для EPAM Systems 0,18 %, для IBA Group получена отрицательная доходность на уровне 0,03 %, для Yandex — 0,1 %. При использовании простейшей версии модели Марковица из портфеля исключается ценная бумага с отрицательной ожидаемой доходностью.

В результате решения нелинейной оптимизационной задачи для заданной общей доходности портфеля в размере 0,21 % он оказался оптимальным при долевом инвестировании средств (0,47; 0,53) в акции компаний EPAM и Yandex соответственно. Доходность составит 0,1143 % и 0,0957 % с минимальным риском для инвестора на уровне 2 %.

Источники

1. Investing.com – котировки и финансовые новости [Электронный ресурс]. — Режим доступа: https://ru.investing.com. — Дата доступа: 20.03.2021.

2. *Читая, Г. О.* Математические модели анализа и прогнозирования динамики финансовых активов / Г. О. Читая, А. Е. Тарасюк // Белорус. экон. журн. — 2016. — № 4. — С. 132–141.

А. А. Гордич, *канд. техн. наук, доцент*
gordich@tut.by
БГЭУ (Минск)

ТЕХНОЛОГИЯ КОМПЛЕКСНОЙ ЗАЩИТЫ ЭКОНОМИЧЕСКОЙ ИНФОРМАЦИИ

Экономическая безопасность предприятий, организаций и государства в целом напрямую зависит от информационной безопасности. Обеспечение информационной безопасности деловой переписки является чрезвычайно важной задачей любой частной компании или государственной организации. Информация, конфиденциальность которой нарушена, теряет свою ценность, поэтому исследование и изучение методов и средств обеспечения информационной безопасности является весьма важной научной и практической задачей.

Основными методами обеспечения информационной безопасности являются криптография и стеганография. Криптография позволяет шифровать секретное сообщение, при стеганографии скрывается сам факт наличия секретных данных. Для сокрытия секретных данных используется стегоконтейнер, называемый также файлом-носителем или контейнером.

Существует достаточно большое количество программных средств, с помощью которых обеспечивается стеганографическая защита информации. В настоящей работе были выбраны и исследованы такие программы, как WbStego4.3 open, OpenPuff v3.30, Jphswin, Silenteye, QuickStego, Deepsound и Xiao Stenografy. В них, за исключением QuickStego, реализуются два метода защиты — криптографический и стеганографический. Для криптографического преобразования могут использоваться различные алгоритмы шифрования.

Стеганографические программы WbStego4.3 open, OpenPuff v3.30, Jphswin, Silenteye, QuickStego, Deepsound и Xiao Stenografy имеют различные возможности. Так, программа WbStego4.3 open позволяет в качестве контейнеров использовать текстовый документ формата *.txt, графические контейнеры форматов *.pdf и *.bmp, а также web-страницу, а программы Jphswin и QuickStego — лишь графическое изображение. Отличительной особенностью программ OpenPuff v3.30, Xiao Stenografy и Silenteye является то, что они скрывают секретные данные в аудиоконтейнерах и графических изображениях. Программа Deepsound внедряет секретные данные в аудиоконтейнер. Как видим, программа WbStego4.3 open поддерживает большее число форматов контейнеров по сравнении с другими программами. С помощью рассмотренных стеганографических программ можно внедрять секретные данные небольшого размера в любые контейнеры, однако целесо-

образно использовать графический контейнер, поскольку он позволяет скрыть больший объем информации при помощи любой стеганографической программы.

В настоящей работе предлагается технология комплексной защиты экономической информации, включающая стеганографический и криптографический методы, реализуемая следующим образом. С помощью стеганографической программы WbStego4.3 open, OpenPuff v3.30, Jphswin, Silenteye, Deepsound или Xiao Stenografy шифруются и внедряются секретные данные в любой контейнер. Как отмечалось ранее, лучше всего использовать графический контейнер. В процессе криптографического преобразования необходимо задавать секретный ключ, с помощью которого происходит шифрование и расшифровывание. Размер ключа небольшой и составляет, как правило, десятки и сотни байт. Ключ предлагается внедрять в другой графический контейнер. Таким образом, абонент получает два стегоконтейнера: один содержит секретный ключ, другой — секретные данные. Для расшифровывания секретных данных абонент вначале извлекает из первого стегоконтейнера с помощью стеганографической программы секретный ключ, а затем из второго стегоконтейнера извлекает и расшифровывает секретные данные.

Э. В. Дашук, *ассистент*
ellina.dashuk@gmail.com
БГЭУ (Минск)

PROCESS MINING КАК ИНСТРУМЕНТ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ БИЗНЕС-ПРОЦЕССОВ

Практически любой бизнес состоит из процессов. Одни из них выполняются исключительно людьми, другие автоматизированы, но многие представляют собой комбинацию того и другого. В современной организации почти все процессы поддерживаются или активируются программным обеспечением и ИТ-системами, а значит, оставляют после себя цифровые следы. Сканирование электронных журналов событий программного обеспечения и систем организации может помочь выявить закономерности и тенденции в этих системах и продемонстрировать, как на самом деле работает бизнес. Процесс получения и расшифровки данных из информационных логов журналов событий представляет собой интеллектуальный анализ бизнес-процессов или Process Mining.

Наиболее глубоко исследованием технологии Process Mining занимается датский профессор Эйндховенского технического университета Вил ван дер Аалст, который на протяжении 25 лет анализирует методы и инструменты интеллектуального анализа бизнес-процессов.

Углубленный анализ бизнес-процессов позволяет не только смоделировать реальную картину того, как действительно реализуется процесс, но также понять причины отклонений от спроектированных моделей, определить «узкие» места процессов и в дальнейшем избежать неверного выполнения шагов бизнес-процессов. Вместе с тем важнейшим условием объективных результатов Process Mining является обязательная фиксация событий в информационных журналах (системах), поскольку неполная информация приведет в итоге к искаженным закономерностям и не позволит однозначно визуализировать бизнес-процесс и, как следствие, решить имеющуюся проблему [1, с. 46].

Применение технологии Process Mining целесообразно как для простых массовых процессов, которые производятся несколько тысяч (десятков тысяч, сотен тысяч) раз в день (например, банковское обслуживание клиентов), так и для сложных длинных многоуровневых процессов, затрагивающих работу множества департаментов. И если в первом случае Process Mining позволит сэкономить на отладке работы каждого звена, что в совокупности