Об одной атаке на протокол IKEv2

И о том, как её предотвратить

Internet Key Exchange version 2 (IKEv2) – протокол аутентифицированного обмена ключами в IPsec

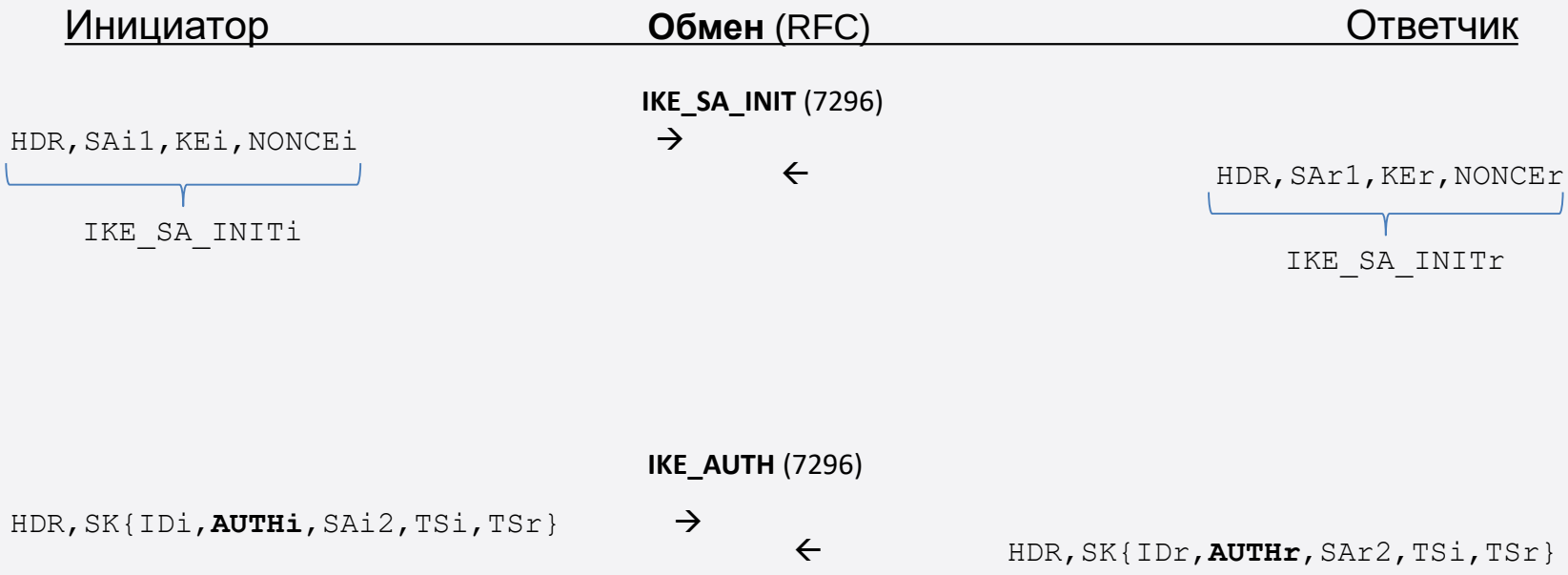
- базовый протокол описан в RFC 7296 (также в Р 1323565.1.048-2023)
- расширения протокола для гибридного пост-квантового обмена ключами описаны в RFC 9242, RFC 9370

Криптографической основой IKEv2 является SIGMA [1] в варианте SIGMA-R.

[1] Hugo Krawczyk , “SIGMA: The ‘SIGn-and-MAc’ Approach to Authenticated Diffie-Hellman and Its Use in the IKE Protocols” (CRYPTO 2003), https://link.springer.com/chapter/10.1007/978-3-540-45146-4_24

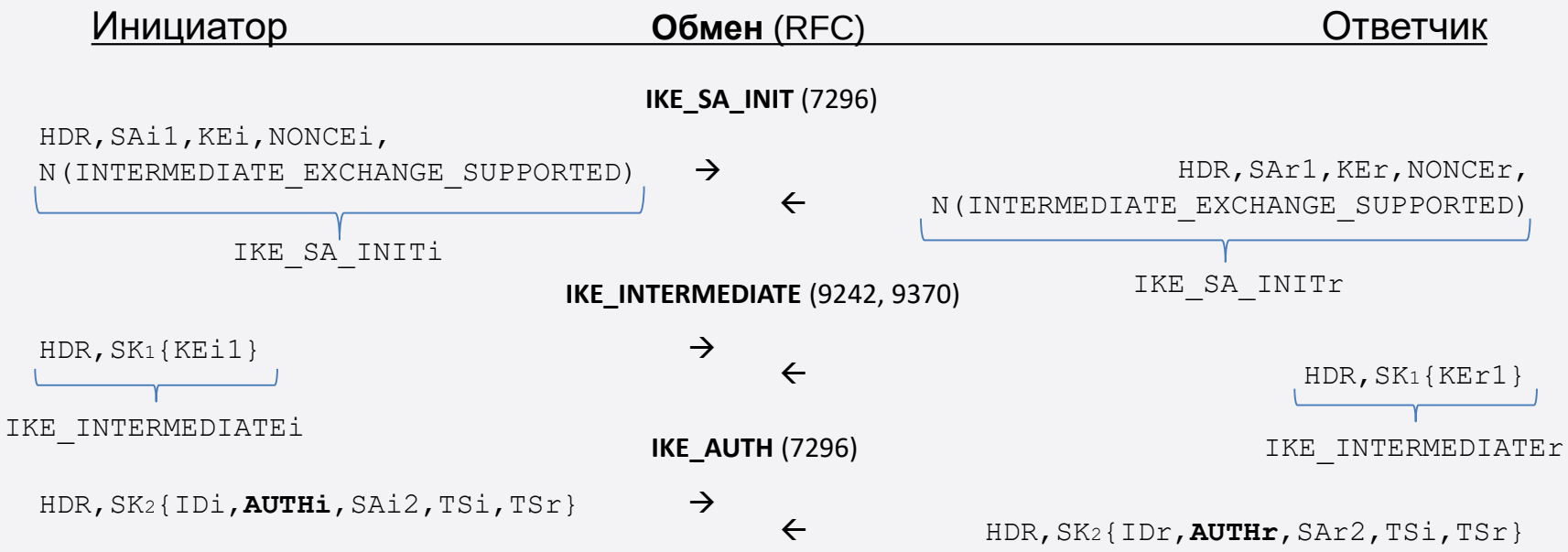
ЭЛВИС-ПЛЮС

Инициатор	**Обмен** (RFC)	Ответчик
	IKE_SA_INIT (7296)	
HDR,SAi1,KEi,NONCEi	→	
	←	HDR,SAr1,KEr,NONCEr
	IKE_AUTH (7296)	
HDR,SK{IDi,AUTHi,SAi2,TSi,TSr}	→	
	←	HDR,SK{IDr,AUTHr,SAr2,TSi,TSr}



