ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р
(проект,
первая редакция)

Защита информации
ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ИЗ ПРОГРАММНОЙ СРЕДЫ ИНФОРМАЦИОННЫХ И АВТОМАТИЗИРОВАННЫХ СИСТЕМ
Общие положения

Настоящий проект стандарта не подлежит применению до его утверждения

Москва

Российский институт стандартизации

202X

Предисловие

1 РАЗРАБОТАН Обществом с ограниченной ответственностью «СОЛАР СЕКЬЮРИТИ» (ООО «СОЛАР СЕКЬЮРИТИ»), Обществом с ограниченной ответственностью «Центр безопасности информации» (ООО «ЦБИ»). Разработан при экспертной поддержке организаций, представленных в приложении А.

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 362 «Защита информации»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от №

4 ВВЕДЕН ВПЕРВЫЕ

Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». 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 ежемесячного 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 (www.rst.gov.ru)

Содержание

Введение

К утечке защищаемой информации из информационной (автоматизированной) системы могут приводить следующие группы угроз безопасности информации:

- угрозы безопасности информации, связанные с использованием нарушителем технических каналов утечки защищаемой информации;

- угрозы безопасности информации, связанные с осуществлением внутренними и внешними нарушителями попыток получения несанкционированного доступа к информации, к которой они не имеют прав доступа в программной среде информационных (автоматизированных) систем;

- угрозы безопасности информации, связанные с распространением защищаемой информации лицами, имеющими права доступа к ней с использованием программной среды информационных (автоматизированных) систем.

Меры защиты информации, реализуемые в информационных (автоматизированных) системах в соответствии с нормативными правовыми актами и методическими документами по защите информации, позволяют реализовать систему защиты информации, обеспечивающую защиту от угроз безопасности информации, относящихся к первым двум группам.

Настоящий стандарт содержит положения по регламентированию мероприятий, направленных на защиту информации от утечки в результате действий пользователей, имеющих права доступа к защищаемой информации в программной среде информационной (автоматизированной) системы, выполняемых с использованием средств защиты информации от утечки из программной среды информационной (автоматизированной) системы (далее – средств защиты информации от утечки).

Целью настоящего стандарта является определение состава участников и основного содержания процессов, направленных на обеспечение защиты информации от утечки из программной среды информационных (автоматизированных) систем в результате действий пользователей, имеющих права доступа к защищаемой информации в программной среде информационной (автоматизированной) системы (далее – защиты информации от утечки).

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Защита информации
ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ИЗ ПРОГРАММНОЙ СРЕДЫ ИНФОРМАЦИОННЫХ И АВТОМАТИЗИРОВАННЫХ СИСТЕМ
Общие положения

Information protection. Data leakage protection of information and automated systems software environment. General provisions

Дата введения - _____

1 Область применения

Настоящий стандарт предназначен для федеральных органов исполнительной власти, государственных корпораций (компаний) и иных организаций, созданных на основании федеральных законов, стратегических предприятий, стратегических акционерных обществ и системообразующих организаций, юридических лиц, являющихся субъектами критической информационной инфраструктуры Российской Федерации, организаций, являющихся операторами государственных информационных систем, а также операторами информационных систем персональных данных (далее - организации). При этом изложенные в настоящем стандарте положения могут применяться иными органами и организациями независимо от их типа, размера, структуры и сферы деятельности.

Настоящий стандарт содержит положения о:

- мероприятиях по защите информации от утечки из программной среды информационной (автоматизированной) системы;

- применении средств защиты информации от утечки из программной среды информационной (автоматизированной) системы;

- защите данных, собираемых и формируемых в рамках мероприятий по защите информации от утечки из программной среды информационной (автоматизированной) системы.

Положения настоящего стандарта применяют при организации мероприятий по защите информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, от утечки из программной среды информационной (автоматизированной) системы.

Настоящий стандарт содержит положения, относящиеся к мероприятиям, направленным на обеспечение защиты информации от угроз безопасности, связанных с воздействием на защищаемую информацию факторов, которые в соответствии с ГОСТ Р 51275 относятся к субъективным внутренним факторам, воздействующим на безопасность защищаемой информации, связанным с разглашением защищаемой информации лицами, имеющими к ней право доступа.

Настоящий стандарт не содержит положений, касающихся мероприятий, направленных на обеспечение защиты информации от угроз безопасности, связанных с воздействием на защищаемую информацию иных факторов, определенных в ГОСТ Р 51275, в том числе, связанных с утечками по техническим каналам.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ Р 50922 Защита информации. Основные термины и определения.

ГОСТ Р 51275 Защита информации. Объект информатизации. Факторы, воздействующие на информацию.

ГОСТ Р 59547 Защита информации. Мониторинг информационной безопасности. Общие положения.

ГОСТ Р 59548 Защита информации. Регистрация событий безопасности. Требования к регистрируемой информации.

ГОСТ Р 59710 Защита информации. Управление компьютерными инцидентами. Общие положения.

ГОСТ Р 59853 Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения.

П р и м е ч а н и е – При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования – на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по

состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем стандарте применены термины по ГОСТ Р 50922, ГОСТ Р 59853, а также следующие термины с соответствующими определениями.

3.1 **защита информации от утечки из программной среды информационной (автоматизированной) системы (в результате действий пользователей, имеющих права доступа к защищаемой информации):** Деятельность, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате её разглашения с использованием штатных программных средств информационной (автоматизированной) системы лицами, имеющими к ней право доступа.

Примечание – Заинтересованными субъектами могут быть: государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

3.2 **канал утечки информации из программной среды информационной (автоматизированной) системы (в результате действий пользователей, имеющих права доступа к защищаемой информации):** Программное или программно-аппаратное средство, предназначенные для обмена или хранения информации, использование которых с нарушением установленных в организации правил передачи или хранения защищаемой информации может привести к ее утечке.

3.3 **объект контроля (при защите информации от утечки из программной среды информационной (автоматизированной) системы в результате действий пользователей, имеющих права доступа к защищаемой информации):** Элемент информационной (автоматизированной) системы, который используется в качестве источника данных, необходимых для выявления признаков возможной утечки информации из программной среды информационной (автоматизированной) системы.

3.4 **программная среда (информационной (автоматизированной) системы)**: Совокупность программного обеспечения, используемого в информационной (автоматизированной) системе для решения одной или нескольких задач.

3.5 **средство защиты информации от утечки из программной среды информационной (автоматизированной) системы:** Средство защиты информации, предназначенное для выявления нарушений пользователями, имеющими права доступа к защищаемой информации, установленных в организации, правил её передачи или хранения, которые привели или могут привести к утечке защищаемой информации, а также для реагирования на такие нарушения.

3.6 **уровень контроля защиты информации от утечки:** Совокупность мероприятий по защите информации от утечки, объединенных по определенному признаку в единую группу.

Примечание – В настоящем стандарте определены четыре уровня контроля. Первым уровнем контроля является уровень объектов контроля, определяющий совокупность мероприятий по защите информации от утечки, выполняемых в отношении объектов контроля, которые могут предоставить информацию, необходимую для защиты информации от утечки. Вторым уровнем контроля является уровень взаимодействия с объектами контроля, который определяет совокупность мероприятий по защите информации от утечки, выполняемых с целью получения информации, необходимой для защиты информации от утечки от объектов контроля. Третьим уровнем контроля является уровень выявления признаков возможной утечки, который определяет совокупность мероприятий по защите информации от утечки, выполняемых с целью анализа полученной информации и выявления в ее составе признаков, указывающих на возможную утечку информации, а также реагирования на выявленные факты утечки информации. Четвертым уровнем контроля является уровень представления результатов выявления признаков возможной утечки, который определяет совокупность мероприятий по защите информации от утечки, выполняемых с целью представления информации о результатах защиты информации от утечки лицам, ответственным за обеспечение защиты информации от утечки.

3.7 **утечка информации (из программной среды информационной (автоматизированной) системы):** Неконтролируемое распространение защищаемой информации в результате её разглашения с использованием программной среды информационной (автоматизированной) системы.

4 Общие положения

4.1 Мероприятия по защите информации от утечки в результате действий пользователей, имеющих права доступа к защищаемой информации в программной среде информационной (автоматизированной) системы (далее – защита информации от

утечки из программной среды информационной (автоматизированной) системы), реализуются одновременно или после создания системы защиты информации информационной (автоматизированной) системы в соответствии с требованиями нормативных правовых актов и методических документов по защите информации уполномоченных федеральных органов исполнительной власти.

