

РАЗРАБОТКА МЕТОДИЧЕСКИХ РЕКОМЕНДАЦИЙ ПО РЕЗУЛЬТАТАМ АУДИТА ИНФРАСТРУКТУРЫ ОТКРЫТЫХ КЛЮЧЕЙ

Арзуманян Эрик Араикович

магистрант, Московский институт электронной техники, РФ, г. Москва

Методические рекомендации давались по результатам аудита инфраструктуры открытых ключей компании АО «НК «НЕФТЕГАЗ»

На данный момент в АО «НК «НЕФТЕГАЗ» отсутствует собственный УЦ, а также нет производственной необходимости в его внедрении. АО НК «НЕФТЕГАЗ» сотрудничает с УЦ Такском в части выпуска усиленных квалифицированных ЭП. В течение года в среднем выпускаются 30 сертификатов. В перспективе это число может вырасти. При учете дочерних и связанных обществ АО «НК «НЕФТЕГАЗ» количество может возрасти до 300 сертификатов.

Во всех ситуациях, специально не предусмотренных Федеральными законами или иными нормативными правовыми актами, работники АО НК «НЕФТЕГАЗ» применяют простую ЭП.

ЭП в АО «НК «НЕФТЕГАЗ» используется для решения следующих задач:

- Обеспечение юридически значимого электронного документооборота в информационной системе 1С;
- Возможность участия в тендерах, аукционах, закупках и котировках на электронных площадках;
- Создание VPN-соединений для установления удаленного доступа.

В настоящее время в АО «НК «НЕФТЕГАЗ» работа с ЭП регламентируется в документе «Положение об ЭП». «Положение об ЭП», утвержденное приказом АО «НК «НЕФТЕГАЗ» от 14 октября 2021 г. №34, является локальным нормативным актом постоянного действия. Область действия данного документа распространяется на всех сотрудников компании, использующих ЭП при исполнении своих должностных обязанностей. В нем перечислены общие положения, порядок использования и выдачи ЭП и меры обеспечения безопасности. По предоставленной информации часть требований и рекомендаций данного положения не исполняется.

Другие документы или инструкции, описывающие взаимодействие сотрудников с ЭП в компании, отсутствуют [1].

Сведения о нормативно-методических документах, на основании которых разработан перечень документов, необходимых для организации работы с сертификатами и ключами КЭП, приведен в таблице (см. Таблица 1) [2]:

Таблица 1.

Нормативно-методические документы, на основании которых разработан перечень документов, необходимых для организации работы с сертификатами и ключами КЭП

№ п/п	Наименование документа
1	Федеральный закон (ФЗ) от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи».
2	«Требования к защите персональных данных при их обработке в информационных системах персональных данных», утвержденные постановлением Правительства

№ п/п	Наименование документа
	Российской Федерации от 01.11.2012 № 1119.
3	«Требования к средствам электронной подписи» и «Требования к средствам удостоверяющего центра», утвержденные приказом ФСБ России от 27 декабря 2011 г. № 796.
4	Руководящий документ ФСБ России от 31.01.2014 № 149/7/1/3-58 «О порядке перехода к использованию новых стандартов ЭЦП и функции хэширования».
5	Приказ ФСБ РФ от 9 февраля 2005 г. N 66 "Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)" (далее - Приказ ФСБ от 09.02.2005 N 66)
6	Приказ ФАПСИ от 13 июня 2001 г. № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»
7	ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».
8	ГОСТ 2.106-96. «Межгосударственный стандарт. Единая система конструкторской документации. Текстовые документы».
9	ГОСТ 2.105-2019. «Межгосударственный стандарт. Единая система конструкторской документации. Общие требования к текстовым документам».
10	ГОСТ 34.201-89. «Государственный стандарт Союза ССР. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем».
11	ГОСТ 34.602-89. «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы».
12	ГОСТ 34.601-90. «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы-стадии создания».
13	ГОСТ 34.603-92. «Информационная технология. Виды испытаний автоматизированных систем».
14	ГОСТ 34.003-90. «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения».
15	РД 50-682-89. «Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Общие положения».