AUTHi = SIGi(IKE_SA_INITi | NONCEr | MACsk(IDi))

AUTHr = SIGr(IKE_SA_INITr | NONCEi | MACsk(IDr))



AUTHi = SIGi(IKE_SA_INITi | NONCEr | MACsk2(IDi) | MACsk1(IKE_INTERMEDIATEi) | MACsk1(IKE_INTERMEDIATEr))

AUTHr = SIGr(IKE_SA_INITr | NONCEi | MACsk2(IDr) | MACsk1(IKE_INTERMEDIATEi) | MACsk1(IKE_INTERMEDIATEr))

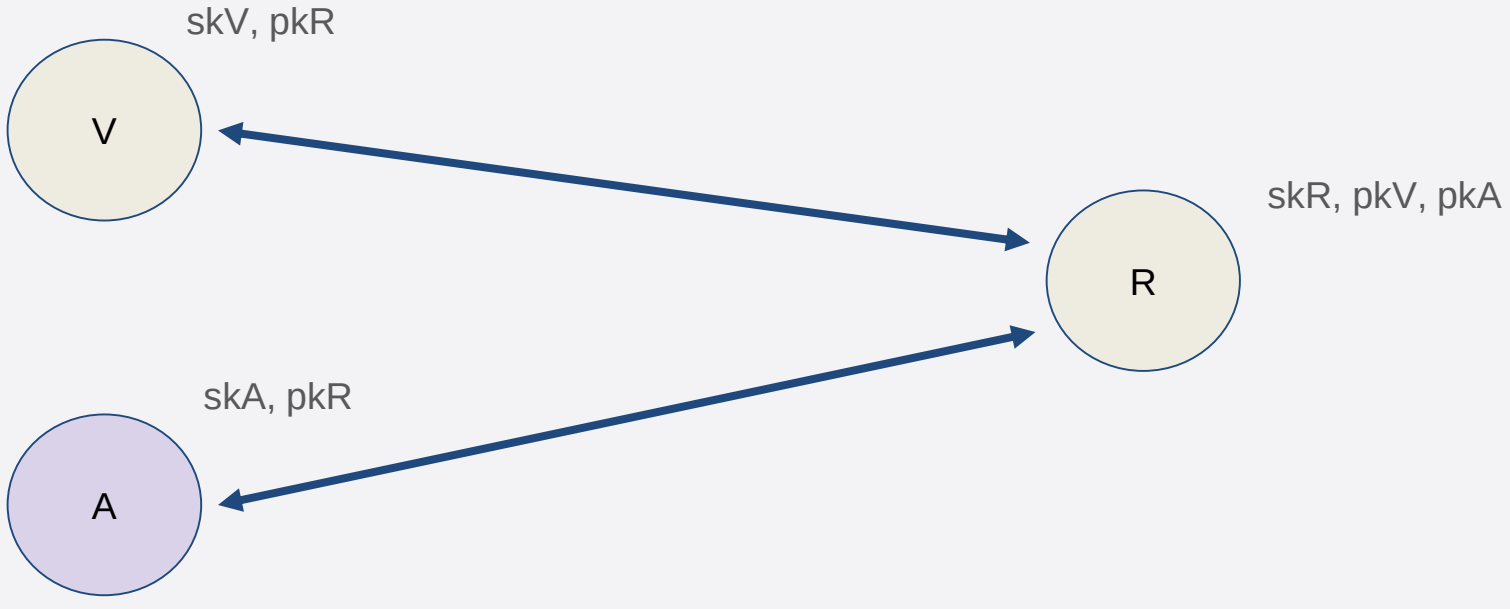
Downgrade атака на IKEv2 впервые была описана в [2], как модификация протокола SIGMA с возможностью выбора вариантов (SIGMA-N). Для ее реализации атакующий должен «взламывать» (EC)DH с какими-то (слабыми) параметрами в реальном времени. Поскольку для IKEv2 слабые параметры (EC)DH не определены, то атака носит теоретический характер.

Вариант этой атаки на гибридный пост-квантовый обмен в IKEv2 был предложен в 2025г. Кристофером Паттоном (Christopher Patton) [3]. Предполагается, что атакующий при этом обладает квантовым компьютером.

[2] Karthikeyan Bhargavan, Christina Brzuska, Cédric Fournet, Markulf Kohlweiss, Santiago Zanella-Béguelin, Matthew Green, “Downgrade Resilience in Key-Exchange Protocols”, 2016, https://eprint.iacr.org/2016/072.pdf
[3] https://mailarchive.ietf.org/arch/msg/ipsec/5oSGMBl8RQm4-ZT15CJHNqkSqr8/

ЭЛВИС-ПЛЮС

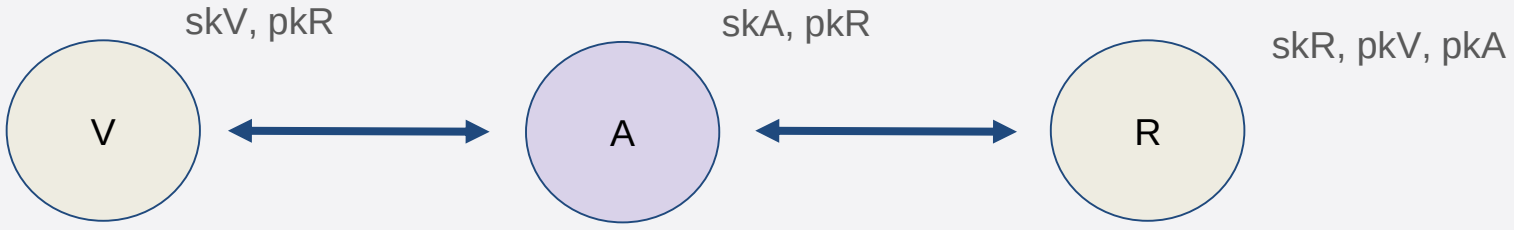
Предположим, что два инициатора V и A могут устанавливать соединение с ответчиком R используя цифровую подпись для аутентификации.