П р и м е ч а н и е – Защита информации от утечки не может быть обеспечена, если в информационной (автоматизированной) системе не создана система защиты информации, обеспечивающая защиту технических средств, идентификацию и аутентификацию пользователей, управление доступом субъектов доступа к объектам доступа, антивирусную защиту, обнаружение вторжений, защиту каналов связи, защиту машинных носителей информации (при необходимости с использованием в соответствии с законодательством Российской Федерации методов криптографической защиты информации) и реализацию иных мер защиты информации в соответствии с требованиями нормативных правовых актов и методических документов по защите информации уполномоченных федеральных органов исполнительной власти.

4.2 Деятельность по защите информации от утечки из программной среды информационной (автоматизированной) системы включает следующие стадии:

- организация деятельности по защите информации от утечки из программной среды информационной (автоматизированной) системы;

- защита информации от утечки из программной среды информационной (автоматизированной) системы;

- реагирование на выявленные утечки информации из программной среды информационной (автоматизированной) системы;

- анализ результатов деятельности по защите информации от утечки из программной среды информационной (автоматизированной) системы.

4.3 Организация деятельности по защите информации от утечки из программной среды информационной (автоматизированной) системы.

4.3.1 Мероприятия по защите информации от утечки из программной среды информационных (автоматизированных) систем являются одной из составляющих деятельности по обеспечению информационной безопасности в организации, поэтому функции по реализации данных мероприятий также осуществляются подразделением по информационной безопасности под руководством заместителя руководителя организации по информационной безопасности.

4.3.2 Целью мероприятий по защите информации от утечки является блокирование (нейтрализация) угроз безопасности информации, связанных с действиями пользователей в программной среде информационной (автоматизированной) системы, при-

водящими к утечке защищаемой информации из программной среды информационной (автоматизированной) системы. К таким действиям могут относиться действия пользователей в информационной (автоматизированной) системе, в результате которых защищаемая информация становится или может стать доступной другим пользователям информационной (автоматизированной) системы или иным лицам, которые не должны иметь доступ к такой информации. К утечке информации могут приводить как намеренные, так и не намеренные действия пользователей информационной (автоматизированной) системы.

Примечание – К примерам действий, которые приводят к возникновению угроз, связанных с утечкой информации можно отнести:

- неправомерную отправку защищаемой информации (в виде электронного сообщения или файла) лицам, которые не должны иметь к ней доступ;

- сохранение защищаемой информации в местах хранения (машинные носители информации или общие файловые ресурсы), из которых доступ к защищаемой информации могут получить лица, которые не должны иметь к ней доступ.

4.3.3 Подразделение по информационной безопасности в части реализации мер защиты информации от утечки из программной среды информационной (автоматизированной) системы выполняет:

- разработку перечня видов информации, подлежащих контролю при выявлении признаков утечки информации, и правил использования служебных средств вычислительной техники и программного обеспечения при обработке информации, требующей обеспечения конфиденциальности, а также правил и процедур реализации мер защиты информации от утечки из программной среды информационной (автоматизированной) системы, которые должны быть отражены в документе, регламентирующем вопросы информационной безопасности в организации, в подведомственных организациях (филиалах, представительствах);

Примечания:

1) Перечень видов информации, подлежащих контролю при выявлении признаков утечки информации, формируется исходя из целей и назначения информационной (автоматизированной) системы. Например, к таким видам информации могут относиться персональные данные, финансовая информация, информация об объекте интеллектуальной собственности и другие виды информации, которые могут обрабатываться.

2) Правила использования служебных средств вычислительной техники и программного обеспечения при обработке информации, требующей обеспечения конфиденциальности, должны определять:

- допустимые места хранения видов информации, подлежащих контролю при выявлении признаков утечки информации, на общих сетевых ресурсах информационной (автоматизированной) системы (общие каталоги, системы документооборота, базы данных, почтовые архивы и иные ресурсы);

- списки лиц, которые могут передавать соответствующие виды информации, а также допустимые получатели такой информации как в рамках информационной (автоматизированной) системы, так и за её пределами;

- способы передачи соответствующих видов информации получателям (передача файлов по сети, передача с использованием сервисов коммуникаций, размещение на веб-ресурсе, печать, копирование на съемный машинный носитель информации).

- эксплуатацию средств защиты информации от утечки из программной среды информационной (автоматизированной) системы;

- мониторинг и контроль эффективности мероприятий по защите информации от утечки из программной среды информационной (автоматизированной) системы и принятие мер по её совершенствованию;

- разработку регламента по реализации мер защиты информации от утечки из программной среды информационной (автоматизированной) системы;

- участие в анализе событий безопасности, связанных с утечкой защищаемой информации из программной среды информационной (автоматизированной) системы.

Примечание – Специалисты подразделений принимают непосредственное участие в анализе событий безопасности, связанных с утечкой защищаемой информации. Обработка (передача и хранение) информации, полученной в ходе анализа, осуществляется в соответствии с требованиями законодательства Российской Федерации.

4.3.4 Для реализации мероприятий по защите информации от утечки из программной среды информационной (автоматизированной) системы заместитель руководителя организации по информационной безопасности должен обеспечить согласование и утверждение в организации документа, содержащего перечень видов информации, подлежащих контролю при выявлении признаков утечки информации и правила использования служебных средств вычислительной техники и программного обеспечения при обработке информации, требующей обеспечения конфиденциальности.

4.3.5 Для составления перечня видов информации, подлежащих контролю при выявлении признаков утечки информации, в информационной (автоматизированной) системе должна быть проведена инвентаризация обрабатываемой информации, по результатам которой должно быть установлено какие виды обрабатываемой информации требуют обеспечения конфиденциальности. Все виды информации, требующие обеспечения конфиденциальности, подлежат обязательному включению в перечень видов информации, подлежащих контролю при выявлении признаков утечки информации.

Примечание – Режим обеспечения конфиденциальности обязательно должен вводиться в отношении охраняемой законом тайны (коммерческой тайны, инсайдерской информации, персональных данных, профессиональной тайны и иной).

4.3.6 Правила и процедуры реализации мер защиты информации от утечки из программной среды информационной (автоматизированной) системы, отражаемые в документе, регламентирующем вопросы информационной безопасности в организации, должны предусматривать:

- инвентаризацию обрабатываемой в информационной (автоматизированной) системе информации с целью определения видов обрабатываемой информации, требующих обеспечения конфиденциальности, и составление по её результатам перечня видов информации, подлежащих контролю при выявлении признаков утечки информации;

- определение правил использования пользователями информационной (автоматизированной) системы служебных средств вычислительной техники и программного обеспечения (в том числе средств коммуникаций) при обработке информации, требующей обеспечения конфиденциальности;

- периодический анализ в информационной (автоматизированной) системе назначенных пользователям прав доступа к объектам доступа на предмет избыточности;

- введение организационных мер, предусматривающих отнесение информации, создаваемой в программной среде информационной (автоматизированной) системы, к защищаемой информации;

- введение организационных мер, предусматривающих запрет использования в информационной (автоматизированной) системе личных СВТ и средств коммуникаций;

- введение организационных мер, предусматривающих уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания);

- реализацию организационных и технических мер защиты информации от утечки из программной среды информационной (автоматизированной) системы;

- реализацию организационных и технических мер, предусматривающих реагирование на выявленные утечки информации из программной среды информационной (автоматизированной) системы;

- реализацию организационных мер, предусматривающих анализ результатов деятельности по защите информации от утечки из программной среды информационной (автоматизированной) системы.

4.3.7 Для осуществления мероприятий по защите информации от утечки из программной среды информационной (автоматизированной) системы в организации должно быть обеспечено наличие персонала, прошедшего специальное обучение. По итогам прохождения обучения персонал, осуществляющий защиту информации от утечки из программной среды информационной (автоматизированной) системы, должен обладать навыками, необходимыми для анализа информации, предоставляемой средством защиты информации от утечки, и участия в анализе событий безопасности, связанных с утечкой защищаемой информации.

Мероприятия по защите информации от утечки могут осуществляться уполномоченными специалистами самой организации или с привлечением сторонней организации или отдельных специалистов привлекаемой организации.

