



Кибербезопасность финансовых организаций

Контроль безопасности по стандартам SWIFT

Общество всемирных межбанковских каналов связи SWIFT выпустило набор базовых стандартов безопасности. Требования обязательны к исполнению для всех участников SWIFT и сгруппированы по трем основным аспектам. В их основу легли восемь принципов. Соблюдение этих принципов проверяется с помощью 16 обязательных и 11 рекомендованных контрольных показателей.

Контроль соблюдения обязательных требований начнется с января 2018 г. Меры будут включать проверочные инспекции отдельных участников SWIFT внутренними и внешними аудиторами.

Решения «Лаборатории Касперского» помогут вашей организации соблюсти ключевые требования SWIFT к безопасности.

2.2 Обновления безопасности

Все компоненты оборудования и программное обеспечение в периметре безопасности и на пользовательских компьютерах должны поддерживаться производителями; должны быть установлены обязательные обновления программного обеспечения, а также актуальные обновления безопасности*.

- Компонент Мониторинг уязвимостей и управление установкой исправлений, входящий в Kaspersky Systems Management и Kaspersky Security для бизнеса (начиная с версии Расширенный) обеспечивает безопасное обновление продуктов Microsoft и других поставщиков.

2.3 Усиление защиты систем

Во всех системах и инфраструктурах в периметре безопасности и на пользовательских компьютерах должен поддерживаться режим усиленной защиты.

- Kaspersky Embedded Systems Security обеспечивает усиление защиты систем благодаря режиму «Запрет по умолчанию» для приложений, драйверов и библиотек, а также за счет централизованного контроля за использованием дисков CD/DVD и USB-устройств для хранения данных.

6.1 Защита от вредоносных программ

На всех системах должна быть установлена своевременно обновляемая защита от вредоносных программ, предоставляемая производителем с надежной репутацией.

- «Лабораторию Касперского» признают лидером рынка защиты рабочих мест такие компании, как Gartner, IDC и Forrester. Продукты компании регулярно удостоиваются высших оценок в независимых тестах. Подробнее о результатах тестов: kaspersky.ru/top3.

<p>6.2 Целостность программного обеспечения</p>	<p>В организации должна регулярно проводиться проверка целостности ПО для интерфейсов систем обмена сообщениями, коммуникационных систем и других приложений, поддерживающих работу SWIFT.</p> <ul style="list-style-type: none"> · Функция мониторинга целостности файлов в решении Kaspersky Embedded Systems Security обеспечивает целостность системных файлов, записей журналов и критически важных приложений.
<p>7.1 Планирование реагирования на инциденты кибербезопасности</p>	<p>В организации должен действовать план реагирования на киберинциденты.</p> <ul style="list-style-type: none"> · Тренинги по реагированию на инциденты входят в состав сервисов кибербезопасности «Лаборатории Касперского». Эти тренинги учат сотрудников разрабатывать и исполнять планы реагирования на инциденты кибербезопасности.
<p>7.2 Обучение основам безопасности и осведомленность о киберугрозах</p>	<p>Тренинги, информирующие об опасностях киберугроз, должны ежегодно проводиться для всех сотрудников. Те сотрудники, которые имеют расширенные права доступа в системах SWIFT, должны проходить дополнительное обучение, соответствующее их ролям.</p> <ul style="list-style-type: none"> · Тренинги «Лаборатории Касперского» по кибербезопасности мотивируют сотрудников на соблюдение правил безопасности и дают им необходимые практические навыки. Тренинги проводятся в различных форматах и по разным темам на базе конкретных ролевых моделей.
<p>2.7A Мониторинг уязвимостей</p>	<p>Мониторинг уязвимостей в периметре безопасности и на пользовательских компьютерах должен проводиться с помощью актуальных версий инструментов проверки, соответствующих отраслевым стандартам.</p> <ul style="list-style-type: none"> · Решение Kaspersky Security для бизнеса (начиная с версии Расширенный) позволяет централизованно вести мониторинг уязвимостей и управлять установкой новейших исправлений.
<p>6.5A Обнаружение вторжений</p>	<p>Чтобы предотвратить несанкционированный доступ к сети, должна быть развернута система обнаружения вторжений.</p> <ul style="list-style-type: none"> · Решение Kaspersky Anti Targeted Attack Platform способно обнаруживать несанкционированный доступ к сети и аномальную активность потенциально вредоносных программ. Kaspersky Security для бизнеса отслеживает подозрительные действия в корпоративной сети и позволяет заранее настроить сценарий реагирования на такие действия.
<p>7.3A Тестирование на проникновение</p>	<p>В периметре безопасности и на пользовательских компьютерах должны не реже чем раз в год проводиться тестирования на проникновение для проверки защиты приложений, узлов и сети в целом.</p> <ul style="list-style-type: none"> · В набор сервисов кибербезопасности «Лаборатории Касперского» входит тестирование на проникновение различного типа, проводимое как с выездом на объекты клиента, так и дистанционно.

www.kaspersky.ru

© 2020 АО «Лаборатория Касперского». Все права защищены. Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.