



18

Юрий ПРИПАЧКИН
РАКИБ
«Цифровой рубль
должен быть!»



34

Наталья КАСПЕРСКАЯ
АРПП «Отечественный софт»
«Импортозамещение
в ИБ почти полное»



46

Алексей ВОЙЛУКОВ
АБР
Радикально менять
законодательство

54

Василий ОКУЛЕССКИЙ
Банк «Возрождение»
Нужен ли нам PCI DSS?

63

Владимир КУСТОВ,
Сергей КИРЮШКИН
УЦ ГИС, «Газинформсервис»
Почему в РФ нет
WebTrust CA

110

Борис СТОЛПАКОВ
Историк криптографии
За боевые заслуги

БЕЗОПАСНОСТЬ ЦИФРОВОГО РУБЛЯ. БЕЗ ДЫРКИ В КОШЕЛЬКЕ





КИБЕРАРЕНА

28 апреля 2022 года

НОВОЕ ОНЛАЙН-ШОУ

**Проект Медиа Группы «Авангард»
и компании «Газинформсервис»**

Команды ведущих профессионалов в области информационных технологий и информационной безопасности встретятся на шоу «Киберарена», чтобы в соревновании показать свой профессионализм и доказать, что именно они умеют находить лучшие решения для сложнейших задач по защите информации.





Игорь НЕКРАСОВ
главный редактор BIS Journal

Дорогие читатели, этот номер мы посвятили импортозамещению. Информационных поводов, как вы понимаете, достаточно. Но нам не хочется, чтобы эта тема воспринималась в узком, местечковом значении слова. Дело в том, что и само слово это, и набор понятий, которые из него только начинают прорасти, ещё мало осмыслены, по крайней мере, в массах. Например, в интернете нашлась только одна (попробуйте, поройтесь!) фраза, содержащая намёк на такое осмысление. Блогер под ником Демарио замечательно заявляет: «Главная опасность импортозамещения — снижение уровня знания географии». Мне, честное слово, понравилось. Соединив немного пафоса и немного юмора, он зафиксировал предельно ограниченное понимание идущих в стране процессов, фактически свёл их к возврату к натуральному хозяйству, мол, смартфоны теперь будем ковать в своей деревеньке на своей маленькой коленке. Удивительно, но так думают многие.

Надеюсь, почитав материалы этого номера, вы поймёте, что это не так. Понятно, большинство посвящено прикладному аспекту: что делать, как быть сегодня-сейчас, но статьи о цифровом рубле и выступление Натальи Касперской вырывают нас в другую реальность. Реальность, где наше импортозамещение (а создание цифрового рубля — не более, чем его составляющая) — это часть мировых процессов, меняющих окружающую действительность, всю планету на наших глазах. То есть речь идёт не о сужении знаний географии, а, как минимум, об открытии эры новых Великих географических открытий.

Как в своё время Колумб и Васко да Гама открыли Новое время — эпоху капитализма, так и сегодня мы участвуем в трансформации Истории. (Сказал бы «в цифровой трансформации Истории», но, думаю, так говорить всё же неправильно, дело не только в цифре). Слом, сдвиг, точка бифуркации... — слов, обозначающих такие моменты, много — суть одна: завтра мы будем жить уже в другую эпоху.

Так что я собственно хочу сказать? Импортозамещение — это не наша маленькая деревенька и наша маленькая коленка, импортозамещение — это портал возможностей. Читайте номер, смотрите шире, и вы услышите, как Время величаво даёт команду:

— Поднять паруса!

ОБЩЕСТВЕННЫЙ РЕДАКЦИОННЫЙ СОВЕТ

Войлуков А.А. — вице-президент Ассоциации банков России
Сычёв А.М. — доцент МГТУ им. Баумана, доктор технических наук
Шипилов В.В. — исполнительный директор Ассоциации российских банков, кандидат технических наук

РЕДАКЦИОННАЯ КОЛЛЕГИЯ

Велигура А.Н. — председатель комитета по банковской безопасности Ассоциации российских банков, руководитель комитета по безопасности НП «НПС», CISA, кандидат физико-математических наук
Виноградов А.Ю. — специалист Службы информационной безопасности КБ Максима (ООО)
Вихорев С.В. — советник генерального директора по информационной безопасности IT Expertise
Дзержинский Ф.Я. — независимый эксперт
Зубков А.Н. — генеральный директор ООО «Медиа Группа „Авангард“», директор Фонда содействия развитию безопасных информационных технологий (ФСРБИТ)
Курило А.П. — советник по вопросам ИБ ФБК и FBK CyberSecurity, кандидат технических наук
Левиев Д.О. — председатель Совета НП «Партнёрство специалистов по информационной безопасности»
Мельников С.Ю. — заместитель генерального директора ООО «Лингвистические и информационные технологии», доктор физико-математических наук
Некрасов И.В. — главный редактор журнала
Одудалов М.В. — руководитель службы Управления по обеспечению ИБ Банка ВТБ (ПАО)
Окулесский В.А. — заместитель начальника службы ИБ банка «Возрождение», кандидат технических наук
Пазизин С.В. — заместитель начальника Управления по обеспечению ИБ Банка ВТБ (ПАО), кандидат физико-математических наук
Рачкова Е.В. — управляющий директор Управления по обеспечению ИБ Банка ВТБ (ПАО)
Филипчук А.А. — технический директор ГК ЦРТ
Шумский Л.С. — руководитель службы информационной безопасности Яндекс Банка
Янсон И.А. — бизнес-партнер по информационной безопасности, Департамент безопасности ПАО «Сбербанк России», кандидат физико-математических наук

ЭКСПЕРТНАЯ ГРУППА

Баранов А.П. — руководитель департамента информационной безопасности факультета информационных технологий Финансового университета при Правительстве РФ, доктор физико-математических наук, академик Академии криптографии РФ
Батранков Д.В. — руководитель направления сетевой безопасности Positive Technologies
Гадарь Д.А. — вице-президент — директор департамента информационной безопасности, Tinkoff.ru
Калемберг Д.А. — генеральный директор ООО «СэйфТек»
Лукацкий А.В. — бизнес-консультант по безопасности
Сабанов А.Г. — заместитель генерального директора АО «Аладдин РД»
Сумманен К.Т. — директор по управлению проектами — вице-президент, Банк ВТБ (ПАО), кандидат физико-математических наук
Хайретдинов Р.Н. — директор по росту компании Bi.ZONE

РЕДАКЦИЯ ЖУРНАЛА

Главный редактор: **Некрасов И.В.**
Директор по развитию: **Минаков А.В.**
Арт-директор: **Мельников Н.С.**
Руководитель интернет-проектов: **Воробьева А.А.**
Ответственный редактор: **Седов О.В.**
Обозреватели: **Куликов В.А., Бродская М.А., Покатаева Е.Н.**
Иллюстрация на 1-й обложке: **Зинаида Серебрякова**
Фото в номере: **Unsplash.com, Pixabay.com**
Цветокорректор: **Науменко М.Б.**

УЧРЕДИТЕЛЬ-ИЗДАТЕЛЬ

ООО «Медиа Группа „Авангард“»
Адрес: 127473, Россия, Москва, 3-й Самотечный переулок, д. 21
Тел.: +7 495 921 42 44
Интернет-версия: ib-bank.ru/bisjournal
E-mail: bis@ib-bank.ru

Зарегистрирован 13 августа 2010 года Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). Свидетельство ПИ № ФС 77-61378 от 10 апреля 2015 г.

Все права на материалы, опубликованные в номере, принадлежат журналу «BIS Journal — Информационная безопасность банков». Перепечатка и воспроизведение иными способами без разрешения редакции запрещаются. При использовании материалов ссылка на журнал обязательна. Мнение редакции может не совпадать с мнением авторов. Присланные материалы не рецензируются и не возвращаются.

Подписан в печать 05.04.2022. Тираж 5000 экз. Заказ № 402022. Цена договорная. Отпечатан в типографии «Московский Печатный Двор», 123298, г. Москва, 3-я Хорошевская 18, корп. 1, офис 201А

© BIS Journal, 2022



НОВОСТИ

5 В России, криминал, технологии

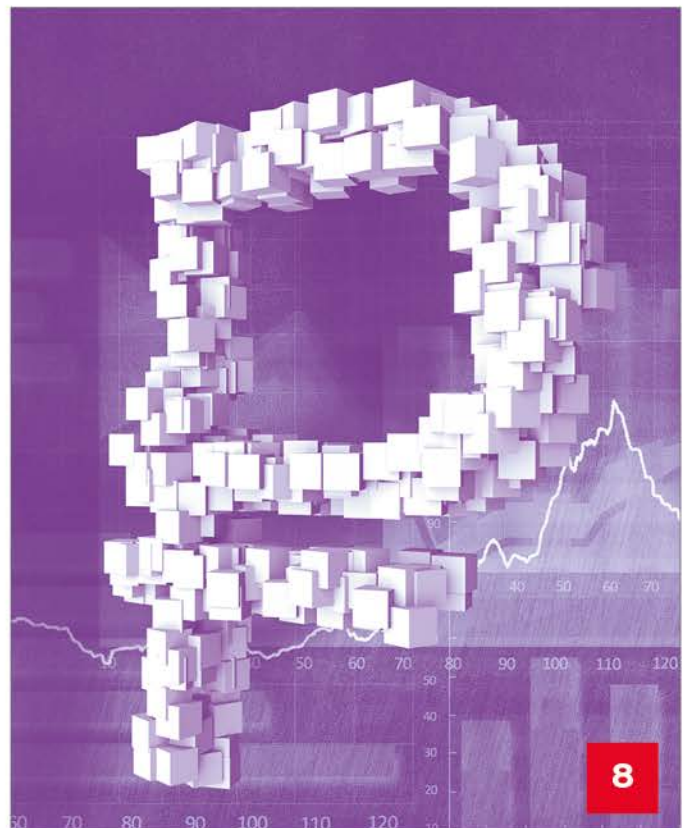


ТЕМА НОМЕРА: ЦИФРОВОЙ РУБЛЬ. ЭКСПЕРТИЗА ПРОБЛЕМЫ

- 8 Елена Покатаева (BIS Journal)
Цифровой рубль: благодаря или вопреки?
- 18 Юрий Припачкин (РАКИБ)
«Цифровой рубль должен быть элементом новой финансовой системы и обеспечиваться государством»
- 21 Виктор Достов (Ассоциация участников рынка электронных денег и денежных переводов)
«Отказ от децентрализованного подхода делает цифровой рубль менее защищённым»
- 23 Тимур Аитов (ТПП РФ)
О возможных путях использования стейблкоинов в России
- 24 Вадим Мазин (Surf)
«Практические аспекты внедрения цифрового рубля вызывают аналогии с системой быстрых платежей»
- 25 Артём Калихов (Waves Enterprise)
«Создание национальной системы цифрового рубля связано с рядом технологических вызовов»

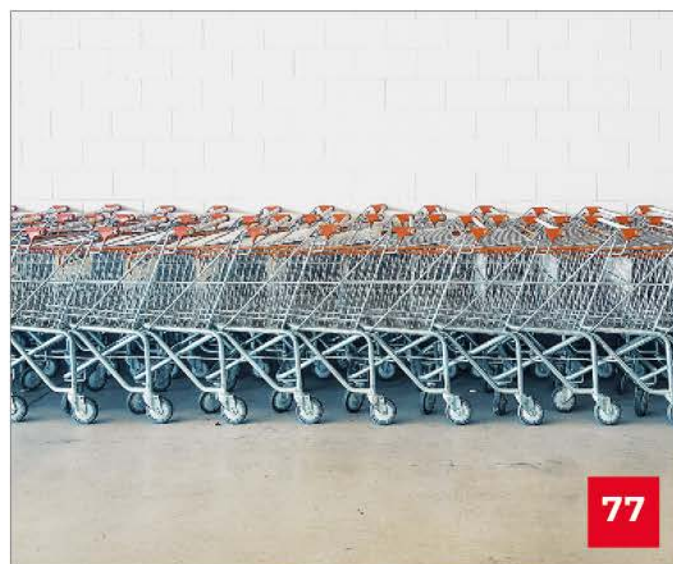
ИМПОРТОЗАМЕЩЕНИЕ

- 28 Денис Батранков (BIS Journal)
Импортозамещение грянуло
- 34 Наталья Касперская (АРПП «Отечественный софт»)
«Импортозамещение в ИБ почти полное»
- 36 Андрей Арефьев (ГК InfoWatch)
Приняли огонь на себя
- 39 Дмитрий Михеев (АйТи Бастион)
Тактика сегодня определит стратегию завтра
- 40 Дмитрий Левиев (Партнёрство специалистов по информационной безопасности)
Импортозамещение на практике — это...
- 42 Артём Прохоров (эксперт ИБ)
Не всё так плохо...
- 44 Корней Ревт (BIS Journal)
От культуры мировых брендов к проверенным отечественным платформам



БАНКИ

- 46 От первого лица**
Алексей Войлуков
(Ассоциация банков России)
Трендов немного, но они принципиальные
- 49 Вредные советы**
Екатерина Рачкова (Банк ВТБ)
Как съесть слона?
- 52 Технологии**
Валерия Мещерякова (BIS Journal)
Приоритеты расставлены
- 54 Полемика**
Василий Окулесский (эксперт BIS Journal)
Нужен ли нам PCI DSS?
- 57 Полемика**
Евгений Безгодов (Deiteriy)
Некоторые мифы о PCI DSS
- 60 Полемика**
Александр Крупчик (ДиалогНаука)
О необходимости PCI DSS
- 62 Полемика**
Евгений Бабицкий (Комплаинс Контрол)
Так нужен или нет?
- 63 SSL-сертификаты**
Владимир Кустов (УЦ ГИС),
Сергей Кирюшкин (Газинформсервис)
Весна пришла, как всегда, неожиданно
- 67 Опыт Сбербанка**
Иван Янсон (Сбербанк)
Новый статус: доверенные лица



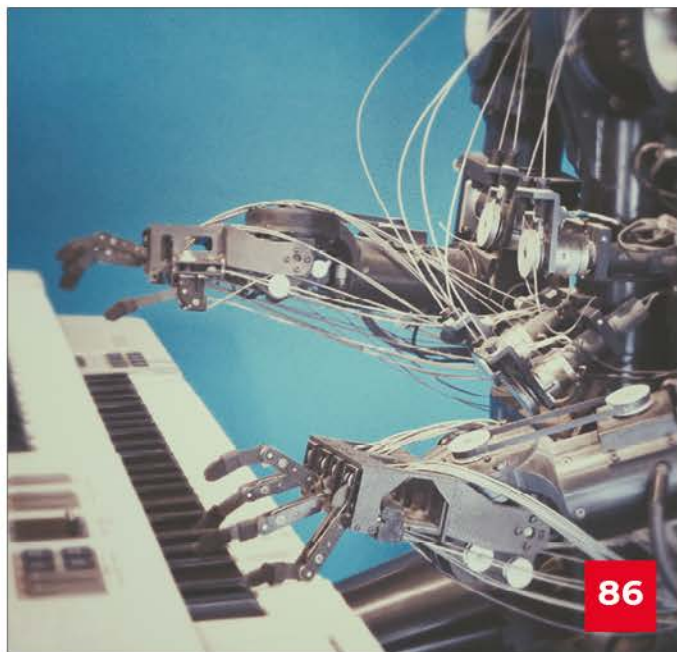
УГРОЗЫ И РЕШЕНИЯ

- 74 Финтех**
Олег Хныков (Positive Technologies)
Уязвимости в финтехе
- 77 Ритейл**
Павел Коваленко (Информзащита)
Между супермаркетами и покупателями
- 80 Комплаенс**
Тамара Деменкова (ЦИБИТ)
Сложные вопросы



ИНФРАСТРУКТУРА

- 82 Деловые мероприятия**
Сергей Вихорев (ИТ-Экспертиза)
Инфофорум-2022, ТБ-Форум-2022
- 84 Деловые мероприятия**
Валерий Куликов (BIS Journal)
Нужна ли вавилонская башня на цифровом фундаменте?
- 86 Искусственный интеллект**
Павел Былевский (Финансовый университет при Правительстве РФ)
«Искусственный интеллект». Исправление имени
- 90 Искусственный интеллект**
Елена Покатаева (BIS Journal)
Разные грани одной мечты
- 94 Обмен опытом**
Антон Нечипоренко, Андрей Эли (Ингосстрах)
Думайте сами, решайте сами...



СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

- 96** Андрей Жаркевич (Антифишинг)
А не перебор?

ОБРАЗОВАНИЕ И КАРЬЕРА

- 99 Мероприятия**
Мария Сидорова (RISC)
Вышли на международный уровень!
- 100 Обзор**
Марина Бродская (BIS Journal)
Приёмная кампания — 2022
- 103 Обзор**
Анна Катанкина (BIS Journal)
Будущее кибербезопасности — за женщинами!
- 106 Обзор ИноСМИ**
Злонамеренная киберактивность в глобальном масштабе



СУБЪЕКТЫ

- 110 История**
Борис Столпаков (историк криптографии)
За боевые заслуги
- 115 История**
Борис Столпаков (историк криптографии)
Реликвии криптографического фронта
- 118 Мнение**
Павел Никифоров (BIS Journal)
«Как некультурно!»
- 120 Заметки безопасника**
Александр Игонин (BIS Journal)
Семь аудитов на сундук безопасника

ФСТЭК ДАЁТ СРОК — 90 ДНЕЙ

ФСТЭК временно приостановила действие сертификатов на программные продукты крупных иностранных ИТ-компаний: IBM, Microsoft, Oracle, SAP и т.д.

Уже приостановлено более полусотни сертификатов. Их действие будет полностью прекращено, если вендоры не возобновят поддержку своих продуктов в течение 90 дней (со дня приостановки сертификатов).

Сертификация ведомством нужна для подтверждения соответствия

решений для управления предприятием, облачного хранения, аналитики, кибербезопасности и проч. требованиям по безопасности информации по разным классам защищённости и возможности использования в ГИС, автоматизированных системах управления технологическими процессами или на значимых объектах КИИ.

Теперь госинформсистемы и объекты КИИ должны будут ещё быстрее найти замену зарубежным продуктам.



ЕЩЁ ОДИН РЕЕСТР

Уполномоченный при президенте России по защите прав предпринимателей Борис Титов предложил кабмину создать федеральный реестр высокотехнологичных и/или инновационных компаний.

Со слов бизнес-омбудсмена, в условиях санкционного давления основная задача импортозамещения ложится именно на хай-тек-предприятия, но для эффективной господдержки нужно очертить круг её объектов.

По плану в реестр должны попасть компании, отвечающие нескольким критериям: общая система налогообложения, выручка за последний год — не более 15 млрд рублей, среднегодовой темп роста выручки за три последних года — не менее 30% для микропредприятий, 20% для малых и средних предприятий, 15% — для крупных, доля расходов на НИОКР за последние три года — более 3% от выручки, наличие исключительных прав на результаты интеллектуальной деятельности.



МИНЦИФРЫ ПОДДЕРЖИТ

Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации готовит план поддержки специалистов в области информационной безопасности в условиях санкций. В пресс-службе ведомства сообщили, что в перечень адресатов финпомощи планируют добавить ОКВЭД 74.90.9 (деятельность в области защиты информации).

Меры, разрабатываемые Минцифры совместно с ИБ-компаниями, направлены на разработчиков отечественных ИБ-решений, которые потенциально смогут заменить ушедшие с рынка средства защиты зарубежных вендоров.

«ИБ-специалисты — это важная и неотъемлемая часть ИТ-отрасли. Мы должны их поддерживать наравне с другими специалистами в области информационных технологий», — заявили представители министерства.

ГРАНТЫ И СУБСИДИИ

Замглавы Минцифры Максим Паршин рассказал, что на поддержку ИТ-компаний в бюджете заложено 7,5 млрд рублей. Также скоро будут утверждены постановления кабмина, обозначающие правила предоставления ИТ-субсидий.

Сейчас, чтобы заполнить предварительную заявку на грант, нужно зайти на сайт госуслуг как юрлицо.

Помимо этого, стало известно, что лимиты грантов по РФРИТ планируются увеличить до полумиллиона рублей, а по «Сколково» — до 300 млн рублей. Сроки реализации проектов продлят, зарплаты сотрудникам компаний-участников увеличат, а процедуру отбора и предоставления грантов при этом «серьёзно изменят».

По данным Министерства цифрового развития, связи и массовых коммуникаций, за прошлые два года гранты получили 378 проектов и компаний на общую сумму 12,5 млрд рублей.

ПРЕДСТАНУТ ПЕРЕД СУДОМ

Шестерых киберпреступников из разных регионов РФ ждёт суд в Ярославской области. Им приписываются 80 эпизодов взлома мобильного банкинга.

Члены группировки находили номера телефонов на сайтах объявлений и рассылали их владельцам SMS с фишинговыми ссылками. Далее на смартфоны жертв устанавливался софт, при помощи которого фигуранты получали доступ к личным кабинетам в банковских приложениях. Украденные таким образом средства переводились на подконтрольные счета и впоследствии обналичивались.

Преступная схема была раскрыта ещё в 2016 году. Сегодня потерпевшими по делу проходят жители 27 регионов, а объём уголовного дела превышает 200 томов. Если вина подсудимых будет доказана, им грозит лишение свободы на срок до десяти лет.

Впрочем, шесть лет они уже отсидели.

«ЕДУ» СЛИЛИ В СЕТЬ

Ссылка на базу данных в виде карты была опубликована в двух Telegram-каналах (общее число подписчиков — около 150 тысяч). По данным Whois, домен сайта создан и занят с 14 марта.

В начале марта компания «Яндекс.Еда» сообщила об утечке клиентских данных, причиной которой стали недобросовестные действия одного из сотрудников. Тогда были скомпрометированы адреса, номера телефонов, детализация заказов, время доставки и другое. Но, как сообщалось, ни платёжные данные, ни информация для входа в аккаунт опубликованы не были.

В компании заверили: новых инцидентов с того момента не происходило, а сервис — в сотрудничестве с надзорными и правоохранительными органами — делает всё возможное, чтобы минимизировать распространение данных.



СКИММЕР, КАМЕРА, СНОРОВКА

В Санкт-Петербурге раскрыто многомиллионное хищение средств с банковских счетов россиян, сообщили в МВД России. По подозрению в серии преступлений подобного рода задержан 27-летний житель Новосибирска.

По версии следствия, фигурант установил на потолке торгового центра скрытую камеру, которая была направлена на клавиатуру банкомата, находящегося в помещении — она фиксировала вводимые PIN-коды и передавала изображения

по мобильной связи. В сам банкомат при этом было вмонтировано скимминговое устройство, предназначенное для считывания данных с пластиковых карт. Это позволило преступнику изготавливать дубликаты карт и снимать деньги со счетов граждан, после чего переводить их на свои, а дальше конвертировать в криптовалюту.

Следствие полагает, что за два месяца жертвами злоумышленника стало больше сотни человек. Сумма ущерба превышает 12 млн рублей.

«КАК РАБОТАТЬ, НЕ ЗНАЕМ»

В конце марта была зафиксирована мощная кибератака на ИТ-инфраструктуру Росавиации. Была обрушена сеть, уничтожены документооборот, электронная переписка за полтора года и файлы на серверах. Также пропали все документы.

Суммарные потери — 65 Тб данных. Заявлено, что бэкапы не создавались, так как средства Минфином на это не выделялись.

«Сейчас идёт поиск реестра воздушных судов и авиационного персонала, удалена система государственных услуг <...> Как работать, не знаем», — сообщил источник в федеральном управлении.

Инцидент произошёл из-за некачественного исполнения договорных обязательств со стороны предприятия ООО «ИнфАвиа», осуществляющего эксплуатацию ИТ-инфраструктуры российских авиавластей.



ДАЁШЬ «ИНТЕЛОЗАМЕЩЕНИЕ»!

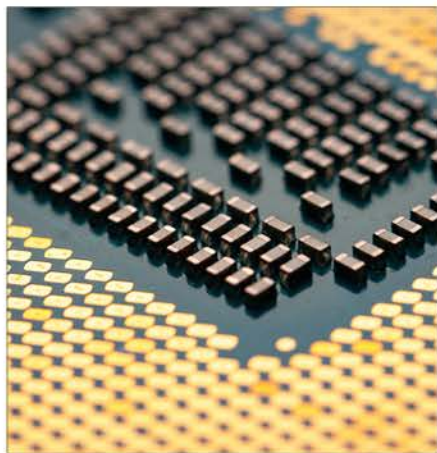
Крупнейшие производители процессоров компании AMD и Intel в начале марта объявили о полном прекращении поставок своей продукции в Россию.

В рамках пресс-конференции РУССОФТ представители отечественных компаний сообщили, что в ближайшее время планируют «поддержаться на старых запасах», а в

дальнейшем намерены перейти на российские процессоры. Появился даже термин «интелозамещение» — замещение процессоров компании Intel на российские аналоги. Правда, анонсировать конкретные продукты пока никто не готов.

Директор по развитию бизнеса компании Vinteo Б. Попов рассказал: «Мы ещё до 24 февраля вкладывали очень большие средства и главное — время наших разработчиков — в изучение всех процессоров, имеющихся на рынке. Не готов сейчас что-то анонсировать, но «интелозамещение» точно произойдёт».

Президент НП «РУССОФТ» Валентин Макаров со своей стороны отметил всеобщую готовность переходить на отечественную продукцию. Конечно, если таковая будет иметься в наличии: «Мы готовы переходить на российские процессоры, если их кто-то будет производить, их просто сейчас не производят».



РЕД ОС ОПТОМ И В РОЗНИЦУ

Обычные пользователи уже могут купить компьютер с российской операционной системой РЕД ОС в розничных магазинах, — заявил заместитель генерального директора компании «РЕД СОФТ» Р. Рустамов на пресс-конференции РУССОФТ.

Р. Рустамов рассказал: «Мы как разработчики системного ПО и ОС регулярно работаем с партнёрами, которые занимаются внедрением этого ПО. Необходимая экосистема создана, она интенсивно развивается, еженедельно выходит по несколько пресс-релизов. Мы развиваем экосистему и в части образовательной среды: не все пользователи могут быстро переключиться с Windows на российские решения, поэтому идёт работа с вузами, образовательными центрами, созданными по всей России».

«Обычные пользователи уже могут купить в розничных магазинах компьютер с российской операционной системой РЕД ОС, — подчеркнул Р. Рустамов. — Раньше мы понимали,

что обычному человеку российская ОС пока не очень интересна, но неожиданно для себя обнаружили, что на неё есть спрос (причём, ещё до февральских событий). И он растёт, об этом свидетельствуют розничные продажи ноутбуков и рабочих станций в магазинах. В настоящее время есть проблема с «железом», но логистические вопросы будут решены и ситуация стабилизируется».



СЛЕПОЙ УПРАВЛЯЕТ ГЛУХИМ

Закари Келленборн, учёный из Школы политологии и теории управления им. Шара, заявил в статье в журнале *Bulletin of the Atomic Scientists*, что предоставление искусственному интеллекту контроля над ядерным оружием может спровоцировать глобальную катастрофу.

Власти не имеют полных данных о военных платформах, а имеющаяся информация — структурно предвзята и не учитывает ожидаемых изменений. Обучение программ ядерного оружия на базе ИИ является проблемой — по причине недостатка реальных данных о поведении взрывов, — считает эксперт. Тем не менее сегодня с помощью ИИ осуществляется управление, например, американским ядерным бомбардировщиком B-21, российским ядерным беспилотником «Посейдон» и китайскими гиперзвуковыми ракетами.

ПО «ЦИФРОВОМУ» ПОЧЕРКУ

Специалисты IARPA (Агентства передовых исследований в сфере разведки) разработали ИИ-инструмент, анализирующий цифровые отпечатки текстовых сообщений — «это может сыграть важную роль в выявлении лиц, стоящих за кампаниями по дезинформации».

Новый метод называется NIATUS и работает он примерно так же, как инструменты, с помощью которых криминалисты определяют личность подозреваемого по почерку. В IARPA уверены: точно так же, как у людей есть индивидуальные различия при написании слов от руки, авторы в Сети имеют свои особенности при наборе текстов.

Так, при наличии достаточного количества вводных с помощью NIATUS можно будет детализировать цифровой отпечаток человека исключительно на основе письменного текста. Например, узнать, пытался ли злоумышленник выдать себя за кого-то другого или на самом деле текст написал бот-дезинформатор.



Елена
ПОКАТАЕВА
обозреватель
BIS Journal

ЦИФРОВОЙ РУБЛЬ: БЛАГОДАРЯ ИЛИ ВОПРОТРЕКИ?

Цифровая валюта как новая сущность и структура мировых финансов формируется прямо на наших глазах: прорастает из трещин системы глобальной гегемонии доллара США. Каков путь России в этот новый мир?

ПРЕДИСЛОВИЕ. ДЕДОЛЛАРИЗАЦИЯ ШАГАЕТ ПО ПЛАНЕТЕ

Китай ведёт активные переговоры с Саудовской Аравией об отказе от доллара США в расчётах за нефть. Это знаковое событие мирового масштаба, ведь Саудовская Аравия — важнейший игрок на глобальном нефтяном рынке, а Китай — ключевой потребитель нефти в мире. Беларусь и Россия приняли решение отвязаться от доллара в расчётах за энергоресурсы. И — вишенка на торте дедолларизации: отказ от поставок в так называемые недружественные страны российского газа с помощью скомпрометировавших себя валют.

По оценкам экономистов, фактически Владимир Путин решил заменить нефтедоллар на газорубль. Это означает разрушение традиционной структуры валютной системы РФ и ЕС. «Логика санкционной войны требует от Центробанка России полной дедолларизации (избавление от доллара США, евро, британского фунта, японской иены, швейцарского франка и др.), — подчёркивает Валентин Катаонов, председатель Русского экономического общества им. С. Ф. Шарапова. — В активах ЦБ из международных резервов могут остаться только китайский юань и золото».