4.3.8 Для обеспечения мероприятий по защите информации от утечки из программной среды информационной (автоматизированной) системы необходимо довести до пользователей информационной (автоматизированной) системы о том, что вся созданная в программной среде информационной (автоматизированной) системы информация является защищаемой информацией и о праве обладателя информации и средств её обработки обеспечивать контроль их сохранности и целевого использования, в том числе с применением средств защиты информации от утечки.

П р и м е ч а н и е – Соответствующее уведомление пользователям информационной (автоматизированной) системы о мониторинге средств вычислительной техники, с которыми они работают и мониторинге их действий с использованием средств защиты информации от утечки, выдается при приеме на работу или в процессе ввода в эксплуатацию новой информационной (автоматизированной) системы. Кроме того, одновременно с уведомлением, необходимо ознакомлять под подпись пользователей с перечнем защищаемой информации, с правилами передачи и хранения защищаемой информации.

4.3.9 Для пользователей информационной (автоматизированной) системы должен быть введен запрет на:

- нарушение установленных в документе, регламентирующем вопросы информационной безопасности в организации, правил использования пользователями информационной (автоматизированной) системы служебных средств вычислительной техники и программного обеспечения (в том числе средств коммуникаций) при обработке информации, требующей обеспечения конфиденциальности;

- хранение личных данных на корпоративных файловых ресурсах и устройствах;

- использование личных устройств и программных средств коммуникаций в служебных целях;

- несанкционированный вынос съемных машинных носителей информации и оборудования;

- использование пользователями в неслужебных целях оборудования и программного обеспечения информационной (автоматизированной) системы.

Примечание – Описание действий, запрещающих проводить пользователям при эксплуатации информационной (автоматизированной) системы, могут включаться в трудовой договор при приеме на работу или в дополнение к трудовому договору, в случаях назначения пользователя на должность, предусматривающую эксплуатацию информационной (автоматизированной) системы.

4.3.10 Основными каналами утечки информации из программной среды информационной (автоматизированной) системы рассматриваются:

- сервисы коммуникаций (сервисы, предоставляемые средствами электронной почты, средствами мгновенного обмена сообщениями, видеоконференцсвязи, аудиосвязи и иные сервисы коммуникаций);

Примечание – В качестве каналов утечки должны рассматриваться как штатные сервисы коммуникаций, функционирующие в информационной (автоматизированной) системе, (например, сервис корпоративной электронной почты) так и сервисы коммуникаций в иных сетях, к которым имеет подключение информационная (автоматизированная) система (например, общедоступные почтовые сервисы или сервисы обмена сообщениями в сети Интернет).

- сервисы публикации на веб-ресурсах;

Примечание – В качестве каналов утечки должны рассматриваться как штатные сервисы публикации на веб-ресурсах, функционирующие в информационной (автоматизированной) системе, (например, корпоративный веб-портал) так и сервисы публикации на веб-ресурсах в иных сетях, к которым имеет подключение информационная (автоматизированная) система (например, сайты в сети Интернет).

- сервисы печати файлов (локальные и сетевые);

- съемные машинные носители информации;

Примечание – В качестве каналов утечки должны рассматриваться и иные подключаемые устройства, имеющие в своем составе встроенные носители информации (фото и видео камеры, смартфоны и другие устройства которые могут подключаться как съемные машинные носители информации)

- общие файловые ресурсы.

Примечание – В качестве каналов утечки должны рассматриваться как штатные общие файловые ресурсы, функционирующие в информационной (автоматизированной) системе, (например, корпоративный файловый сервер) так и общие файловые ресурсы в иных сетях, к которым имеет подключение информационная (автоматизированная) система (например, сервисы файловых хранилищ в сети Интернет).

4.4 Защита информации от утечки из программной среды информационной (автоматизированной) системы

4.4.1 Защита информации от утечки из программной среды информационной (автоматизированной) системы предусматривает выполнение мероприятий, направленных на выявление признаков возможных утечек защищаемой информации, с использованием средств защиты информации от утечки из программной среды информационных (автоматизированных) систем.

4.4.2 Реализуемые мероприятия по защите информации от утечки из программной среды информационной (автоматизированной) системы должны обеспечить контроль всех видов информации, которые определены в документе, регламентирующем вопросы информационной безопасности в организации, как виды информации, подлежащие контролю при выявлении признаков утечки информации, а также обеспечивать контроль всех потенциальных каналов утечки, которые имеются в информационной (автоматизированной) системе.

Примечание – Для осуществления мероприятий по защите информации от утечки из программной среды информационной (автоматизированной) системы в соответствии с положениями настоящего стандарта требуется контролировать не все каналы утечки, которые перечислены в п. 4.3.10, а только те каналы утечки, которые имеются в конкретной информационной (автоматизированной) системе.

4.4.3 Выделяются следующие уровни контроля защиты информации от утечки из программной среды информационной (автоматизированной) системы:

- уровень объектов контроля;
- уровень взаимодействия с объектами контроля;
- уровень выявления признаков возможной утечки;
- уровень представления результатов выявления признаков возможной утечки.

Рекомендации по реализации мероприятий контроля в рамках указанных уровней контроля представлены в разделе 5.

Примечание – Для осуществления мероприятий по защите информации от утечки из программной среды информационной (автоматизированной) системы в соответствии с положениями настоящего стандарта требуется не реализовать все мероприятия, представленные в разделе 5, а выбирать с учетом рекомендаций объекты контроля, состав которых зависит от каналов утечки, имеющихся в конкретной информационной (автоматизированной) системе, и определять состав механизмов, которые позволят контролировать эти каналы утечки, в том числе с учетом возможного представления информации (текстовый, графический или иные виды).

Общий подход к организации защиты информации от утечки из программной среды информационной (автоматизированной) системы представлен на рисунке 1.

4.5 Реагирование на выявленные утечки информации из программной среды информационной (автоматизированной) системы

4.5.1 Реагирование на выявленные утечки информации из программной среды информационной (автоматизированной) системы целесообразно осуществлять в рамках деятельности по управлению инцидентами информационной безопасности (компьютерными инцидентами).

Для этих целей необходимо обеспечить передачу событий безопасности, регистрируемых в рамках мероприятий по защите информации от утечки из программной среды информационной (автоматизированной) системы, в систему управления событиями безопасности в соответствии с ГОСТ Р 59547, а при организации деятельности по управлению инцидентами информационной безопасности (компьютерными инцидентами) предусмотреть правила для регистрации признаков инцидентов информационной безопасности (компьютерных инцидентов) на основе событий безопасности, регистрируемых при обнаружении признаков возможной утечки информации.

4.5.2 Если деятельность по управлению инцидентами информационной безопасности (компьютерными инцидентами) не организована, то реагирование на утечки должно осуществляться специалистами подразделения по информационной безопасности, осуществляющими эксплуатацию средства защиты информации от утечки. Такое реагирование должно предусматривать немедленное блокирование, в случае возможности, действий, приводящих к утечке информации, установление причин утечки информации из программной среды, а также принятие организационных, технических и (или) правовых мер, направленных на устранение причин утечки информации.