Условие проведения атаки:

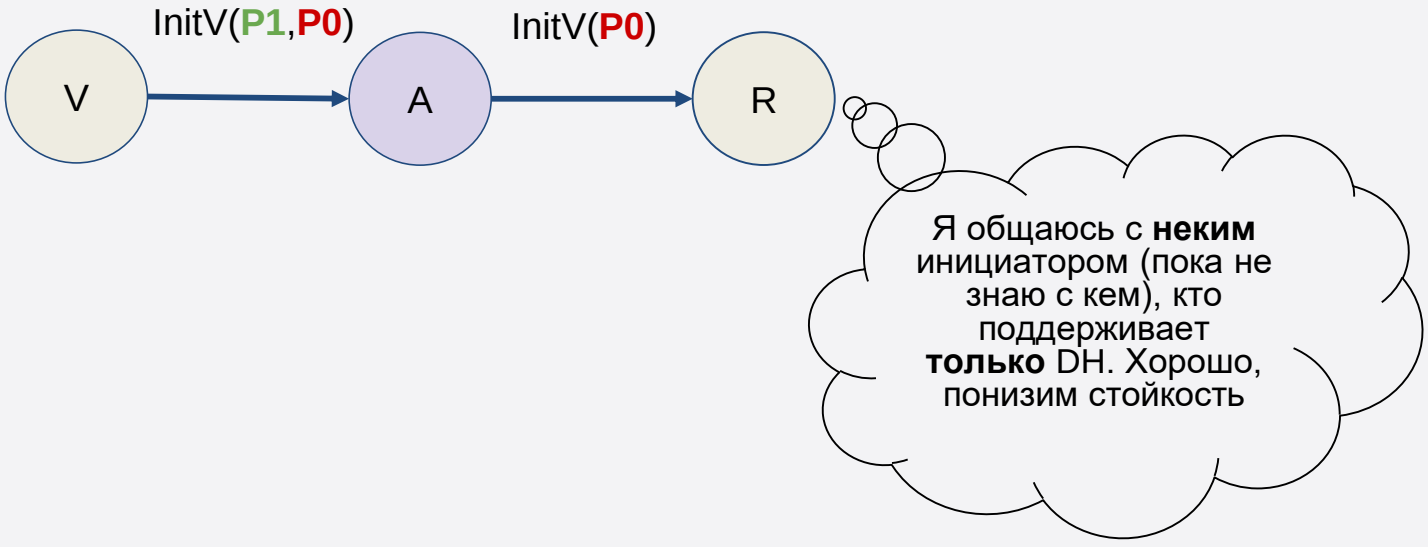
- Конфигурации обоих участников допускают использование как гибридного пост-квантового обмена, так и одного DH
- A находится на пути между V and R и хочет перехватывать их трафик
- A имеет в распоряжении технические средства (например, квантовый компьютер) позволяющие ему «взламывать» DH в реальном времени.

При этом A не имеет доступа к закрытому ключу R и не может подделывать его подпись в реальном времени



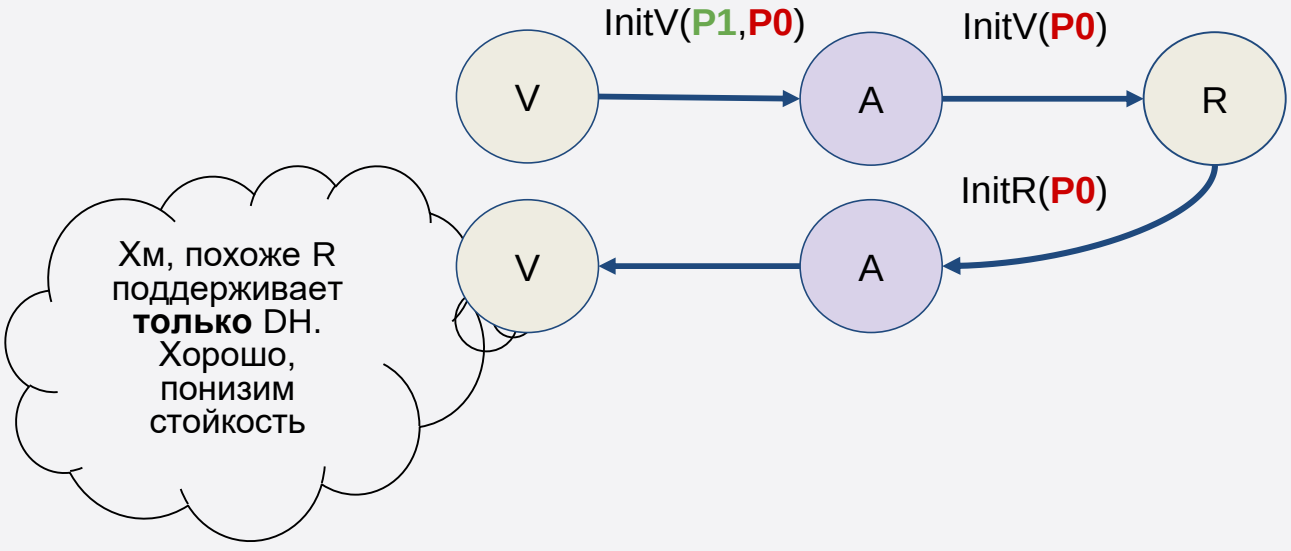
ЭЛВИС-ПЛЮС

Шаг 1: A перехватывает сообщение IKE_SA_INIT от V, меняет его, удаляя предложение **пост-квантового** МИК, и оставляяя только предложение DH, и пересылает сообщение R.



