# Эффективное управление цифровыми сертификатами – очередной вызов для ИБ

**Мария Дордий,** *начальник отдела ИБ, розничная сеть "Магнит"*

Мария Дордий, начальник отдела ИБ,ГК "Магнит", рассказала корреспонденту журнала "Информационная безопасность" о том, как повысить эффективность обеспечения безопасности крупного ритейла.

**– Мария, расскажите, пожалуйста, о себе.**

– Я закончила университет в Краснодаре по направлению "Информационные технологии в экономике". Уже на третьем курсе у меня было огромное желание осваивать профессию на практике: я начала работать и программировать, проба пера была на Delphi. Закончив институт, поняла, что хочу работать в крупнейшем российском ритейлере. Меня, как магнитом, притягивала возможность работы в современной, перспективной компании, использующей эффективные инновации.

Закончив институт, поняла, что хочу работать в крупнейшем российском ритейлере.

**– Почему выбрали ИБ для развития карьеры?**

– Все сложилось очень неожиданно. На собеседовании в "Магните" мне предложили попробовать силы в направлении ИБ – и 12 лет в компании пронеслись как одно мгновение. Я окунулась в очень динамичную сферу электронного документооборота и использования электронной подписи (ЭП). Появилось множество абсолютно новых и интересных задач. У меня была возможность с нуля создать в компании свод организационных и технических правил использования и аудита электронной подписи. Нам постоянно приходилось искать и внедрять новые решения, например, для использования ЭП в виртуальной среде, адаптировать процессы компании под изменения в законодательстве, принимать активное участие в миграции с бумажного документооборота на электронный. Иногда нам удавалось взаимодействовать с разработчиками систем электронного документооборота, банками для развития их продуктов. Благодаря совместным усилиям с нашим участием в некоторых продуктах появился функционал управления доступом, журналирование событий, удобная разблокировка пользователей и СКЗИ.

Нам постоянно приходилось искать и внедрять новые решения.

Благодаря совместным усилиям с нашим участием в некоторых продуктах появился функционал управления доступом, журналирование событий, удобная разблокировка пользователей и СКЗИ.

**– Какова специфика организации информационной безопасности в ритейле?**

– Все мы понимаем, что в любой организации всегда на первом месте стоит достижение бизнес-целей. В случае с коммерческими организациями это рост доходов, масштабирование, опережение конкурентов, предложение покупателям новых сервисов. Задачи ИТ и ИБ как раз и направлены на достижение этих целей за счет автоматизации и оптимизации затрат на бизнес-процессы.

В нашей отрасли сильно востребованы средства базовых уровней ИБ (управление доступом и сертификатами как раз относится к ним), которые не только повышают уровень защиты, но и оптимизируют затраты рабочего времени на управление теми или иными операциями. Учитывая масштабы, количество филиалов и сотрудников, даже небольшая экономия на одного пользователя позволяет сэкономить значительную сумму в рамках всей компании.

По этим причинам мы делаем больший упор на средства автоматизации физической защиты, – в разрезе всей компании это позволяет нам не только сэкономить значительные средства, но и предотвратить воровство товаров.

**– Используете преимущественно облачные технологии или собственную инфраструктуру?**

– Здесь приходится балансировать. Для повышения операционной эффективности, оптимизации затрат и гибкости масштабирования ИТ-сервисов, конечно же, мы используем облачные решения.

Одно из таких решений – Microsoft Azure. Платформа позволяет развертывать и тестировать сервисы быстрее, чем расширение инфраструктуры в локальных центрах обработки данных, при этом обеспечивается соблюдение строгих правил безопасности.

Ранее я упоминала сервис облачной ЭП. Этот сервис позволяет снижать затраты на обслуживание токенов (СКЗИ), нивелировать компрометацию физических токенов, повысить уровень безопасности за счет журналирования всех действий администраторов и пользователей сервиса, а также повысить отказоустойчивость благодаря имеющемуся горячему резервированию.