По сути, Россия выходит из Бреттон-Вудской системы, которая разрешала стране печатать свою национальную валюту (рубль) только под заходящие в страну резервные валюты МВФ, получаемые главным образом от нефтегазового экспорта. Причём самый большой «гвоздь в крышку гроба» традиционной финансовой системы, привязанной к американскому доллару, забил сам нынешний гегемон: санкции в форме заморозки золотовалютных резервов России в США и ЕС фактически означают дефолт для доллара и евро, поскольку страны,

генерирующие эти валюты, отказались от своих обязательств.

Но уже к этому моменту доллар США утратил свою роль в качестве главной резервной валюты в международных резервах, уступив место китайскому юаню и другим валютам. Об этом говорится в мартовском отчёте МВФ: долларовая доля в международных резервах снижается в течение двух десятилетий, а главной причиной такого положения дел стало стремление центробанков многих стран диверсифицировать свои активы, предпочитая юань.

«Отказ от доллара и евро как от мировых резервных валют не такая уж фантастическая перспектива, наступает эра региональных валют», — написал в своём телеграм-канале зампред Совета безопасности РФ Дмитрий Медведев.

Наступление новой эры ускоряет поиски альтернативных платёжных инструментов. Так, Евразийский экономический союз (ЕАЭС) и Китай занимаются разработкой проекта независимой международной валютно-финансовой системы. В Евразийской экономической комиссии (ЕЭК) поясняют, что её основой станет новая валютная единица, которая будет рассчитываться как индекс национальных валют стран-участниц и цен биржевых товаров. Первый вариант новой системы должен появиться в ближайшее время.

В русле данного тренда Россия и Индия прорабатывают механизм расчётов в национальных валютах (рубли — рупии), причём за эквивалент предполагается взять валюту третьей страны — юань.

Ведущий аналитик Credit Suisse Золтан Позар считает, что мир находится в состоянии перехода к новой финансовой системе — «Бреттон-Вудс 3.0», в которой будет усиливаться роль незападных валют, чья стоимость опирается на сырьевые товары — золото, нефть, газ, металлы и т.д.

Рождение новых валют и расчётных механизмов происходит в формате кризиса и потому чревато дестабилизацией финансовой сферы, отмечает академик Александр Некипелов,

директор Московской школы экономики МГУ им. М.В. Ломоносова. По его мнению, России требуются инструменты для сглаживания последствий разрушения традиционных экономических и финансовых механизмов: переформатировать производства, обеспечить занятость трудовых ресурсов и т.д.

ЛЁД ТРОНУЛСЯ

Поиск новых финансовых инструментов уходит в цифру. Объединённые Арабские Эмираты решили превратить страну в криптооазис на Ближнем Востоке. Там наблюдается небывалый рост торговли криптовалютами. Эксперты говорят, что в страну поступают миллиарды долларов в обход банковской системы для инвестиций и бизнес-сделок. А госрегулятор ОАЭ срочно готовит специальные законодательные меры, разрешающие выдавать федеральные лицензии поставщикам услуг виртуальных активов.

Поскольку криптовалюты становятся одним из фронтов санкционной войны, а Китай демонстрирует явные успехи в практическом использовании цифрового юаня, США спохватились и, забыв о недавних объявлениях криптовалют угрозой нацбезопасности, решили пробиваться на позиции мирового лидера в формирующейся цифровой финансовой структуре мира. Соответствующий Указ об обеспечении ответственного развития цифровых активов (Executive Order on Ensuring Responsible Development of Digital Assets) президент США Джоозеф Байден подписал в начале марта.

В нём чёрным по белому заданы ключевые ориентиры: создавать международные правила и стандарты в сфере криптовалют, обеспечивать с их помощью укрепление позиций США как экономического лидера, снижать угрозы, провоцируемые геополитической нестабильностью. Подразумевается, в числе прочего, препятствование попыткам стран и персон, находящихся под санкциями США, использовать цифровые активы для обхода введённых ограничений.

В фарватере США, как всегда, следует Европа: председатель Европейского центрального банка Кристин Лагард призвала к скорейшему введению единого механизма регулирования криптовалют на территории ЕС. Примечательно, что положения о рынках криптоактивов (Markets in Crypto-assets Regulation, MiCA) и пилотном режиме инфраструктуры рынка на основе технологии распределённого реестра, опубликованные в сентябре 2020 г., предполагали полный запрет использования криптовалют и криптоуслуг, полученных методом PoW (Proof-Of-Work, «доказательство работы» — алгоритм

функционирования криптовалют, основанный на доказательстве выполненной работы), который используют, в частности, криптомеханизмы Bitcoin и Ethereum. Запрет должен был вступить в силу в январе 2025 г., но в середине марта парламентарии комитета по экономическим и валютным вопросам (ECON) Европейского Союза решили исключить из проекта MiCA ограничение обращения Bitcoin и Ethereum.

Выступая на этом совещании, Кристин Лагард указывала на важность данной европейской инициативы для того, чтобы пресечь обход Россией санкций при помощи цифровых активов. Кстати, евросанкции, объявленные в начале марта, затрагивают криптоактивы РФ, а также доступ к российским цифровым активам с помощью Беларуси.

России также необходимо внедрять цифровые инструменты в свою финансовую систему, подчёркивает академик РАН Сергей Глазьев, чтобы снижать воздействие международных санкций на банковскую систему России. Внедрение цифровых валют в оборот — это неизбежное будущее, согласен Анатолий Аксаков, глава Комитета Государственной думы по финансовому рынку, ведь в значительной степени торговый оборот перейдёт в блокчейн. «Другое дело, что необходимо точно определить такие сущности, как наличный рубль, безналичный рубль, цифровой рубль, чтобы не возникало противоречий при их совместной работе на финансовом рынке», — подчёркивает он.

ЦЕЛЬ ОПРАВДЫВАЕТ СРЕДСТВА

В разных странах мира центральные банки создают национальные цифровые валюты (CBDC, Central Bank Digital Currency или ЦВЦБ, цифровые валюты центральных банков). По прогнозам PwC, в ближайшие 20 лет именно они станут одним из ключевых факторов развития платёжных рынков. По состоянию на конец 2021 г. около полутора десятков проектов CBDC находятся в фазе пилота или реального функционирования, а ряд проектов такого рода даже успел закрыться.

Судьба национальных цифровых денег во многом определяется целеполаганием, а также адекватностью выбранных механизмов, поставленным целям и их работоспособностью. Например, в числе первопроходцев ЦВЦБ стал Эквадор — страна, которая в 2000 г. отказалась от национальной денежной единицы сукре и приняла в качестве официальной валюты страны доллар США. Запуская проект цифрового сукре, правительство Эквадора намеревалось таким образом вновь вернуть национальную

валюту, но на новом уровне развития, и одновременно решить проблему недоступности финансовых услуг для населения. Однако ввиду низкого спроса со стороны населения и высоких затрат по содержанию новой системы проект был свёрнут.

Уругвайский проект e-Peso, запущенный в пилотную эксплуатацию в 2017 г. в форме бизнес-проекта полностью на базе частных инвестиций, был закрыт, и до сих пор нет признаков его восстановления.

Более успешными стали национальные ЦВЦБ, появившиеся в октябре 2020 г. в Камбодже и Содружестве Багамских Островов. Обе преследовали цель улучшения финансового обслуживания населения. Обе привязаны к доллару США. ЦВЦБ Sand Dollar оценивается в соотношении 1:1 к багамскому доллару, который, в свою очередь, привязан к доллару США. Цифровая валюта Камбоджи Bakong поддерживает транзакции не только с камбоджийским риелем, но и с долларом США, поскольку значительная часть расчётов в стране осуществляется именно в этой валюте.

Интересно, что разработала Bakong японско-российская компания «Сорамитсу», которая является резидентом особой экономической зоны «Иннополис» в Татарстане.

Задачу повышения качества финансовых услуг и ускорения денежных переводов решают государства валютного союза Организации Восточно-Карибских государств (OECS), которые запустили в прошлом году цифровую валюту D Cash, а также Нигерия со своей цифровой найрой (eNaira).

Однако наибольший интерес для анализа представляет ЦВЦБ Китая — цифровой юань eCNY. В начале 2021 г. его начали тестировать шесть ведущих китайских банков, к которым затем присоединилось свыше ста финансовых организаций и партнёров. Уже летом цифровой юань стал использоваться в пекинском метро, и к зимней Олимпиаде-2022 был приурочен полномасштабный запуск этой валюты. В частности, планировалось обеспечить установку банкоматов для обмена иностранной валюты (включая российский рубль) на цифровой юань.

По сообщению Wall Street Journal, в день церемонии открытия зимних Олимпийских игр в Пекине посетители мероприятия совершили больше транзакций с eCNY, чем через платёжную систему Visa.

В этом проекте Народный Банк Китая решает две задачи: вытеснение американского доллара и других валют из международных расчётов и

выход юаня на уровень мировой цифровой валюты. В русле этой идеи регулятор КНР присоединился к проекту Инновационного хаба Банка международных расчётов m-CBDC Bridge для проведения совместных экспериментов по тестированию трансграничных возможностей ЦВЦБ.

Европейский центральный банк (ЕЦБ) запустил пилотный проект цифрового евро. Главная цель — обеспечение собственного цифрового суверенитета и недопущение зависимости от электронных платёжных систем, которые контролируются из-за пределов ЕС. В частности, платёжные компании из США не вошли в состав Консультативной группы ЕЦБ по цифровому евро.

Весь мир с интересом следит за экспериментом с цифровой валютой Сальвадора, которую власти страны запустили осенью прошлого года. Ею стал биткоин, который получил свободное хождение в стране наряду с американским долларом. Он стал собственной валютой Сальвадора после того, как в 2004 г. национальную денежную единицу колон вывели из оборота из-за высокой инфляции и резких скачков курса.

Власти страны полагают, что такое решение станет стимулом для развития экономики. Правда, есть нюансы: большая часть населения страны занята в теневом секторе экономики, который неплохо развивается за счёт транзита наркотрафика. В перспективе, полагают эксперты, Сальвадор может превратиться в криптовалютный офшор.

Нужно сказать, что отношение к криптовалюте различается в разных странах мира. Так, в Швейцарии с помощью криптовалюты можно заплатить налоги, а во Франции биткоин признан взаимозаменяемым активом, что уравнивает его в правах с официальной валютой.

А КАК У НАС?

В нашей стране отношение финансового регулятора к криптовалютам лежит в русле классического противоречия между уходящей натурой — миром централизованных финансовых учреждений — и приходящим миром децентрализованных финансов, устраняющим необходимость в посреднике (классической банковской системе) при проведении финансовых операций.

Глубинное проявление этого конфликта — вопрос доверия, который представляет собой краеугольный камень любой денежной системы. В этом смысле Банк России видит угрозу в децентрализованных финансах и



настроен на запрет использования криптовалют в Российской Федерации, объясняя такую позицию спекулятивным характером рыночной стоимости криптовалют с признаками финансовой пирамиды.

В докладе Банка России для общественных консультаций «Криптовалюты: тренды, риски, меры», который был опубликован в январе, указывается: «Потенциальное использование криптовалют в качестве средства платежа за товары и услуги создаёт риск подрыва денежного обращения и утраты суверенитета национальной валюты... в случае дальнейшего распространения криптовалюты могут нести существенные угрозы для экономики и финансового сектора».

Вместо криптовалюты Банк России предлагает использовать цифровой рубль. С одной стороны, он обладает полезными в цифровом мире свойствами криптовалюты, выступает цифровым аналогом наличного рубля, может легко задействоваться в смарт-контрактах блокчейна. С другой стороны, государство сохраняет за

собой контроль за эмиссией и даёт обеспечение своими ресурсами.

В то же время ключевое понятие доверия в денежной системе в последнее время подвергается сильнейшей эрозии, в первую очередь в результате действия санкционных механизмов. Вместе с доверием уходят и былые представления о том, чем должны быть наполнены цифровые валюты. Всё говорит о том, что концептуальные основания финансовой системы в формирующемся цифровом мире должны быть пересмотрены.

«Мир изменился. Надо мыслить в новых категориях. Каким содержанием должно быть наполнено понятие «валюта»? Это товары, которые можно купить и продать», — говорит политолог Дмитрий Дробницкий. «Национальная валюта должна быть наполнена товарами», — подтверждает Дмитрий Абзалов, президент Центра стратегических коммуникаций.

Вице-спикер Госдумы Александр Бабаков призывает как можно быстрее запускать цифровой рубль в России, а потом распространять его

	Государственные	Частные			
	Цифровая валюта центрального банка (ЦВЦБ) ¹	Электронные деньги (eMoney)	Стейблкоины	Необеспеченные крипто- валюты	Токенизированные активы
			Предмет доклада		
Соответствие российской практике	Цифровой рубль	Электронные денежные средства в соответствии с ФЗ от 27.06.2011 № 161-ФЗ «О национальной платежной системе»	Цифровые валюты в соответствии с 259-ФЗ ² , а также ЦФА, которые могут использоваться в иностранной юрисдикции для платежей (в данном докладе – криптовалюты)		ЦФА, выпущенные в соответствии с 259-ФЗ от 31.08.2020, и утилитарные цифровые права, выпущенные в соответствии с 259-ФЗ ³ от 02.08.2019
Эмитент	Центральный банк	Частная компания	Неопределенные лица или частная компания	Неопределенные лица или частная компания	Частная компания
Предназначение для платежей	Да	Да	Да/нет	Да	Нет
Анонимность операций/невозможность проведения процедур КУС	Нет ⁴	Нет	Возможна, в зависимости от дизайна и требований посредников	Возможна, в зависимости от дизайна и требований посредников	Нет
Погашение обязательства	Конвертируемо в другие формы денег центрального банка	По номинальной стоимости	По номинальной стоимости или рыночной стоимости обеспечения либо отсутствует	Отсутствует	По номинальной стоимости или рыночной стоимости обеспечения или получение прав
Обеспечение	Баланс центрального банка, доверие к уже существующей национальной валюте	Полное обеспечение активами и капиталом; наличие специальных структур для осуществления банкротства	Полное или частичное обеспечение набором активов либо использование алгоритма для поддержания стабильности	Отсутствует	Обеспечение активами (ценные бумаги, товары, недвижимость и др. реальные или финансовые активы, право на получение определенного товара или услуги)
Примеры	Sand Dollar (Багамские острова)	AliPay, mPesa	Tether, USD Coin, Terra	Bitcoin, Ethereum	Tesla tokenized stock FTX, Amazon tokenized stock FTX ⁵

Рисунок 1. Классификация цифровых денег и криптоактивов. Источник: «Криптовалюты: тренды, риски, меры». Доклад для общественных консультаций. Банк России, 2022 г.

на страны ЕАЭС, но таким образом, чтобы при этом деньги стимулировали промышленность и потребительский спрос: «Процессы надо закольцевать: бизнес знает, на что есть спрос, а деньги для стимулирования потребительского спроса идут напрямую от государства, минуя частные банки». Так Бабаков описывает идею прямого госкредитования бизнеса под 2–4% годовых, что достижимо, если принять решение о целевой эмиссии цифровых рублей.

Примерно об этом Александр Лосев, генеральный директор УК «Спутник — управление капиталом», член Совета по внешней и оборонной политике, говорил в интервью РБК ещё в 2017 г.: «Вся дискуссия вокруг национальной электронной валюты выглядит как отчаянная попытка уговорить Центральный банк увеличить монетизацию экономики, страдающей от кредитного сжатия, или хотя бы вывести часть денежного оборота за пределы банковской системы, внутри которой сейчас происходит оседание финансовых ресурсов, и

дать дополнительную свободу движению капитала внутри страны. В частности, предлагается сделать небольшую эмиссию добавочной электронной валюты, чтобы запустить рост хотя бы в цифровом сегменте российской экономики».

ВАРИАНТЫ ОРГАНИЗАЦИИ ЦИФРОВОГО РУБЛЯ

Сергей Глазьев подчёркивает, что выбор цифровых инструментов для модернизации финансовой системы России достаточно широк: если криптовалюты смущают своей волатильностью, в качестве альтернативы банковским переводам могут выступать стейблкоины. Такой вариант цифровой валюты, чья стоимость, в отличие от необеспеченных криптовалют, привязана к реальному материальному активу (золоту, нефти, газу, металлу и т.д.), позволяет разрешить проблему доверия к традиционным валютам (рис. 1).

Это интересный вариант цифровой валюты, который, с одной стороны, помогает

противостоять волатильности за счёт привязки к активу с устойчивой стоимостью, но, с другой стороны, одновременно обеспечивают свойственную криптовалютам доступность и мобильность, предоставляя возможность более быстрых трансграничных переводов. По сути, это своеобразная и удобная форма цифровых денег, а не спекулятивный актив.

Надо отметить, что сегодня к числу устойчивых активов стейблкоинов относятся разнообразные варианты американского доллара: доллары США, хранящиеся в американских банках (Binance USD, Pax Dollar, True USD, HUSD), резервы на банковских счетах, в акциях и других активах (Tether), эквивалентная фиатная валюта на банковских счетах (USD Coin), а также алгоритмические механизмы криптовалют, привязанные к доллару США (Dai — Ethereum, Neutrino USD — токен WAVES) (рис. 2).

Государственный банк Бразилии National Social Development Bank выпустил в 2019 г. стейблкоин Brazilian Digital Token (BRZ), который работает в режиме поддержания паритета с национальной валютой. Он выпущен в формате токена, то есть цифрового актива, который выпускается на определённом блокчейне (в данном случае — Ethereum) с целью использования как главного платёжного инструмента, и обеспечен бразильским реалом в соотношении один к одному.

В рамках пилотного проекта банк выпустил цифровую валюту для Национального агентства по кинематографии для создания и продвижения сценариев и кинопроизводства в Бразилии и далее продолжил работу в этом сегменте. Сегодня BRZ является крупнейшим стейблкоином, привязанным к национальной валюте, отличной от доллара. В мае прошлого года он достиг отметки в 1 миллиард выпущенных токенов.

Интересно, что в процессах блокчейна BRZ использованы электронные идентификационные сертификаты Национального реестра налогоплательщиков (Cadastro Nacional da Pessoa Jurídica, CNPJ), которые уже широко применяются бразильскими компаниями в качестве официальных регистрационных документов. Это позволяет контролировать, что компания, которая получает деньги, может потратить их только на цели, связанные с киноиндустрией.

В связи с национальной цифровой валютой особый интерес представляет цифровая валюта Венесуэлы El Petro, которая была запущена в феврале 2018 г. Президент Венесуэлы Николас Мадуро создал «цифровой боливар» El Petro для

имя	Цена	24ч %	Циркулирующее предложение	Объем	Рыночная капитализация
 Tether	\$0.999	↓ -0.08%	81,331,736,008.26 USDT	\$33,512,580,412.00	\$81,239,759,296.00
 USD Coin	\$1.000	↑ 0.040%	51,984,358,583.69 USDC	\$1,900,623,115.00	\$51,975,898,277.00
 Binance USD	\$1.000	↓ -0.09%	17,566,012,245.93 BUSD	\$2,264,731,555.00	\$17,554,434,406.00
 TerraUSD	\$1.000	↓ -0.01%	16,168,768,444.16 UST	\$386,469,387.00	\$16,174,963,785.00
 Dai	\$0.998	↓ -0.14%	9,248,788,952.91 DAI	\$136,790,895.00	\$9,230,685,164.00
 Frax	\$0.997	↓ -0.11%	2,791,591,604.01 FRAX	\$20,612,962.00	\$2,784,676,100.00
 Magic Internet Money	\$0.987	↓ -0.36%	2,785,296,692.98 MIM	\$20,337,625.00	\$2,749,449,691.00
 TrueUSD	\$0.999	↓ -0.06%	1,360,748,205.75 TUSD	\$79,662,508.00	\$1,359,621,523.00
 Pax Dollar	\$0.999	↓ -0.05%	961,811,853.76 USDP	\$5,090,555.00	\$960,937,207.00
 Fei USD	\$0.998	↑ 0.870%	559,117,718.27 FEI	\$1,242,670.00	\$558,541,605.00

Рисунок 2. Топ-10 мировых стейблкоинов. Источник: Profinvestment.com, 26.03.2022.

обхода международных санкций, в первую очередь американских, а также для нивелирования негативных последствий гиперинфляции. Цифровая валюта эль-петро — это, по сути, государственный стейблкоин, привязанный к стоимости нефти.

Основанием для определения цены El Petro стала цена одного барреля сырой нефти — на уровне 60 долларов. По данным, которые приводились в различных СМИ, выпуск 100 млн токенов El Petro подкреплялся 5,3 млрд баррелями сырой нефти (общей стоимостью порядка 267 млрд долларов) месторождения Аякучо в одном из бассейнов реки Ориноко. Таким образом, El Petro стала первой криптовалютой в мире, выпускаемой официально под государственным контролем и для решения конкретной проблемы — облегчения давления американских санкций.

Данный проект государственного стейблкоина, что называется, «выстрелил»: в ходе преисейла он привлёк 5 млрд долларов буквально из воздуха. Только в первый день продаж криптовалюта El Petro собрала 735 млн долларов, причём инвесторы остались анонимными. Криптовалютный суперинтендант Венесуэлы Карлос Варгас заявил, что принять участие в предпродаже решили 83 тыс. покупателей из 127 стран. При этом 36% транзакций были осуществлены в долларах США, 15% — в евро, 18% — в криптовалюте Ethereum и 31% — в биткойне.

Запуск El Petro, действительно, помог стране справиться с чудовищной инфляцией. Эксперты, знакомые с ходом проекта, говорят, что там даже привязали к нему среднемесячную зарплату.

С целью обеспечения спроса на цифровую валюту власти Венесуэлы сразу перевели на неё оформление всех консульских услуг в посольствах Венесуэлы по всему миру, разрешили ассоциации авиакомпаний закупать топливо для самолётов и использовать El Petro при оплате туристических услуг. Эта цифровая монета получила статус обязательного платёжного средства: токенами El Petro можно оплачивать налоги, госпошлины, а также получать кредиты.

А вот с защитой от санкций США не всё получилось гладко. Через месяц после запуска El Petro президент США Дональд Трамп подписал указ, запрещающий гражданам США какие-либо операции с этой цифровой валютой. И действительно, США удалось весьма быстро заблокировать трансграничную активность El Petro, и это несмотря на все заявления о том, что глобальная криптовалютная индустрия абсолютно независима от каких-либо внешних воздействий! Так «цифровой боливар» превратился в локальную цифровую валюту, его рыночная стоимость резко упала, однако весомые плюсы от её внедрения для национальной экономики остались.

Пример Венесуэлы вдохновил на создание собственных цифровых валют Иран и Турцию. Обе эти страны против легализации классических криптовалют и решили создавать собственные цифровые валютные системы. Есть сведения, что турецкая денежная единица Turkcoin будет обеспечена ценными бумагами самых крупных публичных компаний страны, в том числе Turkish Airlines, Istanbul Stock Exchange и Turk Telekom.

В среде российских экономистов циркулирует идея о том, что стейблкоин с обеспечением золотом («золотой рубль») поможет справиться со стремлением США заморозить существенную часть оставшихся золотовалютных резервов России. Конечно, есть вероятность, что США смогут помешать внешнеторговым операциям такого рода, но такая криптовалюта всё же будет востребована для взаиморасчётов между государствами, столкнувшимися с ограничениями глобалистов.

ЧТО СТРОИМ?

О прагматических целях российского цифрового рубля известно немного: это некая третья форма рубля, которая будет запущена в полномасштабную эксплуатацию к 2030 г. (рис. 3).

В концепции цифрового рубля, которую Банк России принял в апреле прошлого года, отмечается: «Наряду со свойствами традиционных наличных и безналичных денег, цифровой рубль будет обладать дополнительными преимуществами, повышающими его привлекательность как платёжного средства. Цифровой рубль позволит гражданам и бизнесу иметь доступ к своему цифровому кошельку через любую финансовую организацию, клиентами которой они являются. Также цифровой рубль обеспечит расчёты без доступа к сети Интернет (офлайн-режим)».

Ещё известны некоторые параметры технологической инфраструктуры цифрового рубля, которая уже создана, и к её тестированию приступил ряд российских банков: гибридная архитектура, комбинирующая технологии распределённых реестров и централизованных компонентов. Есть также двухуровневая розничная модель взаимодействия Банка России, который является эмитентом цифровых рублей и оператором платформы цифрового рубля, финансовых организаций и клиентов (рис. 4).

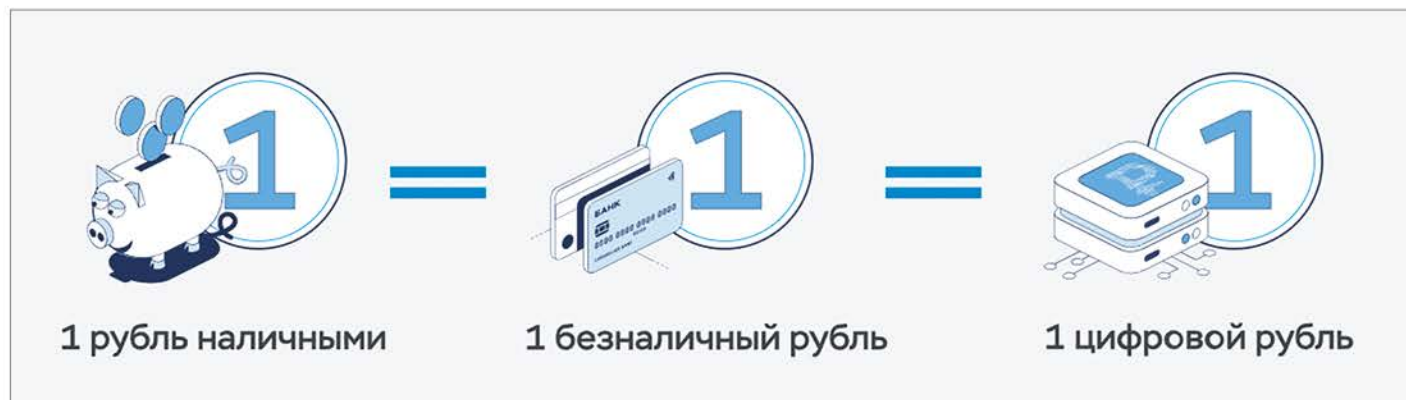


Рисунок 3. Три формы российских денег. Источник: <http://www.cbr.ru>



Рисунок 4. Схема двухуровневой розничной модели цифрового рубля. Источник: презентация концепции цифрового рубля, Банк России, апрель 2021 г.

Несколько больше конкретики в части целей проекта — в концепции законодательного регулирования оборота цифровых валют, которую Правительство РФ утвердило 9 февраля 2022 г. Там заявляется цель создания цифрового рубля — стабильность финансовой системы.

«Установление правил оборота криптовалют и мер контроля позволит минимизировать угрозу стабильности финансовой системе и снизить использование криптовалют в противоправных целях, поскольку полный запрет сегмента операций, связанных с их оборотом, невозможен. Реализация концепции обеспечит создание необходимой нормативной правовой базы, позволит вывести из тени индустрию и создать возможность для осуществления легальной предпринимательской деятельности», — говорится в документе. Иными словами, оборот этих финансовых активов будет регулироваться государством через жёсткие обязательства для всех участников профессионального рынка и акцентом на защиту прав рядовых инвесторов.

Эксперты отмечают как положительный факт то, что в данном тексте впервые на официальном уровне связываются понятия «цифровые валюты» и «криптовалюты», что, несомненно, способствует терминологической прозрачности рассматриваемой темы. Но то, что основные

сводки с фронтов «битвы за урожай» цифровой валюты относятся к позиционным боям за легализацию традиционных криптовалют, не может не удивлять.

К ЦИФРОВОМУ РУБЛЮ МНОГО ВОПРОСОВ

Действительно, важно понимать, какой механизм цифровой валюты в нынешних условиях наилучшим образом отвечает задаче беспроblemных денежных расчётов с недружественными странами. А какой наиболее эффективен для работы России в рамках формирующихся блоков дружественных стран? Могут ли коммерческие банки выпускать свои стейблкоины, обеспеченные собственными денежными ресурсами?

