatch.ru
infowatch.ru

Приложение А (справочное). Термины и определения общетехнических понятий

А.1 информация: Сведения (сообщения, данные) независимо от формы их представления [1].

А.2 данные: Факты, понятия или команды, представленные в формализованном виде и позволяющие осуществлять их передачу или обработку как вручную, так и с помощью средств автоматизации [2].

А.3 обработка информации: Совокупность операций сбора, накопления, ввода, вывода, приема, передачи, записи, хранения, регистрации, уничтожения, преобразования, отображения, осуществляемых над информацией [3].

А.4 доступ к информации: Возможность получения информации и ее использования [1].

А.5 доступ (в автоматизированной информационной системе): Получение возможности ознакомления с информацией, ее обработки и (или) воздействия на информацию и (или) ресурсы автоматизированной информационной системы с использованием программных и (или) технических средств. Примечание — Доступ осуществляется субъектами доступа, к которым относятся лица, а также логические и физические объекты [4].

А.6 правило доступа к защищаемой информации; правило доступа: Совокупность правил, устанавливающих порядок и условия доступа субъекта к защищаемой информации и ее носителям [2].

А.7 несанкционированный доступ (к информации [ресурсам автоматизированной информационной системы]); НСД: Доступ к информации [ресурсам автоматизированной информационной системы], осуществляемый с нарушением установленных прав и (или) правил доступа к информации [ресурсам автоматизированной информационной системы]. Примечания 1 Несанкционированный доступ может быть осуществлен преднамеренно или непреднамеренно. 2 Права и правила доступа к информации и ресурсам информационной системы устанавливаются для процессов обработки информации, обслуживания автоматизированной информационной системы, изменения программных, технических и информационных ресурсов, а также получения информации о них [4].

А.8 правила разграничения доступа (в автоматизированной информационной системе): Правила, регламентирующие условия доступа субъектов доступа к объектам доступа в автоматизированной информационной системе [4].

А.9 предоставление информации: Действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц [1].

А.10 распространение информации: Действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц [1].

А.11 утечка информации: Неконтролируемое распространение защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации иностранными разведками [3].

А.12 разглашение информации: Несанкционированное доведение защищаемой информации до лиц, не имеющих права доступа к этой информации [3].

А.13 автоматизированная система; АС: Система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций [5].
Примечания:
1. В зависимости от вида деятельности выделяют, например, следующие виды АС: автоматизированные системы управления (АСУ), системы автоматизированного проектирования (САПР), автоматизированные системы научных исследований (АСНИ) и др.
2. В зависимости от вида управляемого объекта (процесса) АСУ делят, например, на АСУ технологическими процессами (АСУТП), АСУ предприятиями (АСУП) и т.д.

А.14 организация: Группа работников и необходимых средств с распределением ответственности, полномочий и взаимоотношений [6].

Библиография

[1] Российская Федерация. Федеральный закон от 27.07.2006 г. N 149-ФЗ — Об информации, информационных технологиях и о защите информации

[2] ГОСТ Р 50922-2006 — Защита информации. Основные термины и определения

[3] Рекомендации по стандартизации Р 50.1.056-2005 — Техническая защита информации. Основные термины и определения

[4] ГОСТ Р 53114-2008 — Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения

[5] ГОСТ 34.003-90 — «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения»
Применение ГОСТ 34.003-90 на территории Российской Федерации прекращается с 01.01.2022 в связи с утверждением и введением в действие ГОСТ Р 59853-2021 (приказ Росстандарта от 19.11.2021 N 1520-ст).

[6] ГОСТ Р ИСО 9000-2017 — Системы менеджмента качества. Основные положения и словарь

Лист регистрации изменений

История изменений документа:

Версия документа	Дата	Автор	Суть изменения
1.00	23.12.2021	М.Б. Смирнов	Разработка первой версии документа