**– Известно, что, к примеру, банковская сфера сильно зарегулирована в отношении информационной безопасности, но нельзя сказать то же самое о ритейле. Как вы считаете, необходимо ли более пристальное внима-**

**ние законодателей и регуляторов к этой сфере?**

– В последние годы к ритейлу не менее пристальное внимание со стороны регуляторов. Примерами тому служат такие законодательные проекты, как ЕГАИС – контроль оборота алкогольной продукции, маркировка товаров, Меркурий – контроль учета ветеринарных свидетельств, реформа 63-ФЗ "Об электронной подписи" и т.д. Это очень масштабные проекты, заставившие перестроить большинство процессов компаний.

**– Как вы думаете, к чему может привести усиление законодательства в сфере ИБ в отношении ритейла?**

– Все зависит от позиции регулятора. Совместными силами и экспериментами можно создавать качественные решения, если, конечно, регулятор открыт для взаимодействия с бизнесом. На самом деле я думаю, что ритейл самостоятельно должен выбирать, стоит ли ему экономить на ИБ, где это допустимо, где является необходимой мерой.

Риски доступа к сети компании, хакерские атаки, утечка конфиденциальной информации или персональных данных могут повлечь серьезные убытки, поставить под угрозу репутацию и положение на рынке, потерю покупателей.

**– Почему вашей организации потребовалась автоматизация управления жизненным циклом цифровых сертификатов? Что послужило толчком к поиску решения и реализации проекта?**

– В нашей компании около 20 тыс. цифровых сертификатов, перевыпускаемых ежегодно. Такие объемы – это серьезный вызов для внутренней службы ИТ. А когда речь заходит об управлении ключами электронной подписи, выданными внешним аккредитованным удостоверяющим центром, сложность существенно возрастает.

Особенно остро мы прочувствовали проблему при старте ЕГАИС, когда за несколько месяцев нам нужно было выпустить порядка 12 тыс. цифровых сертификатов для торговых объектов, подключенных к ЕГАИС. Сотрудникам приходилось работать круглосуточно, их ошибки при вводе ПИН-кода приводили к блокировке токенов, как следствие затягивались сроки подключения торговых объектов к ЕГАИС, поэтому возникала необходимость поставки новых устройств.

Не будем забывать и об обязательных требованиях со стороны ФСБ в части эксплуатации ключей квалифицированной электронной подписи и их носителей. Особую сложность вызывают требования по ведению соответствующих журналов учета СКЗИ.

Поэтому мы искали решение, которое не только оптимизирует операции с сертификатами и их учет, но и позволит мониторить весь объем и сроки действия сертификатов, выданных удостоверяющим центром.

**– Внедрена ли такая система в розничной сети "Магнит"? По каким ключевым критериям осуществляли поиск решения?**

– Да, мы приобрели и внедрили такое решение в 2018 г.

В первую очередь нам требовалось автоматизировать управление несколькими десятками тысяч токенов и цифровых сертификатов, поддержка работы с самыми распространенными в нашей стране моделями токенов (SafeNet eToken, JaCarta, Rutoken и т.д.) и компонентами ИТ-инфраструктуры (Active Directory, КриптоПРО УЦ, Windows CA и т.п.), мы внимательно изучали функциональные возможности различных решений, представленных на рынке.

Вторым ключевым критерием была возможность доработки решения под наши требования. За время эксплуатации мы активно участвовали в развитии решения, важнейшей доработкой для нас были журналы учета средств криптографической защиты и цифровых сертификатов, управление различными параметрами СКЗИ на уровне политик, разработка дашборда.

