Министерство образования и науки Российской Федерации
Санкт-Петербургский политехнический университет Петра Великого
—
Институт компьютерных наук и технологий
Кафедра «Информационная безопасность компьютерных систем»

ОТЧЕТ
ПО ЛАБОРАТОРНОЙ РАБОТЕ № 1

РАЗРАБОТКА ПОЛИТИКИ БЕЗОПАСНОСТИ
по дисциплине «Модели безопасности компьютерных систем»

Выполнил
студент гр. 33508/3 Проценко Е.Г.
_____

Руководитель Жуковский Е.В.
_____

Санкт-Петербург
2016

ЦЕЛЬ РАБОТЫ

Разработать политику шифрования данных в государственной организации.

РЕЗУЛЬТАТЫ РАБОТЫ

Виды организация являющихся государственными:

-военные организации;

-научные организации;

-правоохранительные организации;

-образовательные организации;

-организации в сфере здравоохранения.

1 Цель этой политики заключается в предоставлении руководства, которое устанавливает правила использования шифрования для обеспечения защиты конфиденциальной, важной и критичной информации, предотвращения актов кражи, искажения, компрометации данных.

2 Эта политика применяется ко всему программному обеспечению, используемому в государственных организациях, и касается всех сотрудников организации, включая отдел по информационной безопасности и отдел по разработке алгоритмов шифрования.

3 Вся информация организации должна храниться в зашифрованном виде. При передаче информации между двумя узлами сети должно использоваться ассиметричное шифрование.

4 Таким образом все сотрудники обязаны пользоваться только сертифицированным программным обеспечением, которое было предложено к использованию отделом по информационной безопасности.

5 Все программное обеспечение, настройка сети предоставляется системным администратором. Так же они обязаны следить за поддержкой актуальной версии программ, проводя обновление еженедельно.

6 Все программное обеспечение, котором пользуются сотрудники должно быть проверено и сертифицировано отделом по информационной безопасности.

7 Правила использования шифрования:

-электронная подпись документов проводится только при помощи отечественных криптопровайдеров;

-для подключения к внешним офисам и офисам используется VPN;

-подключение в интернет только по HTTPS;

-передача данных по сети интернет только с использованием криптографических протоколов SSH, TLS;

-общение между сотрудниками производится только с использованием приложений со сквозным шифрованием. Например, Telegram;

-хранение паролей производится в закрытом виде: хранение не самого пароля, а его хэша;

-шифрование диска производится при помощи программы BitLocker.

8 Специалист по информационной безопасности должен следить за соответствием этой политики с помощью различных методов:

-периодической проверкой оборудования, которым пользуются сотрудники;

-проверка программного обеспечения на наличие уязвимостей;

-следить за логами приложений;

-обратная связь с владельцем политики;

-проверка трафика.

9 Все программное обеспечение, настройка сети предоставляется системным администратором. Так же они обязаны следить за поддержкой актуальной версии программ, проводя обновление еженедельно.

10 Все программное обеспечение, котором пользуются сотрудники должно быть проверено и сертифицировано отделом по информационной безопасности.

11 Специалист по информационной безопасности должен следить за соответствием этой политики с помощью различных методов:

-периодической проверкой оборудования, которым пользуются сотрудники;

-проверка программного обеспечения на наличие уязвимостей;

-следить за логами приложений;

-обратная связь с владельцем политики;

-проверка трафика.

12 Требования к алгоритмам для разработчиков:

- Симметричные алгоритмы шифрования должны соответствовать AES-совместимым или частично AES-совместимым шифрам в соответствии с каталогом шифров IETF/IRTF.
- Алгоритмы должны соответствовать стандартам NIST.
- Использование криптографического алгоритма RSA настоятельно рекомендуется для ассиметричного шифрования.
- Использование хэш алгоритмов [1]:

а) **SHA-1**: Государственные организации должны прекратить использование SHA-1 для создания цифровых подписей, хэширования и хранения паролей и в других приложениях, которые требуют использование хэш-функций. Государственные организации могут использовать SHA-1 только для подтверждения старых цифровых подписей, для создания и проверки подлинности ключей аутентификации, как механизм

проверки целостности информации при передаче и хранении в ненадежней среде, для генерации случайных битов/чисел,

б) **SHA-2 (например, *SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 и SHA-512/256*):** Государственные организации могут использовать эти хэш-функции для всех приложений, которые используют алгоритмы хэширования. Для приложений и создания протоколов рекомендуется использовать хотя бы SHA-256 или лучше,

в) **SHA-3:** Государственные организации могут использовать эти хэш-функции для всех приложений, которые используют алгоритмы хэширования.

- Генерация ключей:

а) Криптографические ключи должны создаваться и храниться используя безопасные способы, которые предотвращают возможность потери, кражи, компрометации. Например, вместо хранения открытого ключа, хранится его хэш.

б) Для генерации ключей должен использоваться генератор случайных чисел, удовлетворяющий международным стандартам.

13 Все работники при исполнении своих должностных обязанностей должны использовать только программное обеспечение, удовлетворяющее политике и следить за выполнением других пунктов политики.

14 Любые исключения из политики должны быть обсуждены с отделом по информационной безопасности и подтверждены.

15 Работник нарушивший данную политику может быть подвергнут дисциплинарному высказыванию, вплоть до увольнения.

ВЫВОД

Я познакомился с важным элементом, обеспечивающим безопасность, политикой безопасности. Ознакомился со структурой документов: с тем, о чем политика, и для кого.

Познакомился с теми пунктами политики безопасности, которые должны быть в некоторой организации. Рассмотрел, как политики касается разных сотрудников организации: от обычных сотрудников до разработчиков криптографических алгоритмов.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. http://csrc.nist.gov/groups/ST/hash/policy.html
2. https://www.sans.org/security-resources/policies/general/pdf/acceptable-encryption-policy
3. https://tools.ietf.org/html/draft-irtf-cfrg-cipher-catalog-01#section-3.1
4. https://www.wikipedia.org/