устройств. Внимание также уделяется контролю сетевых протоколов, портов и служб для ограничения возможностей подключения к сети организации.

Во-вторых, применение активных средств управления защитой сети, таких как непрерывный анализ и устранение уязвимостей, организация защиты от вредоносного кода, обеспечение безопасности прикладного ПО и возможности восстановления данных, а также ведение, мониторинг и анализ журналов регистрации событий безопасности.

В-третьих, все стандарты большое значение придают квалификация персонала — как отдела ИБ, так и остальных сотрудников, поскольку их осведомленность в области ИБ играет большую роль в защищенности сети. Для этого предлагается периодически проводить обучение, повышение осведомленности, а затем и оценку навыков по безопасности и проведение тренингов по ИБ. Эффективность работы персонала отдела ИБ оценивается в том числе и по возможности реагирования на инциденты информационной безопасности и результатам тестирования на проникновение, упражнений и учений.

В-четвертых, важным аспектом ИБ организации является безопасно построенная сеть, что предполагает определенную архитектуру сети, защиту ее периметра и контроль входящих и исходящих потоков данных, предотвращение утечки данных.

В-пятых, для защиты информации в локальной сети необходим мониторинг и контроль учетных записей — как привилегированных аккаунтов администраторов, так и обычных пользователей. использования административных привилегий, контроль и управление их доступом.

ЗАЩИТА ИНФОРМАЦИИ ПРИ ИСПОЛЬЗОВАНИИ ОБЛАЧНЫХ ПЛАТФОРМ

А.Р. ОКОЛОВ, В.В. ХОДЬКО, А.В. ДРОЗД

Облачные платформы — это модель предоставления вычислительных ресурсов по требованию, охватывающая всё — от конкретных приложений до центров обработки данных, через Интернет. Такой подход к организации вычислений дает небывалые возможности клиентам, независимо от мощности их компьютеров и при этом обеспечивает доступ к облаку миллионам пользователей в каждый момент. Однако, при такой заманчивости использования облачных сервисов, пользователи предъявляют к ним и высокие требования, связанные с аутентификацией, сохранностью данных и их защищенностью.

Аутентификация. Самым распространенным способом аутентификации является защита паролем. Однако некоторые провайдеры, для обеспечения более высокой надежности, прибегают к помощи таких средств, как сертификаты и токены. Желательно, что бы провайдеры имели возможность работы с такими стандартами как LDAP и SAML. Это важно для обеспечения прозрачного взаимодействия провайдера с системой идентификации пользователей клиента при авторизации и определении выдаваемых пользователю полномочий.

Сохранность данных. Лучший способ защиты расположенных в хранилище данных — использование шифрования. С целью предотвращения случаев неправомерного доступа, провайдер должен шифровать хранящуюся на своих серверах информацию клиента, безвозвратно удалять данные, когда они больше не нужны и не потребуются в будущем.

Защита данных при передаче. Передаваемые данные должны быть зашифрованы и доступны пользователю только после аутентификации. Это является гарантией того, что эти данные не сможет изменить или прочитать ни одно лицо, даже если оно получит к ним доступ посредством ненадежных узлов сети. Для этих целей созданы и эффективно используются надежные протоколы и алгоритмы, такие как TLS, IPsec и AES.