СЛОНА ПО ЧАСТЯМ

Денис СУХОВЕЙ, «Аладдин Р.Д.»: Как начать миграцию на отечественное ПО в финансовом секторе и при этом не потерять конфиденциальные данные

Организацию, которая полностью независима от ситуации на внешнеполитической арене и последствий конфронтации западных стран с нашим государством, встретить сегодня практически невозможно, в разной степени это коснулось всех сфер бизнеса. Финансовые и банковские организации наряду с ИТ-сектором оказались на передовой, им первым приходится преодолевать экономические и политические сложности нашего времени. Спектр рисков в банковском бизнесе довольно широк, однако область ИТ-технологий выделяется на фоне остальных. В своей авторской статье специально для NBJ Денис СУХОВЕЙ, руководитель департамента развития технологий компании «Аладдин Р.Д.» рассказывает о том, как начать миграцию на отечественное ПО в финансовом секторе и при этом не потерять конфиденциальные данные.

Запрет использования ИТ-технологий, отказ от лицензирования и полное прекращение технической поддержки – наиболее частые способы санкционных ограничений. Понимая всю тяжесть последствий реализации таких рисков, российский банковский рынок начинает предпринимать вполне определённые шаги в области замещения западных технологий отечественными, и этот процесс весьма быстро набирает темп. Чувствуя реалистичность ИТ-рисков, многие организации переходят от так называемой «бумажной безопасности» к реальной практике импортозамещения. Переход к конкретным шагам вскрывает важную проблему – как обеспечить конфиденциальность ценной информации во время непростого и длительного переходного периода импортозамещения?

Начать путь замещения существующих импортных решений отечественными следует с самых базовых аспектов трансформации ИТ-инфраструктуры. Время ярких, красочных презентаций и долгосрочных планов с амбициозными целями заместить всё и вся закончилось. Большинство крупных организаций усвоило ряд вполне очевидных истин:

1 ИТ-поддержка бизнеса выстраивалась десятилетиями, и перейти за год-два на совершенно другие платформы не получится.

2 Государство всячески мотивирует организации на импортозамещение и даже реализует определённую финансовую поддержку этого процесса, однако основные затраты на такую масштабную трансформацию всё равно ложатся на плечи бизнеса.

3 Рынок отечественных ИТ-продуктов развивается, поэтому их выбор пока ограничен. Переход на сложные российские решения может обернуться для организации длительной и болезненной кастомизацией стандартных версий коммерческого ПО и оборудования.

4 Поскольку трансформации подлежит практически вся ИТ-инфраструктура, справиться своими силами, даже при наличии сильной команды, будет невозможно. Придётся вовлекать экспертные подрядные организации и обеспечивать коммуникации между ними.

Все эти факторы не только влияют на устойчивость и работоспособность ИТ-инфраструктуры, но и создают питательную среду для возникновения угроз утечки ценной и конфиденциальной информации. Банковский бизнес максимально чувствителен к этому виду угроз – компрометация данных приводит к серьёзным финансовым и репутационным потерям. Таким образом, возникает сложнейшая задача – не только пройти длительный путь перехода на отечественные решения, но и при этом не потерять контроль над защитой конфиденциальности в непростых условиях трансформации.

Грамотное структурирование процесса перехода является первым обязательным условием постановки задач по импортозамещению и обеспечению защиты конфиденциальности банковской информации.

Опыт решения задач по переходу на новую инфраструктуру укладывается в последовательную реализацию трёх этапов базового плана импортозамещения.

РИС.1 БАЗОВЫЙ ПЛАН ИМПОРТОЗАМЕЩЕНИЯ

Адаптация – первый этап, на котором организация проводит анализ всех своих ИТ-решений и акцентирует наиболее чувствительные к ограничениям области. Как правило, к таковым относятся информационные системы и отдельные сегменты рабочих станций сотрудников, от работы которых зависят основные бизнес-процессы. Именно ключевые информационные системы являются наиболее зрелыми и сложными, риск потерять или скомпрометировать их вынуждает подходить к процессу замены осторожно, поэтому переход на отечественную альтернативу может занять несколько лет. Задачей отдела ИБ на первом этапе является обеспечение конфиденциальности информации в этих системах. Ключевой принцип, реализуемый на данном этапе – «Если не можешь заменить ИТ-систему быстро, обеспечь снижение ИБ-рисков».