Закону «О цифровых финансовых активах» это не противоречит, и первый такой проект — стейблкоин на основе рубля под названием «сберкоин» — Сбербанк планирует запустить уже нынешней весной. Но как будет регулироваться совместное функционирование этой и подобных цифровых валют с цифровым рублём банка России и друг с другом? А если и иной банк решит выпустить собственную валюту, привязанную, скажем, к золоту или материальной продукции предприятий — своих

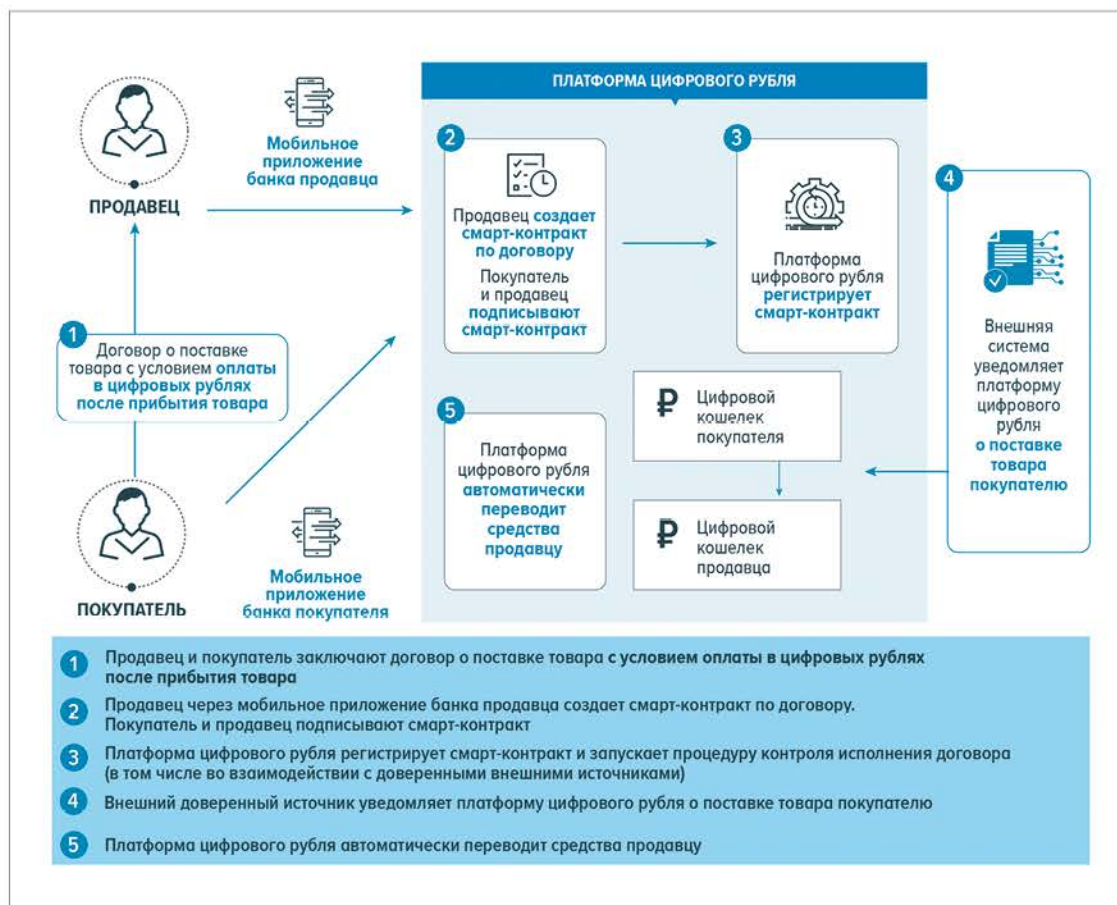


Рисунок 5. Пример использования смарт-контракта для бизнес-сделок с помощью цифрового рубля. Источник: «Концепция цифрового рубля». Банк России, апрель 2021 г.

клиентов? Список возможных вариантов можно продолжать, поскольку в условиях плотных экономических санкций могут пригодиться и старые добрые бартерные схемы, оформленные на новом цифровом уровне.

Ещё один блок вопросов: какие новые услуги банки смогут предложить бизнесу, который страдает и от недофинансирования, и от разрыва сложившихся цепочек поставок? Российские компании уже набирают опыт практической эксплуатации крупных блокчейн-проектов: сеть ФНС для субсидирования малого и среднего бизнеса с помощью беспроцентных и льготных кредитов, B2B-сервис «Альфа-Банка» для работы с самозанятыми гражданами, выборы в нескольких регионах депутатов Государственной думы в сентябре 2021 г. с использованием технологии распределённого реестра (рис. 5). Как превратить прозрачные смарт-контракты цифрового рубля в информацию, полезную для эффективного оперативного управления бизнес-цепочками в рамках отдельных отраслей, крупных холдингов, госкомпаний и отдельных предприятий различного масштаба и профиля деятельности?

ПРО БЕЗОПАСНОСТЬ

Отдельной группой стоят вопросы информационной безопасности системы цифрового рубля. С одной стороны, разработана архитектура безопасности (рис. 6), включающая:

- ♦ удостоверяющие центры различного уровня, в том числе выделенный удостоверяющий центр Банка России для эмиссии цифровых рублей;

- ♦ API-интерфейс платформы цифрового рубля, через который кредитные организации будут к ней подключаться;

- ♦ мобильные приложения, предоставляемые кредитными организациями своим клиентам. Они включают специализированный программный модуль Банка России и защищённое хранилище ключевой информации на устройстве пользователя.

Однако есть риски, для минимизации которых ещё предстоит провести специальные исследования. Например, высокая сложность реализации решения по обеспечению конфиденциальности в распределённых реестрах, практическая реализация офлайн-режима на платформе цифрового рубля.

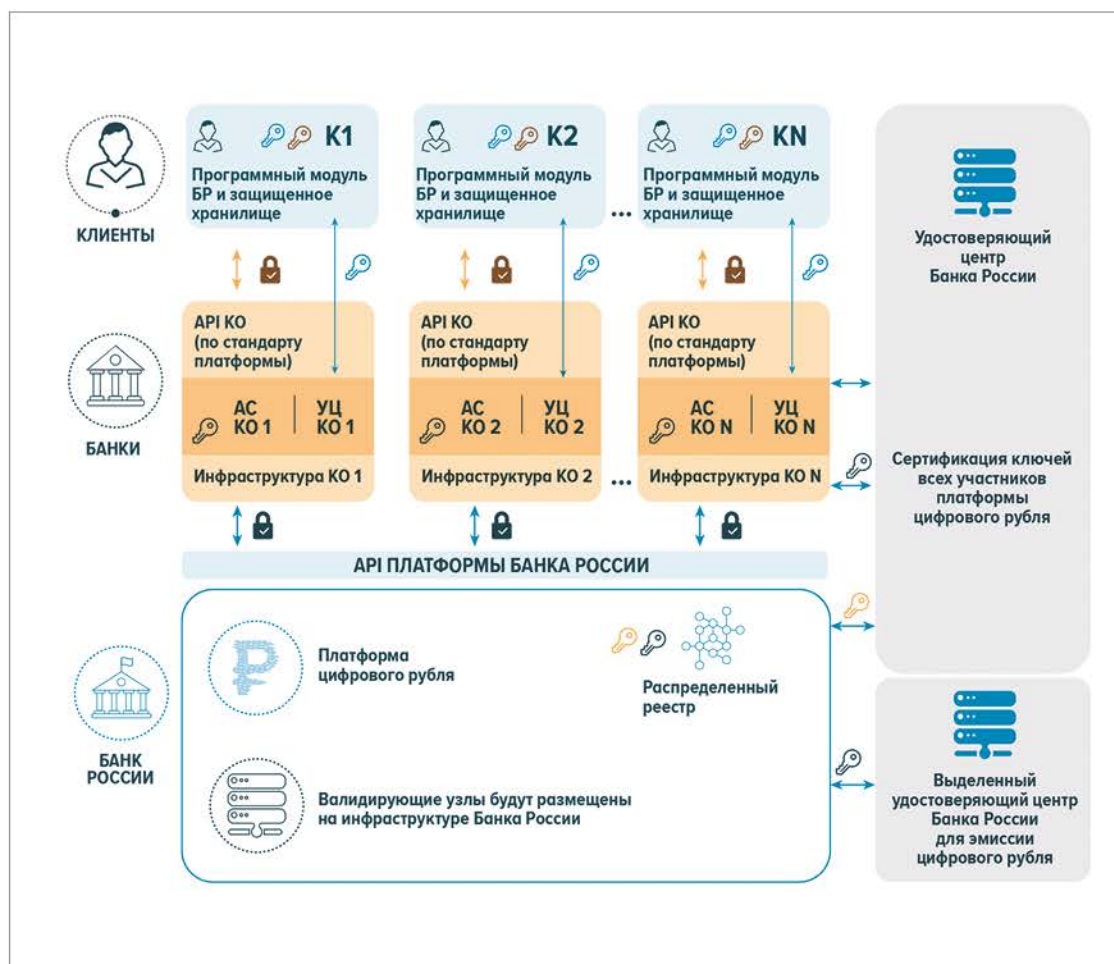


Рисунок 6. Подходы к информационной безопасности платформы цифрового рубля. Источник: «Концепция цифрового рубля». Банк России, апрель 2021 г.

Кроме того, страна вступила, образно говоря, в фазу импортозамещения 2.0: в связи с недружественными действиями зарубежных ИТ-компаний необходимы полноценные, а не паллиативные отечественные, как аппаратные (платёжные терминалы, высокопроизводительные системы хранения и обработки блокчейн-данных), так и программные решения. Также надо уже вести речь о блокчейн- и криптовалютных биржах российского происхождения, поскольку растёт давление США не только на международные платёжные системы, но и на криптовалютные биржи.

Не так давно Украина обратилась к Coinbase, Binance, Huobi, KuCoin, Bybit, Gate.io с просьбой заблокировать все российские аккаунты. Несмотря на то что блокировка личных аккаунтов — спорный шаг в криптопространстве, некоторые организации выполнили эту просьбу.

Так, биржа Coinbase заблокировала 25 тыс. российских кошельков, сославшись на то, что их владельцы подозреваются в незаконной деятельности. И крупнейшая криптобиржа Binance

заявила, что будет блокировать аккаунты пользователей, которых заподозрит в злонамеренных действиях.

Возможно, для кого-то это станет разрывом шаблона, ведь в течение многих лет заказчики ИТ-систем ставили обязательное требование ответственности разработок международным (читай американским) стандартам. Сегодня в ряде случаев это может оказаться недостатком продукта.

В свете того, что санкции, судя по всему, пришли к нам надолго, восьмилетний период взросления цифрового рубля может оказаться непозволительной роскошью. О том, как строить российскую систему цифровой валюты, способную помочь экономике страны пройти без фатальных потерь через горнило санкций, нужно думать уже сегодня.

BIS Journal организовал виртуальный раунд такого обсуждения, в котором принял участие ряд российских экспертов.

«ЦИФРОВОЙ РУБЛЬ ДОЛЖЕН БЫТЬ ЭЛЕМЕНТОМ НОВОЙ ФИНАНСОВОЙ СИСТЕМЫ И ОБЕСПЕЧИВАТЬСЯ ГОСУДАРСТВОМ»



Юрий ПРИПАЧКИН
президент
Российской
ассоциации
криптоиндустрии
и блокчейна
(РАКИБ)

Сегодня многочисленные эксперты говорят, что на фоне разрушения сложившейся мировой финансовой системы в России начинается создание новой валютной системы, и важная роль в этой новой системе принадлежит цифровому рублю. Это, несомненно, важный тезис. Вот только необходимо договориться, что понимается под этим цифровым рублём. Ведь то, как сегодня позиционирует цифровой рубль Банк России, — это просто новая форма записи безналичных рублей. По факту наш финансовый регулятор цепляется за старую аналоговую экономику и аналоговую систему денежных отношений со свойственной ей централизованной функцией выпуска денег, которую монополизирует государство либо группа частных лиц, как в случае с ФРС США. Но время такого подхода технологически ушло в прошлое, и вызывает удивление стремление регулятора насильно запихнуть в устаревшую модель финансов ту экономику, которая сегодня бурно развивается.

ОТКРЫЛСЯ ПОРТАЛ В НОВУЮ ЭКОНОМИЧЕСКУЮ РЕАЛЬНОСТЬ

На наших глазах осуществляется выход в новую экономическую реальность, которая требует совместного развития как цифровых валют центральных банков, так и частных валют тех или иных компаний. И санкционное давление только стимулирует это движение. Поэтому центральный вопрос сегодняшнего дня — дальнейшее развитие криптоэкономики и использования блокчейна в финансовых схемах.

Отрицать необходимость формирования рынка криптовалют и участия их в обновляемой финансовой системе по меньшей мере недальновидно. Да, и ссылки на Китай, который якобы запретил криптовалюту, — это только половина правды. Китай ввёл в обращение цифровой юань, который, в том числе, использует криптотехнологии, и, действительно, ограничил использование криптовалюты на основной территории. Но при этом разрешил их в Гонконге — там на территории опережающего развития используются различные криптовалютные механизмы.

Таким образом, Китай активно отработывает взаимодействие своего цифрового юаня с этими криптовалютами. Почему он это делает?

Китай понимает, что централизованная валютная система ушла в прошлое, а децентрализованная экономика, к которой мы все движемся, требует создания совместной валютной системы, включающей частные деньги. Они уже активно используются во всём мире. Да и у нас тоже. Ведь любая программа кэшбэка или программа лояльности — это, по сути, и есть частные деньги той компании, которая выпустила программу лояльности, и эта компания обеспечивает их своими товарами и услугами. Фактически, получая скидку, вы её зачисляете себе на некий виртуальный счёт или кошелек и потом расплачиваетесь, покупая товары этой компании. В этом смысле бонусные мили «Аэрофлота» — это тоже частные деньги «Аэрофлота», которые вы сами производите (или майните), когда летаете самолётами «Аэрофлота». Вы можете также потратить их на услуги других перевозчиков, покупки в магазинах Duty Free или «Азбуке вкуса». Частные деньги уже здесь, и мы ими уже пользуемся. И их наличие заставляет по-новому посмотреть, например, на функцию эмиссии денег.

В децентрализованной экономике денежная эмиссия производится также децентрализованно, а эмитентом выступает либо конкретная компания, которая обеспечивает эти деньги реальными услугами, либо работает некоторый механизм децентрализованной эмиссии, как, например, биткоин, у которого вообще нет единого эмиссионного центра. Он ничем не обеспечен, кроме доверия сообщества.

Но посмотрите на наш рубль, который эмитирует Банк России, или доллар США. Они тоже ничем, кроме доверия, не обеспечены. Об этом говорит, в частности, та инфляция, которая бушует в мире, — наполненность доллара или рубля реальными активами исчезла. А раз Банк России не гарантирует наполненность рубля реальными активами, то все утверждения о борьбе с инфляцией превращаются в пустые слова...

Руководству страны нужно незамедлительно принимать решение: исключать нашу финансовую систему из общей англосаксонской

Бреттон-Вудской системы и приступить к формированию собственной независимой платёжеспособной системы на базе новых технологий. И для осуществления этой идеи сегодня сложилась уникальная ситуация.

Все страны мира, не привязанные напрямую к США военными обязательствами, с надеждой смотрят на создание альтернативной долларовой системы. Они больше не верят в доллар, и это подтверждает тот уровень инфляции, который стремительно нарастает в США. А санкции, которые США ввели против России в том числе в нефтегазовом секторе, разрушили наполненность доллара нефтью. Плюс к этому все крупные страны БРИКС отказались поддерживать США, даже Саудовская Аравия и ОАЭ заявили, что не будут замещать нашу нефть своей продукцией.

Это крах стратегической системы нефтяного доллара: если раньше мир предполагал, что доллар обеспечен нефтью, то сегодня оказалось, что он не обеспечен вообще ничем. И в ближайшее время, когда мы введём обратные санкции против недружественных стран, перестанем наполнять их валюты нашими реальными товарами: платиной, никелем, углем, нефтью и т.д., начнётся стремительное разрушение этой устаревшей финансовой системы. Ведь, по сути, это мы сами обеспечиваем платёжеспособность доллара США, продавая наши ресурсы за их напечатанные бумажки.

Сегодня эта система начала рушиться, и мы уже видим трещины, которые пошли по фасаду ранее монолитной экономики Запада. Уже в этом году мы увидим стремительно нарастающее дальнейшее разрушение. Но только в том случае, если будем последовательны в осуществлении своей стратегической политики по созданию независимой финансовой системы. Потому что это — война, серьёзная геополитическая война, где на нашей стороне достаточно много стран, понимающих значение радикальной отвязки от доллара.

КАК ОРГАНИЗОВАТЬ ИНФРАСТРУКТУРУ ЦИФРОВОГО РУБЛЯ

Цифровой рубль должен быть элементом новой финансовой системы и обеспечиваться государством. Важная составная часть этой финансовой системы — децентрализованные частные валюты. Они будут обеспечиваться либо конкретными поставщиками товаров и услуг, которые выпускают собственные частные деньги, либо носить децентрализованный характер криптоденег, которым доверяет сообщество. По сути, сегодня мировое сообщество доверяет биткоину, и именно к биткоину привязываются все

остальные криптовалюты в процессах эквивалентного обмена их между собой или на частные деньги. Иными словами, биткоин уже сегодня выполняет роль «второго золота», то есть стандарта обмена криптовалют между собой.

Поэтому будущая финансовая система, которая сложится буквально в течение ближайшего года, будет составлена из цифровых валют центральных банков CBDC (Central Bank Digital Currency), частных валют с теми или иными поставщиками сервисов и децентрализованных криптовалютных механизмов, обеспеченных доверием людей.

В эту структуру естественным образом вписываются трансграничные операции. Они обеспечиваются нашим российским крипторублем, который имеет определённое содержание. Например, для стран ЕАЭС в новой структуре будет организовано виртуальное подпространство — совокупность их частных валют, которые обеспечены их товарами и услугами. Внутри каждой страны будет реализовано хождение собственной валюты, а на более высоком уровне оно станет частью общего цифрового пространства. Это, кстати, не новинка — основные криптовалюты успешно взаимодействуют друг с другом на основе взаимнообмена, пересчёта котировок и т.д., хотя имеют различный функционал.

Однако для эффективного управления этой структурой предстоит принять некие организационные решения в том числе по поводу переподчинения Банка России, например, правительству РФ. Центр эмиссии всех видов денег в стране должен быть подчинён государству!

А в нынешнем состоянии у нас даже нет ответственного органа, который подчинён интересам государства и отчитывается, например, перед правительством за новую финансовую систему и за функционирование денежно-монетарной системы в целом. Но в условиях военного противостояния — давайте называть вещи своими именами — мы не можем позволить себе иметь неконтролируемый финансово-экономический центр. Поэтому правительство должно разработать и утвердить продуманную концепцию новой финансовой системы, отвечать за её выполнение и иметь в своём подчинении инструментарий в лице Банка России. Пока же нет смысла обсуждать, каких результатов достиг регулятор в создании каких-то блокчейн-систем, которые он сам себе заказал и подписал акт приёмки-сдачи продукта.

Понимаю, что это достаточно тяжёлые политические решения, но их нужно принимать сейчас, поскольку политика банка России не может быть независимой, она должна подчиняться

целям и задачам, стоящим перед государством. Ставки в этой задаче чрезвычайно высоки: даже завершив с успехом специальную военную операцию, даже решив проблемы денацификации и демилитаризации Украины, мы можем проиграть стратегическую войну, если кардинально не изменим нашу финансовую модель.

ИНФРАСТРУКТУРА ЦИФРОВОГО РУБЛЯ КАК ОСНОВА НОВОГО УПРАВЛЕНИЯ ЭКОНОМИКОЙ

Экономисты знают, что в нашей стране уже работала двухуровневая система, состоящая из безналичного и наличного рубля. Это та советская финансовая система, которая успешно пережила и индустриализацию, и Великую Отечественную войну, и последующее восстановление страны. Но ведь безналичный рубль тех времён, по сути, очень близок к сегодняшнему понятию цифрового рубля: он подлежал учёту, был наполнен товарами и услугами и на 100% обеспечен. Инфляции не было. Потому, собственно, стоимость буханки хлеба не менялась десятилетиями.

И лишь с течением времени, по мере роста товарной массы стало труднее справляться с планированием. Собственно, тогда были идеи создания единой автоматизированной системы управления страной и некоторые разработки, которые, к сожалению, не удалось воплотить в жизнь. А вот если бы в те времена был блокчейн и понятие крипторубля, то наш Госплан СССР спокойно пережил бы трудности роста, и мы давно идеологически пребывали бы в цифровом пространстве. На самом деле, сегодня нам нужен Госплан, совмещённый с Центральным Банком, подчинённым правительству. Правда, Госплан XXI века был бы большой системой искусственного интеллекта, работающей над блокчейн-системой национального масштаба. Что это за система?

По аналогии с передовой налоговой системой, которая в последней версии АИС 4.0 создана на базе блокчейна, реализуется блокчейн-система госконтрактов. На госзаказы, как известно, приходится большая часть экономики страны — 70–80%. И цифровой рубль, построенный на блокчейне, выполняет очень простую функцию. Скажем, для строительства нового большого объекта заказчик получает из государственного Казначейства определённую сумму. На эту сумму выпускаются цифровые рубли, однозначно связанные с конкретным госконтрактом и его генподрядчиком.

Далее по цепочке исполнителей все эти цифровые рубли перемещаются вплоть до последнего песчаного карьера, который использует

эти цифровые рубли для выплаты заработной платы сотрудникам или уплаты налогов: просто предъявляет в Казначейство полученные цифровые рубли и получает зарплатные средства или оплачивает налоги. Вот и вся система крипторубля! Его преимущества очевидны — крипторубль может быть «окрашен» особым образом под каждый госконтракт. Причём под каждый контракт могут эмитироваться цифровые рубли разного цвета.

Таким образом, возникает экономическая система, прочно стоящая на двух «ногах»: одна — это система доходов (сбора налогов), вторая — система расходов (казначейская система). А над ними — современный Госплан, который с помощью механизмов искусственного интеллекта понимает, какие транзакции уже проведены, чего не хватает и на что надо направить резервы.

Ещё в эту картинку надо добавить цифровой профиль человека или предприятия. Они уже сегодня формируют пространство запросов. Интеллектуальный Госплан с успехом может их оценивать, прогнозировать, формировать соответствующий ресурс и затем размещать заявки на предприятия или госзаказы на те или иные виды продукции.

Вот почему я уверен, что мы обязательно вернёмся к системе Госплана, основанного на искусственном интеллекте и двух «ногах» нашей экономики, построенных с помощью блокчейна и других цифровых технологий. А этажом ниже в этой конструкции будет располагаться пространство частных криптовалют, эмитируемых частными производителями и обеспечиваемыми их товарами и услугами. Люди будут их получать за счёт своего потребления, как сегодня они получают разные блага в рамках программ лояльности. Вот и вся модель экономики, которую нам предстоит создать, — независимая и не подверженная санкциям.

У этой схемы есть два ключевых риска. Первый — текущая система организации финансовой системы, которую надо серьёзно менять. Второй — риски, связанные с кошельками российских пользователей на международных криптовалютных биржах. Их можно ликвидировать одним способом — созданием собственной криптовалютной инфраструктуры. Если это будет НАША инфраструктура, включающая собственные биржи, обменники и т.д., то мы переключим часть мировой инфраструктуры криптоиндустрии на себя и будем её контролировать. Хотя надо отметить, большая часть криптосообщества заявила, что децентрализованная экономика не воспринимает санкции США в отношении России.

«ОТКАЗ ОТ ДЕЦЕНТРАЛИЗОВАННОГО ПОДХОДА ДЕЛАЕТ ЦИФРОВОЙ РУБЛЬ МЕНЕЕ ЗАЩИЩЁННЫМ»

Прежде всего, надо сказать, что пока ни одна страна не может полностью спрогнозировать, как цифровая валюта центрального банка (CBDC) повлияет на экономику. Эта дискуссия по-прежнему ведётся. При этом практически все обсуждаемые проблемы и задачи (как архитектура цифровой валюты, так и аспекты безопасности, доступности и конфиденциальности) не являются специфическими для России, а присутствуют в большинстве юрисдикций, обсуждающих введение цифровых валют.

В России появление цифрового рубля с большой вероятностью может стать фактором трансформации действующей банк-центричной модели платёжного рынка. Хотя изначально цифровая валюта задумывалась как альтернатива наличным расчётам, нам представляется более реалистичным вариант, что она будет вытеснять именно традиционные безналичные платежи. Такая перспектива без вмешательства Банка России может привести к некоторому оттоку ликвидности кредитных организаций в кошельки цифрового рубля. Кроме того, цифровой рубль неизбежно лишит банки части комиссионных доходов. Последнее в целом вписывается в стратегию Банка России: по мнению регулятора, процентный доход для банков должен быть предпочтительнее комиссионного.

С другой стороны, снижение комиссионных доходов действительно может привести к значительной перестройке финансовой системы. В этом контексте для сохранения стабильности необходимо предоставить банкам новые сервисы для замещения выпадающих доходов, например, отслеживание переводов, их «окраска», программирование смарт-контрактов и т.д.

Вопрос скорости перехода к цифровому рублю фактически зависит от активности двух игроков — Банка России как главного бенефициара проекта и конечных потребителей цифровой валюты. Для регулятора цифровой рубль достаточно привлекателен. В отличие от криптовалют он отвечает интересам денежных регуляторов и налоговой системы, предполагая централизованное управление в лице Банка России и полную прозрачность платежей для государства. С другой стороны, платёжная система России уже достаточно развита: пользователю

доступны мгновенные переводы, используются QR-коды, бесконтактная оплата, удобные интерфейсы приложений банков. В связи с этим привлекательность перехода на цифровой рубль для потребителя далеко не так очевидна. Кроме того, санкционное давление на экономику России и нестабильность платёжной инфраструктуры побуждают пользователей доверять преимущественно классическим наличным способам оплаты, что также может привести к низкой популярности цифрового рубля. Наконец, банковские учреждения также не заинтересованы в том, чтобы информация о счетах клиентов и их транзакциях переходила из-под их контроля в собственность государства. Банку России придётся приложить усилия, чтобы убедить население и бизнес в наличии у цифрового рубля ощутимых преимуществ.

Что касается практических шагов по запуску цифрового рубля, то нужно отметить появление федерального закона № 259-ФЗ «О цифровых финансовых активах, цифровой валюте» — он является законодательным фундаментом для создания цифрового рубля. Закон определяет базовые термины и подходы к регулированию цифровых активов, а также их правовой статус, экосистему и ответственность участников их оборота. Тем не менее в отношении цифрового рубля, который является новым аналогом фиатных денег, правовое поле всё ещё имеет много белых пятен. Банк России собирается проработать их после завершения периода тестирования. Скорее всего, этот процесс будет осуществляться при помощи издания дополнительных к федеральному закону № 259-ФЗ подзаконных актов. Тогда же, вероятно, окончательно



Виктор ДОСТОВ
председатель
Совета Ассоциации
участников рынка
электронных
денег и денежных
переводов

Санкционное давление на экономику России и нестабильность платёжной инфраструктуры побуждают пользователей доверять преимущественно классическим наличным способам оплаты, что также может привести к низкой популярности цифрового рубля

Благодаря использованию токена, Банк России получит возможность отследить конкретную «монету» через несколько транзакций, что упростит поиск средств для целей возврата или, например, для ПОД/ФТ

решится судьба стейблкоинов — при широком использовании CBDC с большой вероятностью стейблкоины могут быть запрещены. Эти процессы уже видны — последний консультационный доклад Банка России по криптовалютам предполагает запрет использования стейблкоинов на территории страны.

Конечно, отказ от децентрализованного подхода делает цифровой рубль менее защищённым. С другой стороны, Банк России делает ставку на стабильность сервиса и высокую пропускную способность, для чего централизованные решения более применимы. При этом основным фактором, делающим цифровой рубль безопаснее, например, классического банковского счёта, является эмиссия и хранение актива на счетах Банка России. Кроме того, благодаря использованию токена, Банк России получит возможность отследить конкретную «монету» через несколько транзакций, что упростит поиск средств для целей возврата или, например, для ПОД/ФТ.

При этом масштабирование цифрового рубля на национальный уровень приведёт к фактической трансформации анонимности транзакций. С одной стороны, анонимность при использовании цифрового рубля в платежах фактически будет потеряна, так как Банк России заинтересован в прозрачности и контролируемости транзакций. С другой, конфиденциальность сохранится и даже усилится: доступ к данным пользователей со стороны коммерческих организаций может быть ограничен. Это, как предполагается, позволит повысить уровень защищённости персональных данных при полной прозрачности платежей для Банка России.

Однако в рамках той модели, которая была выбрана Банком России для построения цифрового рубля (преобладание централизованного подхода над распределённым), цифровой рубль, при всей своей надёжности, гарантируемой хранением данных и средств на серверах Банка России, фактически подвержен тем же рискам, что и классический безналичный кошелёк. В частности, создание цифрового рубля

не решает проблем, например, социальной инженерии.

Большинство мошенников вряд ли будут пытаться атаковать саму инфраструктуру цифрового рубля, пользуясь в основном доверчивостью граждан-владельцев CBDC. В этом случае, благодаря использованию токенов, Банк России потенциально сможет отследить платёж до конечного получателя. В случае замещения наличных денег это позволило бы исключить риски мошенничества. Тем не менее так как цифровой рубль вряд ли полностью заменит наличные деньги, риск незаконного вывода средств для цифрового рубля фактически сопоставим с классическими безналичными деньгами.

Отдельный вопрос — трансграничные операции с цифровым рублём. Большинство центральных банков, занимающихся разработкой CBDC, так или иначе допускают трансграничность своих цифровых валют. В то же время большинство этих же регуляторов с опасением смотрит на появление иностранных CBDC в своей юрисдикции. Основной проблемой для регуляторов в контексте трансграничности является вопрос отслеживаемости и контроля транзакций с иностранными валютами при использовании мобильных устройств. Представляется, что контроль за такими транзакциями будет достаточно сложным. При этом запрос на получение средств (например, зарплаты) в иностранной валюте среди населения может быть достаточно высок. В связи с этим центральным банкам, в том числе Банку России придётся вводить какие-либо дополнительные меры регулирования.

Просматриваются и организационные риски. Главной технологической проблемой, с которой, вероятно, столкнётся Банк России, является интеграция цифрового рубля в функционал банковских приложений. CBDC должна иметь единую точку входа, а доступ к цифровому кошельку должен быть обеспечен через приложения всех банков. Сами банки при этом должны работать с этой инфраструктурой в рамках той роли, которую они будут исполнять в проекте. Весьма вероятно, что для осуществления этих целей Банком России будет применена стратегия распространения, аналогичная системе быстрых платежей (СБП), — через интегрируемые в приложения интерфейсы API. Наученный задержками при внедрении СБП, Банк России попытается избежать ситуации, когда некоторые финансовые организации будут затягивать процессы интеграции цифрового рубля в свои сервисы.

О ВОЗМОЖНЫХ ПУТЯХ ИСПОЛЬЗОВАНИЯ СТЕЙБЛКОИНОВ В РОССИИ

Стейблкоины (от англ. stablecoin) — один из видов криптовалют. Стейблкоины существенно отличаются от общей массы по своим качествам в лучшую сторону — они имеют вполне конкретный финансовый смысл. Стабильность, предсказуемость, и, главное, осмысленность курса стейблкоинов обеспечивается за счёт его привязки к существующим твёрдым валютам или ценам биржевых товаров (таких как золото или нефть).