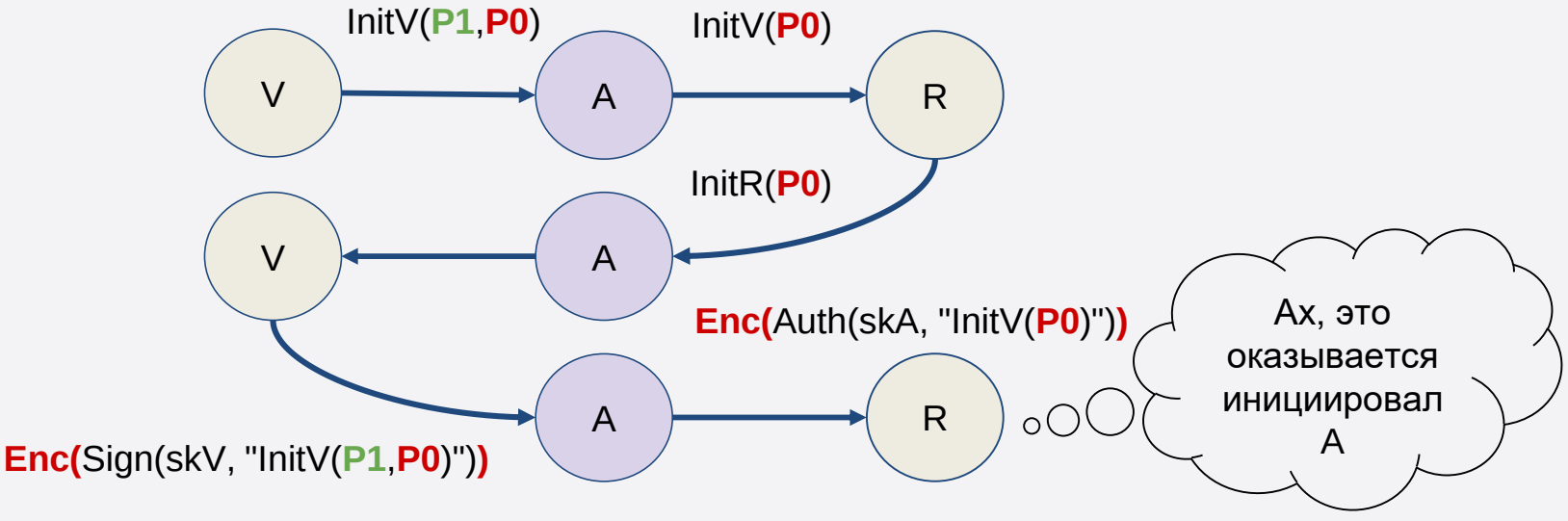
ЭЛВИС-ПЛЮС

Шаг 2: A пересылает обратное сообщение IKE_SA_INIT от R к V не меняя его. A при этом, имея оба открытых ключа DH, «взламывает» его, получая разделяемый секрет.



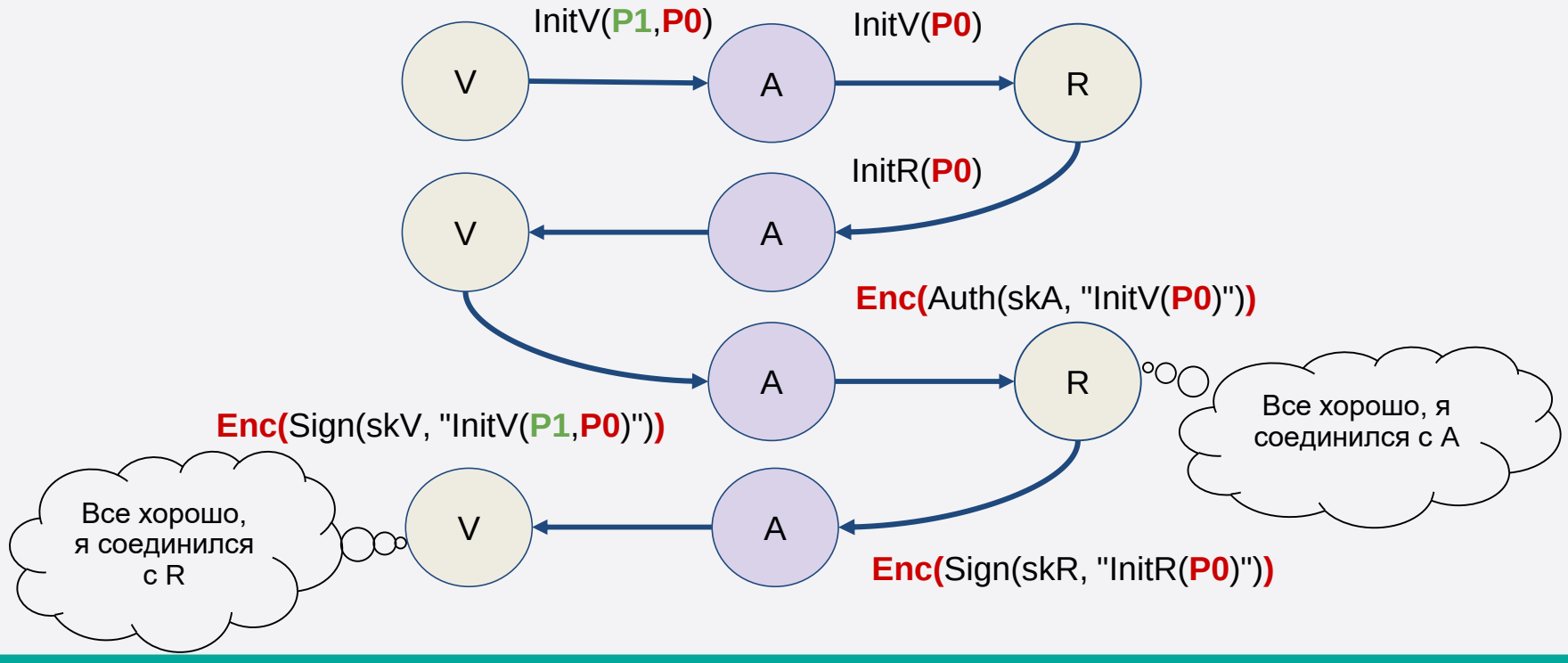
ЭЛВИС-ПЛЮС

Шаг 3: A перехватывает сообщение IKE_AUTH от V, расшифровывает его, пересчитывает MAC(IDv), заменяет подпись V собственной подписью, повторно зашифровывает, и отправляет измененное сообщение R.