Интеграция – на втором этапе организация должна позаботиться о формировании ИТ-инфраструктуры переходного периода и построить технологическую основу для новых информационных систем. Наиболее логичным решением сегодня является создание пилотных зон из серверов приложений, баз данных и сегментов рабочих станций на ОС Linux. Во-первых, на таких участках производится апробация отечественных платформ и продуктов, во-вторых, появляется технологическая основа для построения новых информационных систем. На данном этапе задачей отдела ИБ является подбор и обкатывание российских средств защиты информации (далее СЗИ), поддерживающих ОС Linux. Важнейшим критерием для средств защиты будет являться способность интегрироваться в гетерогенную среду управления, т.е. СЗИ для ОС Windows и Linux должны иметь одни принципы эксплуатации и настройки. В идеале средства защиты должны управляться из единой консоли администратора.

ОТ ПРИМЕНЯЕМЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ПОТРЕБУЕТСЯ ВЫСОКИЙ УРОВЕНЬ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОСТИ И, С ДРУГОЙ СТОРОНЫ, МАКСИМАЛЬНОЕ УДОБСТВО И ПРОЗРАЧНОСТЬ ДОСТУПА ДЛЯ АВТОРИЗОВАННЫХ ПОЛЬЗОВАТЕЛЕЙ

Полный переход – построение новых информационных систем на подготовленной инфраструктуре с дальнейшей миграцией данных и пользователей. Данный этап наиболее важный, ведь он подразумевает перезапуск бизнес-процессов на отечественных ИТ-решениях. Как и говорилось ранее, для реализации этого этапа потребуется участие экспертов из нескольких областей – консультантов, вендоров, ИТ-интеграторов. На данном этапе обеспечение конфиденциальности данных и предотвращение утечек информации из инфраструктуры переходного периода является ключевой задачей отдела ИБ. Логично предположить, что от применяемых СЗИ потребуется высокий уровень защиты конфиденциальности и, с другой стороны, максимальное удобство и прозрачность доступа для авторизованных пользователей.

Итак, для решения задач безопасности на всех трёх этапах необходимо:

1 Определить метод предотвращения утечки и защиты от возможной компрометации важной и конфиденциальной информации.

2 Выбрать и опробовать средство защиты, обеспечивающее единый подход и бесшовное применение шифрования информации в операционных системах Windows и Linux.

3 Обеспечить защиту наиболее критичных участков существующей ИТ-инфраструктуры. Установить контроль конфиденциальности на дисках серверов приложений и рабочих станциях под управлением ОС Windows.

4 Обеспечить создание защищённых рабочих станций на ОС Linux, что позволит решить непростую задачу предотвращения утечек конфиденциальной информации на этапе создания новой архитектуры ИТ-системы.

Всем предъявляемым требованиям соответствует новый продукт линейки Secret Disk от компании «Аладдин Р.Д.» – Secret Disk Linux. Secret Disk Linux является полностью отечественным средством защиты информации, реализующим криптографическую защиту данных на дисках серверов и рабочих станциях. Решение обеспечивает максимальный уровень прозрачности доступа к защищаемым данным для авторизованных пользователей. Secret Disk Linux является наследником технологий шифрования от сертифицированного ФСБ России модуля шифрования Secret Disk Crypto Engine (для Windows), обеспечивает единый универсальный подход к защите конфиденциальности на компьютерах под ОС Windows и Linux.

Криптографическая защита информации в Secret Disk Linux обеспечивает превентивную защиту от утечки и компрометации банковских данных.

Комплексное применение продуктов линейки Secret Disk создаёт безопасную среду и возможность защитить данные в гетерогенной среде, что критически важно на этапе перехода в новую инфраструктуру:

- Secret Disk 5 обеспечивает защиту от утечек на рабочих станциях под управлением ОС Windows.
- Secret Disk Enterprise с клиент-серверной архитектурой гарантирует централизованное управление и контроль большого количества рабочих станций.
- Secret Disk Server предотвращает утечки данных на файловых серверах и серверах приложений.
- Новый Secret Disk Linux позволяет прозрачно встроить криптографическую защиту уровня ядра операционной системы и обеспечивает работу пользователей только с зашифрованной информацией. NBJ