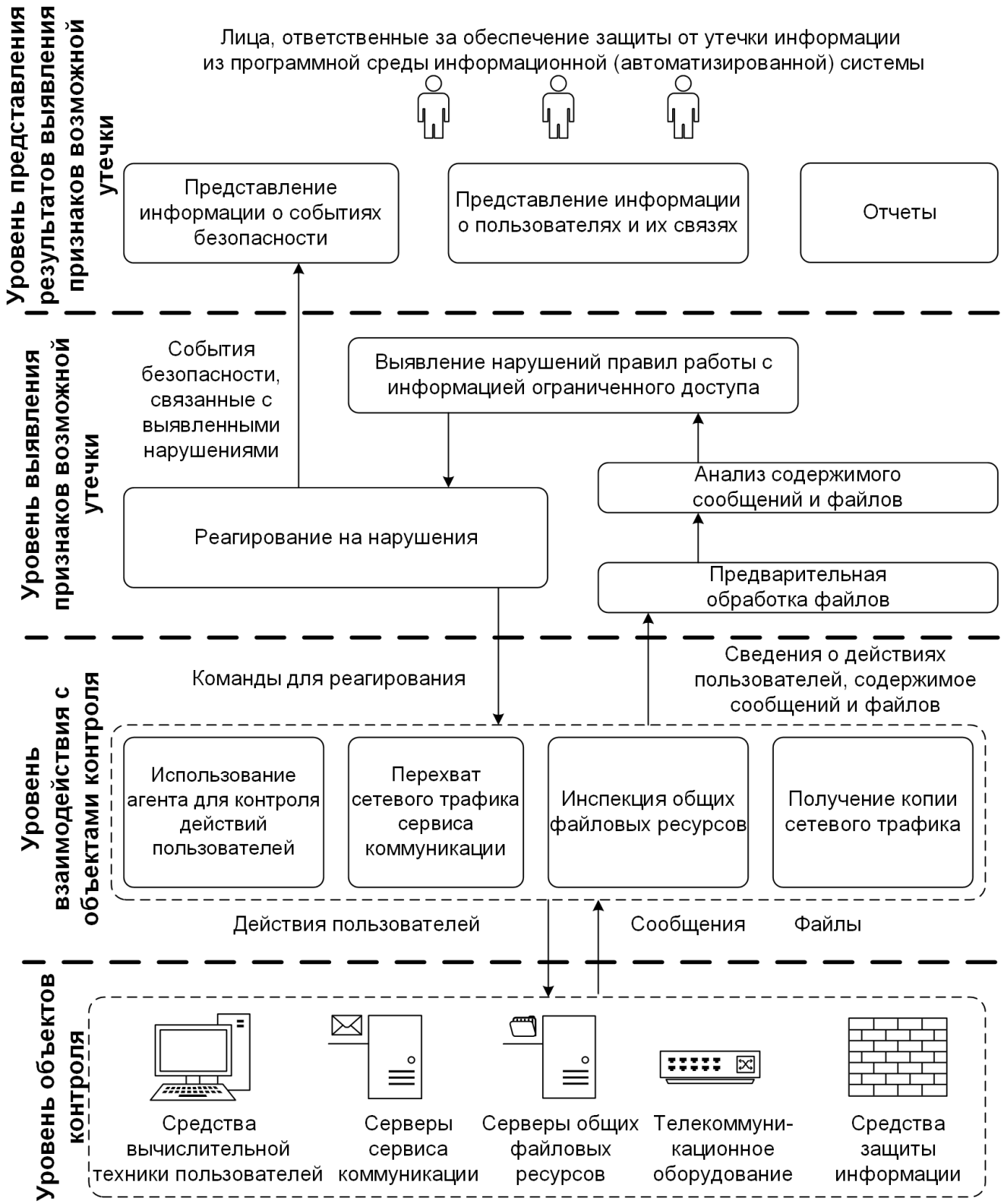

Рисунок 1 – Общий подход к организации защиты информации от утечки из программной среды информационной (автоматизированной) системы

4.6 Анализ результатов деятельности по защите информации от утечки из программной среды информационной (автоматизированной) системы

4.6.1 Анализ результатов деятельности по защите информации от утечки из программной среды информационной (автоматизированной) системы предусматривает:

- анализ эффективности мероприятий по защите информации от утечки из программной среды информационной (автоматизированной) системы;

Примечание – Анализ эффективности мероприятий по защите информации от утечки из программной среды информационной (автоматизированной) системы предусматривает периодический анализ реализуемых процедур с целью выявления недостатков, связанных с выявлением потенциальной утечки информации из программной среды информационных систем. Например, выявление неполного покрытия контролем потенциальных каналов утечки, выявление неполноты покрытия контролем некоторых видов информации, выявление недостатков параметров, по которым идентифицируются потенциальные утечки, выявление неполноты применяемых механизмов анализа для выявления утечки. Необходимость периодического анализ реализуемых процедур связана с тем, что такие недостатки могут возникнуть в процессе жизненного цикла информационных (автоматизированных) систем. Например, при модернизации могут возникнуть новые каналы утечки или появиться новые виды обрабатываемой информации.

- оценку эффективности мероприятий по реагированию на выявленные утечки информации из программной среды информационной (автоматизированной) системы;

Примечание – Если реагирование на выявленные утечки информации из программной среды информационной (автоматизированной) системы осуществляется в рамках деятельности по управлению инцидентами информационной безопасности (компьютерными инцидентами), то анализ эффективности мероприятий по реагированию на выявленные утечки информации осуществляется в рамках реализованных в организации процедур по анализу результатов деятельности по управлению инцидентами информационной безопасности (компьютерными инцидентами).

Если деятельность по управлению инцидентами информационной безопасности (компьютерными инцидентами) не организована, то анализ эффективности мероприятий по реагированию на выявленные утечки информации должен предусматривать определение методов и способов реагирования на выявленные утечки информации из программной среды информационной (автоматизированной) системы, которые показали свою эффективность в рамках уже завершенных процедур реагирования.

- разработка рекомендаций по устранению причин и условий для утечки информации из программной среды информационной (автоматизированной) системы.

Примечание – Разработка рекомендаций по устранению в информационных ресурсах причин и условий для утечки информации из программной среды информационной (автоматизированной) системы осуществляется с целью предотвращения их повторного возникновения;

4.6.2 На основе результатов деятельности по защите информации от утечки из программной среды информационной (автоматизированной) системы осуществляется

(при необходимости) доработка (актуализация) документа, регламентирующего вопросы информационной безопасности в организации, в части:

- перечня видов информации, подлежащих контролю при выявлении признаков утечки информации;

- правил обращения с защищаемой информацией в информационной (автоматизированной системе;

- правил и процедур реализации мер защиты информации от утечки из программной среды информационной (автоматизированной) системы.

5 Рекомендации по реализации мероприятий по защите информации от утечки из программной среды информационной (автоматизированной) системы

5.1 Уровень объектов контроля

5.1.1 При формировании перечня объектов контроля для реализации защиты информации от утечки следует учитывать необходимость в обеспечении контроля всех имеющихся в информационной (автоматизированной) системе каналов утечки информации из числа, определенных в п. 4.3.10.

5.1.2 В качестве объектов контроля, с которых могут быть получены данные, необходимые для выявления признаков возможной утечки информации из программной среды информационной (автоматизированной) системы, рассматриваются:

- телекоммуникационное оборудование, используемое в информационной (автоматизированной) системе;

- средства вычислительной техники, с которыми работают пользователи информационной (автоматизированной) системы;

- серверы информационной (автоматизированной) системы, на которых функционируют сервисы коммуникаций;

- серверы информационной (автоматизированной) системы, на которых размещаются общие файловые ресурсы;

- средства защиты информации, используемые в информационной (автоматизированной) системе.

К данным, используемым в целях выявления признаков возможной утечки информации из программной среды информационной (автоматизированной) системы, относятся:

а) для передаваемых в рамках используемых сервисов коммуникации информации и для передаваемых файлов:

- содержание информации, передаваемой с использованием сервисов коммуникации, или содержимое передаваемых файлов, при их передаче как в рамках информационной (автоматизированной) системы, так и за её пределы (в том числе при осуществлении печати файла и копирования на съемные машинные носители информации);

- сведения об отправителе и получателях (кроме случаев вывода на печать файла и копирования на съемный машинный носитель информации) (в том числе идентификаторы учетных записей, адреса отправителя и получателя, сетевые адреса);

- способ передачи информации (передача файлов по сети, передача с использованием сервисов коммуникаций, размещение на веб-ресурсе, печать, копирование на съемный машинный носитель информации);

- дата и время передачи;

б) для файлов, хранящихся на общих сетевых ресурсах:

- содержимое файла, хранящегося на общем файловом ресурсе;

- сетевой адрес размещения файла на общем файловом ресурсе (включая каталог размещения);

- сведения о пользователе, разместившем файл.

5.1.3 Телекоммуникационное оборудование, используемое для передачи сетевого трафика, может использоваться для получения копии сетевого трафика, в составе которого имеются данные, необходимые для выявления признаков возможной утечки информации.

При выборе телекоммуникационного оборудования, которое может использоваться в качестве объекта контроля, следует учитывать, что телекоммуникационное оборудование должно обладать возможностью ответвления копии сетевого трафика на выделенный сетевой интерфейс, с которого она может быть передана для проведения анализа с целью выявления признаков возможной утечки информации из программной среды информационной (автоматизированной) системы.