Если говорить о дополнительных опциях, нам было интересно подобрать решения, делающие упор не только на задачи администраторов и операторов PKI, но и упрощающие типовые задачи рядовых пользователей. Как я упоминала ранее, у нас в обороте находится около 20 тыс. сертификатов, чрезвычайно сложно следить за ними даже при наличии специализированных и эффективных средств мониторинга. Очевидно, что мониторинг собственных сертификатов отвечает интересам рядовых сотрудников. Соответственно, наличие полноценного и качественного пользовательского интерфейса (для отслеживания тех же сроков действия сертификатов) отвечает интересам всей компании.

**– Как проходило внедрение системы?**

– Для начала мы провели пилотное тестирование всех рассматриваемых решений. В рамках тестирования мы не только проверяли возможности автоматизации и оптимизации рутинных операций по обслуживанию PKI, нам важно было убедиться в готовности решения работать со спецификой "Магнита": например, не все точки были в домене, у одного пользователя мог быть "зоопарк" токенов и сертификатов, которые нужно было взять под управление.

По итогам тестирования при содействии вендоров мы оценили результаты и смогли принять взвешенное решение и выбрать продукт, обладающий наилучшим соотношением "цена/качество", разумеется, с нашей точки зрения потенциального потребителя.

Весь процесс внедрения и масштабирования решения, учитывая опыт, полученный при тестировании и поддержке вендора, занял несколько месяцев. Хочется отдельно отметить важность этапа пилотного тестирования. Мы смогли намного лучше понять возможности всех продуктов и особенности их функционирования, что значительно упростило промышленное внедрение. Более того, как раз на этапе пилотного тестирования были выявлены все подводные камни построения процесса централизованного управления и мониторинга ключей электронной подписи, а также их носителей. Разумеется, к этапу внедрения все эти подводные камни были благополучно нейтрализованы.

**– Как оцениваете результаты внедрения?**

– Признаюсь, система централизованного управления и мониторинга ключей электронной подписи, а также их носи-

В последние годы к ритейлу не менее пристальное внимание со стороны регуляторов. Примерами тому служат такие законодательные проекты, как ЕГАИС.

Я думаю, что ритейл самостоятельно должен выбирать, стоит ли ему экономить на ИБ.

Особенно остро мы прочувствовали проблему при старте ЕГАИС, когда за несколько месяцев нам нужно было выпустить порядка 12 тыс. цифровых сертификатов для торговых объектов, подключенных к ЕГАИС.

телей существенно увеличила эффективность ряда наших бизнес-процессов.

Решение снизило нагрузку на ИТ-подразделения, повысило уровень информационной безопасности, улучшило степень мониторинга процесса эксплуатации СКЗИ и выпуска цифровых сертификатов.

**– А как именно изменились рабочие процессы и как они повлияли на работу сотрудников? Позволила ли система сократить издержки компаний на рутинные операции обслуживания инфраструктуры PKI?**

– Из наиболее существенных изменений: количество операций, время настройки СКЗИ сократились в несколько раз, ошибки типа "человеческий фактор" и блокировка СКЗИ сведены к минимуму.

У сотрудников появился сервис самообслуживания: они самостоятельно меняют ПИН-код к токену, минуя внутреннюю систему обработки заявок (Service Desk), автоматизированный мониторинг сроков действий сертификатов своевременно уведомляет пользователей и операторов о необходимости обновления сертификатов. Теперь пользователь сам может принять меры для обновления сертификата, не дожидаясь напоминания от оператора или руководителя.

В свою очередь, функционал ИТ с операциями инициализации токенов, формирования ПИН-кода пользователя и администратора, а также заполнение параметров для сертификата, формирование закрытого ключа и запроса на сертификат, установка сертификата пользователю полностью автоматизированы.

Система позволяет централизованно управлять и отслеживать состояние любого цифрового сертификата или носителя у любого сотрудника компании. Вся эта информация отображается в соответствующей карточке пользователя.

