deiteriy compliance

Особенности реализации требований ГОСТ 57580.1 с учетом размера инфраструктуры и ограниченных ресурсов

АЛЕКСАНДР ИВАНЦОВ | DEITERIY COMPLIANCE | НАУФОР: ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ | 2023

Александр Иванцов

Старший инженер по защите информации
Deiteriy Compliance
aleksandr.ivantsov@deiteriy.com
+7 (911) 785-97-96

Уникальность требований по противодействию утечкам информации

- В ГОСТ 57580.1 впервые появились обязательные требования по противодействию утечкам информации – 5 процесс.

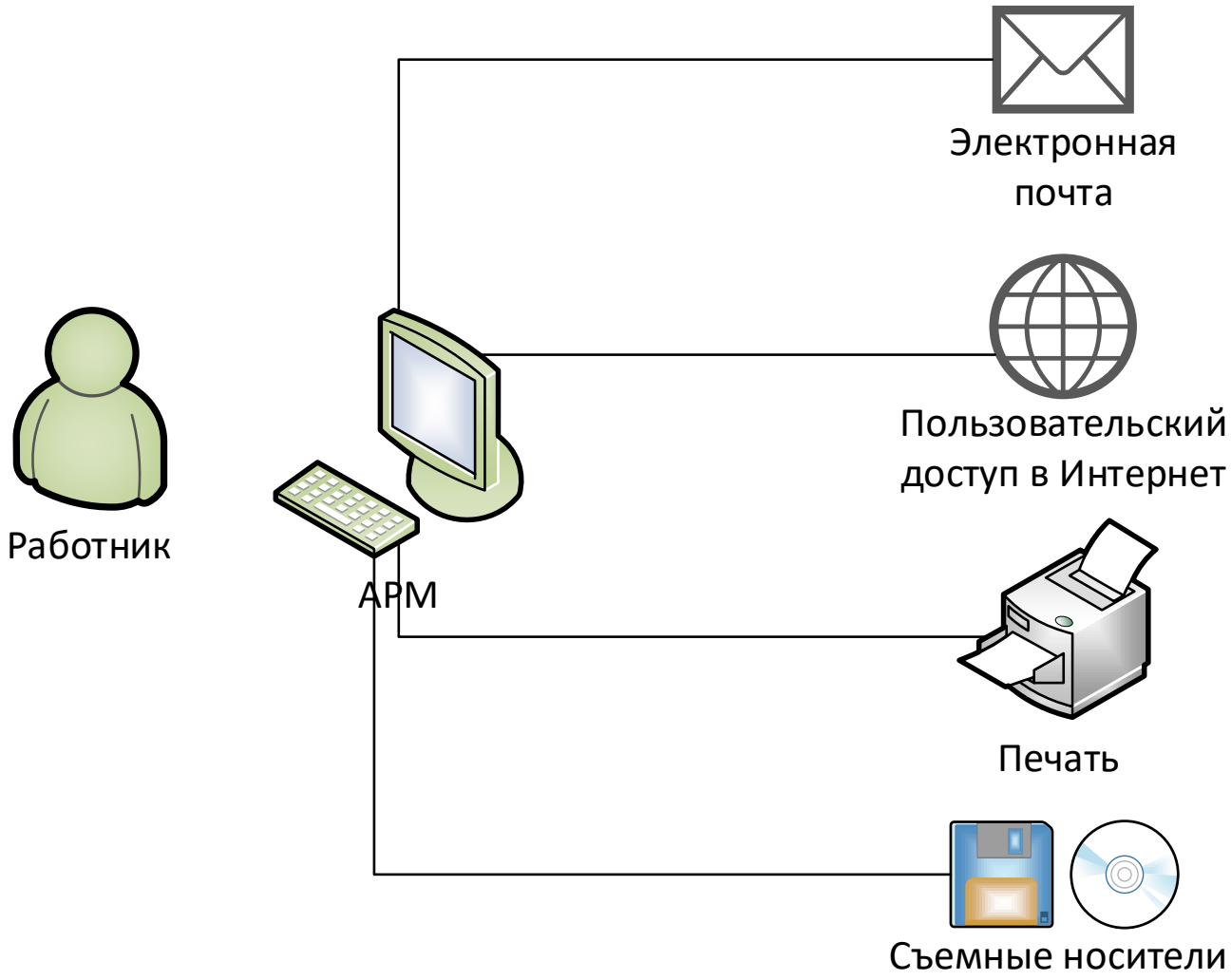
- Данный процесс – один из самых проблемных даже в крупных организациях, не говоря уже о небольших.

ГОСТ 57580.1: риск-ориентированный подход к реализации защитных мер

- Меры защиты из ГОСТ 57580.1 имеют под собой исходный риск, который не всегда закрывается исключительно специализированным средством защиты.