СТАБИЛЬНОСТЬ ВЫЗЫВАЕТ ДОВЕРИЕ

Стейблкоин даёт покупателям уверенность в том, что стоимость их токенов не будет непредсказуемо расти или падать. Стабильность курса внушает доверие, и на криптовалютном рынке появляется всё большее количество покупателей стейблкоинов, его популярность растёт. Увеличение числа участников, в свою очередь, приводит к росту объёма торгов и увеличивает рыночную капитализацию в целом, а это уже приводит к большей ликвидности. К числу системных недостатков стейблкоинов обычно относят необходимость наличия и поддержания высокого уровня доверия к централизованному механизму их генерации и обмена. Хотя, заметим, уже появляются и децентрализованные альтернативы.

Успешным примером эмиссии стейблкоина служит государственная криптовалюта Эль-Петро в Венесуэле — проект сразу принёс \$4 млрд. Стейблкоины используют внутри своей корпоративной сети Ситибанк («ситикоин») и Mastercard. Стейблкоины под брендом Libra анонсировал для

использования в своей соцсети М. Цукерберг, однако не получил добро на этот проект от американского регулятора SEC (U.S. Securities and Exchange Commission, надзорный орган, представляющий комиссию по ценным бумагам).

ИНВЕСТИЦИИ ДЛЯ ВСЕХ

Если стейблкоины в России легализовать как инвестиционный инструмент, то их можно использовать для уменьшения спроса граждан на валюту. Например, эмитировать стейблкоин, стоимость которого будет привязана к стоимости кубометра газа. Российский газ — экологически «чистое» топливо, привлекательный актив, его цена в нынешний кризис постоянно растёт. Эмитентом стейблкоина может выступить Банк России или иная подконтрольная ЦБ структура. Одно это обеспечит доверие граждан к механизму генерации и обмена, даст гарантии возврата инвестиций. Стейблкоины позволят снять напряжённость на внутреннем рынке — появится надёжное средство сбережения в кризис, стейблкоины станут привлекательным средством инвестирования в периоды «медвежьего» рынка.

Кроме этого, отметим, что:

- ♦ стабильность курса стейблкоинов подойдёт для инвестиций как новичкам, так и квалифицированным инвесторам;
- ♦ трейдеры и инвесторы смогут получать процентный доход с помощью стейблкоинов путём стейкинга (процесса, посредством которого осуществляется проверка криптовалютных транзакций: внося свои монеты, владелец получает вознаграждение);



Тимур АИТОВ
член Совета ТПП
РФ по финансово-
промышленной
и инвестиционной
политике, зампред
комиссии
по цифровым
финансовым
технологиям

СЕРГЕЙ ГЛАЗЬЕВ, МИНИСТР ПО ИНТЕГРАЦИИ И МАКРОЭКОНОМИКЕ ЕЭК: «НЕОБХОДИМО СРОЧНО ЛЕГАЛИЗОВАТЬ ИСПОЛЬЗОВАНИЕ ЦИФРОВЫХ ВАЛЮТ»

Возможный вариант — возврат к модели «переводного рубля», привязанного к ресурсам России: к нефти и газу, металлам, золоту, зерну. При этом обязать страны-импортёры поставлять за рубли (переводные рубли) товары по требуемой нам номенклатуре.

И, да, безусловно, на фоне санкций стран НАТО, фактически парализовавших международные расчёты, нужно внедрять цифровые инструменты. В качестве альтернативы

банковским переводам могут выступать не только криптовалюты, но и цифровые валюты, привязанные к стоимости других активов (стейблкоины). Эти инструменты доступны уже сегодня.

Если Центробанк не будет их легализовывать, то хозяйствующие субъекты все равно будут вынуждены их использовать. Но в нелегитимном ключе они будут делать это с риском для себя. Поэтому сейчас необходимо срочно легализовать использование цифровых валют для, по меньшей мере, стейблкоинов в целях проведения трансграничных расчётов.

Из интервью С. Глазьева РИА Новости, 04.04.2022

♦ «газовый» стейблкоин ЦБ позволит легко и быстро переводить активы в любую точку России.

РИСКИ И ПРОГНОЗЫ

Ключевым в проекте эмиссии станет вопрос о формировании мировой инфраструктуры приёма стейблкоинов. Возможно ли это?

Если говорить о продажах и переводах в формате worldwide, это будет, по сути, означать, что валюта должна котироваться на всех мировых криптобиржах (типа Binance), должны быть желающие её купить или продать. ЦБ также должен обладать достаточным запасом фиатной ликвидности в твёрдых валютах. Если эмитент и страна находятся в условиях санкций, то проблема заключается в том, что перечисленные требования непросто обеспечить. Венесуэла, например, сегодня использует криптовалюту Эль-Петро только внутри страны, поскольку её государственный стейблкоин подпал под санкции. Рыночная цена Эль-Петро из-за этого резко упала. Тем не менее и здесь остались весомые плюсы — криптовалюта Венесуэлы заменила в стране бумажные деньги, удешевила обращение денег в стране, обеспечила прозрачность в платежах. Очевидно, что для запуска «газового» стейблкоина в России также логично будет использовать элементы идеологии «цифрового рубля».

Существует значительный риск, что российский стейблкоин подпадёт под санкции стран Запада, и поэтому гарантированно будет использоваться только внутри России или в странах-союзниках (Белоруссия, возможно, Китай и др.). Однако, и этих возможностей может оказаться достаточно для обоснования запуска проекта газового стейблкоина.

ЗАКЛЮЧЕНИЕ

В то время, когда твёрдые мировые валюты постепенно теряют своё значение, появление финансового актива, «привязанного» своей ценой к биржевому товару, пользующегося спросом, является логичным. Возможно, в развитие этой идеи появятся и другие проекты выпуска стейблкоинов: один — с привязкой к нефти, другой — к газу, третий — к определённым видам полезных ископаемых, уверенно растущих в цене, возможностей здесь много. Уверен, что эмиссией стейблкоинов с удовольствием займутся и коммерческие банки, если им это поручить, а главное, разрешить. Два родственных проекта: эмиссия стейблкоина и будущая эмиссия цифрового рубля ЦБ — при этом могут существовать независимо, «не мешая» друг другу. Хотя, возможно, для запуска стейблкоина окажутся полезными как элементы идеологии, так и инфраструктуры цифрового рубля — почему бы и нет?

«ПРАКТИЧЕСКИЕ АСПЕКТЫ ВНЕДРЕНИЯ ЦИФРОВОГО РУБЛЯ ВЫЗЫВАЮТ АНАЛОГИИ С СИСТЕМОЙ БЫСТРЫХ ПЛАТЕЖЕЙ»



Вадим МАЗИН
коммерческий
директор компании
Surf

Первым и важным шагом на пути создания национальной системы цифрового рубля, вероятнее всего, станет подготовка законодательной базы под регулирование и оборот цифрового рубля. В концепции цифрового рубля, представленной Банком России, говорится о корректировках налогового, бюджетного и уголовного законодательства. Кроме того, на цифровой рубль возлагается роль обеспечения платформы, обеспечивающей прозрачность и контроль в сфере ПОД/ФТ/ФРОМУ (противодействие отмыванию денег и финансированию терроризма). Помимо существующих правовых норм, скорее

всего, будет установлена новая норма, регулирующая непосредственно цифровой рубль.

Состоялся первый этап тестирования прототипа платформы цифрового рубля. Причём уже два банка из 12 участников пилотного проекта провели полный цикл операций по переводу цифровых рублей между клиентами с использованием мобильных приложений. Результатом тестирования станет дорожная карта внедрения платформы цифрового рубля. Эти мероприятия можно назвать основным по трудозатратам этапом.

Практические аспекты внедрения цифрового рубля вызывают аналогии с системой быстрых платежей (СБП). Сегодня это популярный метод

«СОЗДАНИЕ НАЦИОНАЛЬНОЙ СИСТЕМЫ ЦИФРОВОГО РУБЛЯ СВЯЗАНО С РЯДОМ ТЕХНОЛОГИЧЕСКИХ ВЫЗОВОВ»



Артём КАЛИХОВ
генеральный
директор Waves
Enterprise

Безусловно, пока рано говорить, что инфраструктура цифрового рубля готова для массового использования. В нынешнем году стартовал пилотный проект в нескольких банках, и на текущий момент ни один из участников не отчитался об успешной интеграции с платформой. Для запуска же массового использования необходимо, чтобы банки научились работать с платформой, выпускать и обслуживать кошельки юридических и физических лиц. Также остро будут стоять вопросы обеспечения информационной безопасности, сертификации платформы в соответствии с требованиями ИБ-регуляторов (ФСБ и ФСТЭК), обеспечения крайне высокой пропускной способности и масштабируемости блокчейн-платформы. Это очень важные инфраструктурные вопросы и пока они не решены до конца.

В целом, создание национальной системы цифрового рубля связано с рядом технологических вызовов. Так, обеспечение конфиденциальности ляжет в первую очередь на банки, так как они будут работать непосредственно с клиентами и персональными данными. Несмотря на то что эта задача является классической для банков, в контексте цифрового рубля она имеет особую важность, так как утечка из банка сведений о связи персональных данных с идентификатором в блокчейне (открытым ключом) пользователя деанонимизирует все его финансовые операции. Можно попробовать решить этот вопрос с помощью продвинутой криптографии, но это станет дополнительным вызовом, учитывая масштабы использования платформы.

С точки зрения незаконного доступа к финансовым средствам пользователей, применение технологии блокчейн при построении инфраструктуры цифрового рубля как раз направлено

перевода безналичных средств. Однако для того, чтобы его внедрить потребовалось много усилий со стороны регулирующих органов, коммерческих банков и разработчиков. Распространение цифрового рубля потребует комплексных изменений в логике и структуре мобильных приложений. Добавление новой функциональности потребует серьёзных корректировок существующих мобильных приложений банков, что повлечёт связанные с этим затраты.

Скорее всего, по аналогии с СБП, Банк России подготовит единые рекомендации по реализации платформы цифрового рубля для коммерческих банков. И каждому банку придётся под них подстраиваться даже в ущерб существующим возможностям в мобильном приложении. Вероятно, как и в СБП, это будет строгая последовательность запросов для перевода цифровой валюты, которая может в корне расходиться с логикой приложения банка. Чтобы реализовать её, банкам придётся не только внести изменения в само мобильное приложение, но и реализовать новую логику на бэкенде (в программной части сервиса).

Вероятнее всего, ЦБ предложит единые требования к дизайну модуля приложения, связанного с цифровой валютой. Чтобы соблюсти единообразие, банкам придётся перерабатывать дизайн всего мобильного приложения или его отдельных частей. Резюмируя, в любом случае внедрение цифрового рубля в мобильные сервисы не произойдёт «по щелчку», это потребует серьёзной переделки существующих у банков решений и не менее серьёзных вложений.

При этом согласно концепции цифрового рубля Банк России берёт на себя роль главного эмитента, а также разработку основной инфраструктуры — программного модуля, интегрированного в мобильные приложения банков. А, банки, вероятно, обяжут реализовать инструмент для работы с цифровым рублём, что потребует обновления мобильных приложений банков, новых интеграций и новых этапов согласований с регулирующими органами. И эти аспекты нужно будет учесть собственникам цифровых финансовых продуктов.

Однако эти технологии существенно более медленные, чем банковские переводы, которыми мы привыкли пользоваться: вы никогда не сможете получить перевод в Bitcoin за несколько секунд — это издержки децентрализации

на снижение риска незаконного доступа к средствам. Доступ к ним и право распоряжаться имеет только пользователь, поскольку каждый перевод средств — это запись в распределённом реестре, лично подписанная электронной подписью пользователя. И давно работающие глобальные блокчейн-решения, такие как Bitcoin, Ethereum, Ripple, считаются более безопасными для пользователей, чем хранение средств на счетах банка.

Однако эти технологии существенно более медленные, чем банковские переводы, которыми мы привыкли пользоваться: вы никогда не сможете получить перевод в Bitcoin за несколько секунд — это издержки децентрализации. Это будет ещё один вызов — дать людям привычный пользовательский опыт, но при использовании технологии распределённых реестров.

А для Банка России основным технологическим вызовом будет обеспечение необходимой пропускной способности платформы и её безопасности. Эта задача не является классической, и пока мало кто в мире её успешно решил. Поэтому, однозначно, основные технологические вызовы стоят перед Банком России.

Интересен вопрос о том, какое количество блокчейн-операторов является оптимальным для обеспечения полномасштабного функционирования инфраструктуры цифрового рубля. На мой взгляд, более устойчивой будет инфраструктура, построенная на нескольких блокчейн-платформах, соответствующих определённым правилам. Это позволит в первую очередь решить вопрос с масштабированием: платформа Банка России остаётся базовой, а в неё из других платформ заносятся результирующие записи о переводах между различными лицами в рамках этих платформ, так же как и слепки реестров транзакций для аудита. Это позволит обеспечить и высокую скорость операций и прозрачность.

Трансграничным операциям с цифровыми валютами — быть, однозначно. Проблема

будет в том, чтобы на уровне государств договориться о технологической и регуляторной интеграции разных цифровых валют. Нужно также заниматься интеграцией децентрализованных финансов (DeFi) в модернизируемую финансовую систему страны. Однако рынок децентрализованных финансов базируется на криптовалюте, поэтому первый шаг для интеграции DeFi в существующую финансовую систему — принятие закона о регулировании криптовалюты.

Здесь сразу встают вопросы незаконного оборота цифровой валюты на территории страны, отмывания нелегальных доходов и финансирования терроризма (ПОД/ФТ). Пресечь эти потоки, а также те или иные коррупционные схемы, цифровой рубль, безусловно, должен помочь — такова его природа. Но для практической реализации этих задач понадобится его принудительная интеграция в те сферы деятельности, где эти потоки наиболее распространены. Так, мы однозначно приветствовали бы его использование в госзакупках, так как это сделает прозрачным расходование бюджетных средств, одновременно упростив отчётность для честных компаний.

Кстати, № 259-ФЗ «О цифровых финансовых активах, цифровой валюте» не относится к цифровому рублю. Цифровой валютой этот закон называет средства платежа, не являющиеся денежной единицей Российской Федерации, денежной единицей иностранного государства и (или) международной денежной или расчётной единицей. Под цифровой рубль понадобится изменение текущего законодательства. Такая работа уже ведётся. Думаю, мы увидим соответствующие документы вскоре после завершения пилота цифрового рубля.

Создание масштабной национальной доверенной ИТ-среды для функционирования цифровой национальной валюты ставит много вопросов. В их числе — не только создание инфраструктуры, и обеспечение её безопасности, но и поддержка масштабируемости и конфиденциальности этой инфраструктуры, а также интеграция банков и большая просветительская работа с юридическими лицами и населением. В целом, все эти вопросы ещё предстоит решать. И если часть задач можно решить по аналогии, например, задействовав инфраструктуру НСПК, то некоторые придётся решать одними из первых в мире.



Kaspersky Anti Targeted Attack

Специализированная защита от целевых кибератак

- Защита основных точек входа потенциальной атаки
- Повышение эффективности процесса реагирования на инциденты
- Целостная картина происходящего в инфраструктуре
- Сбор, хранение и предоставление информации об инцидентах для соответствия требованиям законодательства
- Вместе с Kaspersky EDR составляет решение класса Extended Detection and Response (XDR)

kaspersky АКТИВИРУЙ
БУДУЩЕЕ

kaspersky.ru/enterprise

ДиалОгНаука

СИСТЕМНАЯ ИНТЕГРАЦИЯ В ОБЛАСТИ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

dialognauka.ru

ИМПОРТО- ЗАМЕЩЕНИЕ ГРЯНУЛО

ОНО СЛУЧИЛОСЬ ВНЕЗАПНО И АВТОМАТИЧЕСКИ

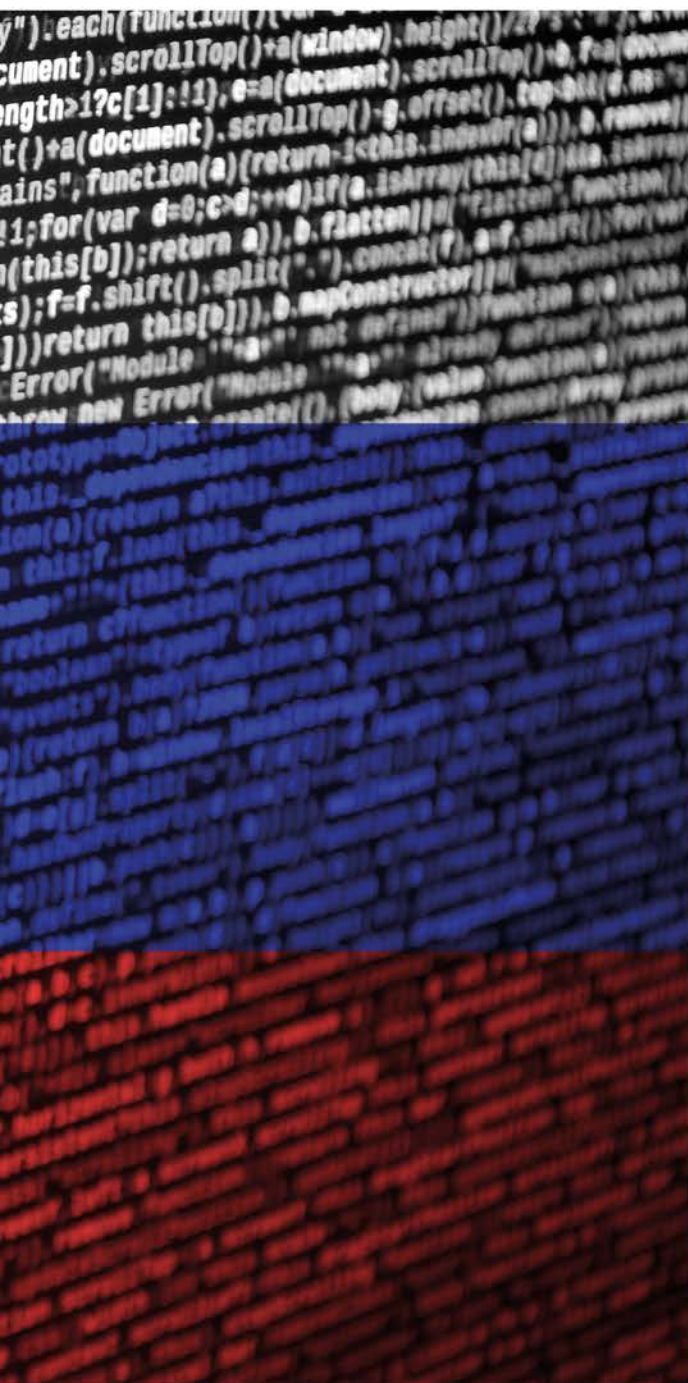


**Денис
БАТРАНКОВ**
член редколлегии
BIS Journal

Западные компании ушли из страны. На рынке информационной безопасности огромные очереди к отечественным производителям систем защиты информации. Иностранные производители в течение первых недель марта 2022 года отключали один за другим свои сервисы обновлений и техподдержки для клиентов из России. При этом в анонсах на сайтах компаний IBM, Citrix, Dell, Fortinet, Microsoft, VMware используется глагол «suspend», то есть компании предполагают, что ещё могут вернуться на рынок России. А в официальных

анонсах Cisco, Dell, ESET используется уже глагол «stop».

По словам сотрудников, представительства компаний Cisco, Fortinet, HPE и VMware в Москве ушли в отпуск на 3 месяца, надеясь, что ситуация улучшится. Представительства компаний Arista, Citrix, IBM, Fortinet, HPE, TrendMicro, Palo Alto Networks продолжают платить зарплату своим сотрудникам. При этом компании Arista, Cisco, Citrix, IBM отключили доступ российским сотрудникам к корпоративной информации. Компания ForcePoint полностью терминировала контракты своим сотрудникам в Москве.



Многие ИТ-компании прекратили техподдержку своих продуктов в России и Беларуси, и заказчики просят вернуть деньги. Особенностью ситуации является то, что в Москве находятся ещё и сотрудники международных компаний, которые обслуживают клиентов из Казахстана, Армении, Грузии, Узбекистана и других стран. Прагматичнее всех поступила компания Amazon, которая перевела ещё несколько лет назад всех своих сотрудников в Мюнхен, и они отвечают за все страны СНГ из Германии.

Самым важным для любого потребителя продукта по безопасности являются обновления

сигнатур для глубокого анализа контента приложений, систем предотвращения атак, антивирусных средств. Также обновлений требует URL-категоризация и базы индикаторов компрометации Threat Intelligence. Чтобы обеспечивать безопасность, нужны ежедневные обновления баз сигнатур. Да и сами продукты требуют обновлений программного обеспечения. Все иностранные производители отзывали лицензии и прекратили обновлять базы сигнатур заказчикам из России. В итоге во всей стране уровень обеспечения информационной безопасности компаний снизился. Перестал работать даже анализ вредоносного кода по поведению в «песочницах».

КАК МИНИМИЗИРОВАТЬ ПОСЛЕДСТВИЯ ОТКЛЮЧЕНИЙ

Если лицензия ещё не истекла, то у некоторых продуктов обновления можно устанавливать вручную при помощи загрузки файлов. Такие файлы можно получить на портале техподдержки, если он обслуживает клиентов из России. Однако общая рекомендация для пользователей из России касается отключения автоматического обновления программного обеспечения и операционных систем. Причин для отключения две. Первая — лицензию для продукта могут отозвать после подключения к серверу обновления. И вторая — есть риск, что в обновлении будут содержаться недокументированные функции. Это особенно важно учесть при обновлении продуктов с открытым исходным кодом. Есть случаи, когда обновления подобных продуктов содержат вредоносный код. Такие случаи были уже: бухгалтерская программа М.Е. Дос внезапно разослала всем своим пользователям вредоносный код Petya, а программа мониторинга SolarWinds внезапно предоставила удаленный доступ к сетям 300000 компаний неизвестным хакерам. Всё случилось после взлома самих серверов поставщиков программного обеспечения, где злоумышленники внедрили нужный им функционал, который уже разошелся по ничему не ведающим клиентам этих компаний.

На сегодня в России не так много компаний, у которых есть собственный экспертный опыт, чтобы проверить сторонний файл на наличие вредоносного кода или самим найти уязвимость в программном обеспечении. Наличие такой исследовательской лаборатории — это база для создания любого продукта по безопасности. В России мало компаний, которые сами создают сигнатуры для решений классов IPS, IDS и антивирусных средств, баз URL и Threat Intelligence (TI). Продукты по безопасности требуют круглосуточной работы команды

Статья также опубликована на портале НКЦКИ: safe-surf.ru/article

Часть компаний смотрит в сторону решений с открытым исходным кодом, но опасность заключается в том, что множество open-source проектов уже получило новые вредоносные куски кода

специалистов, которые разрабатывают сигнатуры для вредоносного кода, систем обнаружения атак, определения контента приложений и также поставляют клиентам индикаторы компрометации. В итоге даже в российских продуктах «под капотом» часто работает иностранный или бесплатно распространяемый движок. Обязательно спрашивайте поставщика, откуда он берет сигнатуры и индикаторы компрометации. Типовым способом создания «своего» продукта является использование сигнатур и кода Snort и Suricata, что скорее удивляет клиентов, чем мотивирует платить деньги. Необходимость наличия собственной исследовательской лаборатории в компании-разработчике подчеркивается тем, что злоумышленники постоянно разрабатывают методики обхода защиты. К примеру, популярная технология URL-фильтрации столкнулась с техникой cloaking, когда вредоносный сайт возвращает «хорошую» страницу серверам анализа, но вредоносную страницу браузеру жертвы. Поэтому сейчас активно развиваются технологии Machine Learning для обнаружения таких вредоносных сайтов, подключений и файлов в режиме реального времени в самом средстве защиты внутри компании.

Часть компаний смотрит в сторону решений с открытым исходным кодом, но опасность заключается в том, что множество open-source проектов уже получило новые вредоносные куски кода. Множество активистов занялось «исправлением» публичных проектов и добавляет не только лозунги и ругательства, но и реальный код, который может вывести вашу ИТ-систему из строя. К примеру, node-ipc удаляет файлы, если видит IP-адрес в заданном списке. Поэтому open-source сегодня — это катастрофический риск. Будьте осторожнее со скачиванием стороннего кода.

ЧТО У ВАС ДОЛЖНО БЫТЬ И ЧТО ПРЕДЛАГАЮТ ПРОИЗВОДИТЕЛИ В РОССИИ

Если говорить о классах продуктов, то первоочередная задача — обновить периметровую защиту. Это первый рубеж защиты, который видит и входящие соединения (например, электронную почту), и, что более важно, исходящие соединения от всех приложений сотрудников. Исходящие

соединения нужно контролировать, потому что именно через них происходят утечки, подключения к системам управления бот-сетями и загрузка вредоносного кода. Типовая ошибка — защитить только входящую почту и только исходящие соединения браузера. Для защиты периметра требуется множество функций, например контроль туннелей внутри DNS и ICMP. Вашим фокусом должны стать два класса продуктов: сетевая и хостовая защита. Они всегда дополняют друг друга. Атаки, которые не увидели в зашифрованном трафике, можно увидеть на рабочей станции, а атаки, которые нельзя посмотреть на принтере или веб-камере — видно по сети (см. врезку справа).

Большинство функций защиты реализовано в таком типе защиты как устройства всё-в-одном — UTM или NGFW и также NTA или NDR. Внутри UTM чаще всего используется VPN для удалённого доступа и затем уже трафик фильтруется различными технологиями: URL-фильтрация, обнаружение атак, антивирус. DNS и IP-адреса, URL-ссылки проверяются по базе известных индикаторов компрометации, которые в потоке идут из исследовательских лабораторий. Когда вы выбираете замену, то исходите из функций, которые вам нужны, а не из названий продуктов. Одну функцию может делать несколько продуктов, или наоборот — одно решение делает несколько функций. Например, возможно, VPN внутри российского NGFW вам не подойдёт и его нужно будет купить отдельно. Система предотвращения атак в потоковом режиме блокировки может не справиться с вашим трафиком, и стоит поставить её в режим мониторинга. Тогда у вас будет больше вариантов: продуктов класса IDS продаётся больше, чем IPS. В основном это связано с ложными срабатываниями, поэтому финансовые организации чаще всего работают с продуктами безопасности именно в режиме обнаружения и последующим анализом найденного сотрудниками SOC. Также в российских компаниях активно используется DLP, и тут отечественные производители уже практически полностью заняли рынок.

Следующим важным классом защиты являются песочницы. Именно они рассматриваются как ядро обнаружения неизвестного вредоносного кода по поведению. И такие продукты есть у пяти российских производителей. Здесь важно найти правильного архитектора, который закроет максимальное количество каналов доставки файлов: HTTP, SMTP, POP3, IMAP, FTP, SMB, NFS и также их SSL-версии. Важно, что вы должны как-то забрать из сетевого трафика или с хостов сотрудника или серверов файлы и отдать в песочницу и ещё как-то получить обратно сигнатуры или хеши для блокировки или оповещения

ФУНКЦИОНАЛ СЕТЕВОЙ ЗАЩИТЫ НА ПЕРИМЕТРЕ

- ♦ Обнаружение и блокировка ненужных компании приложений
- ♦ Выявление утилит удалённого управления
- ♦ Выявление туннелей и проху
- ♦ Контроль аккаунтов пользователей и привязка к текущим соединениям
- ♦ Обнаружение и блокировка атак (IDS и IPS)
- ♦ Анализ IoC по базе Threat Intelligence с базой DNS, IP, URL
- ♦ Адреса бот-сетей
- ♦ Антивирус для файлов в SMTP, POP3, IMAP, FTP, HTTP, SMB
- ♦ Песочница для файлов в SMTP, POP3, IMAP, FTP, HTTP, SMB
- ♦ Журналирование соединений для разбора инцидентов
- ♦ Журналирование атак для разбора инцидентов
- ♦ Анализ атак в трафике SSL
- ♦ Machine Learning для защиты DNS запросов к DGA доменам
- ♦ Определение страны по IP
- ♦ Определение ролей и типов устройств в сети (включая устройства IoT)
- ♦ Обновление сигнатур в реальном времени для новых атак
- ♦ Выявление целевых атак на компанию на разных стадиях MITRE ATT&CK
- ♦ API для интеграции с другими устройствами защиты
- ♦ Обнаружение сканирований и DDoS
- ♦ Разбор атак внутри трафика инкапсулированного в VLAN, MPLS, VXLAN, TEREDO, GRE, ERSPAN
- ♦ Функционал анализа сетевого трафика по поведению (NTA, UEBA)
- ♦ Выявление учётных данных и словарных паролей и паролей по умолчанию в трафике
- ♦ Передача файлов по ICAP в сторонние песочницы и DLP
- ♦ VPN шлюз
- ♦ URL фильтрация

о новой угрозе. Здесь очень подходят продукты, в которых есть парсеры протоколов с движком Deep Packet Inspection. И также в продуктах класса EDR/XDR есть интеграция с песочницей.

Продукты хостовой защиты класса XDR/EDR не только контролируют реестр, порты, проверяют файлы по сигнатурам и пускают сотрудников в сеть по правилам, но и контролируют аномальное поведение приложений и сотрудника на рабочей станции и сервере. Существует угроза, что злоумышленники просто украдут пароль сотрудника или будут атаковать легитимными утилитами, которые уже есть в различных операционных системах. Для защиты от этого класса угроз хорошо подходит функциональность, встроенная в XDR или EDR. XDR — это решения, в которых проверяется не только хостовая активность, как в EDR, а ещё и сетевая. Для анализа трафика и обнаружения атак по его поведению в трафике, рекомендуются продукты класса NTA или NDR. Если злоумышленник украл логин и пароль и работает от имени вашего сотрудника, то обнаружить его действия позволяют только эти решения.

Важным компонентом защиты в современных сетях является инвентаризация для выявления Shadow IT, сканирование уязвимостей и их устранение. Такие решения также присутствуют на российском рынке.