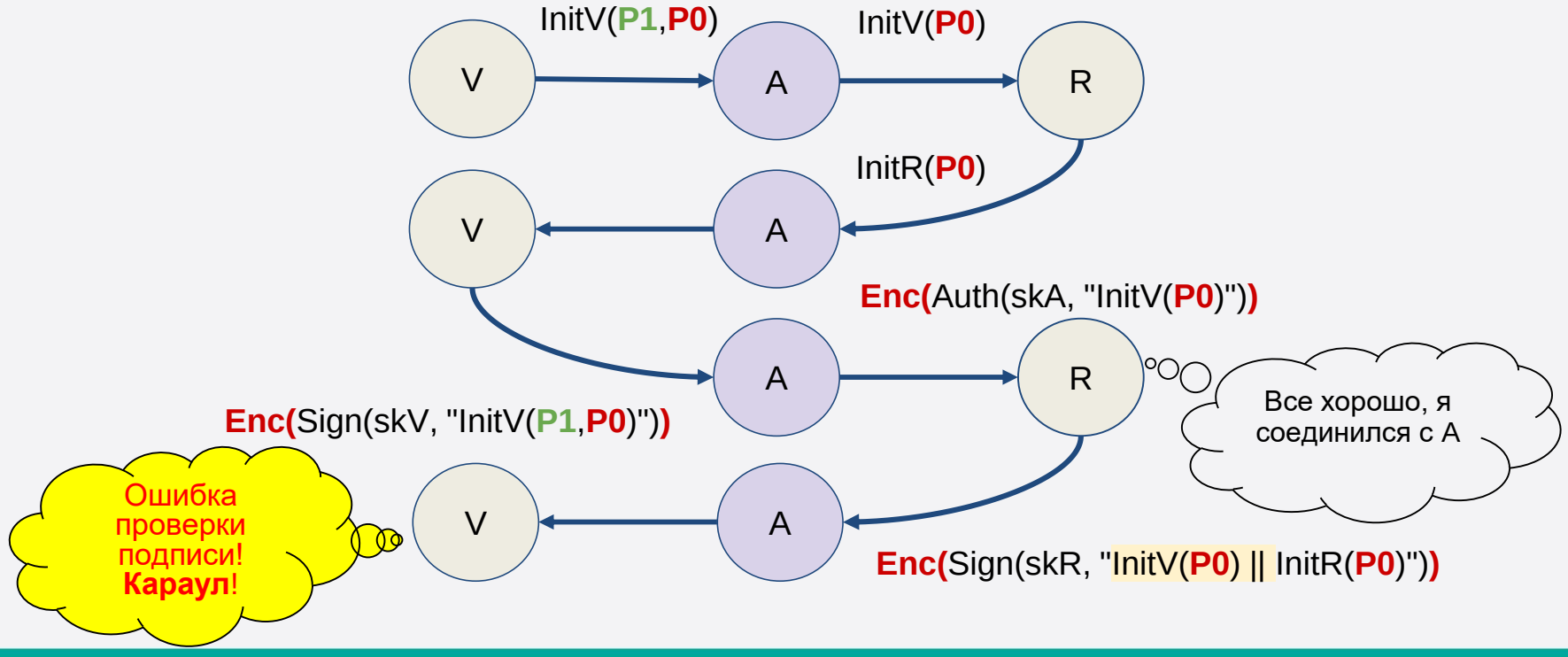
ЭЛВИС-ПЛЮС

Шаг 4: A пересылает обратное сообщение IKE_AUTH от R к V не меняя его.



ЭЛВИС-ПЛЮС

V и R по-разному представляют содержимон начального сообщения IKE_SA_INIT. Если бы R включал в свою подпись реально полученное сообщение от V, то V обнаружил бы атаку.

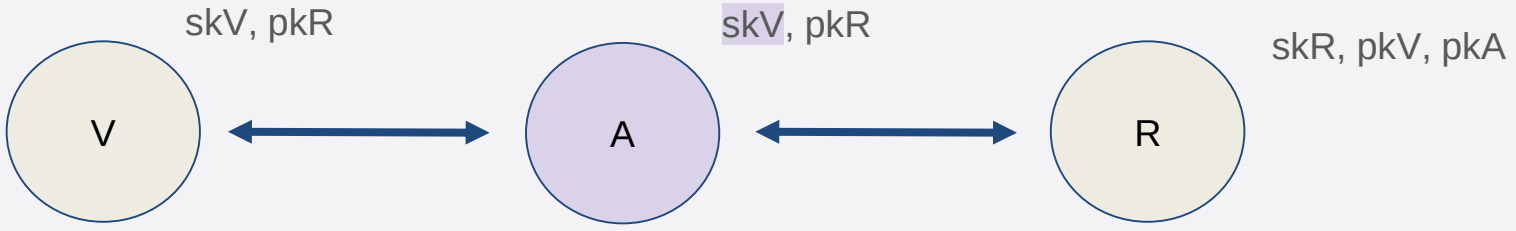


Предположим, что инициатор V может устанавливать соединение с ответчиком R используя цифровую подпись для аутентификации. A не имеет доступа к R.

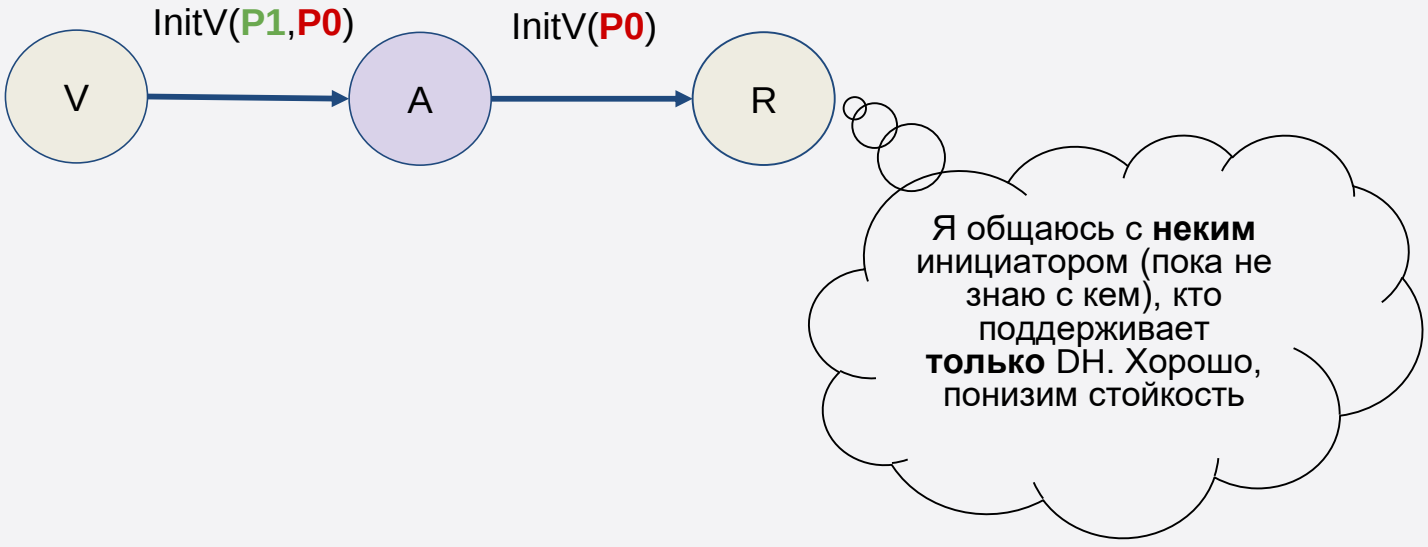
Условие проведения атаки:

- Конфигурации обоих участников допускают использование как гибридного пост-квантового обмена, так и одного DH
- A находится на пути между V and R и хочет перехватывать их трафик
- A может «взламывать» DH в реальном времени
- A имеет доступ к закрытому ключу V или может подделывать его подпись в реальном времени

При этом A не имеет доступа к закрытому ключу R и не может подделывать его подпись в реальном времени

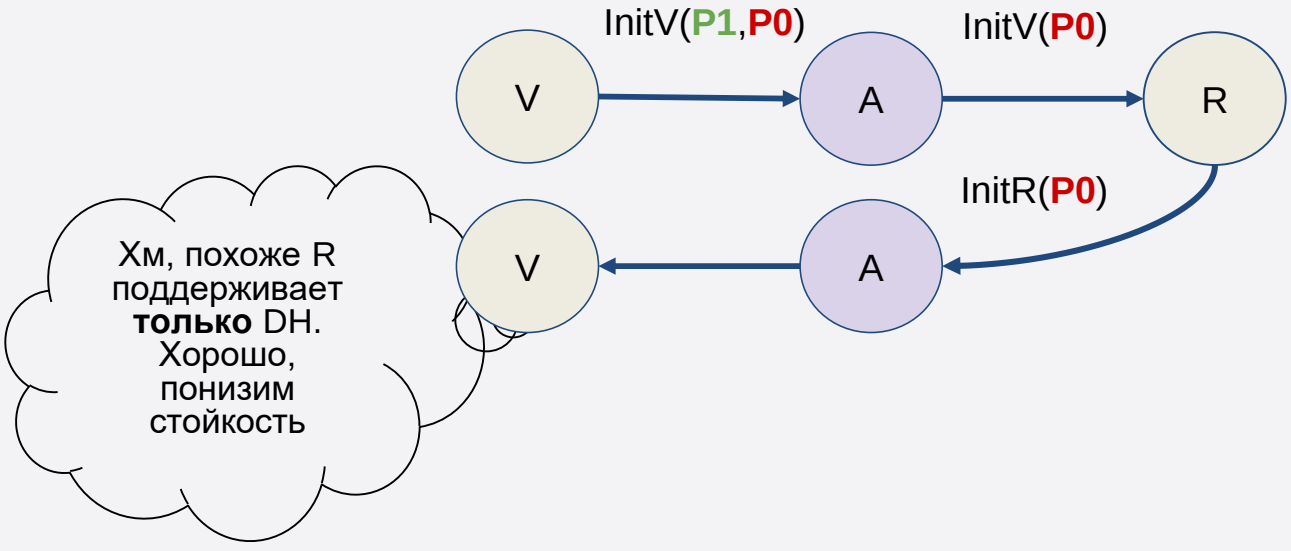


Шаг 1: A перехватывает сообщение IKE_SA_INIT от V, меняет его, удаляя предложение **пост-квантового** МИК, и оставляяя только предложение DH, и пересылает сообщение R.



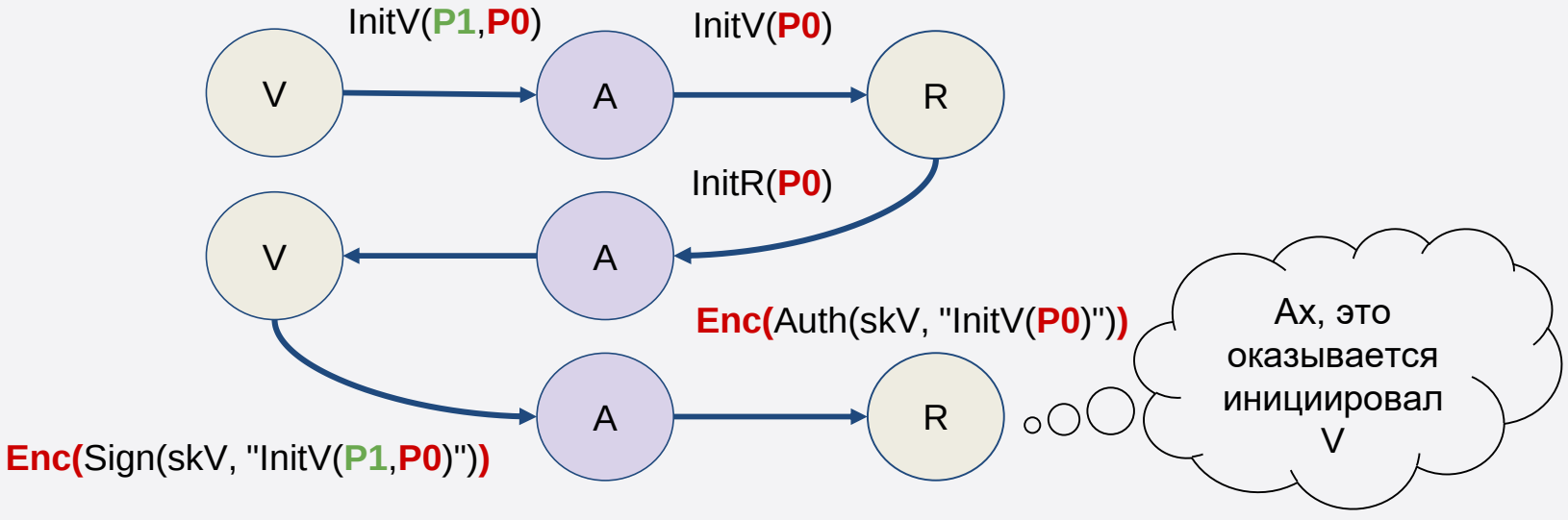
ЭЛВИС-ПЛЮС

Шаг 2: A пересылает обратное сообщение IKE_SA_INIT от R к V не меняя его. A при этом, имея оба открытых ключа DH, «взламывает» его, получая разделяемый секрет.