Из копии сетевого трафика могут быть получены данные, позволяющие осуществлять контроль следующих каналов утечки информации:

- сервисов коммуникации;

- сервисов публикации на веб-ресурсах.

5.1.3.1 К данным, которые могут быть получены от телекоммуникационного оборудования и могут быть использованы для выявления признаков утечки информации, связанных с использованием сервисов коммуникации, относятся:

- содержание информации, передаваемой с использованием сервисов коммуникации, обнаруженной в копии сетевого трафика (в том числе содержание любых прикрепляемых файлов);

- сведения о сервисе коммуникации, с использованием которого передается информация;

- адреса отправителей и получателей информации;

- дата и время коммуникации.

Примечание – Если телекоммуникационное оборудование как объект контроля используется для выявления признаков утечки информации, связанных с использованием сервисов коммуникации, следует учитывать, что в сетевом трафике не всегда возможно обнаружить сообщения, передаваемые между пользователями информационной (автоматизированной) системы, так как такой обмен сообщениями происходит в рамках одного сервиса коммуникации, поэтому телекоммуникационное оборудование в основном используют для контроля сообщений, передаваемых с внутреннего сервера сервисов коммуникации информационной (автоматизированной) системы на внешние сервисы коммуникации. Например, сообщения, передаваемые с внутреннего почтового сервера организации на почтовые серверы сторонних организаций или на почтовые серверы общедоступных почтовых сервисов в сети Интернет. Для контроля сообщений, передаваемых между пользователями информационной (автоматизированной) системы в рамках одного внутреннего сервиса коммуникации, данные для выявления признаков возможной утечки информации целесообразно получать не от телекоммуникационного оборудования, а, например, от средств вычислительной техники, на которых установлены клиентские компоненты сервисов обмена почтовыми сообщениями или от программного обеспечения (агента), осуществляющего контроль действий пользователей.

5.1.3.2 К данным, которые могут быть получены от телекоммуникационного оборудования и могут быть использованы для выявления признаков утечки информации, связанных с использованием сервисов публикации на веб-ресурсах, относятся:

- содержимое файла, обнаруженного в копии сетевого трафика, связанного с использованием сервисов публикации на веб-ресурсах;

- сведения о сервисе, используемом для опубликования файла на веб-ресурсе;

- сетевой адрес средства вычислительной техники, с которого осуществляется опубликование файла на веб-ресурсе;

- дата и время коммуникации.

Примечание – К примерам публикации на веб-ресурсах, которые необходимо контролировать, можно отнести копирование файла в облачное хранилище в сети Интернет.

5.1.4 Средства вычислительной техники, на которых работают пользователи информационной (автоматизированной) системы, могут использоваться для получения от функционирующего на них программного обеспечения (агента), осуществляющего контроль действий пользователей, данных о действиях пользователей, которые могут приводить к утечке защищаемой информации.

Примечание – К примерам действий, которые могут привести к утечке защищаемой информации, можно отнести:

- передачу защищаемой информации с использованием клиентского программного обеспечения сервисов коммуникации;

- копирование файлов на съемные машинные носители информации;

- вывод информации из файлов на печать.

При контроле действий пользователей со средств вычислительной техники могут быть получены данные, позволяющие осуществлять контроль всех каналов утечки информации, указанных в п. 4.3.10, но только на конкретном средстве вычислительной техники пользователя.

5.1.4.1 К данным, которые могут быть получены при контроле действий пользователей на средствах вычислительной техники и могут быть использованы для выявления признаков утечки информации, связанных с использованием сервисов коммуникации, относятся:

- идентификатор учетной записи пользователя, работающего с сервисом коммуникации средства вычислительной техники;

Примечание – Идентификатором может являться логическое имя учетной записи пользователя, используемое им при осуществлении идентификации в информационной (автоматизированной) системе.

- идентификаторы учетных записей пользователей (электронные адреса), участвующих в коммуникации;

- содержание получаемой и передаваемой с использованием сервисов коммуникации информации (в том числе любых прикрепляемых файлов);

- идентификатор средства вычислительной техники, на котором используется сервис коммуникации;

- дата и время коммуникации.

5.1.4.2 К данным, которые могут быть получены при контроле действий пользователей на средствах вычислительной техники и могут быть использованы для выявления признаков утечки информации, связанных с использованием сервисов публикации на веб-ресурсах, относятся:

- содержимое файла, который опубликован на веб-ресурсе;

- сведения о сервисе, используемом для опубликования файла на веб-ресурсе;

- идентификатор учетной записи пользователя, осуществившего опубликование файла на веб-ресурсе;

- идентификатор средства вычислительной техники, с которого осуществлялось опубликование файла на веб-ресурсе;

- дата и время опубликования файла на веб-ресурсе.

5.1.4.3 К данным, которые могут быть получены при контроле действий пользователей на средствах вычислительной техники и могут быть использованы для выявления признаков утечки информации, связанных с использованием сервисов печати файлов, относятся:

- содержимое файла, выданного на печать;

- имя файла, выданного на печать;

- сведения об устройстве, которому выдано задание на печать;

- идентификатор учетной записи пользователя, осуществившего печать;

- идентификатор средства вычислительной техники, с которого осуществлялась печать;

- дата и время печати.

5.1.4.4 К данным, которые могут быть получены при контроле действий пользователей на средствах вычислительной техники и могут быть использованы для выявления признаков утечки информации, связанных с использованием съемных машинных носителей информации, относятся:

- содержимое файла, копируемого на съемный машинный носитель информации;

- сведения о съемном машинном носителе информации, на который осуществлялось копирование файла;

- идентификатор учетной записи пользователя, осуществившего копирование файла;

- идентификатор средства вычислительной техники, к которому был подключен съемный машинный носитель информации;

- дата и время копирования.

5.1.4.5 К данным, которые могут быть получены при контроле действий пользователей на средствах вычислительной техники и могут быть использованы для выяв-

ления признаков утечки информации, связанных с использованием общих сетевых ресурсов, относятся:

- содержимое файла, скопированного на общий файловый ресурс;

- сетевой адрес размещения файла на общем файловом ресурсе (включая каталог размещения);

- атрибуты файла;

- идентификатор учетной записи пользователя, осуществившего копирование файла на общий файловый ресурс;

- идентификатор средства вычислительной техники, с которого осуществлялось копирование файла на общий файловый ресурс;

- дата и время копирования файла.

5.1.5 Серверы информационной (автоматизированной) системы, на которых функционируют сервисы коммуникации, могут предоставлять данные для выявления признаков возможной утечки информации.

При контроле передачи информации на серверах сервисов коммуникации могут быть получены данные, позволяющие осуществлять контроль только канала утечки информации, связанного с использованием определенного сервиса коммуникации.

К данным, которые могут быть получены при контроле передачи информации на серверах сервисов коммуникации и могут быть использованы для выявления признаков утечки информации, связанных с использованием сервиса коммуникации, относятся:

- содержание информации, отправляемой и получаемой с использованием сервиса коммуникаций (в том числе любых прикрепляемых файлов);

- сведения о сервисе коммуникации, с использованием которого передается информация;

- адреса (идентификаторы) участников коммуникации;

- дата и время коммуникации.

5.1.6 Серверы информационной (автоматизированной) системы, на которых размещаются общие файловые ресурсы, имеют возможность предоставлять данные, позволяющие выявлять факты хранения на общих сетевых ресурсах файлов, содержащих информацию, которая в соответствии с установленными правилами хранения защищаемой информации не должна храниться на этих ресурсах.

От серверов информационной (автоматизированной) системы, на которых размещаются общие файловые ресурсы, могут быть получены данные, позволяющие

осуществлять контроль только канала утечки информации, связанного с использованием общих сетевых ресурсов.

К данным, которые могут быть получены от таких серверов и могут быть использованы для выявления признаков утечки информации, связанных с размещением файлов на общих сетевых ресурсах, относятся:

- содержимое файлов, хранящихся на общих сетевых ресурсах;

- сетевые адреса для размещения файлов на общих сетевых ресурсах;

- идентификаторы учетных записей пользователей, сохранявших файлы на общем файловом ресурсе.

5.1.7 Средства защиты информации, используемые на физических или логических границах информационной (автоматизированной) системы могут использоваться для раскрытия преобразованного (закрытого) сетевого трафика, который передается между узлами информационной (автоматизированной) системы и внешними информационными ресурсами в преобразованном (закрытом) виде, с целью анализа передаваемой информации на предмет правомерности такой передачи.

