**ASV-сканирование в одно касание**

*Обязательный формат проверки ИТ-безопасности организаций, принимающих и обрабатывающих данные банковских карт*

Международные платёжные системы предъявляют особые требования к уровню безопасности транзакций. Своевременно установить различного рода уязвимости и некорректные конфигурации сетевой инфраструктуры позволяет процедура ASV-сканирования. О том, для каких целей служит данная проверка, рассказывают специалисты компании ARinteg — одного из ведущих российских системных интеграторов в сфере информационной безопасности, обладающего подтверждённым статусом ASV-провайдера.

**ASV-сканирование: что это такое?**

ASV-сканирование — это процедура ежеквартальной проверки всех точек подключения к сети интернет на наличие уязвимостей. Разработана Советом по стандартам безопасности данных индустрии платёжных карт (создан по инициативе American Express, Discover Financial Services, JCB International, MasterCard Worldwide и Visa, Inc.).

**Кто обязан проходить проверку?**

Процедура ASV-сканирования на предмет соответствия требованиям международного стандарта безопасности PCI DSS распространяется на все организации, которые хранят, обрабатывают или передают данные держателей платёжных карт.

Такие компании классифицируются исходя из объёма транзакций, проводимых в течение года:

* 4 уровень — до 20 тысяч транзакций в год (ежеквартальное сканирование внешних адресов на наличие уязвимостей и заполнение листа самооценки);
* 3 уровень — от 20 тысяч до 1 миллиона транзакций в год (аналогичные требования, что и для компаний 4-го уровня);
* 2 уровень — от 1 миллиона до 6 миллионов транзакций в год (ежеквартальное сканирование с привлечением компании-аудитора);
* 1 уровень — более 6 миллионов транзакций в год (соответствие требованиям проводится только с привлечением независимого аудитора).

Отдельная градация существует в отношении сервисных компаний и процессинговых центров.

**Как подтвердить соответствие требованиям стандарта PCI DSS?**

Для прохождения ASV-сканирования необходимо обратиться к специализированным поставщикам услуг, аккредитованным Советом по стандартам безопасности данных индустрии платёжных карт.

Компании ARinteg статус [ASV-провайдера](https://www.pcisecuritystandards.org/assessors_and_solutions/approved_scanning_vendors) впервые был присвоен более трёх лет назад. Ежегодно системный интегратор успешно подтверждает свой экспертный уровень.

Опираясь на многолетний опыт аудита защищённости внешнего периметра и внутренних сетей, ARinteg помогает организациям финансового сектора и компаниям из других отраслей успешно проходить необходимые процедуры проверки на предмет соответствия PCI DSS.

**Как проходит процедура сканирования?**

Сканирование проводится удалённо в формате выделенного технологического окна в течение 24 часов. Дату и время сканирования можно согласовать индивидуально.

**Необходимо ли заранее готовиться к проверке?**

На время проведения проверки обязательным требованием стандарта PCI DSS является отключение (переключение в режим мониторинга) средств активной защиты, основанных на поведенческом анализе (IPS, WAF).

В случае использования балансировщиков трафика требуется подтверждение синхронизации сетевых потоков.

Процедура ASV-сканирования абсолютно безопасна и не влияет на производительность сетевой инфраструктуры.

**Что происходит во время сканирования?**

В рамках тестирования определяется наличие доступных IP-адресов из списка, предоставленного заказчиком, проводится сканирование всего диапазона TCP-портов и стандартных UDP-портов.

Осуществляется попытка точной идентификации используемых версий операционных систем и запущенных сервисов вне зависимости от используемых платформ.

Процедура проверки проводится на предмет:

* наличия уязвимостей (как известных CVE, так и уникальных);
* ошибок конфигурации серверов приложений;
* обнаружения стандартных веб-скриптов;
* использования встроенных учётных записей;
* применения средств удалённого доступа;
* ошибок конфигурации DNS-серверов;
* защищённости почтовых сервисов;
* подверженности типичным атакам на веб-приложения (SQL-injection, XSS, перемещение по директориям, разбитие HTTP-заголовков и т.д.);
* выявления избыточных стандартных сервисов;
* наличия бэкдоров, руткитов, иного вредоносного ПО;
* использования актуальных версий TLS-шифрования;
* обнаружения POS-терминалов.

**Какой документ выдаётся по итогам проверки?**

По результатам сканирования предоставляется отчёт, в котором указываются как подтверждённые, так и потенциальные уязвимости.

В случае выявления недопустимых уязвимостей критичностью выше 4 уровня (CVE), заказчик может оспорить их справедливость, предоставив подтверждения ложного срабатывания сканера.

При обнаружении средств удалённого доступа, POS-терминалов или иных механизмов приёма платежей, возможности листинга директорий, потребуется обоснование необходимости и защищённости применяемых решений.

Более подробно узнать о преимуществах ASV-сканирования от ARinteg и оставить заявку на проведение проверки можно с помощью специализированного сервиса – <https://asv.arinteg.ru>.

**О компании**

ARinteg — российский системный интегратор в сфере информационной безопасности, предоставляющий полный комплекс экспертно-аналитических, технических и консалтинговых услуг и сервисов.

Многолетний опыт работы ARinteg включает успешное выполнение масштабных проектов в крупных российских банках и финансовых организациях, предприятиях промышленности и топливно-энергетического комплекса, государственном секторе и медицинских организациях.

Компания обладает высшими партнёрскими статусами крупнейших зарубежных и российских вендоров в области информационной безопасности.

Компетенции ARinteg подтверждены соответствующими лицензиями и сертификатами ФСБ РФ и ФСТЭК РФ, сертификатом соответствия ISO 9001:2015 (ГОСТ P ISO 9000-2015).

Компания является аккредитованным ASV-провайдером по версии международного Совета PCI SSC и действительным членом межрегиональной общественной организации «Ассоциация защиты информации» и некоммерческого партнерства «Сообщество пользователей стандартов по информационной безопасности АБИСС».

Контакты для СМИ:

Антон Банько

тел.: +7 (916) 504-06-19

e-mail: Anton.Banko@ARinteg.ru

**Присоединяйтесь к нам в** [**Facebook**](https://www.facebook.com/ARinteg/) **|** [**Instagram**](https://www.instagram.com/arinteg.ru/)