Согласно пункту 26 Приказа ФАПСИ от 13.06.2001 N 152 «Об утверждении Инструкции» для разработки и осуществления мероприятий по организации и обеспечению безопасности хранения, обработки и передачи с использованием СКЗИ конфиденциальной информации лицензиат ФАПСИ создает один или несколько органов криптографической защиты [3].

На основании этого в компании рекомендуется разработать и внедрить следующие документы:

- Приказ о назначении администратора информационной безопасности;
- Инструкция администратора информационной безопасности.

Также согласно пункту 7 Приказа ФАПСИ от 13.06.2001 N 152 «Об утверждении Инструкции» орган криптографической защиты осуществляет:

- Проверку готовности обладателей конфиденциальной информации к самостоятельному использованию СКЗИ и составление заключений о возможности эксплуатации СКЗИ (с указанием типа и номеров используемых СКЗИ, номеров аппаратных, программных и аппаратно-программных средств, где установлены или к которым подключены СКЗИ, с указанием также номеров печатей (пломб), которыми опечатаны (опломбированы) технические средства, включая СКЗИ, и результатов проверки функционирования

- СКЗИ). Готовность обладателей конфиденциальной информации к самостоятельному использованию подтверждается подписанным актом о вводе в эксплуатацию СКЗИ.
- Разработку мероприятий по обеспечению функционирования и безопасности, применяемых СКЗИ в соответствии с условиями выданных на них сертификатов, а также в соответствии с эксплуатационной и технической документацией к этим средствам.
 - Обучение лиц, использующих СКЗИ, правилам работы с ними. Обучение лиц, использующих СКЗИ подтверждается подписанным актом об ознакомлении с Инструкцией пользователя ЭП.
 - Поэкземплярный учет используемых СКЗИ, эксплуатационной и технической документации к ним.
 - Учет обслуживаемых обладателей конфиденциальной информации, а также физических лиц, непосредственно допущенных к работе с СКЗИ.

Согласно пункту 26 Приказа ФАПСИ от 13.06.2001 N 152 «Об утверждении Инструкции» используемые или хранимые СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземплярному учету.

Согласно пункту 48 Приказа ФСБ от 09.02.2005 N 66 СКЗИ и их опытные образцы подлежат поэкземплярному учету с использованием индексов или условных наименований и регистрационных номеров.

На основании этих пунктов в АО НК «НЕФГАЗ» рекомендуется разработать и внедрить следующие документы:

- Приказ о порядке хранения и эксплуатации средств криптографической защиты информации;
- Приказ о назначения пользователя ЭП;
- Форма перечня сотрудников, допущенных к работе с СКЗИ;
- Форма журнала поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов;
- Инструкция по реагированию на инциденты информационной безопасности;
- Инструкция пользователя ЭП.

Согласно пункту 46 Приказа ФАПСИ от 13.06.2001 N 152 «Об утверждении Инструкции» ключевые документы уничтожаются либо пользователями СКЗИ, либо сотрудниками органа криптографической защиты под расписку в соответствующих журналах поэкземплярного учета, а уничтожение большого объема ключевых документов может быть оформлено актом.

На основании этого в компании рекомендуется разработать и внедрить следующий документ:

- Форма акта об уничтожении криптографических ключей и ключевых документов.

Список литературы:

1. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности: учеб. пособие для вузов. – М.: Горячая линия – Телеком, 2006. – 544 с.
2. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения: ГОСТ Р 51275-99. - Введ. 2000-01-01. – М.: Изд-во стандартов, 1999. – 11 с.
3. Об информации, информационных технологиях и о защите информации: федер. закон: [принят Гос. Думой 8 июля 2006 г.: одобрен Советом Федерации 14 июля 2006 г.]. - URL: <http://www.rg.ru/gazeta/rg/2006/07/29> (дата обращения: 18.04.2017).