Примечание – Примером такого взаимодействия является использование межсетевого экрана для раскрытия закодированного веб-трафика, проходящего через межсетевой экран, и отправка копии раскрытого веб-трафика в средство защиты информации от утечки для анализа.

Каналы утечки информации, контролируемые с использованием средств защиты информации, используемых на физических или логических границах информационной (автоматизированной) системы, и состав данных, которые могут быть получены от них, совпадают соответственно с каналами утечки информации, контролируемые с использованием телекоммуникационного оборудования, и составом данных, которые могут быть получены от телекоммуникационного оборудования.

5.1.8 Во многих случаях одни и те же данные, необходимые для защиты информации от утечки из программной среды информационной (автоматизированной) системы могут быть получены от разных объектов контроля. Например, данные, которые могут быть получены с телекоммуникационного оборудования, могут быть получены и на средствах вычислительной техники при контроле действий пользователей, но в этом случае потребуется обеспечить контроль на всех средствах вычислительной техники в информационной (автоматизированной) системе. В связи с этим для обеспечения защиты информации от утечки требуется не обеспечить получение данных от всех видов объектов контроля, указанных в п. 5.1.2, а обеспечить получение данных, которые поз-

воляют контролировать, имеющиеся в информационной (автоматизированной) системе, каналы утечки информации.

5.2 Уровень взаимодействия с объектами контроля

5.2.1 Основными способами взаимодействия с объектами контроля являются:

- получение копии сетевого трафика**;**

- использование программного обеспечения (агента), осуществляющего контроль действий пользователей;

Примечание – Программное обеспечение (агент), осуществляющий контроль действий пользователей, является частью средства защиты информации от утечки, экземпляры которого устанавливаются на средства вычислительной техники с целью выявления нарушений установленных правил обработки (хранения и передачи) защищаемой информации.

- перехват сетевого трафика сервисов коммуникации.

5.2.2 Получение копии сетевого трафика используется, если в информационной (автоматизированной) системе в качестве объектов контроля используется телекоммуникационное оборудование, которое предоставляет копию сетевого трафика для анализа информации, передаваемой с использованием сервисов коммуникации, и передаваемых файлов. Также такой способ может применяться, если в информационной (автоматизированной) системе в качестве объектов контроля применяются средства защиты информации, используемые на физических или логических границах информационной (автоматизированной) системы, которые обеспечивают раскрытие преобразованного (закрытого) сетевого трафика и предоставляют копию раскрытого трафика для анализа информации, передаваемой с использованием сервисов коммуникации, и передаваемых файлов. Если в информационной (автоматизированной) системе отсутствует телекоммуникационное оборудование и средства защиты информации, имеющие возможность предоставлять копию сетевого трафика, то в информационной (автоматизированной) системе могут использоваться специализированные средства перехвата сетевого трафика, устанавливаемые в разрыв каналов связи.

5.2.3 Программное обеспечение (агент) используется на средствах вычислительной техники пользователей и обеспечивает получение от применяемого на средстве вычислительной техники программного обеспечения, в том числе средств защиты информации, данных о действиях пользователей, которые могут приводить к утечке защищаемой информации:

- вывод файла на печать;

- копирование файла на съемный машинный носитель информации;

- копирование файла на сетевой файловый ресурс;

- передача информации с использованием клиентского программного обеспечения компонентов сервисов коммуникации, установленных на его средстве вычислительной технике (в том числе с вложенными файлами);

- передача файлов с использованием клиентского программного обеспечения на различные сетевые файловые ресурсы (файловые хранилища, облачные сервисы для хранения файлов);

- отправка информации или передача файла с использованием веб-интерфейса сервиса коммуникации;

- опубликование файлов, содержащих защищаемую информацию, или отдельных его частей на сторонних файловых ресурсах.

5.2.4 Перехват сетевого трафика, поступающего от сервисов коммуникации, используется в случае, когда в качестве объектов контроля используются серверы, на которых функционируют сервисы коммуникации. Данный способ предусматривает перехват всей входящей и исходящей информации (в том числе с вложенными файлами) с целью анализа правомерности обмена такой информацией пользователями сервиса коммуникации.

5.3 Уровень выявления признаков возможной утечки

5.3.1 Выявление признаков возможной утечки предусматривает выполнение следующих действий:

- предварительная обработка информации, передаваемой с использованием сервисов коммуникации, и передаваемых файлов;

- анализ содержания информации, передаваемой с использованием сервисов коммуникации, и передаваемых файлов;

- проверка наличия признаков нарушения правил обработки (хранения и передачи) информации;

- реагирование на нарушение правил обработки информации.

5.3.2 Предварительная обработка информации, передаваемой с использованием сервисов коммуникации, и передаваемых файлов требуется для извлечения информации, которая в исходном виде не пригодна для проведения анализа. Например, такая предварительная обработка необходима, если требуется проводить анализ текстовой информации в следующих файлах:

- файлы, формат которых предусматривает хранение текстовой информации в сжатом виде;

- архивные файлы, в состав которых включены файлы, содержащие текстовую информацию;

- графические файлы, в которых содержится текстовая информация.

При организации защиты информации от утечки должна быть обеспечена возможность проведения предварительной обработки основных типов текстовых, архивных и графических файлов, используемых в информационной (автоматизированной) системе.

5.3.3 Анализ содержания информации, передаваемой с использованием сервисов коммуникации, и передаваемых файлов проводится с целью определения, осуществляется ли передача информации, в отношении которой требуется осуществлять контроль правомерности её копирования из информационной (автоматизированной) системы (в случае вывода файла на печать или его копирование на съемный машинный носитель информации), правомерности передачи такой информации другим пользователям информационной (автоматизированной) системы или за её пределы, а также правомерности её хранения на средствах вычислительной техники пользователей, серверах информационной (автоматизированной) системы и на общем файловом ресурсе.

Основными методами анализа являются:

- морфологический контентный анализ;

- распознавание документов по графическому образцу;

- распознавание цифровых отпечатков в документе;

- атрибутный анализ файлов.

Метод морфологического контентного анализа позволяет проводить анализ текстовой информации с целью определения вида информации по контенту. Метод морфологического контентного анализа основывается на применении морфологических словарей, включающих словарные формы лексем, с использованием которых может быть определен вид анализируемой информации.

Примечание – Основными видами информации по форме представления являются: текстовая, числовая, графическая, звуковая (акустическая), видеоинформация. Также виды информации можно классифицировать по уровню конфиденциальности, способам её кодирования и хранения.

Метод распознавания документов по графическому образцу применяется для графических объектов, содержащихся в файле.

Примечание – Под графическим объектом понимается изображение или фрагмент изображения в растровой графике, которое классифицируется как компонент определенного типа: круглая печать, фото банковской карты с лицевой стороны, скан-копия паспорта и т.п.

Метод распознавания документов по графическому образцу основан на сравнении анализируемого файла с предварительно созданным графическим образцом. Указанный метод должен позволять распознавать графические фрагменты в случае различных искажений графического образа, в том числе растяжения, поворота, перспективы, частичного отображения и наложения на другие объекты. Данный метод целесообразно использовать, если графический образец может свидетельствовать о виде информации, содержащейся в анализируемом файле.

Примечание – К примерам файлов, которые могут распознаваться по графическому образцу, можно отнести файл, содержащий скан-копию паспорта физического лица. При обнаружении такого файла, он сразу может быть определен как файл, содержащий персональные данные.

Метод распознавания по цифровым отпечаткам основывается на поиске в документе характерных фрагментов (блоков текста, графических элементов и иных фрагментов), для которых предварительно созданы представленные в цифровом виде отпечатки. Цифровой отпечаток представляет собой рассчитанную по определенному алгоритму контрольную сумму для фрагмента документа, содержащего защищаемую информацию.

Для разных типов фрагментов, таких как текстовый фрагмент, графический фрагмент, могут применяться разные алгоритмы вычисления контрольных сумм. В том числе алгоритм должен учитывать необходимость распознавания, если такой фрагмент был изменен. Такой метод должен позволять обнаруживать как оригинал документа, с которого были получены цифровые отпечатки, так и его фрагменты, которые в том числе могут быть включены в другие документы.

Атрибутный анализ файлов может применяться в случае, если вывод о правомерности передачи может быть сделан на основании атрибутов файла.