ПЕРВООЧЕРЕДНЫЕ МЕРЫ РУКОВОДИТЕЛЯ КОМПАНИИ

- ♦ Протестировать работу компании без интернета. Работает ли ваш бизнес и процессы в случае отключения страны от интернета?
- ♦ Проанализировать, в чьей юрисдикции находится каждый поставщик программного и

аппаратного обеспечения, и подготовить меры по переходу к локальному поставщику в случае отказа от поддержки. Сюда входит проверка TLS сертификатов для веб-приложений и хостинга на предмет действий в случае отказа от их поддержки.

- ♦ Перейти из иностранных облачных сервисов HaaS, PaaS, SaaS, FaaS в их российские аналоги.

- ♦ Сделать резервное копирование систем и проверить, что ваши сотрудники умеют делать восстановление из архива. Проведите тест на восстановление систем. Реализуйте полностью процесс периодического архивирования критичных систем и проверок того, что архивы в рабочем состоянии.

- ♦ Проинструктировать сотрудников или провести киберучения по действиям после атаки криптолокера, DDoS-атак, кражи конфиденциальных данных, остановки производства. В случае реального инцидента учиться будет уже некогда.

- ♦ Проконтролировать доступные снаружи ресурсы компании и удостовериться, что они под защитой и не содержат известных уязвимостей. Любые выставленные в интернет ресурсы — веб-сервера, VPN-шлюзы, почтовые сервера, DNS-сервера, каналы связи — сейчас под атакой. Используйте сканеры безопасности для того, чтобы проактивно выявлять и закрывать уязвимости в них. Также стоит обратить внимание на новый класс продуктов External Attack Surface Management. Необходимо прописать у каждого ресурса, кто за него отвечает, чтобы в случае инцидента знать, к кому обращаться.

- ♦ Подготовиться к DDoS-атакам на сервисы компании — установить нужное оборудование

у себя, у провайдера или подключить сервисы защиты от DDoS. Если у вас веб-сервер, то от DDoS-атак на уровне веб-приложений часто используют решения класса WAF.

♦ Провести инвентаризацию учетных записей и провести смену паролей, чтобы быть уверенным, что сотрудники (в том числе бывшие) не скомпрометировали пароли. Одновременно реализовать двухфакторную аутентификацию как минимум на VPN и, желательно, на другие сервисы компании.

♦ Проконтролировать, что процесс собственной разработки не использует публичные библиотеки исходного кода, которые могут быть исправлены злоумышленником. Стоит посмотреть, какие продукты класса SAST/DAST вам помогут в этом.

♦ Контролировать любой входящий и исходящий контент. Это нужно делать в двух точках — непосредственно в сетевом трафике и на каждом хосте компании по возможности. Здесь потребуются решения класса Network DLP и Host DLP, песочницы и TIP.

Класс продукта	Название компании	Российский аналог
NGFW	Palo Alto Networks NGFW Check Point Firewall Fortinet FortiGate Cisco FTD Sophos XG Firewall Juniper SRX	UserGate UTM Ideco UTM Код Безопасности Континент Инфотекс xFirewall Positive Technologies Network Attack Discovery
Хостовая защита EPP/EDR/XDR	Check Point SandBlast Agent Cisco AMP Microsoft ATP Symantec ATP Palo Alto Networks XDR Sophos Endpoint Bitdefender Endpoint Avast Business Antivirus Symantec Endpoint Panda Endpoint McAfee Endpoint	Kaspersky EDR Kaspersky KES Positive XDR Код Безопасности Secret Net Studio BiZone EDR
Защита веб-приложений WAF	F5 Imperva	Positive Technologies AF Код Безопасности WAF SolidWall WAF
Системы анализа и корреляции событий SIEM	Micro Focus ArcSight IBM Qradar FortiSIEM McAfee SIEM	Positive Technologies MP SIEM Kaspersky KUMA RuSIEM
Поведенческий анализ сетевого трафика NDR/NTA/UEBA	Cisco StealthWatch Plixer Scrutinizer Vectra AI Awake Security Platform LogRhythm NetworkXDR RSA NetWitness Network ExtraHop Reveal(x) TrendMicro DDI	Positive Technologies NAD Гарда Монитор
Обнаружение вторжений IDS/IPS	TrendMicro TippingPoint Palo Alto Networks NGFW Check Point Firewall Fortinet FortiGate Cisco FTD Sophos XG Firewall Juniper SRX	VipNet IDS Код безопасности «Континент» Kaspersky KATA и KICS Positive Technologies Network Attack Discovery Гарда Монитор
Сканер безопасности	Tenable Nessus Qualis	Positive Technologies VM

♦ Проверить, есть ли планы реагирования на основные типы инцидентов, и доведены ли они до всех сотрудников: DDoS-атаки, шифрование данных компании, взлом сайта, кража логинов и паролей сотрудников и клиентов, отказ оборудования и возможности по его замене.

♦ Начать контролировать исходящие из сети соединения на предмет перемещения вредоносного контента и подключения к известным вредоносным адресам в интернете. Опять же тут работают как общеизвестные базы

URL-категорий, так и базы Threat Intelligence, специальные блокировщики DGA-доменов, песочницы и другие техники, которые есть в NGFW, UTM и также NTA-решениях.

♦ Проверить, что компания в данный момент уже не заражена и на компьютерах или сетевых устройствах не установлены известные виды вредоносного программного обеспечения. Для этого рекомендуется заказать аудит у Positive Technologies, Лаборатории Касперского, BiZone и других поставщиков услуг.

Класс продукта	Название компании	Российский аналог
Мультифакторная аутентификация MFA	ESET SA Microsoft MFA Okta Google Authenticator	Multifactor Алладин Jakarta Актив Рутокен
Threat Intelligence Platform	Anomali Recorded Future EclectIQ RiskIQ Threat Intelligence Cyjux Threat Intelligence ThreatConnect Palo Alto Networks Autofocus	Positive Technologies Cybsi Kaspersky Cybertrace R-VISION TIP BI.ZONE ThreatVision GIB Threat Intelligence & Attribution
Защита от утечек по сети и на хостах DLP	Symantec ForcePoint McAfee	Infowatch SearchInform Solar Dozor
Антивспам	Fortinet FortiMail Cisco ESA	Kaspersky Antispam
Разработка безопасного кода SAST/DAST	Fortify Static Code Analyzer Checkmarx CxSAST IBM App Scan Source	Solar inCode Infowatch Custom Code Scanner
Обнаружение открытых сервисов External Attack Surface Management (EASM)	Palo Alto Networks Xpanse	Group-IB AssetZero
Защита контейнеризации CWPP	Palo Alto Networks Prisma Cloud Aqua Sysdig	нет
CASB	Netscope Palo Alto Networks CASB Symantec CloudSOC CipherCloud Cisco CloudLock Oracle CloudService Microsoft Cloud App Security	нет
SASE/ZTNA	Palo Alto Networks Prisma Access Skyhigh Networks Netscope NewEdge Cisco SASE Check Point CloudGuard Connect Citrix SASE FortiSASE Versa SASE Vmware SASE Zscaler SASE	нет

НАТАЛЬЯ КАСПЕРСКАЯ: «ИМПОРТОЗАМЕЩЕНИЕ В ИБ ПОЧТИ ПОЛНОЕ»



**Наталья
КАСПЕРСКАЯ**
председатель
правления АРПП
«Отечественный
софт», президент
группы компаний
InfoWatch

Мнение председателя правления АРПП «Отечественный софт», президента группы компаний InfoWatch Натальи Касперской об импортозамещении всегда важно, особенно сегодня. И мнение это в течение последнего месяца Наталья Ивановна высказала неоднократно. С обоюдного согласия BIS Journal публикует цитаты из её выступлений, прозвучавших на телеканале «Россия 24»¹ и на пресс-конференции в ТАСС.

Вопрос. Мы ежедневно получаем сообщения о том, что одна за другой международные компании отказываются от сотрудничества с Россией, приостанавливают свою работу в нашей стране. Если оставить за скобками все их мотивы и целесообразность их решений, то давайте поговорим о том, справимся ли мы собственными силами в этой ситуации? Сможем ли развивать собственные информационные технологии (ИТ) и поддерживать развитие отечественных компаний?

Наталья Касперская. На мой взгляд, ситуация с софтом у нас в России достаточно хорошая. На текущий момент в реестре российского программного обеспечения (ПО) почти 13 тысяч программных продуктов отечественного производства от четырёх с лишним тысяч поставщиков. Эти продукты покрывают основные направления, на которых требуется это ПО. Там есть ПО общего применения, есть решения по информационной безопасности и т.д.

Ситуация, однако, неравномерная: в некоторых случаях мы очень хорошо импортозаместились, в некоторых — нет. Если мы возьмём информационную безопасность (ИБ), то я считаю, что импортозамещение в сегменте ИБ за эти 8 лет произошло практически полностью. На большинстве предприятий сейчас используются отечественные ИБ-решения. Да, сохраняются отдельные «островки», но заменить импортные решения российскими и там можно довольно быстро, потому что решения есть, и они мирового уровня.

С точки зрения офисного ПО ситуация скорее обратная. Там порядка 20% предприятий использует отечественное, остальные — иностранное программное обеспечение, и это, конечно,

тяжело. Тут нужно будет менять модель и менять довольно быстро. То же самое — по системам управления предприятием (ERP), по операционным системам (ОС), по системам управления базами данных.

Но вопрос «А что мы можем сделать?» я слышу на протяжении последних 8 лет, с 2014 года. Как и вопрос «А могут ли российские разработчики покрыть потребность отечественного рынка в ИТ-решениях?» Мы, разработчики, отвечаем, что можем. Говорим: «Приходите к нам». Но у нас, к сожалению, импортозамещение последние 8 лет шло по принципу: «Два шага вперёд — шаг назад».

Вопрос. Помните, вы говорили, что идёт импортозамещение и внутри тех компаний, которые заявляют о себе как об отечественных. Оценивая те компании, что сегодня находятся в реестре, можем ли мы сказать, что это действительно российские компании?

Наталья Касперская. Было видно, куда раскручивается спираль санкций. Она всё время раскручивалась, давление усиливалось. И этот злосчастный американский билль № 1260, который два года назад обсуждался в конгрессе США, и другие меры по запрету передачи в Россию высоких технологий. За это время можно было сообразить, что американцы не просто так придумали этот билль и остальные меры, а чтобы их рано или поздно применить. То есть они вытащили оружие и показали, что будут из него стрелять. А у нас почему-то всё время надеются на какие-то благоприятные сценарии. Мол, этого-то уж точно не произойдёт...

Насколько все эти решения отечественные? По-разному. Отечественных довольно много. Потому что Министерство цифрового развития, связи и массовых коммуникаций РФ за

¹ <https://youtu.be/N1wcxNgD5Yo>

последние три года довольно сильно ужесточило правила попадания отечественных продуктов в реестр. В частности, продукт, доля «российскости» в котором ниже 50%, не рассматривался как тот, что может войти в реестр российского ПО. Кроме того, российские продукты должны были как минимум иметь возможность работы на отечественных платформах, операционных системах и системах управления базами данных (СУБД). То есть, если заявитель подаёт в реестр программный продукт, работающий исключительно на СУБД Oracle, то его заявка будет отклонена...

Вопрос. Вы сказали, что эта ситуация может повлиять на экспорт российских технологий?

Наталья Касперская. Остальной мир сейчас в ужасе смотрит на то, что, оказывается, существует техническая возможность всё выключить. Они понимают, что находятся в зависимости от иностранных технологий. И они, конечно, будут искать альтернативы, особенно азиатские страны.

Вопрос. То есть у России появилось окно возможностей?

Наталья Касперская. Да. Например, несколько наших компаний уже получили предложения от нескольких стран о поставках российского софта, причём в срочном порядке. Санкции по отключению оказались наглядной демонстрацией не только нам, но и всему миру, что работающее западное ПО является уязвимым. Уязвимым для всех стран, которые этим ПО пользуются. Санкции проводятся произвольно, непредсказуемо, и это становится угрозой для всех пользователей. Вы внедряете у себя западные решения, и вдруг оказывается, что по чьей-то указке, непонятно чьей, эти решения могут быть отключены в любой момент. Это продемонстрировано всему миру, и мир, понятно, испугался.

Поэтому, я думаю, у нас сейчас появится возможность системно продавать софт именно с уровня Российской Федерации. Дело в том, что альтернатив в мире нет, и страна наша оказывается чуть ли не единственным поставщиком софта. В Китае софта мало, и он довольно специфичный, и кто остаётся? Запад и Россия. Запад себя скомпрометировал, и получается, что это такая новая гигантская возможность для российских производителей. Её, конечно, надо правильно сформулировать... Причём, отмечу, те страны, которые к нам обратились, не просто хотят получить какие-то отдельные решения, а просят написать им стратегию, потому что они не верят американцам. И получается, что нам придётся передавать свой цифровой суверенитет в эти страны, так как у них нет своих



Пресс-конференция «Российская IT-отрасль: вызовы в новых технологических условиях» (15 марта 2022 года)

возможностей построить такой суверенитет, а доверяют они сегодня только нам.

Вопрос. Как сегодня вести себя обычным пользователям компьютеров и как вести себя компаниям? Например, сразу появились рекомендации не включать обновления. Что ещё нужно сделать, чтобы, во-первых, не стать жертвами злоумышленников, а во-вторых, сохранить спокойствие и свои данные в ситуации всеобщей нестабильности? Потому что санкции включаются одномоментно, а у нас идёт работа, непрерывные коммуникации и т.д.

Наталья Касперская. Мы в компании тоже приостановили скачивание обновлений, потому что в любом обновлении может прилететь то, что позволяет выключить систему или сделать её неработоспособной. Это снизит безопасность систем, потому что в обновлениях есть так называемые патчи безопасности, но позволит сохранить её работоспособность. Я не думаю, что до обычных домашних пользователей эта волна докатится, хотя с той русофобией, что сейчас развивается в так называемом прогрессивном мире, всё может быть. И тогда обновления лучше на всякий случай держать выключенными. Что касается приостановки обслуживания ПО и снижения ИБ, то у нас есть подразделение, которое занимается защитой автоматизированных систем управления технологическими процессами на крупных промышленных предприятиях. И по этому направлению сейчас идёт бешеный рост запросов от крупных предприятий и организаций на установку систем защиты от хакерских атак, который мы не можем удовлетворить, потому что не ожидали настолько резкого роста спроса.



Андрей АРЕФЬЕВ
директор
по инновационным
проектам
ГК InfoWatch

ПРИНЯЛИ ОГОНЬ НА СЕБЯ

ТРАДИЦИОННО БАНКИ ПЕРВЫМИ
СТОЛКНУЛИСЬ С НЕОБХОДИМОСТЬЮ
ТЕХНИЧЕСКОГО ПЕРЕВООРУЖЕНИЯ В СФЕРЕ ИБ

Бурное развитие финтеха в России привело к тому, что значительная часть современных финансовых систем зависит от западного ПО и облачных сервисов. Например, SAS (в моделировании кредитных рисков), инженерные решения ORACLE (Big Data, Exadata и пр.) и т.д. В частности, за 2022 год три крупных банка внедрили Private Cloud на базе таких сред с использованием ИБ-решений Check Point и Palo Alto. Поэтому первоочередной задачей сейчас является замещение таких решений отечественными аналогами. Особенно с учётом того, что финансовые организации, в частности из банковского сектора, традиционно занимают лидирующие позиции по применению передовых технологий для построения комплексных систем информационной безопасности, экспериментируя как с западными, так и с отечественными системами.

НЕ НА ПУСТОМ МЕСТЕ

Нужно отметить, что ИБ-рынок наполнен широким спектром отечественных решений, применяемых в работе с разными задачами. Среди используемых средств защиты информации — системы обнаружения и предотвращения атак, антивирусное ПО, DLP-системы, межсетевые экраны, решения класса EDR для защиты от таргетированных атак и другие инструменты для противодействия современным кибератакам и ИБ-рискам.

В России исторически сложился конкурентный рынок ИБ-решений. Поэтому если говорить об импортозамещении такого ПО (антивирусы, SEIM, сканеры уязвимостей и сканеры кода), то с ходу вспомнятся российские бренды, известные на мировом рынке: «Лаборатория Касперского», Positive Technologies, UserGate и т.д. Не говоря уже о рынке DLP-систем, который в России был и остаётся самым конкурентным, с такими игроками, как InfoWatch. К слову сказать, несколько отечественных DLP-систем отмечались в отчётах аналитического

центра Gartner, что явно говорит об их признании не только на российском рынке, но и на международном.

DLP-ОАЗИС

В России импортных DLP-систем практически не осталось, и на это существуют объективные причины. Российские системы этого класса технологически не уступают, а в ряде случаев превосходят зарубежные аналоги за счёт отраслевого экспертного опыта разработчиков (близость к заказчику), высокой адаптации к техническим условиям заказчика, обеспечения бесперебойной техподдержки и оперативного решения проблем. Эти факторы позволили уже в 2016 году фактически исключить зарубежные DLP-системы из отечественного рынка.

Одной из особенностей отечественных DLP-систем является глубокая интегрируемость DLP с другими ИТ-системами. Например, интеграция клиентов электронной почты на мобильных устройствах и DLP-системы. Если такой интеграции нет, то легко возможны утечки конфиденциальной информации. К примеру, наш флагманский продукт — InfoWatch Traffic Monitor — интегрирован с продуктом WorksPad компании RuPost: через специальный сервер контролируется то, что загружается на мобильный клиент.

ПРОСТО ПОДСТАВА

В прошлом году председатель совета директоров «Киви Банка» Мария Шевченко оценила долю иностранного ПО в банках как превышающую 90%. Однако отметила следующее: «Понятно, что процент разнится в зависимости от класса продукта. Если смотреть, например, на АБС и ПО для решения каких-то специфических отраслевых задач, здесь доля будет меньше — порядка 50%». Это означает, что, несмотря на сравнительно неплохую картину с отечественным ПО в области информационной безопасности, могут возникнуть сложности. Сегодняшний уход с российского рынка зарубежных вендоров оставил не только банки без техподдержки, обновлений

Зарубежный продукт	Российский аналог	Степень готовности
Microsoft Windows, MacOS	«Альт Линукс» «Астра Линукс» «РедОС» «РОСА» «Циркон 37К»	Готовые продукты
Microsoft Office	«МойОфис» «Р7-Офис» CommuniGate Systems	Готовые продукты
Skype, Zoom, Microsoft Teams, Cisco, Poly, Avaya, Google	«Видеомост» Trueconf Vinteo Mind «Яндекс.Телемост» «Сферум»	Готовые продукты
Oracle, SAP	Базы данных: PostgresPro «Ред База Данных» «Линтер» ERP-решения: 1С «Галактика»	Готовые продукты
AutoCAD	«КОМПАС-График» NanoCAD	Готовые продукты

Российское ПО для импортозамещения (примеры)

ПО, продления лицензий, чреватых сбоями работы систем, но и потенциально оставил отечественные компании уязвимыми перед хакерскими атаками. Успешность этих атак, как правило, обеспечивается найденными уязвимостями, и устранить их можно либо наложенными средствами, либо установкой обновлений.

НЕ ПРОСТО АНАЛОГИ

При разговоре об импортозамещении всё выглядит так, будто во многих сферах у нас есть какие-то аналоги западным решениям. Это касается офисного ПО, баз данных, операционных систем, которые присутствуют на российском рынке в достаточном количестве. При упоминании отечественных операционных систем сразу вспоминаются такие компании, как «Базальт», Astra, «Ред ОС» и др. Несмотря на то что разрабатываются эти операционные системы на Open Source, отечественные компании привносят в них что-то новое и, как правило, востребованное заказчиками. Так, компании «Базальт» и Astra расширили базовую функциональность своих решений до уровня Microsoft Active Directory, которая фактически является ключевым ИТ-элементом любой компании, позволяя управлять учётными записями, правами их доступа и политиками, применяемыми к рабочим станциям.

Другой пример хорошего потенциала для импортозамещения — российская СУБД. Oracle ушёл с российского рынка, по некоторым оценкам этот производитель занимает до 70% российского рынка СУБД. Однако мы видим, что в России есть замена высокопроизводительной базе данных — Postgres Pro. Компания существует давно, оказывает профессиональную техподдержку и развивает свою функциональность, которая сопоставима или близка к тому, что было сделано Oracle, но значительно меньшими силами. Учитывая, что многие отечественные банки пользуются СУБД Oracle, то, на мой взгляд, существование достойной российской альтернативы — это большой плюс. Другой вопрос, что поставщики данного решения сегодня перегружены, и процесс перехода потребует усилий от производителей решений, использующих базы данных.

Существуют аналоги ERP, HR, CRM-систем и т.д. На российском рынке всегда был 1С — разработчик, который быстро адаптировался к российскому законодательству и предлагал рынку достойное и эффективное решение для ведения документооборота. Присутствует «Террасофт» — на примере нашей компании можем подтвердить его эффективную работу и жизнеспособность даже в сложных задачах. Мы давно заменили известную американскую систему Salesforce на решение от «Террасофт».

АРПП "ОТЕЧЕСТВЕННЫЙ СОФТ"

ЦЕНТР КОМПЕТЕНЦИЙ ПО ИКТ

О ПРОЕКТЕ

ВХОД

КАТАЛОГ

Совместимости Российского Программного Обеспечения

Продукты

Импортозамещение

Импортозамещение : Банки и финансы

Все разделы →

Банки и финансы

Apple ASR/TTS

- VoiceKey.PLATFORM. Программный комплекс мультимодальной биометрической аутентификации.

Apple Siri

- Омниканальная диалоговая платформа на естественном языке ChatNavigator

Asterisk.IVR

- VoiceKey.PLATFORM. Программный комплекс мультимодальной биометрической аутентификации.
- Омниканальная диалоговая платформа на естественном языке ChatNavigator

Ataccama MDM

- Единый клиент

Ataccama ONE

- Единый клиент

Ataccama ONE MDM

- Единый клиент

Avaya Conversational Intelligence

- Smart Logger II. Программный комплекс системы контроля качества работы операторов и мониторинга удовлетворенности клиентов.

Avaya experience portal

- VoiceKey.PLATFORM. Программный комплекс мультимодальной биометрической аутентификации.
- Омниканальная диалоговая платформа на естественном языке ChatNavigator

Calypso Technology

- Digital Q.FinancialMarkets

CBS-3

- Digital Q.Consumer
- Digital Q.Corporate
- Digital Q.Payments
- FXL 2.0

Cisco Unified Customer Voice Portal

- VoiceKey.PLATFORM. Программный комплекс

Банковское ПО — это в основном продукты компаний «Диасофт», ЦФТ (Центр финансовых технологий), БФТ, но не только. Подробнее о банковских продуктах можно узнать в Каталоге импортозамещения, в разделе «Банки и финансы»: catalog.arppsoft.ru/replacement

Для нас такое импортозамещение прошло легко и безболезненно.

Компания AutoDesk инвестировала достаточно много средств в обучение российских инженеров своим решениям, но даже в такой сложной сфере есть альтернатива — инженерное ПО «Компас». Насколько мне известно, ведущие российские инженерные университеты давно обучают студентов работе с этой системой.

О СОХРАННОСТИ ДАННЫХ

Ещё одним примером импортозамещения в системах безопасности класса SIEM и XDR-систем, на которых строятся, в частности, SOC-центры, — решения от компаний RuSIEM и Positive Technologies. При этом стоит отметить, что главное в области SOC/SIEM (помимо западного ПО в крупнейших банках) — это отключение наших финансовых организаций от получения фидов (сведений об инцидентах в мировом масштабе). Это делает даже импортозамещённые центры кибербезопасности уязвимее, например, в области антифрода и DDoS-атак.

Когда есть ИТ-система, которая обеспечена стабильной работой и средствами защиты, важно иметь возможность сделать бэкап данных; важна и физическая безопасность — может сгореть жёсткий диск или компьютер, и данные могут быть утеряны. В случае необходимости экстренного восстановления инфраструктуры и данных может помочь российская компания «Рубэкап», входящая в ГК Astra Linux.

СМОТРИТЕ КАТАЛОГ

В целом, не так давно Ассоциация разработчиков программных продуктов «Отечественный софт» опубликовала каталог, который включает наименования программного обеспечения, разбитого по классам, и его зарубежные аналоги. См. <https://catalog.arppsoft.ru/replacement>.

Подытоживая вышесказанное, хочу отметить, что особенностью финансовой ИТ-инфраструктуры является то, что она изначально выстраивалась в соответствии с западными стандартами безопасности, например, PCI DSS или нормативами по управлению рисками (в том числе операционными, в составе которых и обеспечение непрерывности бизнеса и рисков ИТ — ряд соглашений BASEL). В последнее время на базе рекомендаций МБФ и Банка Международных Расчетов начала выстраиваться инфраструктура цифровых валют центральных банков (CBDC), в том числе цифрового рубля. А о них известно совсем немного. Поэтому в первую очередь необходим полный переход на отечественное регулирование ИБ в финансах.

ТАКТИКА СЕГОДНЯ ОПРЕДЕЛИТ СТРАТЕГИЮ ЗАВТРА

ГОТОВА ЛИ ОТРАСЛЬ К РЕЗКИМ ИЗМЕНЕНИЯМ?

В текущей ситуации могу описать положение как «могло бы быть лучше». Хотя в России хватает собственных решений ИБ, а также существуют сложившиеся команды по их разработке, нарушения сотрудничества и конкуренции доставят проблем. С одной стороны, собственные ИБ-решения нам нужны. С другой стороны, локально реализовывать и развивать весь существующий в мире спектр продуктов в сфере информационной безопасности, ориентируясь только на местный рынок, — дорого и долго.

ТЕХНОЛОГИИ ЕСТЬ, НО ПРОБЛЕМ НЕ МЕНЬШЕ

В базовых ИБ-технологиях, на мой взгляд, в нашей стране серьёзного недостатка не будет, они представлены достаточно широко. Что-то более сложное, где необходимо реализовывать, например, специфические протоколы, Threat intelligence и широкие сети мониторинга, — очевидно, будут ограничения возможностей.

К проблемам ИТ-сферы добавим очевидно усугубившийся недостаток квалифицированного персонала. Неочевидны пока сложности, связанные с аппаратными платформами. Но ощущения уже неприятные: поиск сотрудников не станет легче, как вы понимаете. А проблема нехватки оборудования, на мой взгляд, становится одной из ключевых, так как многие системы ИБ, сетевого оборудования, средств автоматизации в целом зависят от возможностей платформ и проектируются под те или иные совместимые «железки».

Процесс освоения (закупки, сертификации, документирования) аппаратных платформ сейчас дорог и дорог, с точки зрения разработчика, а уверенности в их доступности в будущем нет. Необходимость заменить платформу у существующих проектов часто означает сделать с нуля или близко к тому. Если бы столпы отрасли смогли организовать «локализованную аппаратную платформу», линейку оборудования разной мощности, на которое разработчики могли бы рассчитывать и получать с ней проверенные средства разработки и рабочую (сертифицируемую) документальную подоснову на базе имеющихся в стране решений (даже и китайских), то, на мой взгляд, это очень помогло бы и прикладникам, и разработчикам ИБ.

Подбирать самостоятельно сейчас — значит тратить время и рисковать, что выберешь не то, что будет доступно. А доступность и наличие будут определяться массовостью, просто потому что мы говорим о производстве материальных вещей. Массово используемые аппаратные решения позволят создать пользовательскую базу и накопить опыт использования быстрее и дешевле, а также позволят оперативнее локализовать производство полностью.

ВОПРОС УРОВНЯ РЕШЕНИЙ

На мой взгляд, это задача государственного уровня или уровня консорциума компаний — производителей оборудования. Использование этого подхода может серьёзно усилить наше положение в средней и долгосрочной перспективе. Задачу такого уровня почти невозможно решать на уровне отдельных компаний, так как всё в итоге упрётся в процент локализации и сертифицируемость (аттестацию) платформы при реализации требований ИБ. Опять же — мы живём в крайне динамическом окружении, в котором сертификация решений будет серьёзным ограничением развития. Лучше базовые вопросы с платформами решать на уровне рынка в целом однократно.

Дополнительно на уровне самих решений надо налаживать кросс-взаимодействие разных производителей. «АйТи Бастион» делает так уже довольно давно, имеет портфель технических интеграций, и это хорошо и для продуктов, и для тех, кто ими пользуется. Это позволяет, не сильно увеличивая бюджеты заказчика, предоставлять лучшие результаты. Договариваться о поддержке протоколов, узлах обмена информацией об инцидентах и т.п. Рассказывать публично коллегам, фиксировать стандарты и протокол

Да, сейчас на фоне невозможности работать с решениями внешних производителей мы наблюдаем серьёзный интерес, например, к нашим продуктам в области контроля действий администраторов (РАМ-системам). Мы в это интересное время стараемся помочь заказчикам, безвозмездно предоставляя наш продукт СКДПУ НТ на время, чтобы коллеги быстро порешали свои проблемы. Если мы сможем на таком турбулентном рынке выстроить взаимодействие и сотрудничать стратегически, то наши тактические шаги сегодня могут привести к значительному усилению возможностей ИБ-решений в России в будущем.



Дмитрий МИХЕЕВ
технический
директор
ООО «АйТи Бастион»



Дмитрий ЛЕВИЕВ
председатель
Совета
НП «Партнёрство
специалистов
по информационной
безопасности»

ИМПОРТОЗАМЕЩЕНИЕ НА ПРАКТИКЕ — ЭТО...

УРОКИ СТАРОГО АДМИНА

Импортозамещение — это срочный переезд всей организации, её клиентов и партнёров из одного мира информационных технологий в другой без остановки, со сменой лошадей прямо на марше. Собственно, как это всегда и было в ИТ (ИБ) российских компаний, когда бизнес начинал быстро, скачкообразно развиваться. Говорить о конкретных примерах, заменах и преодолеваемых трудностях не даёт действующее законодательство и «понятийные» договоры с организациями, точнее с их владельцами. Но предупредить, где необходимо постелить соломку, оставить запас провизии и чистой воды, стоит, поэтому усаживаемся поудобнее с карандашом в руке.

