Рекомендации по предотвращению утечки информации

1. Меры защиты информации

С целью предотвращения реализации угроз безопасности информации, связанных с утечкой защищаемой информации, необходимо принять следующие дополнительные меры защиты информации:

1. Запретить возможность размещения защищаемой информации в облачных сервисах, а также ее передачу через мессенджеры, Google Docs и другие сервисы.

2. Обеспечить контроль содержимого файлов, передаваемых посредством электронной почты, с применением систем предотвращения утечки информации (DLP-систем).

3. Провести аудит подключаемых к автоматизированным рабочим местам съемных машинных носителей информации и анализ записываемой на них информации (например, реализовать технологию «теневого копирования»).

4. Обеспечить отслеживание геолокации пользователей, осуществляющих удаленное подключение к информационной инфраструктуре.

5. Обеспечить мониторинг информационных ресурсов, расположенных в сети «Интернет», на предмет выявления утечек защищаемой информации ведомства (организации), и оперативное принятие мер по предотвращению ущерба такой утечки.

6. В случае выявления фактов утечки защищаемой информации в ведомстве (организации) необходимо выполнить следующие первоочередные мероприятия:

сменить учетные данные пользователей и администраторов информационных систем и реализовать двухфакторную аутентификацию (при возможности);

при утечке конфигурационной информации обеспечить мониторинг запросов на доступ к информационной инфраструктуре и оперативное реагирование на попытки несанкционированного доступа к ней.

7. В связи с прекращением поддержки операционных систем Microsoft Windows 7 и Microsoft Windows Server 2008 R2 и, соответственно, прекращением выпуска обновлений безопасности, необходимо провести мероприятия по выводу из эксплуатации данных операционных систем и замене их на актуальные, поддерживаемые разработчиком.

8. Рассмотреть отечественные альтернативы зарубежным поставщикам информации об индикаторах компрометации (IoC).

9. Обеспечить резервное копирование в изолированном сегменте системы. Провести тестирование восстановления из резервных копий. Доступ к этому сегменту должен быть минимизирован по белым спискам с запретом доступа из сети «Интернет».

10. Запретить отправку событий безопасности во внешние иностранные сервисы (Cloud SIEM, Cloud EDR, SOC и MDR).

11. Не использовать репозиторий хранения кода github для работы над собственными проектами. При необходимости развернуть свой изолированный сервер репозиториев.

12. Исключить применение сервисов обмена текстом, таких, как и его аналогов для передачи чувствительной информации, например, конфигурационных файлов, исходного программного кода при необходимости развернуть частный сервис обмена текстом (например, privatebin).

2. Меры защиты информации от угроз безопасности информации, реализуемых внутренними нарушителями

1. Отключить удаленный доступ к критичным системам и сетям, предоставляя его только по согласованной заявке и на короткий интервал времени для выполнения работ.

2. Реализовать запись действий привилегированного пользователя, включая КОР сессии (при возможности).

3. Организовать ролевую модель доступа пользователей таким образом, чтобы тот, кто имеет административный доступ к системам, не имел прав на удаление и модификацию резервных копий баз данных.

4. Внести изменения в процедуру проведения обновлений программного обеспечения. В особый период должны проводиться только критические обновления, прошедшие тщательную проверку безопасности.

3.Меры защиты информации от угроз безопасности информации, реализуемых уволенные работники, выполнявшие функции администраторов информационных систем или администраторов безопасности

С целью предотвращения несанкционированного распространения уволенными администраторами информационных систем защищаемой

информации рекомендуется дополнительно реализовать следующие организационные и технические меры:

1. после получения информации о намерениях работника уволиться необходимо обеспечить мониторинг его действий в информационной системе, обратив особое внимание на факты копирования (переноса) информации, содержащейся в информационной системе на съемные носители информации, передачи электронных документов по электронной почте, установки и запуска стороннего программного обеспечения;

2. удалить учетные записи уволенного администратора информационной системы, в том числе учетные записи для доступа к электронной почте и иным сегментам информационной системы;

3. после увольнения работника провести инвентаризацию программного обеспечения и данных, содержащихся на его автоматизированном рабочем месте, на предмет наличия стороннего программного обеспечения и каналов удаленного доступа и удалить неиспользуемое в работе программное обеспечение;

4. определить перечень сегментов информационной системы (сервера, контроллер доменов, системы управления базами данных сетевое оборудование, средства защиты информации и другие сегменты), к которым уволенный администратор имел доступ и обеспечить внеплановую смену паролей других администраторов, имеющих доступ к указанным сегментам;

5. до смены паролей других администраторов информационной системы обеспечить мониторинг удаленного доступа к этим сегментам информационной системы (при его наличии).