**– Каким образом система позволила повысить уровень информационной безопасности компании?**

– Одним из ключевых преимуществ данной системы я могу назвать широкие возможности мониторинга действий с сертификатами и их носителями. Действительно, все операции фиксируются в журнале аудита, есть удобная специализированная панель мониторинга (дашборд), позволяющая в реальном времени наблюдать за состоянием СКЗИ, сертификатов, реагировать на инциденты с блокировкой СКЗИ, проблемы с агентами. Более того, в карточке каждого пользователя можно посмотреть не только присвоенные ему сертификаты и носители, но и все события, связанные с действиями этого пользователя.

В руках подразделения ИБ появился инструмент управления политиками настройки СКЗИ и выпуска сертификатов, аудита действий сотрудников, журналирование и отчетность по СКЗИ и цифровым сертификатам. В случае возникновения инцидента или наличия риска компрометации сертификата (или носителя) есть возможность оперативно заблокировать работу токена.

А еще удобные сервисы самообслуживания, которые также повышают общий уровень информационной безопасности. Казалось бы, какая связь между ними? Однако, как показывает практика, если человеку неудобно пользоваться каким-то инструментом, то он старается его обойти и самостоятельно упростить свою работу. Из-за этого возможны частые сбои и прочие инциденты, что негативно сказывается как на уровне ИБ, так и на загрузке соответствующего персонала. Наглядный пример – ситуация с паролями во многих компаниях по всему миру: пользователи порой откровенно саботируют выдвигаемые требования к безопасности паролей, часто забывают их. Это и негативно сказывается на уровне ИБ компании, и генерирует лишнюю нагрузку на персонал отделов ИТ и ИБ.

**– К каким изменениям функционирования корпоративной ИТ-инфраструктуры в перспективе 3–5 лет нужно готовиться АО "Тандер"?**

– Новые реалии, перевод сотрудников на удаленную работу, в том числе и в сфере электронного взаимодействия, задают курс на облачные технологии

Облачные технологии – это тоже определенный вызов. С одной стороны, они позволяют существенно сэкономить на поддержке и обслуживании ИТ-инфраструктуры, а с другой – возникает ряд вопросов в сфере информационной безопасности. На мой взгляд, к операторам облачных сервисов должны предъявляться повышенные требования по защите информации, в том числе по защите коммерческой тайны. Ведь фактически мы и другие коммерческие организации доверяем им самое ценное. Увы, облачные технологии являются относительно новым явлением, чтобы можно было составить достоверную, качественную статистику и выявить ключевых доверенных игроков. Я думаю, в ближайшие пять лет мы столкнемся с целой волной поглощений небольших организаций сферы облачных технологий более крупными игроками, в первую очередь потому, что они не только будут предоставлять более качественный сервис, но и станут обладать куда большими возможностями по защите информации внутри облачной инфраструктуры.

Отмечу, что прошлогодний массовый переход на удаленную работу мы как специалисты ИБ ожидали не ранее чем через пять лет. Увы, пандемия катализировала этот процесс. Далеко не все оказались к нему готовы. Также в полный рост встала проблема бесконтактных способов взаимодействия с нашими покупателями.

В остальном мы стараемся шагать в ногу со временем и изменениями в законодательстве. В этом году мы взяли курс на облачную электронную подпись для комфортной дистанционной работы наших сотрудников, это неизбежный шаг.

Ближайшая перспектива – интеграция внедренной системы централизованного управления и мониторинга PKI с облачными решениями для сертификатов. Уже совсем скоро, в рамках пилота, часть наших сотрудников смогут поближе познакомиться с этой технологией. ●

Облачные технологии – это тоже определенный вызов. С одной стороны, они позволяют существенно сэкономить на поддержке и обслуживании ИТ-инфраструктуры, а с другой – возникает ряд вопросов в сфере информационной безопасности.

Я думаю, в ближайшие пять лет мы столкнемся с целой волной поглощений небольших организаций сферы облачных технологий более крупными игроками.

Прошлогодний массовый переход на удаленную работу мы как специалисты ИБ ожидали не ранее чем через пять лет.

Ваше мнение и вопросы присылайте по адресу is@groteck.ru