ПЕРВОЕ ПРАВИЛО

Первое и основное правило импортозамещения — всё придётся делать самому: проверять совместимость ПО, придумывать схемы управления и т.д. В 1990–2000-е годы так жили старые админы: к ним приходили вендоры, предлагали новые решения, которые внедрялись с применением известного приёма в виде палок, костылей и наשלёпок. Со временем решения становились лучше, временные «шалашики» убирались, и Z-поколение админов видит уже красивую работающую безотказную инфраструктуру. Практически все современные крупные решения на первых шагах своего развития были «некрасивыми», угловатыми и жутко глючными. Придётся этот путь пройти во второй раз.

АЙСБЕРГ ПРОБЛЕМ. РЕШАЕМО

Для понимания объёма работ и проблем для планирования импортозамещения недостаточно иметь перечень ПО, установленного на серверах и рабочих станциях, и описанные бизнес-процессы обработки. Как правило, если это всё и есть, то это только вершина айсберга. Глубина залегания айсберга проблем зависит от монолитности ИТ-ландшафта. Под этим мы понимаем унифицированность аппаратной платформы и управления: даже бюджетные организации и учебные центры не могут похвастаться типовыми рабочими местами (одинаковые материнские платы, периферия, сетевое оборудование) и единым управлением (единый домен безопасности и управления). Например, для учебных заведений характерно

наличие так называемого научного оборудования, купленного на деньги от выполнения НИР и НИОКР с лицензиями для коммерческого использования, а ИТ-ландшафт рабочих мест студентов представляется всем многообразием ИТ-платформ.

Для фиксации объёма работ необходимо достаточно длительное наблюдение за эксплуатацией имеющейся ИТ-инфраструктуры во всех «временных рамках» бизнес-процесса: обычная деятельность, квартальные авралы, сессия, закрытие года, отчётности в разные периоды и сроки и т.д. с фиксацией всего запускаемого ПО, в том числе пользовательских скриптов офиса, батников и т.д. Без внешнего воздействия получить полный объём с использованием такого наблюдения в учебном заведении занимает примерно 14–16 месяцев, так как основной цикл — это обучение в течение 10 месяцев и набор обучаемых в течение 3–5 месяцев. Для организаций проектного плана, работающих в режиме годовых контрактов, — по немногочисленным наблюдениям — 14–15 месяцев. Что же делать, если этого времени нет? Как и с планами ОНВД и требованиями ГО и ЧС и пожарного надзора — надо провести учения: ставим на все АРМ-программы, логирующие используемое ПО и действия пользователей, и проводим учения. Таким образом, мы получаем следующие важные параметры:

- ♦ используемое программное обеспечение с перечнем локальной автоматизации;
- ♦ перечень мест реального хранения информации, которая подлежит защите и резервному копированию;
- ♦ проект программы-методики тестирования работоспособности ИТ-ландшафта после замены компонентов.

ТИПИЧНЫЙ ПРИМЕР

В одной из проектных организаций в рамках замещения прикладного ПО был указан закупленный на всех АРМ MS Office. При проверке оказалось, что проектный отдел в рамках выполнения государственного контракта уже два года использует portable (переносимую) версию LibreOffice, которая пересобирается одним из разработчиков сопроводительной документации для выполнения требований по представлению документации по ГОСТ 2.106, ГОСТ 7.32 в формате ODF. Скрипты, используемые для

оформления документации, реализованы, соответственно, на Python. Поддержка решения фактически минует ИТ- и ИБ-отделы.

ДОЛГИ НАШИ

Второе большое направление анализа — это выявление технического долга собственного ИТ, которое не выполняло заявки подразделений в силу нехватки сил, средств, времени и т.д. Как правило, пользователи такой технической долг автоматизируют локально, через Excel, VBA-скрипты, Bat-ники и т.д. Ликвидация технического долга, как правило, дешевле, чем импортозамещение локальной автоматизации.

ОСТОРОЖНО, ОБОРУДОВАНИЕ!

Есть рабочие места, на которых импортозамещение необходимо выполнять с особой осторожностью: это системы управления технологическим оборудованием (рентген-оборудование, различные насосы, клапаны, станки и т.д.). Как правило, всё это оборудование имеет требования по безопасности помимо информационной. Например, замена ПО сервера СКУД (системы контроля и управления доступом) может привести к большому числу пострадавших при нештатной ситуации на объекте, что грозит команде импортозамещения уголовной ответственностью даже после увольнения с работы.

ПРОСТОЙ ВОПРОС

Перейдём к самому, пожалуй, простому вопросу — выбору замещающих систем управления баз данных (СУБД). Вопрос этот прост по причине малого числа пар, которые позволяют провести замену.

Правда, отдельно стоит сказать про замену СУБД Oracle с хранимыми процедурами (фактически размещённым сервером приложений). Замена такому решению один в один нет. Но есть два направления движения. Первое — Tiberio от южнокорейской корпорации TmaxSoft. На её базе работает АО НСПК. Совместимость — переносимая. Необходимо специальным программным обеспечением от разработчика пройти по коду PL/SQL и определить порядок перехода. В среднем такой переход можно осуществить в течение 6 месяцев, но надо помнить: количество сертифицированных админов СУБД надо увеличить в ИТ-отделе в два раза, а в ИБ-отделе необходим минимум один человек, который понимает особенности работы с Tiberio. Второе направление — PostgreSQL. Замена возможна только в плане базы данных с фактическим переписыванием кода сервера приложений (хранимых процедур). Что касается замены MS SQL на PostgreSQL, то в моей практике такая замена не приводила к большим затратам ресурсов на переход.

ЗАМЕНА СЕРВЕРНОГО ПО

Замена серверного программного обеспечения вызывает трудности только для двух классов ПО: удостоверяющий центр и сервер приложений, завязанный на IIS. В остальных случаях это стандартный выбор окружения прикладного серверного ПО и привычек ИТ-отдела с учётом пожеланий ИБ.

ОПЫТ ЗАМЕНЫ ОС

Отдельно хочется поделиться опытом замены ОС на рабочих местах. На опыте при массовом импортозамещении выявлено, что построение только на базе одной конкретной ОС невозможно в силу ограничений поддержки драйверами как конфигурации используемых АРМ, так и периферийных устройств, которые используются в работе.

Перечень ОС, которые стоит рассматривать для установки на АРМ, можно взять из документации на СКЗИ, которые используются в организации. Это позволит ограничить круг рассматриваемых ОС. Хотя коллеги из банковской сферы могут и не знать такого количества существующих на рынке ОС.

Если вопросы электронного документооборота уже вошли в область ответственности ИТ и ИБ, то для применения СКЗИ на отечественных ОС имеются серьёзные ограничения:

- ♦ нельзя получить класс СКЗИ выше КС2 без использования HSM;
- ♦ стоимость лицензий на программные СКЗИ под некоторые ОС в разы выше, чем используемые для Windows. Так, эксплуатация «КриптоПро CSP» под FreeBSD всегда считается как серверная (есть целый научный институт, который работает на рабочих местах FreeBSD; дизайн рабочих мест очень похож на Windows XP);
- ♦ необходимо использовать аппаратные хранилища с неизвлекаемыми ключами («Аладдин», «Актив», «Мультисофт», «АТ Бюро», «Смарт-Парк»);
- ♦ для работы с СКЗИ на порталах госорганов необходимо тестирование как носителей (аппаратных СКЗИ), так и плагинов в браузерах.

НЕ СТОИТ ЗАБЫВАТЬ

При импортозамещении прикладного ПО необходимо помнить, что основную ценность для расчётных программных систем составляет не алгоритмы расчёта, а база ошибок операций с плавающей точкой. Из-за этого результаты моделирования в системах MatLab, MultiSim и других при запуске в среде эмуляции Wine могут сильно отличаться от результатов как эксперимента, так и запуска на родных ОС.

НЕ ВСЁ ТАК ПЛОХО...

РОССИЙСКИЕ АНТИФРОД-СИСТЕМЫ НИ В ЧЁМ НЕ УСТУПАЮТ ЗАРУБЕЖНЫМ



Артём ПРОХОРОВ
эксперт ИБ

С учётом текущей ситуации в мире наступило непростое время для всей ИТ-индустрии в нашей стране, и вопрос импортозамещения встал как никогда остро. В условиях каждодневных изменений на политической арене многие компании, в первую очередь банки, столкнулись с тем, что на российском рынке просто нет отечественных аналогов иностранным продуктам. А сами иностранные продукты становится поддерживать небезопасно и дорого. Если и есть «что-то» похожее, то это «что-то» не дотягивает до импортного уровня по качеству, производительности, функциональности, уровню защищённости и безопасности. Не говоря уже о необходимом уровне сертификации в соответствии с требованиями НПС.

Но не всё так плохо на российском рынке, как могло показаться изначально.

Конечно, о плавном переходе банков как субъектов КИИ на отечественное оборудование и замене иностранного ПО в ближайшее время можно забыть. Нужно проработать план: каким образом, какие системы и на какие отечественные аналоги переводить в первую очередь, чтобы процесс прошёл бесшовно, не затронул деятельность по переводу денежных средств и не нарушил механизмы проверки переводов в части противодействия мошенничеству. Исторически так сложилось, что банки, внедряя ДБО отечественных разработчиков, внедряли по мере исполнения нормативных требований антифрод-системы зарубежных разработчиков, так как на рынке просто не было аналогов иностранных систем противодействия мошенничеству.

Но за последнее десятилетие отечественный рынок данных систем сильно вырос, и на нём появились решения, не уступающие, а иногда и превосходящие антифрод-системы зарубежных разработчиков. Отечественные разработчики ДБО стали предлагать свои решения в части антифрод-систем, которые хорошо интегрируются и работают друг с другом. Уже многие отечественные системы имеют необходимый уровень сертификации и соответствуют требованиям Федеральных законов и Положениям Банка России.

ПРОЙДЁМСЯ ПО ПУНКТАМ

Федеральный закон от 27 июня 2011 г. № 161-ФЗ «О национальной платёжной системе»:

1. Статья 8 пункт 5.1. Оператор по переводу денежных средств при выявлении им операции, соответствующей признакам осуществления перевода денежных средств без согласия клиента, обязан до осуществления списания денежных средств с банковского счёта клиента на срок не более двух рабочих дней приостановить исполнение распоряжения о совершении операции, соответствующей признакам осуществления перевода денежных средств без согласия клиента.

Российские антифрод-системы даже «из коробки» умеют выявлять соответствующие признаки и обрабатывать переводы денежных средств с признаками осуществления перевода денежных средств без согласия клиента и работать с фидами. Требование выполняется в полной мере.

2. Статья 9 пункт 9.1. В случаях выявления оператором по переводу денежных средств операций, соответствующих признакам осуществления перевода денежных средств без согласия клиента, оператор по переводу денежных средств приостанавливает использование клиентом электронного средства платежа и осуществляет в отношении уменьшения остатка электронных денежных средств плательщика действия, предусмотренные частями 5.1–5.3 статьи 8 настоящего Федерального закона. При получении от клиента подтверждения возобновления исполнения распоряжения, указанного в пункте 2 части 5.2 статьи 8 настоящего Федерального закона, оператор по переводу денежных средств обязан незамедлительно возобновить использование клиентом электронного средства платежа. При неполучении от клиента подтверждения возобновления исполнения распоряжения, указанного в пункте 2 части 5.2 статьи 8 настоящего Федерального закона, оператор по переводу денежных средств возобновляет использование клиентом электронного средства платежа по истечении двух рабочих дней после дня совершения им действий, предусмотренных частью 5.1 статьи 8 настоящего Федерального закона.

Многие антифрод-системы по приостановке и возобновлению операций умеют обмениваться с другими банковскими системами для возможности приостановки/возобновления операций на их стороне. Современные системы становятся кросс-канальными.

Положение Банка России от 17 апреля 2019 г. № 683-П «Об установлении обязательных для кредитных организаций требований

к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента»:

1. Пункт 4.1. Кредитные организации должны обеспечить использование для осуществления банковских операций прикладного программного обеспечения автоматизированных систем и приложений, распространяемых кредитной организацией клиентам для совершения действий в целях осуществления банковских операций, а также программного обеспечения, обрабатывающего защищаемую информацию на участках, используемых для приёма электронных сообщений, к исполнению в автоматизированных системах и приложениях с использованием информационно-телекоммуникационной сети «Интернет» (далее — сеть «Интернет»), сертифицированных в системе сертификации Федеральной службы по техническому и экспортному контролю на соответствие требованиям по безопасности информации, включая требования по анализу уязвимостей и контролю отсутствия недеklarированных возможностей, или в отношении которых проведён анализ уязвимостей по требованиям к оценочному уровню доверия (далее — ОУД) не ниже чем ОУД 4 в соответствии с требованиями национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 15408-3-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности», утверждённого приказом Федерального агентства по техническому регулированию и метрологии от 8 ноября 2013 года № 1340-ст «Об утверждении национального стандарта» (М., ФГУП «Стандартинформ», 2014).

Многие антифрод-системы уже проходят оценку разработки по оценочному уровню доверия ОУД 4, чего нельзя сказать об иностранных антифрод-системах. Отечественные разработчики регулярно проводят анализ на уязвимости новых версий систем, как того требует Положение.

2. Пункт 5.2. Кредитные организации должны обеспечивать регламентацию, реализацию, контроль (мониторинг) технологии обработки защищаемой информации, указанной в абзацах втором — четвёртом пункта 1 настоящего Положения, при совершении следующих действий (далее — технологические участки):

- ♦ идентификация, аутентификация и авторизация клиентов при совершении действий в целях осуществления банковских операций;
- ♦ формирование (подготовка), передача и приём электронных сообщений;
- ♦ удостоверение права клиентов распоряжаться денежными средствами;
- ♦ осуществление банковской операции, учёт результатов её осуществления;
- ♦ хранение электронных сообщений и информации об осуществлённых банковских операциях.

Российские антифрод-системы в полной мере научились обеспечивать контроль всех операций (транзакций) клиентов на всех этапах жизненного цикла осуществления банковских операций.

3. Пункт 5.2.2. Кредитные организации должны обеспечивать регистрацию результатов выполнения действий, связанных с осуществлением доступа к защищаемой информации, на всех технологических участках, указанных в подпункте 5.2 настоящего пункта, которая включает регистрацию действий работников, а также регистрацию действий клиентов, выполняемых с использованием автоматизированных систем, программного обеспечения.

Российские системы в полной мере обеспечивают регистрацию и проверку на всех технологических участках.

САМОЕ ВРЕМЯ ДЛЯ ПЕРЕХОДА

Помимо выполнения нормативных требований и выявления операций без согласия клиента в различных каналах, отечественные антифрод-системы могут быть многофункциональными комплексами. Умеют контролировать параметры устройств и выявлять риски на их стороне, проводить поведенческий анализ и строить профиль клиента, распознавать фото, видео, речь, решать задачи комплаенс-мониторинга, контролировать действия и операции сотрудников в офисе на рабочем месте или удалённом рабочем месте вне офиса. Умеют интегрироваться с другими банковскими системами с минимальными доработками. Примеры таких систем: Smart Fraud Detection (разработчик Fuzzy Logic Labs), Fraudwall (разработчик «Фродекс»), Fraud Prevention (разработчик Bi.Zone), Fraud-анализ (разработчик BSS) и другие.

Ещё одним безусловным плюсом отечественных систем является цена, которая в условиях санкций более адекватна в сравнении с иностранными аналогами.

Подводя итоги, можно сказать, что российские антифрод-системы хоть и похожи на иностранные (содержат в себе best practice), но ни в чём им не уступают, а порой и превосходят по функциональности, удобству, скорости работы. Адаптированы под российский рынок и законодательство. В быстро меняющихся реалиях современного времени банкам, особенно подпавшим под санкции, необходимо максимально проработать вопрос импортозамещения. Оценив и приняв риски, переходить на аналоги систем от отечественных разработчиков.

ОТ КУЛЬТУРЫ МИРОВЫХ БРЕНДОВ К ПРОВЕРЕННЫМ ОТЕЧЕСТВЕННЫМ ПЛАТФОРМАМ

АВТОМАТИЗАЦИЯ УПРАВЛЕНИЯ ПРАВАМИ ДОСТУПА
В БАНКЕ ОТ ОДНОГО ИЗ ВЕДУЩИХ РОССИЙСКИХ
РАЗРАБОТЧИКОВ IDM-СИСТЕМ

Мартовские анонсы прессы о «мировых» ИТ-брендах, выстроившихся в очередь для заявлений о своём разрыве с рынком России, переместили решение задач импортозамещения в число первоочередных мер безопасности «оцифрованных» отечественных компаний. При этом маркетплейсы и ДБО приходят и уходят, а краеугольные «камни» цифровой инфраструктуры должны быть защищены, особенно от политкапризов рыночной конъюнктуры.

В числе ИТ-систем, включаемых в обязательном порядке в экзоскелет информационной безопасности современных средних и крупных банков, — системы автоматизированного управления учётными данными (Identity Management или IDM). За рубежом для обозначения этого класса систем широко используется аббревиатура IGA (Identity Governance & Administration). Их разработка и внедрение приобрели актуальность в начале 2000-х после выявления ряда подделок отчётности крупных западных корпораций. Это оказалось возможным в том числе из-за неправомерного доступа к «чувствительной» финансовой и иной деловой информации.

ЭКСКУРС В ИСТОРИЮ

«Промсвязьбанк» (ПСБ) внедрил систему IDM, отвечающую самым современным требованиям, более 10 лет назад. Это внедрение было осуществлено на базе решения от Oracle, что на

тот момент полностью соответствовало представлениям о корпоративной ИТ-культуре организации, имеющей широкие международные связи. Ведь встречаются по одежке, а IDM Oracle — признанный лидер «магического квадранта Gartner».

Развёрнутая тогда система позволила в полной мере решить предъявленные службой ИБ и стратегией банка задачи: консолидировать в едином хранилище учётные данные сотрудников; автоматически создавать и изменять их в соответствии с должностными обязанностями и политиками безопасности во всех целевых системах на основе данных от крупных ИТ-систем. За эти годы были отработаны автоматизированный быстрый сервис согласования заявок на доступ к корпоративным системам и сервис «самообслуживания» для кастомизации выбора требуемых ресурсов сотрудником.

ЭПОХА ПЕРЕМЕН

Эксплуатация системы IDM на базе решения Oracle была практически безоблачной до того момента, когда вендор сделал своим заказчикам предложение о переходе на обновлённую платформу. Предложение, от которого, как выяснилось, нельзя было отказаться. При этом, когда необходимые ресурсы на предложенный переход были подсчитаны, выяснилось, что такой переход, по сути, подразумевал проведение нового проекта по обновлению IDM-системы с теми же стоимостными и временными характеристиками миграции, что и проект первоначального развёртывания системы IDM.

Взяв тайм-аут для принятия решения, ИТ-служба ПСБ некоторое время вела эксплуатацию «старой» системы без помощи вендора и его аккредитованного системного интегратора.

Точкой бифуркации в создавшейся ситуации стал момент, когда внутренние требования к

Маркетплейсы и ДБО приходят и уходят, а краеугольные «камни» цифровой инфраструктуры должны быть защищены, особенно от политкапризов рыночной конъюнктуры

обеспечению доступности системы IDM банка и к её функциональному масштабированию уже не позволяли рассчитывать исключительно на собственные Oracle-компетенции и ресурсы ИТ-службы банка.

Этот момент совпал также с чётко артикулированным требованием регуляторов к переходу на политику импортозамещения в критической информационной инфраструктуре банков.

Опираясь на стандартные конкурсные процедуры, банк пришёл к решению об использовании IDM-платформы от одного из ведущих отечественных разработчиков таких продуктов — для переноса на неё уже отработанной функциональности своей предыдущей системы автоматизации управления «учётками» и правами доступа с намерением последующего развития её возможностей.

К моменту победы в конкурсной процедуре ПСБ компания-разработчик уже около 5 лет присутствовала на рынке. И в число критериев, обеспечивших эту победу, входило не только её присутствие в Реестре отечественного ПО, но и ряд успешных внедрений в организациях, сопоставимых с ПСБ по размерам бизнеса и масштабам цифровизации.

ВСЁ ЧТО НУЖНО ДЛЯ УДОБНОЙ И БЕЗОПАСНОЙ РАБОТЫ

Сегодня отечественная IDM-система, внедрённая в ПСБ, позволяет работать с различными типами учётных записей (персональные, сервисные, привилегированные), а встроенный инструмент автоматического аудита обеспечивает полное устранение «бесхозных» учётных записей, оперативно контролирует соответствие текущих прав доступа с согласованным состоянием, в удобной для анализа форме предоставляет информацию о том, что было изменено, каким образом, кем и в какое время. Фиксация всех событий изменения прав позволяет получить ИТ-специалистам банка полную картину по имеющимся привилегиям пользователя на любую дату.

В IDM-системе ПСБ используется комбинированная ролевая модель доступа, где каждому пользователю присваивается базовый набор прав доступа в зависимости от должности, а все остальные права добавляются по заявке самого сотрудника. Заявка подтверждается владельцами ИТ-ресурсов, к которым запрошен дополнительный допуск. В ближайшем будущем банк планирует внедрить предусмотренный в системе механизм контроля «конфликта полномочий» (прав доступа, которые не могут находиться одновременно у одного сотрудника). Всё это

Используемая в ПСБ отечественная IDM-система сочетает в себе законченность «коробочного» решения и возможности кастомизации и развития даже силами самой организации

позволяет избегать ошибок, вызываемых человеческим фактором.

Развёрнутая сегодня в ПСБ IDM-система позволяет реализовать идеологию «моментального предоставления доступа» сотрудникам в соответствии с утверждённой ролевой моделью, сократить время обработки заявок на расширение доступа с предоставлением пользователю в реальном времени информации о текущем статусе согласования и исполнения заявки.

Использование отечественной платформы позволило в полной мере реализовать планы ИТ-службы ПСБ по сокращению затрат на выполнение операций по управлению учётными записями пользователей в информационных системах банка.

С точки зрения информационной безопасности система автоматизации управления правами доступа позволила банку не только минимизировать риски неправомерного доступа, связанные с так называемым человеческим фактором, но и упростить аудит текущих доступов пользователей.

ФУНДАМЕНТ БЕЗОПАСНОСТИ

IDM-система ПСБ имеет внутри «коробки» все необходимые интеграционные механизмы, поддерживающие популярные ОС, СУБД и браузеры, что обеспечило высокую скорость внедрения и кастомизации.

Используемая в ПСБ отечественная IDM-система сочетает в себе законченность «коробочного» решения и возможности кастомизации и развития даже силами самой организации. И этих сил требуется не так уж и много — несколько человек. При этом банк получает от разработчика регулярные обновления, включая коннекторы к ИТ-ресурсам банка, инцидентную поддержку и индивидуальное обслуживание.

Открытый исходный код внедрённой программы даёт ИТ-специалистам ПСБ возможность самостоятельно производить кастомизацию конечного решения в ходе конкретного проекта и оперативно актуализировать возможности уже работающей IDM-системы по мере появления новых потребностей.



**Алексей
ВОЙЛУКОВ**
вице-президент
Ассоциации банков
России

ТРЕНДОВ НЕМНОГО, НО ОНИ ПРИНЦИПИАЛЬНЫЕ

ЧТОБЫ СОКРАТИТЬ ОБЪЁМЫ
МОШЕННИЧЕСТВА, НУЖНО РАДИКАЛЬНО
МЕНЯТЬ ЗАКОНОДАТЕЛЬСТВО

Вице-президент Ассоциации банков России Алексей Войлуков поделился в интервью BIS Journal своей точкой зрения на актуальные вопросы информационной безопасности финансовой отрасли и обозначил ряд законодательных инициатив, принятие которых будет способствовать активизации борьбы с киберпреступностью.

— Алексей Арнольдович, 18 апреля запланировано проведение конференции «Информационная безопасность банков», организаторами которой выступают Ассоциация банков России и Медиа Группа «Авангард». Это мероприятие — новое по формату, но с хорошо известными участниками и вопросами для обсуждения. В чём вы видите актуальность и необходимость проведения такой конференции?

— Действительно, анонсирована крупнейшая конференция по информационной безопасности в финансовой сфере, и её актуальность не вызывает никаких сомнений в силу постоянного роста числа киберинцидентов, хакерских атак, случаев социальной инженерии. Кроме того, конференция — это отличная возможность рассказать о последних технологиях в области ИБ, причём речь идёт о решениях как уже хорошо известных и зарекомендовавших себя вендоров, так и о небольших организациях, стартапах.

Важно, что подобное мероприятие позволяет понять те запросы и тренды, потребности, которые на сегодняшний день есть у заказчиков финансовой сферы — банков, страховых, лизинговых, факторинговых компаний.

— Основная тема нашего интервью — информационная безопасность банков. Какие, по вашему мнению, вопросы ИБ можно назвать наиболее актуальными на сегодняшний день?

— Существует два самых актуальных вопроса. Первый — это противодействие кибермошенничеству и социальной инженерии, ущерб от которых растёт из года в год гигантскими темпами, а меры, применяемые в настоящее время,

к сожалению, не столь эффективны. Здесь возможно объединение усилий всех заинтересованных сторон, и в первую очередь необходимо изменить законодательство, потому что технические вопросы в большинстве случаев уже решены. Однако с социальной инженерией бороться исключительно техническими методами, как оказалось, недостаточно эффективно.

Второй вопрос — импортозамещение, о чём речь ведётся давно. В связи с введением санкций возникла потребность замены и выстраивания собственной инфраструктуры как по технологическим разработкам, так и по программным решениям. Написание своих собственных систем и независимость от внешних подрядчиков стали сверхактуальными.

— Главным фактором ускоренного роста рынка кибербезопасности стало изменение бизнес-процессов организаций, вызванное пандемией COVID-19. Как вы думаете, продолжится ли этот тренд в 2022 году?

— Эпидемиологическая ситуация радикально ускорила цифровизацию взаимодействия банков с потребителями, и такое взаимодействие должно быть обеспечено процедурами безопасности.

Это создало новые рынки по предложению услуг ИБ, и этот тренд будет развиваться. Тем более клиенты уже почувствовали вкус удобства дистанционного взаимодействия по очень многим параметрам.

Однако важно не только развивать технологические решения, но и принимать более жёсткие нормы и правила, потому что законодательство очень отстаёт от произошедших цифровых изменений.

— Какие законодательные инициативы вы считаете важными?

— Во-первых, дать возможность финансовым организациям блокировать средства на законном основании при подозрении совершения мошеннических операций. Необходимо, чтобы банки имели полноценные механизмы приостанавливать движение украденных сумм по счетам до судебных разбирательств. На сегодняшний день, к сожалению, таковых не существует, и мошенники этим пользуются.

У нас ведётся серьёзная дискуссия на эту тему с Банком России, и мы надеемся, что в ближайшее время этот вопрос будет решён на законодательном уровне.

Во-вторых, оптимизация взаимодействия между финансовыми учреждениями, ЦБ РФ, правоохранительными органами и судебной системой (судами) и главное — перевод этого взаимодействия на цифровую основу.

К сожалению, сейчас расследование хищений, независимо от того, что украли — сумку с деньгами или средства со счёта, происходит по одной и той же процедуре, которая сильно затянута и формализована.

Перевод на цифровое взаимодействие по электронным каналам указанных ведомств ускорит процесс возбуждения предварительных дел в правоохранительных органах, передав туда имеющуюся у банка информацию по движению денежных средств по счетам. Необходимо иметь возможность оперативно подать заявления от имени клиента в суд и получить предварительное решение на защиту его средств, для того чтобы можно было заморозить их на пути движения.

Изменение процесса взаимодействия позволит радикально перестроить систему и ускорить поиск, разбирательство и возврат денег клиенту, а также позволит привлечь мошенников к ответственности, потому что в настоящее время, с учётом длительности и сложности получения информации, это затягивается на месяцы и даже годы, и преступники остаются безнаказанными.

— Какие тренды вы могли бы выделить в сфере безопасности цифровых платежей?

— Основное — это обогащение банковских антифродовых систем той дополнительной информацией, которую можно собирать и быстро актуализировать. Здесь крайне важно выстраивание взаимодействия между антифрод-системами различных финансовых учреждений через Центральный банк и обмен информацией. Крупные банки могли бы помочь более мелким игрокам, предоставляя им необходимые данные для защиты клиентов.

— Если говорить о проблемах идентификации и аутентификации в банковском взаимодействии, что здесь вызывает вопросы в настоящее время?

— Большой вопрос со стороны государства — это создание единой биометрической системы (ЕБС), которую все банки (за исключением организаций с базовой лицензией) обязаны внедрить во всех точках своего присутствия.

Затраты на установление этой системы существуют, а вот отдачи от неё нет, она практически не функционирует из-за того, что клиенты боятся утечки или подменных данных в ЕБС. К сожалению, и законодательство недостаточно проработано в этой части, существуют сложности с поиском и доказательствами того, кто проводил операцию — клиент или мошенник.

В то же время у каждого банка есть свои системы, которые позволяют идентифицировать и аутентифицировать клиентов. Но здесь уже вопросы к надёжности подобных систем возникают у государства — насколько они гарантируют защиту от хакеров и мошеннических схем.

— Как вы думаете, будет ли расти востребованность цифровой идентификации? И соответственно, ускорится ли отказ от аутентификации на основе паролей и вопросов/ответов?

— Если говорить о цифровых ключах, то они давно применяются, хотя, конечно, в большей степени ими пользуются юрлица. Выпуск и поддержание таких цифровых ключей из года в год — достаточно дорогое удовольствие, тем более для физлиц. При этом более удобных и надёжных инструментов пока для клиентов не существует.

— Как вы оцениваете практику борьбы с социальной инженерией за последний год?

