SFB LAB

Дистанционная подпись Характеристика внутреннего нарушителя

Аристархов И.В.

Дистанционная подпись

АУЦ, аккредитованные по требованиям предусмотренным частью 3.1 статьи 16 Федерального закона «Об ЭП», для реализации предусмотренных частью 2.2 статьи 15 Федерального закона «Об ЭП» вправе осуществлять:

- хранение ключа ЭП пользователя, с обеспечением его защиты от компрометации и НСД;

  уточненное требование - исключение возможности доступа работников АУЦ к ключам электронных подписей заявителей

- создание ЭП по поручению пользователя с использованием средств ЭП, имеющих подтверждение соответствия требованиям, установленным в соответствии с пунктом 2.1 части 5 статьи 8;
- информирование пользователя об использовании его ключа ЭП и предоставление по его требованию истории использования такого ключа ЭП.

Требования к ЗИС

АУЦ должен использовать защищенную информационную систему, удовлетворяющую требованиям по:

- хранению ключей квалифицированной электронной подписи и автоматическому созданию такой подписи с их использованием по поручению соответствующих владельцев квалифицированных сертификатов;
- аутентификации владельцев квалифицированных сертификатов, по поручению которых аккредитованный удостоверяющий центр создает и проверяет квалифицированную электронную подпись;
- защите информации, передаваемой по каналу взаимодействия между владельцем квалифицированного сертификата и аккредитованным удостоверяющим центром, осуществляющим создание и проверку квалифицированной электронной подписи по поручению такого владельца;
- доказательству невозможности отказа владельца квалифицированного сертификата от поручения на создание квалифицированной электронной подписи.

История проблемы

	криптография	область применения	потенциальный ущерб	страхование последствий	уровень угроз
Мобильное приложение банковской организации (МП БО)	сторонняя	банковские операции	финансовые убытки	+	высокий
Клиентское приложение владельца квалифицированного сертификата (КП ВКС)	отечественная	совершение юридически значимых действий	убытки во всех областях применения ЭП	+	очень высокий

Приказ от 26.11.2020 г. №624 Минцифры России

Основные угрозы, исходящие от внутреннего нарушителя АУЦ
угрозы нарушения целостности (подмены, удаления) и конфиденциальности ключа ЭП
угроза нарушения доступности ключа электронной подписи
угроза нарушения целостности (подмены) поручения
угроза нарушения конфиденциальности персональных данных, содержащихся в поручении
угроза нарушения конфиденциальности подписываемой информации
угроза нарушения целостности (подмены) информации о результате исполнения поручения
угроза нарушения доступности информации о результате исполнения поручения, а также истории использования ключа электронной подписи

Приказ от 26.11.2020 г. №624 Минцифры России (продолжение)

Основные возможности внутреннего нарушителя АУЦ
получение из находящихся в свободном доступе источников информации об удостоверяющем центре, использующем средство ЭП;
использование аппаратных средств и программного обеспечения из состава средств удостоверяющего центра (далее - штатные средства) и доступ к средствам вычислительной техники, на которых реализованы средства ЭП и СФ;
создание способов атак, подготовки и проведения атак с привлечением специалистов, имеющих опыт разработки и анализа средств ЭП, включая специалистов в области использования для реализации атак возможностей прикладного программного обеспечения, не описанных в документации на прикладное программное обеспечение и имеющих доступ к исходным текстам входящего в СФ прикладного программного обеспечения;
проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа средств ЭП и СФ.

КЛАСС ЗАЩИТЫ ЗИС

СРЕДСТВА ЭЛЕКТРОННОЙ ПОДПИСИ – КВ2;

СРЕДСТВА УДОСТОВЕРЯЮЩЕГО ЦЕНТРА – КС3 (УСИЛЕНИЕ ОТДЕЛЬНЫХ ТРЕБОВАНИЙ).

Требование

Исключение возможности доступа работников АУЦ к ключам электронных подписей заявителей:

КВ2 для всех средств.

РЕШЕНИЕ ПРОБЛЕМЫ

- использование средств сертифицированных по требованиям пункта 2.1 части 5 статьи 8 Федерального закона «Об ЭП»;
- внедрение недоступной администратору базовой ОС системы аудита;
- **АККРЕДИТАЦИЯ УЦ** по требованиям части 3.1 статьи 16 Федерального закона «Об ЭП».

Тот, кто предоставляет услуги дистанционной подписи без указанной аккредитации, не выполняет требования по информационной безопасности.

СПАСИБО ЗА ВНИМАНИЕ