- В ГОСТ 57580.1 есть возможность обосновать применение компенсирующих мер защиты вместо определенных в требованиях стандарта.

ГОСТ 57580.1: каналы утечки данных



Контентный анализ

Мера	Содержание
ПУИ.5	Контентный анализ передаваемой информации по протоколам исходящего почтового обмена.
ПУИ.11	Контентный анализ информации, передаваемой в сеть Интернет с использованием информационной инфраструктуры финансовой организации.
ПУИ.15	Контентный анализ информации, выводимой на печать.
ПУИ.17	Контентный анализ информации, копируемой на переносные (отчуждаемые) носители информации.
ПУИ.31	Регистрация результатов выполнения контентного анализа информации, предусмотренного мерами ПУИ.5, ПУИ.11, ПУИ.15, ПУИ.17.

- Требования не применимы только если канал полностью исключен.

Электронная почта

Мера	Содержание	Реализация
ПУИ.6	Ведение единого архива электронных сообщений с архивным доступом на срок не менее 6 месяцев и оперативным доступом не срок не менее 1 месяца.	Резервирование
ПУИ.8	Ограничение на перечень протоколов сетевого взаимодействия, используемых для осуществления передачи сообщений электронной почты.	Настройки почтового сервера Межсетевой экран
ПУИ.9	Ограничение на перечень форматов файлов данных, разрешенных к передаче в качестве вложений в сообщениях электронной почты.	Настройки почтового сервера
ПУИ.10	Ограничение на размеры файлов данных, передаваемых в качестве вложений в сообщениях электронной почты.	Настройки почтового сервера

Доступ в Интернет

Мера	Содержание	Реализация
ПУИ.12	Классификация ресурсов сети Интернет с целью блокировки доступа к сайтам или типам сайтов, запрещенных к использованию в соответствии с установленными правилами.	Межсетевой экран
ПУИ.13	Ограничение на перечень протоколов сетевого взаимодействия и сетевых портов, используемых при осуществлении взаимодействия с сетью Интернет.	Межсетевой экран
ПУИ.14	Запрет хранения и обработки информации конфиденциального характера на объектах доступа, размещенных в вычислительных сетях финансовой организации, подключенных к сети Интернет.	Терминальный сервер
ПУИ.29	Регистрация операций, связанных с осуществлением доступа работниками финансовой организации к ресурсам сети Интернет.	Межсетевой экран

Печать

Мера	Содержание	Реализация
ПУИ.30	Регистрация фактов вывода информации на печать.	ОС

Съемные носители

Мера	Содержание	Реализация
ПУИ.18	Блокирование неразрешенных к использованию портов ввода-вывода информации СВТ	ОС Device Lock
ПУИ.19	Блокирование возможности использования незарегистрированных (неразрешенных к использованию) переносных (отчуждаемых) носителей информации в информационной инфраструктуре финансовой организации	Средства антивирусной защиты Device Lock
ПУИ.28	Регистрация использования разблокированных портов ввода-вывода информации СВТ	ОС

Нужна ли DLP?

- Мер защиты, не связанных с использованием системы DLP, достаточно для закрытия большинства требований 5 процесса ГОСТ 57580.1.

Оценка	Без DLP	С внедренной DLP
Выбор мер защиты	0,82	1

Мониторинг событий – нужна ли SIEM?

- 2 способа реализации:
  - Ежедневно смотреть все события на всех компонентах информационной инфраструктуры.
  - Настроить правила корреляции и отправку оповещений.

Оценка	Без SIEM	С внедренной SIEM
Выбор мер защиты	0,6	1

Мониторинг событий

- Хорошо реализованный мониторинг также повлияет на возможность контроля ИБ на всех уровнях информационной инфраструктуры.

- Мониторинг – важный инструмент, позволяющий внедрять компенсационные меры.

SIEM – это дорого

- Смотрим на opensource:
  - ELK
  - Wazuh
  - Opensearch

- Возможно ли настроить оповещения на события в ПО и на срабатывания средств защиты?

Безопасная разработка

Имеется один разработчик. Как выполнять анализ кода на уязвимости?

- Code review – обучить специалиста по ИБ или администратора.
- Внедрить инструменты для безопасной разработки.
- Обратиться к тому, кто умеет.

Способы реализации

- Своими силами.
  - Ресурс – время работников.

- Реализация доступными инструментами, в том числе внедрение opensource-решений.

- Покупка готовых решений.

- Аутсорсинг.
  - Ресурс – деньги

Спасибо за внимание!

Александр Иванцов

Старший инженер по защите информации
Deiteriy Compliance
aleksandr.ivantsov@deiteriy.com
+7 (911) 785-97-96