Примечание – К примерам атрибутов файлов относятся: наименование файла, расширение файла, специальные метки и иные атрибуты.

5.3.4 Выявление нарушений

Проверка наличия признаков нарушения правил обработки информации выполняется, если в результате анализа информации, передаваемой с использованием сервиса коммуникаций, или анализа содержимого файла выявлен вид информации, подлежащий защите информации от утечки.

Проверка наличия признаков нарушения правил обработки защищаемой информации доступа в первую очередь предусматривает контроль правомерности со стороны определенных пользователей осуществлять копирование определенных видов информации из информационной (автоматизированной) системы (в случае вывода файла на печать или его копирование на съемный машинный носитель информации), передачу такой информации другим пользователям информационной (автоматизированной) системы или за её пределы.

В случае проведения анализа содержимого файлов на серверах информационной (автоматизированной) системы, предназначенных для размещения общих сетевых ресурсов, осуществляется проверка правомерности хранения информации определенного вида на соответствующем общем файловом ресурсе.

5.3.5 Реагирование на нарушения правил обработки защищаемой информации

Способ реагирования на нарушение правила обработки защищаемой информации зависит от выявленного нарушения.

При выявлении фактов неправомерного копирования определенных видов информации из информационной (автоматизированной) системы (в случае вывода на печать или копирования информации на съемный машинный носитель информации), неправомерной передачи такой информации другим пользователям информационной (автоматизированной) системы или за её пределы могут реализовываться следующие способы реагирования:

- отправка уведомления о нарушении уполномоченному лицу (администратору безопасности, руководителю пользователя информационной (автоматизированной) системы, осуществившего передачу файла или информации, или иным лицам);

- отправка уведомления о нарушении пользователю информационной (автоматизированной) системы, осуществившему передачу файла или информации;

- регистрация события безопасности о нарушении в журнале событий безопасности;

- блокирование неправомерного копирования информации из информационной (автоматизированной) системы или неправомерной передачи такой информации (при наличии возможности);

- внесение изменений в передаваемую информацию (сообщение) и передача её получателям (при наличии возможности).

При выявлении нарушения правил хранения защищаемой информации на общих сетевых ресурсах должна обеспечиваться возможность реализации следующих способов реагирования:

- отправка уведомления о нарушении уполномоченному лицу (администратору безопасности или иным лицам);

- регистрация события безопасности о нарушении в журнале событий безопасности;

- перемещение файла в каталог, заданный пользователем, уполномоченным выполнять действия по защите информации от утечки.

- активные действия в отношении защищаемой информации (перемещение файла в каталог, заданный пользователем, уполномоченным выполнять действия по контролю утечки информации, запрет доступа к файлам и иные действия).

5.4 Уровень представления результатов выявления признаков возможной утечки

5.4.1 На уровне представления результатов выявления признаков возможной утечки осуществляется просмотр сведений о всех зарегистрированных событиях безопасности по результатам защиты информации от утечки. Событие безопасности содержат следующие сведения:

- уникальный идентификатор события безопасности;

- дата и время регистрации события безопасности;

- уровень критичности события безопасности;

- субъект, действия которого привели к регистрации события безопасности;

- действие, которое привело к регистрации события безопасности;

- условия, которые стали причиной регистрации события безопасности (обнаруженные ключевые слова или иные условия);

- объект контроля, на котором зарегистрировано событие безопасности в соответствии с политикой безопасности;

- содержимое фрагмента объекта контроля, которое привело к регистрации события безопасности в соответствии с политикой безопасности;

- способ передачи информации;

Примечание – Способ передачи информации может отсутствовать в составе представляемой информации в случае регистрации события безопасности, связанного с обнаружением неправомерной печати файла, неправомерного копирования файла на съемный машинный носитель информации и неправомерного хранения файла на общем файловом ресурсе.

- субъект, являющийся получателем.

Примечание – Сведения о субъекте, являющемся получателем, не указывается в случае регистрации события безопасности, связанного с обнаружением неправомерной печати файла, неправомерного копирования файла на съемный машинный носитель информации и неправомерного хранения файла на общем файловом ресурсе.

5.4.2 На уровне представления результатов выявления признаков возможной утечки формируются как минимум следующие отчеты:

- по зарегистрированным событиям безопасности;

- по пользователям.

5.4.2.1 Отчет по обнаруженным событиям безопасности представляет собой информацию в наглядном виде, которая демонстрирует:

- общее количество событий безопасности;

- распределение событий безопасности по различным показателям (уровню критичности, группам пользователей, видам информации).

Примечание – Формами представления отчета являются: таблица, список, граф связей и иные.

5.4.2.2 Отчет по пользователям должен представлять консолидированную информацию о нарушениях пользователя (пользователей), его (их) контактных данных, взаимодействиях с другими пользователями и иных действиях за определенный период времени:

- общие сведения о пользователе (например, ФИО, должность, электронный адрес и иная информация);

- сведения о событиях безопасности, которые зарегистрированы в результате действий пользователя;

- сведения о взаимодействиях пользователя;

- сведения о информации, переданной и (или) полученной пользователем;

- сведения о подключении съемных машинных носителей информации и выводе на них информации;

- сведения о выводе информации на печать;

- иные сведения.

5.4.3 Представление данных, в том числе о событиях безопасности, должно осуществляться как в текстовом, так и в графическом видах.

6 Рекомендации по применению средств защиты информации от утечки из программной среды информационной (автоматизированной) системы

6.1 При планировании применения в информационной (автоматизированной) системе средства защиты информации от утечки следует учитывать, что оно должно обеспечить возможность взаимодействия с объектами контроля, выбранными в соответствии с положениями подраздела 5.1, с учетом возможных каналов утечки информации.

Примечание – В первую очередь необходимо убедиться, что входящие в состав средства защиты информации от утечки программное обеспечение (агент), осуществляющее контроль действий пользователей, обеспечивает возможность выполнения своих функций в среде операционных систем, применяемых на средствах вычислительной техники, с которыми работают пользователи информационной (автоматизированной) системы. Также следует убедиться, что средство защиты информации от утечки обеспечивает возможность перехвата информации от тех сервисов коммуникации, которые применяются в конкретной информационной (автоматизированной) системе.

6.2 Применяемое в информационной (автоматизированной) системе средство защиты информации от утечки должно содержать функции безопасности, которые позволяют реализовать защиту информации от утечки из программной среды в соответствии с положениями раздела 5.

6.3 Для выявления событий безопасности, связанных с возможной утечкой информации, в средстве защиты информации от утечки должны быть определены объекты, содержащие защищаемую информацию, и политики безопасности информации.

Описание объектов, содержащих защищаемую информацию, производится для обеспечения возможности идентификации информации, отнесенной к видам информации, подлежащим контролю при выявлении признаков утечки информации. Описание объекта, как минимум, должно включать следующие характеристики:

- наименование объекта;
- признаки, с использованием которых идентифицируется объект;
- вид содержащейся информации объекта.

Примечание – В качестве объекта, содержащего защищаемую информацию, например, может быть определен файл пояснительной записки технического проекта, который содержит информацию о технических характеристиках объекта интеллектуальной собственности. В качестве признаков, с использованием которых может быть идентифицирован объект, может выступать составленный список лексем, которые содержатся в документе.

В политике безопасности информации определяют совокупность правил, которые характеризуются условиями, используемыми для выявления нарушения, и действиями, предпринимаемыми в случае обнаружения нарушения.

Примечание – В качестве условий, например, могут определяться недопустимые места хранения определенных объектов такой информации на общих сетевых ресурсах информационной (автоматизированной) системы, списки лиц, не имеющих право передавать или получать соответствующий вид информации, и иные условия. В качестве действий, которые предпринимаются в качестве реагирования на нарушение, могут быть определены следующие: перемещение файла с защищаемой информацией в определенный каталог, блокирование передачи информации с использованием сервиса коммуникации или иные действия.

6.4 Средство защиты информации от утечки должно обеспечивать возможность передачи информации о зарегистрированных событиях безопасности в систему управления событиями безопасности в качестве источника данных мониторинга в соответствии с ГОСТ Р 59547.

Примечание – В некоторых случаях (при необходимости) в средстве защиты информации от утечки можно предусмотреть передачу информации о зарегистрированных событиях безопасности в систему управления инцидентами в качестве возможного признака инцидента в соответствии с ГОСТ Р 59710.