— Из года в год расширяется инструментарий борьбы с киберпреступлениями, в том числе с социальной инженерией. Но, к сожалению, все нововведения и дополнения (причём не только по финансовой системе, но и в телекоммуникационной отрасли, например, Закон о связи с подменой номеров, который вступил в силу с 1 декабря прошлого года) недостаточно эффективны, чтобы опережать существующий темп роста объёма мошенничеств с помощью социальной инженерии. Поэтому необходимо радикально изменить законодательство по двум направлениям, о чём я уже говорил выше. Первое — дать возможность кредитным организациям, если у них возникают сомнения в законности проведения операций по счетам, замораживать денежные средства и таким образом препятствовать их выводу.

Второе и самое главное — наладить цифровое взаимодействие между финансовыми учреждениями, ЦБ, правоохранительными органами и судебной системой, что позволит радикально продвинуть решение проблем.

— Насколько эффективно взаимодействие государства, банков и операторов связи по предотвращению мошенничества?

— Это сложный вопрос. Такое взаимодействие существует, потому что происходит постоянное общение между всеми его участниками. Возможно, только сотовые операторы стоят несколько в стороне, потому что у них отдельный надзорный контролирующий орган и своё законодательство.

Но если мы видим, что темпы роста киберпреступности постоянно увеличиваются, значит, необходимо менять форму взаимодействия и концентрировать общие усилия, принимая общие решения.

— Требования регуляторов по ИБ для финансовой отрасли постоянно ужесточаются. Для их исполнения требуются дополнительные ресурсы. Как вы думаете, какие пути решения этой проблемы существуют для средних и небольших банков, ресурсная база которых, возможно, не позволяет адекватно реагировать на весь спектр угроз?

— Действительно, из года в год регулятор ужесточает свои подходы к информационной безопасности финансовой сферы, и понятно, что это вызвано обеспокоенностью ЦБ РФ теми дополнительными рисками, которые возникают для клиентов в связи с переводом большой доли операций в цифровое пространство.

Однако мы считаем, что требования регулятора непропорциональны и завышены, потому что риски, возникающие у небольшого банка, не столь высоки, как у крупного, а требования едины. Небольшая кредитная организация вынуждена соблюдать их формально и тратить большие ресурсы на закупку соответствующего программного обеспечения, на содержание в штате ИБ-специалистов. Поэтому мы ведём диалог с ЦБ о том, чтобы выставляемые требования были пропорциональными и дифференцировались в зависимости от размеров банков и технологий, которые они используют. Также необходимо, чтобы все игроки рынка объединились, чтобы не нести расходы на одни и те же продукты и сервисы, а использовать их совместно.

Наша рабочая группа (в неё входят представители банков, регулятора и вендоров) выработала решение о создании общего облака, где будут находиться системы участников, что позволит

радикально снизить административные, финансовые и прочие затраты банков на обеспечение ИБ. Отдельно созданная аутсорсинговая компания будет предоставлять весь необходимый сервис.

— Тема криптовалют в последние месяцы — одна из самых популярных на разных площадках и в СМИ. Прозвучало много заявлений и точек зрения представителей министерств и ведомств. Какова ваша позиция по вопросу регулирования криптовалют в России?

— Безусловно, это дискуссионный вопрос. С учётом того, что Минфин и правительство, с одной стороны, и ЦБ, с другой стороны, разошлись в своих взглядах на проблемы регулирования криптовалюты, он остаётся открытым. При этом, исходя из общей логики и экспертных предположений об огромном объёме вложений в криптоактивы россиян, было бы лучше не запрещать их, а ввести понятное жёсткое регулирование, обложив ряд операций налогом. В последнем случае рынок становится более контролируемым и прозрачным. Кроме того, государство получит дополнительные доходы в бюджет.

— Что вы думаете о целесообразности введения цифрового рубля?

— Цифровые валюты пока что в полной мере не введены ни в одной стране мира. Поэтому очень сложно предположить, какое реальное влияние они могут оказать на финансовую систему и существующие экономические условия. К сожалению, подобных исследований, которые давали бы точный ответ, в мире тоже нет. Многие центральные банки экономически развитых стран ведут проекты по разработке своих цифровых валют, но при этом они то и дело сдвигают сроки их выпуска, пытаются лучше изучить и понять эту проблематику. Любопытно, что все в ожидании смотрят друг на друга, никто не хочет быть первым и наступить на грабли.

Я думаю, что по цифровому рублю пока что больше вопросов, нежели ответов. Например, как внедрять, зачем, для каких расчётов, для какого круга пользователей и т.д. Пока что очевидны преимущества использования цифрового рубля для государства, которое получит действенный способ отслеживания движения денежных средств. Какие преференции это может принести обычному пользователю, на данный момент сказать достаточно сложно.

Беседовала Анна Воробьёва

КАК СЪЕСТЬ СЛОНА?

А ИМЕННО СОЗДАТЬ СИСТЕМУ ЗАЩИТЫ ЗНАЧИМОГО ОБЪЕКТА КИИ, ДАВНО И УСПЕШНО ФУНКЦИОНИРУЮЩЕГО В ИНФРАСТРУКТУРЕ БАНКА, НЕ ИЗОБРЕТАЯ ВЕЛОСИПЕД

Большинство финансовых организаций, попавших под действие Федерального закона 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» от (далее — 187-ФЗ), скорее всего уже завершили этап категорирования идентифицированных в их инфраструктуре объектов критической информационной инфраструктуры (далее — КИИ) и теперь для объектов, признанных в результате категорирования значимыми, должны обеспечить наличие системы безопасности значимых объектов КИИ (далее — ЗОКИИ), в соответствии с установленными требованиями регуляторов.

ТРЕБУЮТСЯ СВИДЕТЕЛЬСТВА

В соответствии со статьёй 10 187-ФЗ основными задачами системы безопасности (далее — СБ) ЗОКИИ являются:

1) предотвращение неправомерного доступа к информации, обрабатываемой ЗОКИИ, уничтожения такой информации, её модифицирования, блокирования, копирования, предоставления и распространения, а также иных неправомерных действий в отношении такой информации;

2) недопущение воздействия на технические средства обработки информации, в результате которого может быть нарушено и (или) прекращено функционирование ЗОКИИ;

3) восстановление функционирования ЗОКИИ, обеспечиваемого в том числе за счёт создания и хранения резервных копий необходимой для этого информации;

4) непрерывное взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

Поскольку эти задачи по сути не новы, а ЗОКИИ — это объекты инфраструктуры организаций, или логические объединения таких объектов, созданные не вчера и не с нуля, в подавляющем большинстве случаев цель обеспечить фактическое наличие и функционирование СБ ЗОКИИ уже решена и требуется только

представить свидетельства достижения этой цели в объёме, форме и формате, требуемом уполномоченными регуляторами в области КИИ.

ДОКУМЕНТЫ КАК НАБОР ЗЕРКАЛ

Специфика требований по обеспечению ЗОКИИ (помимо уже предъявленных к ним требованиям по другим регуляторным направлениям обеспечения безопасности) отражена в следующих основных организационно-распорядительных и нормативно-методических документах:

1. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

2. Постановление Правительства Российской Федерации от 17.02.2018 № 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (далее — 162-ПП).

3. Приказ ФСТЭК России от 21.12.2017 № 235 «Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования» (далее — Приказ ФСТЭК № 235).

4. Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (далее — Приказ ФСТЭК № 239).

5. Приказ ФСБ России от 24.07.2018 № 367 «Об утверждении Перечня информации, предоставляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные



Екатерина РАЧКОВА
управляющий директор
Управления
по обеспечению ИБ
Банка ВТБ (ПАО)

В подавляющем большинстве случаев цель обеспечить фактическое наличие и функционирование СБ ЗОКИИ уже решена и требуется только представить свидетельства достижения этой цели

Задачу нормативного обеспечения СБ ЗОКИИ при желании можно решить разработкой и утверждением одного локального нормативного акта, описывающего, каким образом уже реализованные в инфраструктуре субъекта КИИ процессы и решения применяются в отношении ЗОКИИ

ресурсы Российской Федерации и Порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» (далее — Приказ ФСБ № 367).

6. Приказ ФСБ России от 19.06.2019 № 281 «Об утверждении Порядка, технических условий установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, за исключением средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации» (далее — Приказ ФСБ № 281).

7. Приказ ФСБ России от 19.06.2019 № 282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации» (далее — Приказ ФСБ № 282).

8. Приказ ФСБ России от 24.07.2018 № 368 «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами критической информационной инфраструктуры Российской Федерации информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения» (далее — Приказ ФСБ № 368).

МЕРОПРИЯТИЯ И ИХ СВИДЕТЕЛЬСТВА

Согласно перечисленным документам, в общем случае набор мероприятий и свидетельств их выполнения следующий:

1. Разработка Модели угроз информационной безопасности ЗОКИИ (разово, пересмотр при необходимости).

Источники требований к разработке: 127-ПП: п. 10 буллит «е», п. 11 буллит «а»; Приказ ФСТЭК России № 239 п. 11.1; Методический документ ФСТЭК России от 05.02.2021 «Методика оценки угроз безопасности».

2. Создание СБ ЗОКИИ (разово, модернизация по мере необходимости).

Источники требований: Приказ ФСТЭК России № 235 п.п. 8–9.

2.1. Задачу нормативного обеспечения СБ ЗОКИИ при желании можно решить разработкой и утверждением одного локального нормативного акта (далее — НА) об организации СБ ЗОКИИ, описывающего, каким образом уже реализованные в инфраструктуре субъекта КИИ процессы и решения применяются в отношении ЗОКИИ.

Такой документ должен содержать как минимум:

- ♦ определение СБ ЗОКИИ как совокупности организационных и технических мер, реализованных как в инфраструктуре субъекта КИИ, так и в отдельных автоматизированных системах (далее — ИС), от которых зависит функционирование ЗОКИИ;

- ♦ правила распространения действия нормативных актов субъекта КИИ, описывающих политику информационной безопасности, на ЗОКИИ;

- ♦ указание зон ответственности подразделений и порядка их взаимодействия при реализации задач обеспечения безопасности ЗОКИИ;

- ♦ описание жизненного цикла ЗОКИИ, состава и содержания документации технического и рабочего характера, возникающей в процессе жизненного цикла ЗОКИИ, а также порядка утверждения указанных документов. Например, номенклатура проектной документации ЗОКИИ, устанавливаемая данным документом, может по составу и порядку утверждения отличаться от документации других АС, внедряемых в инфраструктуру субъекта КИИ;

- ♦ описание порядка контроля состояния ЗОКИИ, включая вопросы управления инцидентами в ЗОКИИ, со ссылками на существующие регламенты.

2.2. Реализация программно-технических средств и разработка документов, определяющих политику информационной безопасности (далее — ИБ) ЗОКИИ (модернизация по мере необходимости).

У финансовых организаций уже должно всё быть, исходя из других регуляторных требований, появившихся до КИИ.

3. Назначение подразделения, ответственного за безопасности ЗОКИИ (разово).

Источники требований: П. 10 Приказа ФСТЭК России № 235.

Внесение в нормативный акт, определяющий задачи и ответственность подразделения ИБ, ответственности за безопасность ЗОКИИ в явном виде.

4. Разработка регламента повышения уровня знаний работников (разово), повышение квалификации специалистов по безопасности (на постоянной основе).

Источники требований: п.п.12, 15, 16 Приказа ФСТЭК России № 235.

Добавление вопросов, связанных с КИИ в имеющиеся курсы, памятки, инструктажи. Систематизация накапливаемых в процессе текущей деятельности свидетельств, таких как результаты прохождения курсов, сертификаты об обучении и т.д.

5. Проектирование и внедрение систем безопасности ЗОКИИ.

Источники требований: ст. 10 187-ФЗ, Приказ ФСТЭК России № 239, п. 8 Приказа ФСТЭК № 235.

Пакет технических документов, разработанный и утверждённый в соответствии с НА об организации СБ ЗОКИИ.

6. Подключение СБ ЗОКИИ к ГосСОПКА (разово).

Источники требований: ст. 9 187-ФЗ.

Свидетельства, подтверждающие установление соответствующего информационно-технического взаимодействия.

7. Разработка регламента управления инцидентами, в том числе определение участников процесса управления инцидентами, разработка плана реагирования на компьютерные инциденты (разово, актуализация при необходимости).

Источники требований: ст. 9 187-ФЗ; п. 6 Приказа ФСБ № 282.

Распространение действующего в субъекте КИИ регламента на ЗОКИИ через НА об

организации СБ ЗОКИИ (при необходимости — с какими-то доработками). В течение 90 дней с момента присвоения ФСТЭК России номера ЗОКИИ субъектом КИИ должен быть разработан план реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак. Данный план должен быть направлен в ФСБ России.

8. Доведение до НКЦКИ информации об инцидентах ИБ на ЗОКИИ (по факту возникновения инцидентов).

Источники требований: п. 5 приказа ФСБ № 367.

В банковской сфере допускается выполнение через взаимодействие с ФинЦЕРТ.

9. Разработка Плана мероприятий по обеспечению безопасности ЗОКИИ в случае нештатной ситуации (разово, актуализация при необходимости).

Источники требований: п. 13.6 Приказа ФСТЭК № 239.

Дополнение имеющихся планов обеспечения непрерывности и восстановления деятельности, распространение их на ЗОКИИ через НА об организации СБ ЗОКИИ.

10. Организация контроля за состоянием системы безопасности ЗОКИИ (регулярно). Разработка Регламента контроля системы безопасности ЗОКИИ (не реже чем 1 раз в год).

Источники требований: п. 36 Приказа ФСТЭК России № 235.

В НА об организации СБ ЗОКИИ может быть прописан особый порядок контроля или распространён уже имеющийся в субъекте КИИ общий утверждённый порядок на ЗОКИИ.

В общем случае также должна быть сформирована и наделена полномочиями комиссия из состава работников субъекта КИИ, которая будет осуществлять регулярный контроль СБ ЗОКИИ, или определён порядок и условия привлечения для выполнения указанной задачи сторонней организации. Контрольные мероприятия должны осуществляться по утверждённой программе, в результате контроля должны быть выработаны рекомендации и планы устранения выявленных недостатков.

Всё. Дальше только подготовка отчёта о выполнении Плана и разработка Плана на следующий отчётный период (п. 32 и п. 29 Приказа ФСТЭК России № 235 соответственно).



**Валерия
МЕЩЕРЯКОВА**
корреспондент
BIS Journal

ПРИОРИТЕТЫ РАССТАВЛЕНЫ

ОБ ОТКРЫТЫХ API В ФИНАНСОВОМ СЕКТОРЕ

Ассоциация ФинТех представила результаты исследования по вопросам применения открытых API на российском финансовом рынке. Почему этот документ стоит изучить? В нём содержатся предложения по возможной этапности внедрения и подходу к обязательности стандартов на российском финансовом рынке.

Результаты исследования по открытым API в России вышли в феврале и по понятным причинам остались практически незамеченными. Но тема открытого банкинга, то есть обмена данными между финансовыми организациями с помощью API, является одним из приоритетов, обозначенных Банком России. Вопрос в том, когда и в каком порядке применение API станет обязательным.

ЗАДАЧИ ИССЛЕДОВАНИЯ

В рамках исследования были поставлены следующие задачи:

- ♦ приоритизировать области применения открытых API для разработки стандартов;
- ♦ определить подход к обязательности и рекомендательности предоставления API участниками рынка;
- ♦ определить необходимые условия для внедрения стандартов открытых API с учётом как мировой практики, так и мнения участников рынка.

«Проведённое исследование позволило консолидировать мнения участников финансового рынка и потребителей финуслуг относительно развития открытых API в России и сформулировать предложения по приоритетам и подходам к их внедрению. Открытый и недискриминационный обмен данными с помощью открытых API будет способствовать развитию конкуренции на финансовом рынке, а также расширению возможностей для потребителей по выбору, приобретению и использованию финансовых продуктов и услуг», — прокомментировала генеральный директор Ассоциации ФинТех Татьяна Жаркова.

В ТРИ ЭТАПА

Согласно исследованию, предлагается на первом этапе сделать обязательными следующие API: клиентские данные по банковским

продуктам, публичная информация о продуктах банков, инициирование платежей. Второй этап включает в себя клиентские данные по отдельным категориям страховых продуктов, платёжные сервисы (повторяющиеся платежи, выставление счёта, переводы по требованию). Третий этап — публичные данные о финансовой организации (о точках продаж и обслуживания, терминалах и устройствах самообслуживания).

В РЕКОМЕНДАТЕЛЬНОМ РЕЖИМЕ

Следующие стандарты предлагается внедрять в рекомендательном режиме: идентификация и знания о клиенте (KYC проверки и скоринг), клиентские данные по прочим категориям страховых продуктов и продуктам МФО, публичная информация по страховым, инвестиционным и МФО продуктам, инициирование оформления банковских счетов, кредитных продуктов и страховых полисов.

В исследовании отмечается, что развитие открытых API в России позволит создать условия для появления инновационных сервисов и бизнес-моделей, вовлечения в финансовый рынок новых игроков, расширит возможности для развития партнёрств и кооперации, снизит издержки и риски интеграции, в том числе на кросс-отраслевом уровне.

СТАНДАРТЫ

В настоящее время разработаны и опубликованы следующие стандарты открытых API:

- ♦ Открытые банковские интерфейсы. Общие положения;
- ♦ Открытые банковские интерфейсы. Получение информации о счёте клиента третьей стороной;
- ♦ Открытые банковские интерфейсы. Инициирование перевода денежных средств клиента третьей стороной в валюте Российской Федерации;
- ♦ Безопасность финансовых (банковских) операций. Прикладные программные интерфейсы обеспечения безопасности финансовых сервисов на основе протокола OpenID;
- ♦ Открытые банковские интерфейсы. Получение публичной информации о банке и его продуктах;
- ♦ Стандарт Банка России СТО БР ФАПИ. ПАОК-1.0-2021 «Безопасность финансовых



Для целей данного исследования был проведён опрос 1000 физических лиц и 500 представителей компаний малого и среднего бизнеса в 85 регионах, глубинные интервью и открытый опрос 70 участников финансового рынка (банков, страховых и инвестиционных компаний, МФО, НПФ и финтех-игроков).

(банковских) операций. Прикладные программные интерфейсы. Обеспечение безопасности финансовых сервисов при инициации OpenID Connect клиентом потока аутентификации по отдельному каналу. Требования».

Пройти проверки на соответствие стандартам можно на сертификационном стенде, который запустила в прошлом году Ассоциация ФинТех. Первыми участниками, прошедшими проверки на стенде, стали «Точка», Промсвязьбанк и СКБ-Банк. Был проведён пилот — передача информации о счетах и транзакциях клиента — юридического лица в процессе онлайн-кредитования. На стадии подготовки следующий пилотный проект по переводам между физлицами.

ОБЛАСТИ ПРИМЕНЕНИЯ

В банковском сегменте, где наиболее остро стоит вопрос развития конкуренции на фоне усиливающегося доминирования крупнейших игроков, организация общей доверенной среды обмена данными и внедрение единых стандартов для раскрытия информации по клиентам и продуктам и проведения платежей в обязательном режиме может способствовать выравниванию рыночного ландшафта и расширению возможностей у некрупных и новых участников рынка.

В страховании и микрофинансировании единые стандарты для типовых продуктов могут подстегнуть развитие новых сервисов и бизнес-моделей, создав возможности для лёгкого встраивания страховых и финансовых услуг в платформы других участников рынка.

Для сегмента инвестиционных продуктов введение общих стандартов позволит поддержать дальнейшее развитие инновационных сервисов и бизнес-моделей, способствуя появлению новых возможностей для потребителей по управлению финансовым благосостоянием и поддержке ответственного финансового поведения.

НОВЫЕ РЕШЕНИЯ

Открытые API могут способствовать развитию широкого спектра новых решений по ряду направлений, например:

- ♦ обмен информацией о клиенте (с согласия клиента) и его учётной записи — для новых сервисов по управлению финансами в «едином окне» (PFM-сервисы), персонализации предложений и принятия кредитных решений;
- ♦ сравнение и выбор финансовых продуктов на платформах-агрегаторах и маркетплейсах;
- ♦ «встраивание» финансовых сервисов и услуг в платформы третьих сторон;
- ♦ бесшовные платежи и операции с финансовыми продуктами через платформы третьих сторон;



- ♦ идентификация и знания о клиенте «как-сервис» для финансовых организаций.

МЕЖДУНАРОДНЫЙ ОПЫТ

Международный опыт показывает, что для реализации преимуществ открытых API недостаточно только определить единые стандарты информационного обмена. Необходимо сформировать прозрачные правила для обмена данными и выстроить общую доверенную среду, которая обеспечит безопасное взаимодействие между аккредитованными участниками, с простым подключением для игроков.

ЕЩЁ ПРЕДСТОИТ

Российскому финансовому рынку на пути внедрения открытых API предстоит проделать ещё большую работу, которая будет включать: разработку и доработку стандартов с вовлечением участников рынка; организацию механизмов аккредитации и подключения участников, определение требований по проведению идентификации и управлению согласиями клиентов; создание общей инфраструктуры для безопасного взаимодействия; проработку и введение регулирования для обеспечения прозрачных «правил игры» и стимулирования участников рынка к раскрытию данных по единым стандартам.

НУЖЕН ЛИ НАМ PCI DSS?

*Мы не изучаем информационную
безопасность, а создаём её, сами пишем
эту увлекательную историю*



**Василий
ОКУЛЕССКИЙ**
эксперт BIS Journal,
кандидат
технических наук

Друзья мои, мы живём в интересное время. Не многим повезло так, как нам с вами. Мы опять стоим на пороге глобальных перемен, в том числе в нашей отрасли. Мы получили уникальный опыт борьбы в области защиты информации. Те, кто сегодня находится на реальных рубежах защиты информации, смогли оценить и сравнить, что нужно делать, и то, что мы делали «до». Мы ещё долго будем изучать этот практический опыт, но первые выводы можно уже сделать. Я хочу очень коротко, мазками, остановиться только на двух уроках, хотя их существенно больше.

УРОК ПЕРВЫЙ

Подтверждено одно из главных условий функционирования системы обеспечения защиты информации — там, где есть реально функционирующая система управления ИБ (а не система менеджмента ИБ, давайте начнём говорить по-русски), а не бумажная система, там реагирование и адаптация к новым условиям произошла максимально быстро. Но это базовые принципы. Победят не те, кто купил и установил самое дорогое и совершенное программно-аппаратное обеспечение защиты, а те, кто научился правильно организовывать защиту информационной составляющей бизнеса и его участников



на основе того, что под рукой и можно использовать немедленно! Необходимо постоянно поддерживать и совершенствовать системы управления информационной безопасности.

УРОК ВТОРОЙ

Изменение внешнего окружения и условий функционирования международных платёжных систем вновь поднимает вопрос необходимости использования американских (типа международных) стандартов PCI DSS. Эта тема неоднократно обсуждалась на самых разных площадках — с PCI Consul, с исполнительным директором восточной зоны Джереми Кингом,

на различных конференциях, форумах, в публикациях. Прорабатывались вопросы «гармонизации» PCI DSS с тогдашним Положением Банка России № 382-П, разрабатывалось специальное приложение к стандарту — «RF». Позиции аудиторов очень разные. Хотя зачастую это одни и те же люди, у них возникают очень разные требования, по-разному проводятся проверки и т.д. и т.п. Об общности и различиях этих подходов даже мне пришлось несколько раз писать. Главное, о чём необходимо помнить, применяя те или иные стандарты, зачем мы все это делаем, для чего нужна вся работа по соответствию их требованиям.

Не хочу сейчас поднимать тему технического соответствия требований БР и PCI DSS, просто напомним.

Вот это основные группы требований PCI DSS:

Построение и обслуживание защищённой сети и систем

1. Установить и обеспечить функционирование межсетевых экранов для защиты данных держателей карт.

2. Не использовать пароли и другие системные параметры, заданные производителем по умолчанию.

Защита данных держателей карт

3. Обеспечить безопасное хранение данных держателей карт.

4. Обеспечить шифрование данных держателей карт при их передаче через сети общего пользования.

Программа управления уязвимостями

5. Защищать все системы от вредоносного ПО и регулярно обновлять антивирусное ПО.

6. Разрабатывать и поддерживать безопасные системы и приложения.

Внедрение строгих мер контроля доступа

7. Ограничить доступ к данным держателей карт в соответствии со служебной необходимостью.

8. Определять и подтверждать доступ к системным компонентам.

9. Ограничить физический доступ к данным держателей карт.

Регулярный мониторинг и тестирование сети

10. Контролировать и отслеживать любой доступ к сетевым ресурсам и данным держателей карт.

11. Регулярно выполнять тестирование систем и процессов обеспечения безопасности.

Поддержание политики информационной безопасности

12. Разработать и поддерживать политику информационной безопасности для всего персонала организации.

А вот это «палеты кирпичиков» в форме стандарта ГОСТ-Р 57580.1–2017 и правил оценки правильности «сбора этих кирпичей» ГОСТ-Р 57580.2–2018. Очень кратко это выглядит так: группы процессов объединены направлениями, внутри каждого из которых сгруппированы наборы организационных и технических мер:

1. Обеспечение защиты информации при управлении доступом
2. Обеспечение защиты вычислительных сетей
3. Контроль целостности и защищённости информационной инфраструктуры
4. Антивирусная защита
5. Предотвращение утечек информации, защита машинных носителей информации (МНИ)
6. Управление инцидентами защиты информации
7. Защита среды виртуализации
8. Защита информации при осуществлении удалённого логического доступа с использованием мобильных (переносных) устройств

С учётом новых Положений БР № 672-П, 683-П и 719-П области применения требований практически сравнялись с PCI DSS и где-то значительно их превосходят. Спорным (возможно) остаётся раздел требований к процессу непосредственного выпуска самих платёжных карт. При этом отсылки Положений непосредственно к требованиям одного и того же стандарта (57580.1–2) серьёзно облегчают практическую работу по построению, использованию и последующей оценке системы защиты. Совершенно очевидно, что на основе выполнения требований БР можно построить систему, также одновременно соответствующую требованиям PCI DSS. Оставшаяся нерешённой задача аккредитации аудиторских компаний, подготовки и регулярной аттестации аудиторов — это работа нашего ближайшего будущего.

ДРУГАЯ СТОРОНА

Хотел бы затронуть совершенно другую сторону этого урока.

Мы живём в России. Основным законом, регулирующий нашу деятельность в платёжной системе, — Федеральный закон «О национальной платёжной системе» № 161-ФЗ гласит:

Статья 27. Обеспечение защиты информации в платёжной системе

3. Операторы по переводу денежных средств, банковские платёжные агенты (субагенты), операторы платёжных систем, операторы услуг платёжной инфраструктуры обязаны обеспечивать защиту информации при

осуществлении переводов денежных средств в соответствии с требованиями, установленными Банком России, согласованными с федеральными органами исполнительной власти, предусмотренными частью 2 настоящей статьи.

Статья 32. Осуществление надзора в национальной платёжной системе

2. Банк России определяет формы и сроки предоставления отчётности, в том числе в виде отчётности поднадзорной организации и сводной отчётности по платёжной системе, методику составления указанной отчётности.

В рамках выполнения требований ФЗ Банком России регулярно разрабатываются и совершенствуются соответствующие положения и указания. Некоторые из них я уже упоминал (№ 672-П, 683-П и 719-П). Самое интересное состоит в том, что в них ни слова упоминания о стандартах международных платёжных систем (МПС). То есть с точки зрения Главного регулятора мы, выполняя только его требования, можем обеспечить необходимый уровень защиты! Тогда зачем нам в нашей стране чужой стандарт?

И ещё. По декларации разработчиков Стандарт безопасности данных индустрии платёжных карт (PCI DSS) разработан в целях повышения уровня безопасности данных владельцев платёжных карт и содействия процессу повсеместного внедрения единообразных мер по защите данных держателей карт. В основе стандарта PCI DSS лежат фундаментальные технические и операционные требования, которые разработаны для защиты данных держателей карт. Благородная цель. Но для того чтобы нам поверили, мы должны самые чувствительные данные об организации безопасности нашей платёжной инфраструктуры, наших «слабых» местах и уязвимостях передавать доверенным (с точки зрения PCI Consul) организациям и людям. Напомню, что практически все банки являются объектами критической информационной инфраструктуры, а PCI Consul — это организация, подконтрольная правительству одной из самых недружественных стран, и выполняет все его указания. Из этой конструкции следует вывод:

Выполняя требования стандарта PCI DSS и ежегодной оценки соответствия этим требованиям, мы передаём чувствительные данные о характеристиках и уровне защищённости объектов критической информационной инфраструктуры компетентным органам враждебного государства.

МПС ушли. Зачем нам PCI DSS?

НЕКОТОРЫЕ МИФЫ О PCI DSS

СТОИТ ЛИ ИМИ РУКОВОДСТВОВАТЬСЯ?

В последние недели стало модно обсуждать, «кто уходит, а кто остаётся в России», а также «что нам стоит оставить, а от чего избавиться». В связи с этим появляется много мифов. Не обошли эти мифы стороной и стандарт безопасности данных индустрии платёжных карт PCI DSS. Я решил развеять некоторые из них.

МИФ: PCI DSS — ЭТО СТАНДАРТ

Да, PCI DSS — это стандарт. При этом стоит учитывать, что это один из элементов целой экосистемы безопасности карточной индустрии. В экосистему входит 12 стандартов: PCI DSS, PA-DSS, SSS, SSLCS, P2PE, PTS, Card Production, 3DS CSS, CPoC, PIN Security, SPOC и PCI TSP Security Requirements. Кроме стандартов, в экосистему входят ещё и международный и национальные регуляторы, аудиторы, процедуры контроля качества аудитов, база знаний на основе многолетнего опыта обеспечения безопасности карточной индустрии, а также учебные курсы.