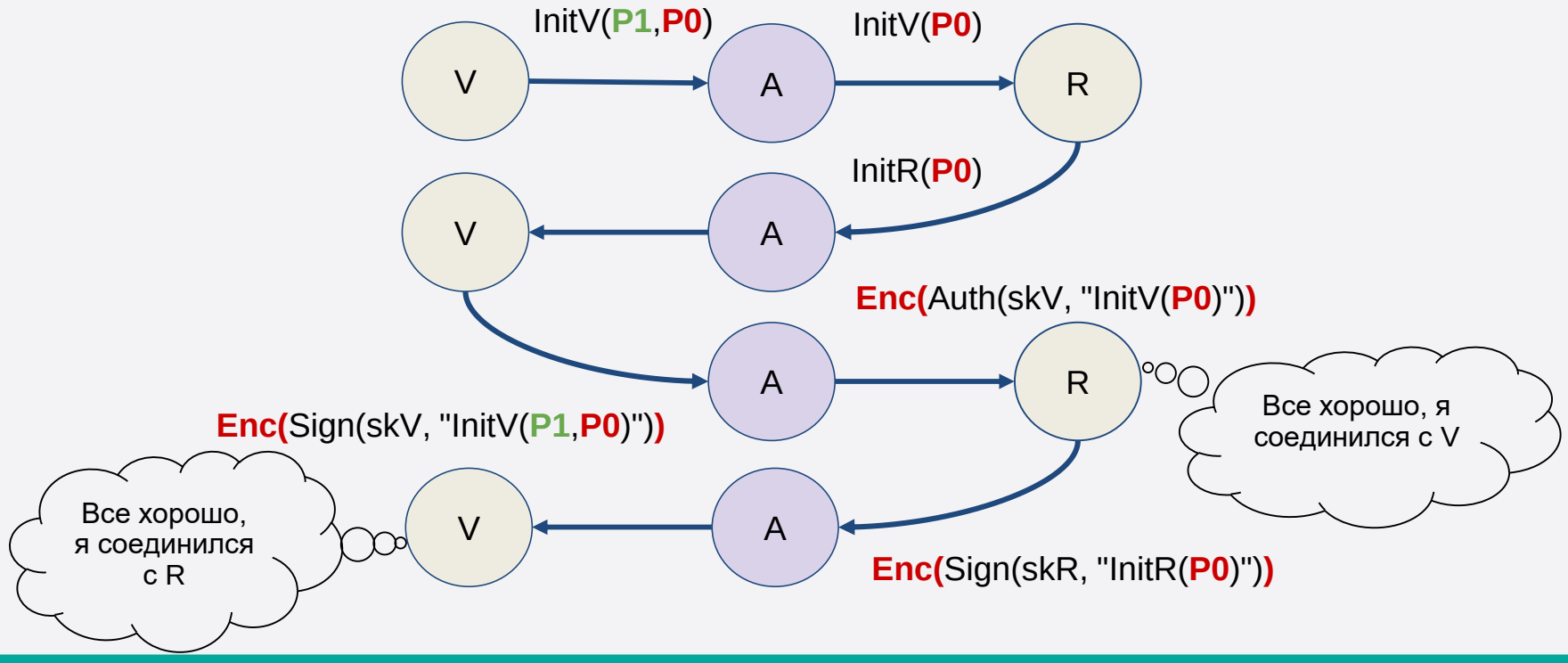
ЭЛВИС-ПЛЮС

Шаг 3: A перехватывает сообщение IKE_AUTH от V, расшифровывает его, пересчитывает MAC(IDv), заново формирует подпись от имени V, повторно зашифровывает, и отправляет измененное сообщение R.