6.5 При эксплуатации средств защиты информации от утечки необходимо обеспечить реализацию мер, направленных на предотвращение: потери данных о зарегистрированных событиях, связанных с обнаружением признаков утечки информации; выхода из строя средства защиты информации от утечки или его элементов, или иных сбоев, повлекших к нарушению защиты информации от утечки. В качестве таких мер необходимо рассматривать:

- предупреждение (сигнализация, индикация) уполномоченного пользователя средства защиты информации от утечки при заполнении установленной части (процент или фактическое значение) объема памяти для хранения данных;

- разделение архива данных на оперативный и долгосрочный;

- архивирование (резервное копирование) данных (части данных) на съемные машинные носители информации, в системы хранения данных, на специализированные устройства или на отдельные серверы.

6.6 Средство защиты информации от утечки может содержать в своем составе функцию инспекции файловых ресурсов.

Примечание – Инспекция файловых ресурсов относится к уровню взаимодействия с серверами файловых ресурсов как объектов контроля.

Инспекция файловых ресурсов применяется в информационной (автоматизированной) системе для выявления нарушений установленных правил хранения защищаемой информации, которые могут привести к её утечке. Данный способ предусматривает сканирование информационной (автоматизированной) системы с целью выявления имеющихся в ней общих сетевых ресурсов и анализа содержимого размещенных на этих ресурсах файлов для выявления нарушений установленных правил хранения защищаемой информации.

Примечание – Нарушением правил хранения считается факт обнаружения на сетевом файловом ресурсе файла, содержимое которого в соответствии с установленными правилами хранения защищаемой информации, не предназначено для хранения на данном сетевом файловом ресурсе.

6.7 Средство защиты информации от утечки может содержать в своем составе функцию поведенческого анализа пользователей информационной (автоматизированной) системы. Функция поведенческого анализа пользователей информационной (автоматизированной) системы может быть реализована в виде отдельного средства.

Примечание – Функция поведенческого анализа основывается на данных, собираемых средством защиты информации от утечки и относится к уровню представления результатов выявления признаков возможной утечки.

Результаты поведенческого анализа целесообразно учитывать при формировании политик безопасности информации, в соответствии с которыми средство защиты информации от утечки осуществляет обнаружение событий безопасности, связанных с утечкой информации.

Примечание – В некоторых крупных организациях, в которых перемещается большой объем информации между собственными подразделениями организации и сторонними организациями, для защиты информации от утечки целесообразно применять человеко-ориентированный подход. Для этого пользователей, в процессе работы которых обнаружены признаки аномального поведения, объединяют по различным признакам в группы контроля, за которыми в дальнейшем отдельно ведется наблюдение.

7 Рекомендации по защите данных, собираемых и формируемых в рамках мероприятий по защите информации от утечки из программной среды информационной (автоматизированной) системы

7.1 В информационной (автоматизированной) системе должна осуществляться защита данных, собираемых и формируемых в рамках мероприятий по защите от утечки информации.

К данным, собираемым в рамках мероприятий по защите информации от утечки, для которых требуется защита информации, относятся:

- файлы, содержащие оригиналы документов, используемые для создания графических образцов и цифровых отпечатков;

- получаемая для проведения анализа на предмет утечки информация из информационной (автоматизированной) системы.

К данным, формируемым в рамках мероприятий по защите информации от утечки, для которых требуется защита информации, относятся:

- политики безопасности, настроенные для применения метода морфологического контентного анализа;

- графические образцы документов, формируемые для применения метода распознавания документов по графическому образцу;

- события безопасности, связанные с обнаружением признаков утечки информации;

- отчеты, формируемые в процессе функционирования средства защиты информации от утечки.

7.2 Для защиты данных, собираемых и формируемых в рамках мероприятий по защите информации от утечки, реализуют следующие меры защиты информации:

- идентификация и аутентификация пользователей, осуществляющих доступ к данным, собираемым и формируемым в рамках мероприятий по защите информации от утечки;

- управление идентификаторами пользователей, осуществляющих доступ к данным, собираемым и формируемым в рамках мероприятий по защите информации от утечки;

- управление средствами аутентификации (аутентификационной информацией) пользователей, осуществляющих доступ к данным, собираемым и формируемым в рамках мероприятий по защите информации от утечки;

- управление учетными записями пользователей, осуществляющих доступ к данным, собираемым и формируемым в рамках мероприятий по защите информации от утечки;

- защита аутентификационной информации пользователей, осуществляющих доступ к данным, собираемым и формируемым в рамках мероприятий по защите информации от утечки, в процессе её ввода, для аутентификации от возможного использования лицами, не имеющими на это полномочий;

- управление доступом пользователей к данным, собираемым и формируемым в рамках мероприятий по защите информации от утечки;

- ограничение неуспешных попыток получения доступа пользователей при доступе к данным, собираемым и формируемым в рамках мероприятий по защите информации от утечки;

- регистрация событий безопасности, связанных с доступом к данным, собираемым и формируемым в рамках мероприятий по защите информации от утечки;

- определение типов съемных машинных носителей информации, на которые разрешен вывод данных, собираемых и формируемых в рамках мероприятий по защите информации от утечки;

- определение категорий пользователей, которым предоставлены полномочия выводить данные, собираемые и формируемые в рамках мероприятий по защите информации от утечки, на съемные машинные носители информации;

- контроль вывода данных, собираемых и формируемых в рамках мероприятий по защите информации от утечки, на съемные машинные носители информации.

Должна обеспечиваться регистрация следующих типов событий безопасности, связанных с доступом к данным, собираемым и формируемым в рамках мероприятий по защите информации от утечки, которые установлены в ГОСТ Р 59548:

- прохождение идентификации и аутентификации субъекта доступа;

- управление учетными записями пользователей;

- управление средствами аутентификации;

- управление атрибутами доступа;

- получение доступа к защищаемой информации;

- подключение съемных машинных носителей информации;

- вывод данных, собираемых и формируемых в рамках мероприятий по защите информации от утечки, на съемные машинные носители информации;

- управление (администрирование) функциями безопасности;

- управление журналами событий безопасности.

Дополнительно должны регистрироваться все действия, которые средство защиты информации от утечки выполняет в отношении полученной для анализа защищаемая информация информационной (автоматизированной) системы.

7.3 Полученная для анализа защищаемая информация информационной (автоматизированной) системы, может сохраняться в каталогах или базах данных, доступ к которым ограничен только допущенными к такой информации лицами, определенными

владельцем информации или оператором информационной (автоматизированной) системы.

7.4 Защита данных, собираемых и формируемых в процессе функционирования средства защиты информации от утечки, осуществляется исходя из классов защищенности (категорий значимости, уровней защищенности информации) информационной (автоматизированной) системы, в которых применяется средство защиты информации от утечки.

7.5 Результаты выявленных событий безопасности, связанных с утечкой защищаемой информации, могут использоваться для:

- проведения служебных расследований в отношении пользователей информационной (автоматизированной) системы, в процессе работы которых обнаружены признаки аномального поведения и возможной утечки информации;

П р и м е ч а н и я Проведение служебных расследований может быть регламентировано нормативными правовыми актами, принятыми в организации.

- передачи результатов служебных расследований в уполномоченные федеральные органы исполнительной власти, в случае наличия состава правонарушения.

П р и м е ч а н и е – Порядок привлечения к ответственности, в случае наличия состава правонарушения, установлен законодательством Российской Федерации. Для того, чтобы данные от средства защиты информации от утечки были приняты в качестве доказательств правонарушения, необходимо обеспечить соответствие таких данных требованиям законодательства Российской Федерации.

Приложение А
(справочное)
Состав организаций, осуществляющих экспертную поддержку стандарта при его разработке

Экспертную поддержку стандарта при его разработке осуществляли следующие организации:

1. Общество с ограниченной ответственностью «Лаборатория ИнфоВотч».
2. Общество с ограниченной ответственностью «СЕРЧИНФОРМ».
3. Общество с ограниченной ответственностью «АТОМ БЕЗОПАСНОСТЬ».
4. Автономная некоммерческая организация «Национальный технологический центр цифровой криптографии».

УДК 004.622:006.354 ОКС 35.020

Ключевые слова: защита информации, утечка информации из программной среды, средства защиты информации от утечки