УДК 004.056.57

Абдурахманова А.Н.,
студент магистратуры
2 курс, факультет «Информатика и робототехника»
Уфимский государственный авиационный технический университет
Россия, г. Уфа

АНАЛИЗ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОЦЕССА РЕГИСТРАЦИИ СЕРТИФИКАТОВ

Аннотация: *Статья посвящена анализу рисков информационной безопасности процесса регистрации сертификатов. В статье описан процесс регистрации сертификатов, а также перечислены основные риски этого процесса.*

Ключевые слова: *информационная безопасность, риск, удостоверяющий центр, сертификат.*

Annotation: *The article is devoted to the analysis of information security risks of the certificate registration process. The article describes the process of registering certificates, and also lists the main risks of this process.*

Key words: *information security, risk, verification Center, certificate.*

Процесс регистрации сертификатов представляет множество последовательных, однотипных и монотонных действий. В последнее время объемы обрабатываемых заявок возросли в несколько раз. К примеру, год назад, когда организация переняла на себя функционал регистрации сертификатов, пользователей было около 200. При таких незначительных объемах вероятность ошибки была мала, а также последствия, которые могла бы повлечь такая ошибка, были не столь критичны для организации. В 2019 году количество пользователей, которых обслуживает и обеспечивает ПКЗИ (персональный комплекс защиты информации), увеличивается, к началу следующего года цифра

будет близка к 15 000. Таким образом, объемы возрастают, и вероятность совершить ошибку при выполнении однотипных действий также возрастает. В связи с этим предлагает максимально автоматизировать работу, связанную с регистрацией сертификатов, с целью минимизировать риски, а также как следствие увеличить скорость обработки заявок и выпуску сертификатов.

Сертификат — это набор данных специального формата, содержащий сам всю информацию: кто владелец, организация, когда ключ создан. Сертификат записывается на защищенный носитель. С помощью сертификата происходит идентификация пользователя в информационных системах — процедура, в результате выполнения которой для субъекта идентификации выявляется его идентификатор, однозначно идентифицирующий этого субъекта в информационной системе.

Процедура идентификации напрямую связана с аутентификацией: субъект проходит процедуру аутентификации, и если аутентификация успешна, то информационная система на основе факторов аутентификации определяет идентификатор субъекта. При этом достоверность идентификации полностью определяется уровнем достоверности выполненной процедуры аутентификации.

ПКЗИ могут использоваться в информационных системах, обрабатывающих конфиденциальную информацию, включая персональные данные, имеющих класс защищенности средств вычислительной техники (СВТ) от несанкционированного доступа (НСД) не ниже 5 (Руководящий документ ФСТЭК России. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации) и класс защищенности автоматизированных систем (АС) от НСД не ниже 1Г, 2Б или 3Б (Руководящий документ ФСТЭК России. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации). Комплексы защиты информации ПКЗИ могут использоваться для целей обеспечения защиты

от несанкционированного доступа к информации на АРМ при его потере или хищении.

Сертификаты ПКЗИ могут использоваться для целей обеспечения защищенного информационного обмена электронными документами, содержащими конфиденциальные данные, включая персональные данные.

Процесс регистрации сертификатов делится на два больших блока.

Удостоверяющий центр:

- обработка заявок, поступающих от пользователей;
- выпуск регистрационных кодов;
- отправка регистрационных кодов ответственным лицам.

Оператор:

- получение регистрационных кодов по защищенному каналу передачи конфиденциальной информации (Vipnet Деловая почта);
- занесение информации в реестр;
- инициализация ключевого носителя;
- регистрация сертификата.

Нейтрализация рисков включает определение приоритетов, оценку и реализацию контрмер, уменьшающих риски и рекомендованных по результатам оценки рисков.

Поскольку полное устранение рисков невозможно, руководство организации должно следовать принципу минимальной достаточности, реализуя только необходимые, наиболее подходящие регуляторы безопасности с целью уменьшения рисков до приемлемого уровня с минимальным негативным воздействием на бюджет, ресурсы и миссию организации.

При использовании сертификатов ПКЗИ в информационной системе нужно учитывать следующие риски:

- риски при идентификации лица или организации, удостоверивших пользователя ПКЗИ;
- риск принятия документа к исполнению, с последующим отказом лица, которого идентифицировали с помощью ключа;

- риск непринятия документа к исполнению, вследствие неверной идентификации лица, использовавшего ключ;
- риски владельца ключа, связанные с несанкционированным использованием ключа другими лицами;
- риски УЦ ЭЦП по ответственности за выполнение взятых на себя обязательств при оказании услуг своим пользователям, в том числе:
  - по недостоверности сведений, указанных в сертификате ключа;
  - по своевременному непредставлению информации о действии сертификатов ключей;
  - по несвоевременному аннулированию сертификата или приостановлению/возобновлению действия сертификата [1].

Риска нельзя избежать, но можно понизить его уровень. Это можно сделать либо уменьшив вероятность наступления неблагоприятного события, либо уменьшив величину возможных потерь [2].

При проектировании системы управления рисками информационной безопасности нужно учитывать экономическую эффективность защиты информации.

В данном случае под экономической эффективностью будем понимать способность системы в процессе ее функционирования производить некий экономический эффект, например, снижение потенциальных потерь, снижение затрат на комплексные меры по защите информации. Расчет экономической эффективности защиты информации основывается на выявлении ущерба, нанесенного владельцу информации и позволяет оценить результативность защиты информации. После анализа расчетов экономической эффективности, можно внести изменения в систему защиты информации для более эффективной ее защиты.

Таким образом, в рамках данной работы были проанализированы возможные риски информационной безопасности процесса регистрации сертификатов ПКЗИ.

Далее планируется сделать следующее:

- составить дерево событий, которые могут повлечь за собой реализацию рисков;
- согласно составленному дереву необходимо оценить вероятности наступления неблагоприятных событий;
- выявление основных параметров, от которых будет зависеть ущерб;
- анализ величины ущерба в зависимости от выявленных параметров;
- непосредственно оценка риска;
- возможные меры по снижению риска;
- сравнение полученных результатов, оценка экономической целесообразности.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Удостоверяющие центры в системе электронного документооборота. Михалевич И.Ф., Жуков А.О., Пантюхов Д.В., Левин Ю.В. 2018.— 4 с.
2. Алгоритм оценки рисков информационной безопасности. Бадердинова О.И., Бадердинова М. В. 2016.— 3 с.