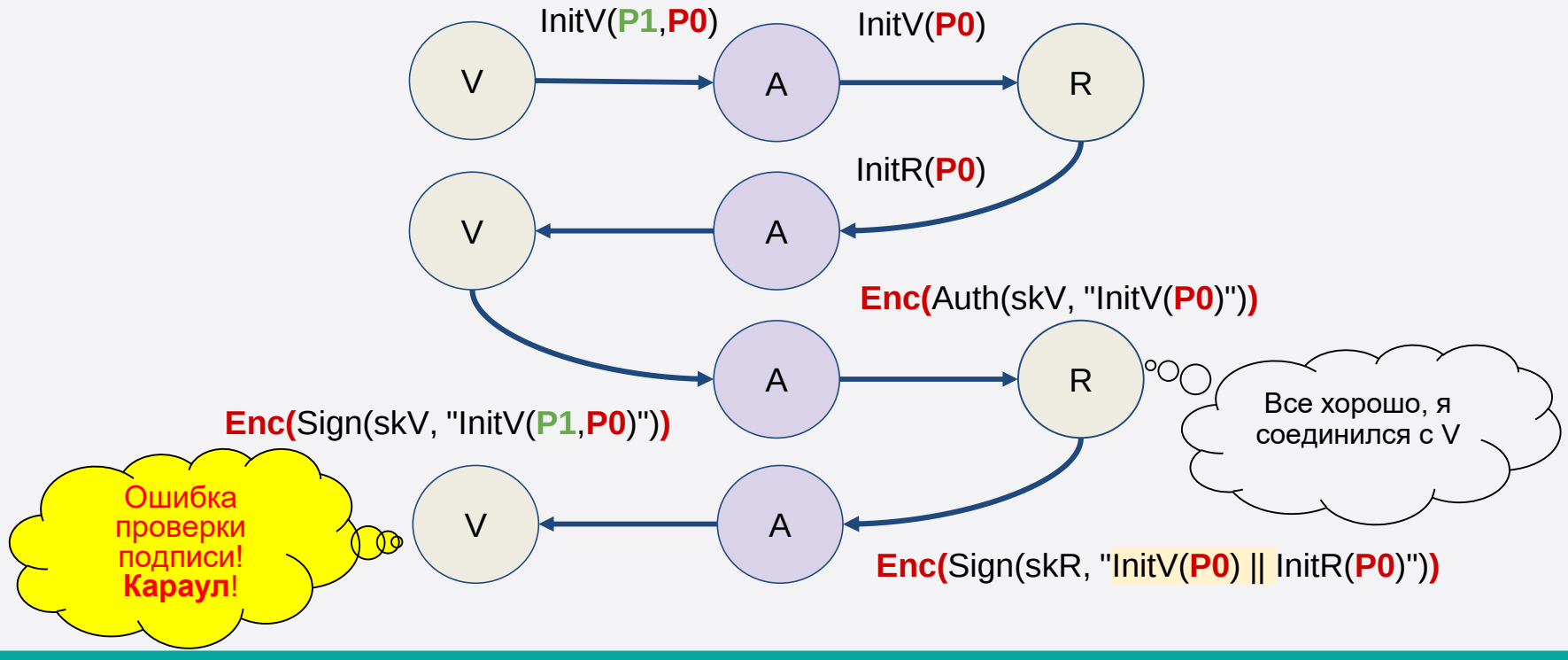
ЭЛВИС-ПЛЮС

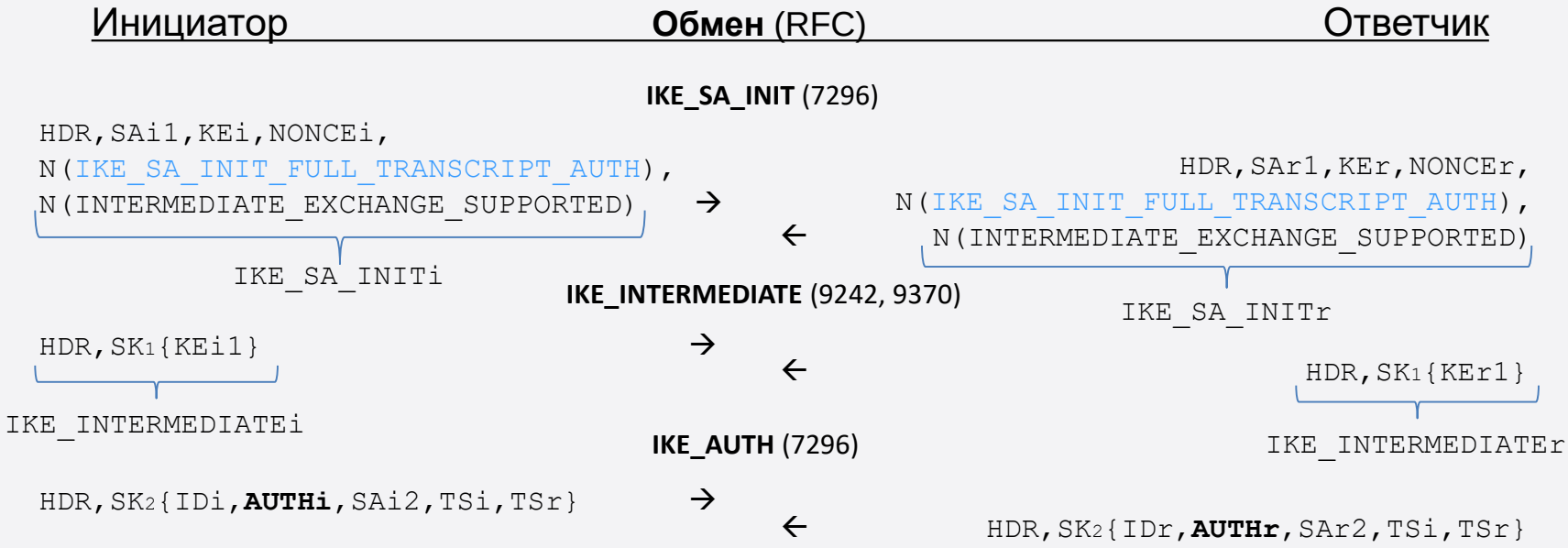
Шаг 4: A пересылает обратное сообщение IKE_AUTH от R к V не меняя его.



ЭЛВИС-ПЛЮС

V и R по-разному представляют содержимон начального сообщения IKE_SA_INIT. Если бы R включал в свою подпись реально полученное сообщение от V, то V обнаружил бы атаку.





AUTHi = SIGi(0 | IKE_SA_INITr | IKE_SA_INITi | NONCEr | MACsk2(IDi) | MACsk1(IKE_INTERMEDIATEi) | MACsk1(IKE_INTERMEDIATEr))

AUTHr = SIGr(0 | IKE_SA_INITi | IKE_SA_INITr | NONCEi | MACsk2(IDr) | MACsk1(IKE_INTERMEDIATEi) | MACsk1(IKE_INTERMEDIATEr))

В IKEv2 использование расширений **как правило** согласуется так:

- инициатор посылает уведомление в запросе; **если ответчик его получает**, то посылает то же уведомление в ответе; если уведомление **и послано, и получено**, то расширение согласовано.

Так как описанная атака строится на возможности атакующего менять содержимое IKE_SA_INIT, то он может удалить уведомления IKE_SA_INIT_FULL_TRANSCRIPT_AUTH и, таким образом, отключить защиту. Для предотвращения этого логика при согласовании данного расширения **изменяется:**

- инициатор посылает уведомление IKE_SA_INIT_FULL_TRANSCRIPT_AUTH в запросе; ответчик посылает это уведомление в ответе **независимо от того**, получал ли он его в запросе; если участник **и послал, и получил** уведомление, то он использует данное расширение, иначе использует старую схему для аутентификации (RFC 7296 + RFC 9242).

При этом:

- удаление уведомления из **одного** сообщения (только из запроса или только из ответа) приведет к ошибке проверки подписи у **обоих** участников, так как один из них будет использовать новую схему, а другой – старую
- удаление уведомления **из обоих сообщений** приведет к ошибке проверки подписи у **обоих** участников, так как, хотя оба будут использовать старую схему, но даже при старой схеме каждый участник включает в подпись свое сообщение
- по условиям атаки атакующий может подделать подпись **одного** из участников, но не обе

Таким образом, атакующий **не может** отключить защиту манипулируя сообщениями IKE_SA_INIT.

ЭЛВИС-ПЛЮС

IETF:

- draft-ietf-ipsecme-ikev2-downgrade-prevention «Downgrade Prevention for the Internet Key Exchange Protocol Version 2 (IKEv2)»
  - прошел Working Group Last Call
  - RFC предположительно в этом году

ТК26:

- Проект МР «Использование нескольких ключевых обменов и дополнительных симметричных ключей в протоколе IKEv2»
  - в стадии «исследовательский период»

Есть несколько совместимых реализаций

ЭЛВИС-ПЛЮС

Благодарю за внимание!

Смыслов Валерий Анатольевич

svan@elvis.ru
+7 (495) 276-0211