МИФ: PCI DSS БОЛЬШЕ НЕ НУЖЕН, ПОСКОЛЬКУ VISA И MASTERCARD УШЛИ ИЗ РОССИИ

Нет. Платёжная система «Мир» продолжает работать и нуждается в эффективной защите всех своих участников. Защита должна быть целенаправленной, должна учитывать всю специфику именно карточных платёжных технологий. Кроме того, карты ушедших платёжных систем, выпущенные российскими банками, продолжают использоваться населением. Транзакции по этим картам внутри России обрабатывает АО НСПК — оператор платёжной системы «Мир». Риски утечки данных этих карт и последующего хищения денежных средств населения в ближайшее время возрастут по нескольким причинам. Во-первых, пользователи чаще будут вводить в Интернете данные карт в открытом виде из-за отключения функций Apple Pay и Google Pay. Во-вторых, срок действия таких карт многие банки объявили теперь неограниченным, а значит, некоторые скомпрометированные карты потенциально будут дольше оставаться

незаблокированными. По этим и другим причинам АО НСПК продолжает требовать от своих участников соответствия PCI DSS и прохождения QSA-аудитов. По моей информации, оператор платёжной системы «Мир» не планирует отказываться от этих требований. Кроме того, российские банки сейчас активно развивают сотрудничество с платёжной системой UnionPay, которая также применяет стандарт PCI DSS в качестве набора требований по защите карточных данных.

МИФ: PCI DSS МОЖНО ПРЯМО СЕЙЧАС ЗАМЕНИТЬ АНАЛОГОМ В РОССИИ

Заменить, конечно, можно всё. Но для этого нужно создать аналог, столь же эффективный в деле защиты индустрии и населения. На данный момент замена не готова. Российского стандарта, учитывающего всю специфику и технологии безопасности карточной индустрии, нет, а задача по его созданию пока, насколько мне известно, не ставилась. Да и все предыдущие обсуждения идей создания такой альтернативы приводили участников дискуссии к выводу, что это будет попытка «изобрести велосипед». Также, как уже сказано выше, PCI DSS — это далеко не только стандарт, но и система сертификации, мотивирующая участников индустрии выполнять требования по защите платёжных карт.

МИФ: ГОСТ Р 57580 УЖЕ СЕЙЧАС ПОЛНОСТЬЮ МОЖЕТ ЗАМЕНИТЬ СОБОЙ PCI DSS

Не может. И не имеет такой цели. По крайней мере, в сегодняшней своей редакции. ГОСТ Р 57580 — это обширный стандарт защиты информации финансовых организаций в целом.



Евгений БЕЗГОДОВ
исполнительный директор компании Deiteriy, CISA, CISM, PCI QSA, PCI QRA

Российского стандарта, учитывающего всю специфику и технологии безопасности карточной индустрии, нет, а задача по его созданию пока, насколько мне известно, не ставилась

A PCI DSS — это локальная инструкция о том, как защитить очень специфичный набор данных: номера карт, проверочные коды, ПИН-коды и ещё несколько столь же конкретных параметров, утечка которых всегда приводит к прямым финансовым потерям населения. Маршрут движения этих данных весьма ограничен, операции, выполняемые с ними, — тоже, технологии во многих компаниях плюс-минус похожие, протокол передачи описан в стандарте ISO 8583 и не особо варьируется от системы к системе. Отсюда и весьма конкретные методики защиты этих данных: принципы сегментации сети, запрет на хранение некоторых видов данных, требования к физической безопасности POS-терминалов и так далее. Если проводить аналогию, то ГОСТ Р 57580 можно сравнить с Федеральным законом, а PCI DSS — с подзаконным нормативным актом, например приказом органа исполнительной власти. В том смысле, что ГОСТ Р 57580 устанавливает общие требования к рассматриваемой области, а PCI DSS даёт инструкцию о том, как эти требования выполнить в отношении конкретной технологии. Разумеется, эта аналогия сильно ограничена, но, надеюсь, хорошо иллюстрирует мысль о том, что частное нельзя заменить общим.

МИФ: ГОСТ Р 57580 ПРЕДОСТАВЛЯЕТ ТАКУЮ ЖЕ СТЕПЕНЬ ЗАЩИТЫ, КАК И PCI DSS

Это нельзя сравнивать, поскольку подход к оценке соответствия этим двум стандартам принципиально разный. В PCI DSS подход бинарный: либо ты соответствуешь на 100 % всем применимым требованиям, и тогда ты молодец, либо ты хоть какое-то актуальное для тебя требование не выполнил, и ты не соответствуешь стандарту. При этом для ГОСТ Р 57580 существует понятие «уровень соответствия», который измеряется от нулевого до пятого. На практике большинство организаций выделяют отдельный контур для PCI DSS, поскольку не готовы соблюдать столь же строгие правила

информационной безопасности для всего контура ГОСТ Р 57580, который обычно в разы шире, чем карточный процессинг, по количеству приложений, баз данных, серверов, сетевого оборудования и людей.

МИФ: В ГОСТ Р 57580 ЕСТЬ ВСЕ ТЕ ЖЕ САМЫЕ ТРЕБОВАНИЯ, ЧТО И В PCI DSS

Нет, далеко не все. Разумеется, основные подходы к обеспечению информационной безопасности во всём мире сильно похожи. Если сравнивать стандарты с этой точки зрения, то между ними мало различий. Но вся суть в конкретике, в методах защиты именно карточных данных. Вот некоторые примеры требований, которые в силу специфики есть в PCI DSS, но отсутствуют в ГОСТ 57580:

- ♦ разделение сети на среду хранения карточных данных и на DMZ;
- ♦ запрет хранения критичных аутентификационных данных после авторизации транзакции;
- ♦ запрет хранения карточных данных в открытом виде;
- ♦ минимизация мест хранения карточных данных;
- ♦ запрет хранения маски и хеша номера карты вместе;
- ♦ множество требований к процессу управления криптографическими ключами, используемыми для шифрования карточных данных;
- ♦ требование о маскировании номеров карт при отображении;
- ♦ запрет использования пользовательских технологий передачи сообщений для передачи карточных данных;
- ♦ требования о контроле соответствия поставщиков услуг и о распределении ответственности за выполнение требований PCI DSS;
- ♦ детальные требования к процессу безопасной разработки программного обеспечения;
- ♦ более строгие требования к процессу управления изменениями, детализирующие участников и этапы внесения изменений в компоненты информационной инфраструктуры, чем раздел ЖЦ в ГОСТ Р 57580;
- ♦ требование о документированном описании инфраструктуры и бизнес-процессов в виде схем и диаграмм, документировании и обосновании всех правил межсетевого экрана;
- ♦ детализация состава стандартов конфигурации компонентов информационной инфраструктуры;
- ♦ запрет совмещения нескольких функций, различных по уровню безопасности, на одном сервере;

PCI DSS — это локальная инструкция о том, как защитить очень специфичный набор данных: номера карт, проверочные коды, ПИН-коды и ещё несколько параметров, утечка которых всегда приводит к прямым финансовым потерям населения

- ◆ требование об отключении всех неиспользуемых служб, протоколов и функций;
- ◆ требование об обязательной смене выданного пароля после первого входа;
- ◆ требования о контроле доступа в помещения с сетевыми розетками;
- ◆ требование о визуально отличимых бейджах для работников и посетителей;
- ◆ требование о проверке устройств, считывающих карты, на наличие скиммеров и прочих несанкционированно установленных устройств;
- ◆ требование о проверке на наличие неавторизованных точек доступа Wi-Fi;
- ◆ детализация состава информации, входящей в журналы протоколирования событий;
- ◆ обязательный ежедневный мониторинг событий;
- ◆ внешнее ASV-сканирование уязвимостей;
- ◆ детализация требований к методологии тестирования на проникновение, обязательное проведение как внешнего, так и внутреннего пентеста, а также пентеста сегментации;
- ◆ требование о кадровых проверках;
- ◆ детализация требований к планам реагирования на инциденты;
- ◆ ежеквартальные внутренние аудиты выполнения регулярных процедур.

МИФ: ПРИМЕНЯЯ В РОССИИ СТАНДАРТ PCI DSS, МЫ СЛИВАЕМ ЗА РУБЕЖ СВЕДЕНИЯ О ЗАЩИЩЁННОСТИ НАШЕЙ КРИТИЧНОЙ ИНФРАСТРУКТУРЫ

Не сливаем. Процедура оценки соответствия PCI DSS не предполагает отправки отчётных документов в Совет PCI SSC. Более того, она не предполагает даже информирования Совета PCI SSC о факте проведённой оценки. Есть, правда, процедура контроля качества работы аудиторов. В рамках этой процедуры Совет PCI SSC может запросить у QSA-аудитора отчётные документы по некоторым попавшим в выборку аудитам. И вот эта тема, с учётом новой мировой ситуации, возможно, требует дополнительного обсуждения и принятия каких-то решений. Следует отметить, что процедура проверки качества очень редкая. Большинство российских QSA-компаний проходили такую проверку всего один раз за всю историю существования. Думаю, если проверка случится, то вопрос непредоставления конфиденциальных отчётов по отдельным российским компаниям можно будет легко решить, поскольку Совет PCI SSC всегда ставит локальное законодательство выше стандарта.

Кроме Совета PCI SSC, есть также международные и национальные платёжные системы. И вот в платёжную систему VISA до сих пор

Использование двигателей внутреннего сгорания не делает наши автомобили уязвимыми или зависимыми от зарубежных структур лишь потому, что западные автомобили тоже оснащены такими же двигателями

аудиторы отправляли детальные отчёты по некоторым российским компаниям. Это делалось не просто с согласия, а по просьбе самих этих компаний. Теперь же, с уходом VISA, эта проблема решится сама собой: если компания не работает с платёжной системой, то и отправлять в эту платёжную систему её отчётные документы не требуется и не имеет никакого смысла. Отчёты по российским компаниям будут отправляться только в НСПК.

Заменить PCI DSS российским аналогом, конечно, можно, но в этом нет никакого смысла. Не зря эта тема прорабатывалась с 2014 года, и после детального анализа было принято решение для российской НСПК наследовать международный опыт в деле защиты платёжных карт. Это ни в коей мере не делает нашу платёжную инфраструктуру зависимой или уязвимой, поскольку стандарт — это инструмент. Использование двигателей внутреннего сгорания не делает наши автомобили уязвимыми или зависимыми от зарубежных структур лишь потому, что западные автомобили тоже оснащены такими же двигателями. Создание собственного аналога стандарта PCI DSS сразу поставит перед отраслью несколько сложных и трудоёмких задач: нужно создать и развить такой аналог, нужно создать систему сертификации, нужно приучить целую отрасль к новому стандарту. На это уйдут годы, а польза от такого решения будет весьма сомнительной. Попытки «на хайпе» протащить замену эффективно-го механизма защиты российской карточной индустрии чем-то новым, или тем, что создавалось совсем с другими целями, лишь подвергнут участников индустрии и всё население нашей страны существенным информационным и финансовым рискам. Аналог, если он будет создаваться, как вариант, может стать развитием ГОСТ Р 57580, неким подчинённым ему документом. Но ГОСТ в сегодняшнем его виде не является таким аналогом и не пытается им быть.



Александр КРУПЧИК
директор
по развитию бизнеса
АО «ДиалогНаука»

О НЕОБХОДИМОСТИ PCI DSS

Сейчас, когда международная общественность ополчилась против российских банков, а ряд международных платёжных систем приостанавливают работу карт, выпущенных в России, встал важный вопрос о необходимости соответствия требованиям стандарта PCI DSS. Не достаточно ли просто соблюдения требований БР, которые предъявляются ко всем банковским информационным системам? В чём преимущества PCI DSS, чтобы российским банкам нужно было соблюдать его требования? Можно назвать целых три причины в пользу соблюдения требований PCI DSS, и в данной статье мы постараемся разобраться с ними.

ТРИ СЛОВА В ЗАЩИТУ PCI DSS

Первое: разные цели. Если сравнить требования БР и PCI DSS, то можно заметить, что цели у них разные. Требования БР направлены на обеспечение стабильного функционирования банковской системы России, а PCI DSS — разработан МПС для защиты конкретно от мошенничества с платёжными картами в организациях различных отраслей. Поэтому и подходы у этих стандартов разные. Требования БР направлены на построение риск-ориентированной защиты банковской системы страны от широкого спектра атак на информационные системы, в то время как требования PCI DSS основаны на оценке рисков, специфичных для индустрии платёжных карт, в том числе с учётом расследования реальных инцидентов.

В своё время МПС столкнулись со всё более увеличивающимися объёмами мошеннических транзакций, которые переросли в целую криминальную индустрию с оборотами в миллиарды долларов в год. PCI DSS возник для решения задач, связанных со снижением ущерба от мошенничества. Требования БР — это результат в большей части теоретической работы по систематизации защитных мер.

То, что требования по безопасности БР и PCI Council становятся более похожими друг на друга, является следствием того, что платёжные технологии с использованием платёжных карт и страновые финансовые системы имеют похожие карты рисков. Кроме того, имеет место повышение уровня зрелости отрасли информационной безопасности в целом, что предполагает более стандартизованные подходы в построении защиты информационных систем. Различные разрозненные «лучшие практики» трансформировались в систематизированные и достаточно стандартизованные архитектуры, структуры, технологии и процессы безопасности.

Второе: теория и практика. Требования БР — законодательные, а PCI DSS — практический стандарт. Банк России разработал свои требования в том виде, в котором ему было удобно, и сейчас они являются неотъемлемой частью законодательного регулирования. В то же время PCI DSS разработан «снизу» — он стал результатом договорённости нескольких платёжных систем по реализации ими мер защиты от мошенничества.

МПС работали в большом количестве стран мира, в том числе в странах, в которых государства никак не регулировали мероприятия по части информационной безопасности либо не уделяли внимания регулированию в области безопасности платёжных карт. Всё большее количество инцидентов и их масштабы начали подрывать доверие к использованию платёжных карт как средства платежа в целом. Каждая платёжная система начала разрабатывать различные требования и подходы к обеспечению безопасности данных платёжных карт. Требования разрабатывались в основном реактивно по результатам расследования различных инцидентов. Вначале требования не носили системного характера и отличались у каждой МПС. Проверку соответствия этим требованиям проводили сами платёжные системы. Компании, работающие с несколькими МПС, должны были проходить аудиты на соответствие у каждой из них по отдельности по разным требованиям, которые при этом могли противоречить друг другу.

Из-за этого возник запрос от участников платёжных систем на систематизацию и гармонизацию требований, а также сокращение

Требования PCI DSS основаны на оценке рисков, специфичных для индустрии платёжных карт, в том числе с учётом расследования реальных инцидентов

количества аудитов. При этом МПС столкнулись с тем, что у них не было необходимых ресурсов для проведения аудитов безопасности. Таким образом, ведущие МПС решили объединиться и создать организацию, которая бы занималась вопросами безопасности в индустрии платёжных карт в интересах МПС. Был создан PCI SSC, который и разработал PCI DSS, а также ряд других стандартов в области безопасности платёжных карт. Были разработаны процедуры аудита, а также процедуры аккредитации аудиторов и контроля качества их работы. При разработке требований PCI DSS учитываются мнения всех заинтересованных сторон, а не только МПС. Любая организация может принять участие в обсуждении новых стандартов PCI DSS или новых технологий, направленных на безопасность. Именно поэтому PCI DSS основан на международном опыте.

Третье: международные системы. Следует отметить, что международное взаимодействие платёжных систем остаётся: в России продолжает работать китайская система UnionPay. Важно при таком международном сотрудничестве обеспечить высокий уровень безопасности платёжных транзакций и защиту от мошенничества. Конечно, это можно сделать с помощью двустороннего договора, однако для защиты российской платёжной системы будет лучше, если её защита будет выполняться по единым и понятным для всех правилам. Собственно, в своё время к PCI SSC присоединились UnionPay и НСПК, которые теперь требуют соответствия стандарту PCI DSS от участников своих платёжных систем.

В России требования безопасности определяет НСПК (как оператор платёжной системы «МИР»). Аналогично упомянутым ранее МПС, НСПК не является регулятором для российских банков. Но НСПК определяет требования ИБ в рамках договорных отношений с участниками платёжной системы.

Организации, работающие с картами «МИР», могут являться и нерезидентами РФ, и в этом случае на них не могут распространяться требования российских регуляторов. Но НСПК в рамках договорных требований может требовать от них соответствия PCI DSS в рамках общепринятых подходов и механизмов, имеющихся в индустрии платёжных карт. Если НСПК откажется от PCI DSS, то нужно будет разрабатывать собственный стандарт безопасности, а это затруднит распространение «МИР» в других странах — кому захочется выполнять специфические требования по безопасности.

К тому же кризис — не навсегда. Остальные МПС, возможно, вернутся в той или иной мере.

Если НСПК откажется от PCI DSS, то нужно будет разрабатывать собственный стандарт безопасности, а это затруднит распространение «МИР» в других странах — кому захочется выполнять специфические требования по безопасности

С НАДЕЖДОЙ НА БУДУЩЕЕ

Если подытожить всё вышесказанное, то можно сделать вывод, что требования стандарта PCI DSS необходимо соблюдать — этого требуют НСПК и UnionPay. Если же говорить о подходах к аккредитации аудиторов по стандарту PCI DSS, то здесь возможны следующие варианты.

- ◆ БР создаёт свою систему аккредитации аудиторов, которые проводят аудиты на соответствие требованиям БР. Они должны полностью перекрывать требования PCI DSS. Отчёты отправляются в БР или уполномоченную им организацию. Минусом является то, что необходимо договориться со всеми МПС, что результаты таких аудитов будут ими признаваться. Этот минус можно устранить на законодательном уровне, издав закон, который обязует МПС, работающие на территории РФ, признавать результаты таких аудитов.

- ◆ БР признаёт аккредитацию аудиторов, которую осуществляет PCI SSC. При этом аудиторы проводят аудиты на соответствие требованиям БР, которые полностью перекрывают требования PCI DSS. Банк проходит один аудит, в рамках которого проверяется соответствие сразу всем стандартам, по результатам аудита составляется отчёт для БР, а также АОС и ROC, направляемые в МПС. Основным минусом является то, что чувствительные данные об организации безопасности нашей платёжной инфраструктуры передаются в МПС враждебных государств (в основном Visa). Этот минус можно устранить распоряжением БР, в котором нужно указать, что за границу могут передаваться только отчёты о результатах аудита, которые содержат деперсонализированные данные, с указанием того, какие данные и каким образом должны быть деперсонализированы и как аудитор должен хранить у себя записи, на основании которых в случае необходимости можно будет сопоставить деперсонализированные и реальные данные, собранные во время аудита. В таком случае реальные данные останутся у аудитора и могут передаваться в сторонние организации только в рамках расследования крупных инцидентов.

ТАК НУЖЕН ИЛИ НЕТ?



Евгений БАБИЦКИЙ
заместитель
генерального
директора, QSA,
ООО «Комплаинс
Контроль»

ИСТОРИЯ ВОПРОСА

Не будем затрагивать политические аспекты возникновения этого вопроса, просто примем как данность, что многие западные вещи (стандарты и средства ИБ здесь не исключение) на текущий момент вызывают сомнения и вопросы.

Если для средств обеспечения информационной безопасности основной вопрос сейчас и в ближайшем будущем — это вопрос доверия и возможности долгосрочного планирования, то со стандартами вопрос в другом. Если раньше успешное завершение проекта по соответствию тому или иному стандарту показывало зрелость, являлось обязательным требованием для ведения бизнеса, повышало значимость в глазах западных компаний и партнёров, то сейчас у бизнеса есть сомнения: «А нужно ли мне всё это в новой реальности?»

После ухода VISA и Mastercard с Российского рынка всё чаще стало звучать мнение, что и PCI DSS теперь не нужен, но это не так. Давайте разберёмся.

УЧАСТЬ COMPLIANCE-ПРОЕКТА

Compliance-проекты и ранее рассматривались как что-то навязанное «внешней силой». Что, в свою очередь, не всегда позволяет реализовать все наиболее интересные и полезные требования. Компании зачастую стремятся реализовать требования стандарта для галочки и с минимальными затратами.

Именно эта коллизия и вызывает самые жаркие споры и порой даже конфликты между аудитором и командой аудируемой компании.

Необходимо искать то небольшое пересечение интересов всех сторон, требований стандарта, временных и денежных затрат.

Любой стандарт безопасности, особенно который существует не первый год, чаще всего содержит наиболее эффективные механизмы для достижения заявленной цели. Например, в случае PCI DSS объектом защиты являются карточные данные. При этом стандарту важна только конфиденциальность данных. На доступность и целостность стандарт не обращает внимания. Это важно для понимания того, какие именно преимущества можно получить, реализовав требования PCI DSS.

ПЛЮСЫ И МИНУСЫ

Давайте рассмотрим, какие основные плюсы и сложности несёт в себе реализация требований стандарта PCI DSS.

Начнём с плюсов:

- ♦ PCI DSS — это сбалансированный и современный стандарт, у которого нет перекоса в «бумажную безопасность». Он содержит в себе большое количество практических требований по реализации системы защиты;

- ♦ успешная реализация требований позволяет добиться такого уровня обеспечения ИБ, который сделает вашу компанию неинтересной для большинства злоумышленников;

- ♦ часто PCI DSS выступает хорошим стартом, чтобы донести важность ИБ до бизнеса, показать им понятный и структурированный подход и план действий.

Но есть сложности и особенности, которые необходимо учитывать.

- ♦ Как я и писал выше, стандарт работает только с конфиденциальностью данных. Проблемы с доступностью и целостностью вы не решите.

- ♦ PCI DSS для успешного прохождения сертификации требует полного выполнения всех требований. И нет градации, является ли требование более важным для выполнения или менее. Это иногда ведёт к распылению ресурсов, увеличению сроков проекта и усталости команды. Другие стандарты часто требуют достижения определённой интегральной оценки выполнения, что в большинстве случаев позволяет сосредоточиться на выполнении наиболее важных пунктов в конкретной инфраструктуре.

ТАК НУЖЕН ИЛИ НЕТ?

Первоначально реализацию единого стандарта безопасности в индустрии платёжных карт реализовали пять платёжных брендов — VISA, Mastercard, American Express, Dinners club и JCB. Они до сих пор остаются основными учредителями совета PCI SSC, который следит за PCI-стандартами и развивает их.

Но в последние годы к этому консорциуму в качестве аффилированных членов присоединились и другие платёжные бренды, в том числе China UnionPay и «МИР».

В документе «Стандарт ПС «Мир». Программа безопасности» требование по соответствию стандарту PCI DSS прописано в явном виде.

Поэтому необходимость подтверждать соответствие PCI DSS для участников российского рынка остаётся в силе. И давайте не будем забывать о том, что реализация требований стандарта — это внедрение минимально необходимых (а чаще даже обязательных) механизмов и процессов защиты данных в собственной организации.

ВЕСНА ПРИШЛА, КАК ВСЕГДА, НЕОЖИДАННО

ПОЧЕМУ СЕГОДНЯ В РФ НЕТ WEBTRUST CA
И КАК ЭТОГО МОЖНО БЫЛО ИЗБЕЖАТЬ

АЗБУКА SSL-ШИФРОВАНИЯ

SSL (аббревиатура от Secure Sockets Layer) — один из способов обеспечения информационной безопасности в киберпространстве. Представляет собой протокол зашифрованной передачи данных с использованием асимметричных криптографических ключей. Закрытый (приватный, секретный) ключ владельца веб-сайта (будем говорить только о сайтах, хотя SSL-сертификат может использоваться для удостоверения подлинности практически любых данных) и открытый (публичный) ключ, который используется на стороне браузера и на который удостоверяющий центр выдаёт SSL-сертификат, позволяют, во-первых, при соединении с сайтом удостовериться, что он действительно принадлежит определённому владельцу. Во-вторых, это даёт возможность шифровать трафик в канале передачи данных — они шифруются передающей и расшифровываются доверяющей (принимающей) стороной.

Для веб-сайтов характерным признаком использования SSL-сертификатов является наименование протокола https, а не http, что обозначается в начале адреса сайта (URL).

Основополагающими понятиями криптографии являются ключ и алгоритм шифрования. Ключ и алгоритм шифрования определяют способы шифрования и расшифрования сообщения. При использовании протокола SSL для создания защищённого соединения используются три типа ключей: публичный, приватный и сеансовый.

Публичный ключ сервера используется браузером для зашифровывания сеансового ключа. Браузер использует его, когда нужно безопасно отправить сеансовый ключ серверу. Например, после того как вы ввели данные банковской карты и нажали «Оплатить». Этот ключ виден всем, браузер прикрепляет его к передаваемому зашифрованному сообщению.

Приватный ключ сервера расшифровывает зашифрованный сеансовый ключ. Его использует сервер, когда получает зашифрованный сеансовый ключ от браузера. Приватный ключ постоянно хранится в защищённой области памяти сервера и никогда не передаётся вместе с сообщением.

Сеансовый ключ служит для шифрования и расшифрования передаваемого сообщения. Веб-браузер генерирует его только на время сеанса, который пользователь проводит на сайте. Стоит пользователю закрыть сеанс, и ключ будет далее недействителен и не будет использоваться в дальнейшем.

Публичный и приватный ключи генерируются одновременно один раз при создании запроса на выпуск SSL-сертификата. Поэтому приватный ключ нужно хранить очень внимательно. Если ключ попадёт в руки другому человеку, он сможет расшифровывать сеансовый ключ и затем расшифровать передаваемое сообщение. В этом случае требуется незамедлительно уведомить удостоверяющий центр о компрометации приватного ключа, SSL-сертификат будет отозван удостоверяющим центром, а владельцу сертификата придётся обращаться за выпуском нового сертификата и переустанавливать его на сервере (рис. 1).

Шифрование с двумя разными ключами называют двухключевым, или асимметричным.

Никто из отечественных IT-компаний, в том числе производители отечественных браузеров и российские УЦ, не являются участниками CA / Browser Forum и, таким образом, не придерживаются единой политики в области доверия SSL-сертификатам



Владимир КУСТОВ
ООО «УЦ ГИС»,
доктор технических
наук, профессор



Сергей КИРЮШКИН
ООО «Газинформ-
сервис», кандидат
технических наук

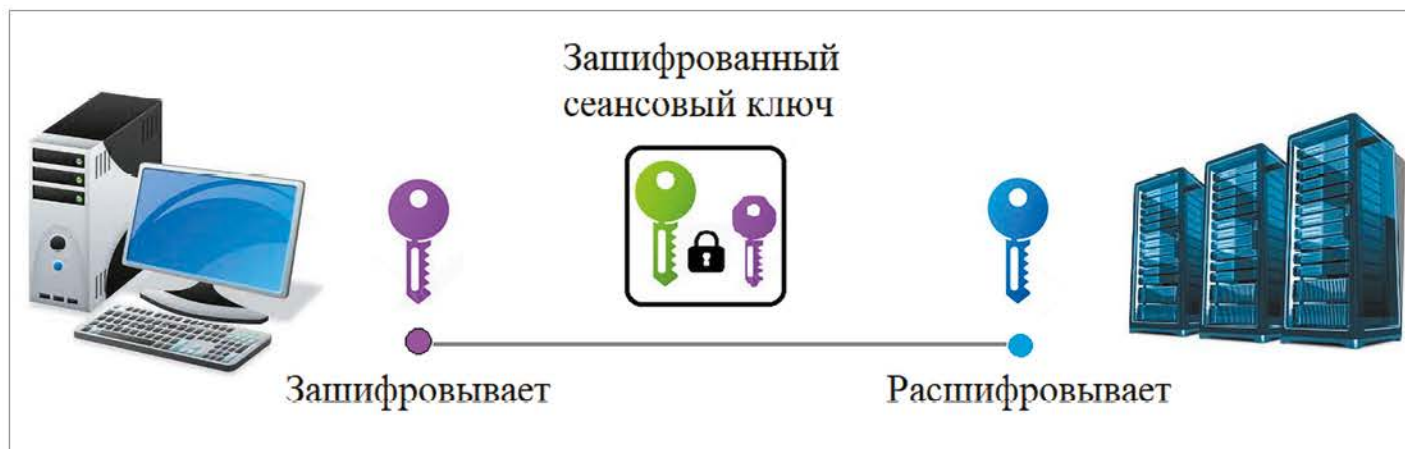


Рисунок 1. Зашифрованный сеансовый ключ



Рисунок 2. Зашифрованное сообщение

Отличительная черта асимметричного шифрования — его высокая трудоёмкость. Поэтому этот тип шифрования эффективно применяется только к коротким блокам информации, например к ключам. Поэтому браузер и сервер используют его один раз: чтобы создать и конфиденциальным образом передать сеансовый ключ (рис. 2).

Шифрование с одним ключом называют одноключевым, или симметричным. Этот метод удобен и безопасен для конфиденциальной передачи сообщений большого объёма. В целях безопасности сеансового ключа браузер делает уникальный симметричный ключ для каждого сеанса, а не хранит его на сервере для многократного использования.

КАК БРАУЗЕР И СЕРВЕР УСТАНОВЛИВАЮТ БЕЗОПАСНОЕ СОЕДИНЕНИЕ?

Браузер и сервер устанавливают SSL-соединение каждый раз, когда пользователь заходит на сайт. Это занимает несколько секунд во время загрузки сайта. Это так называемый handshake (рукопожатие).

Когда вы вводите адрес сайта в браузере, он запрашивает у сервера, установлен ли для сайта сертификат. В ответ сервер отправляет общую информацию об SSL-сертификате и публичный ключ. Браузер сверяет информацию со списком доверенных центров сертификации. Такой список есть во всех популярных браузерах.

Производители популярных браузеров (MsEdge, Safari, Opera, Chrome и др.), как правило, ведут согласованную политику определения доверия к удостоверяющим центрам, сертификатам которых доверяют эти браузеры. Известным объединением производителей популярных браузеров, операционных систем, другого ПО и доверенных удостоверяющих центров, в рамках которого вырабатывается эта единая политика, является CA/Browser Forum. Следует отметить, что никто из отечественных IT-компаний, в том числе производители отечественных браузеров («Яндекс», «Спутник», Atom) и российские удостоверяющие центры, не являются участниками CA/Browser Forum и, таким образом, не придерживаются единой политики в области доверия SSL-сертификатам. В результате отечественные издатели SSL-сертификатов в

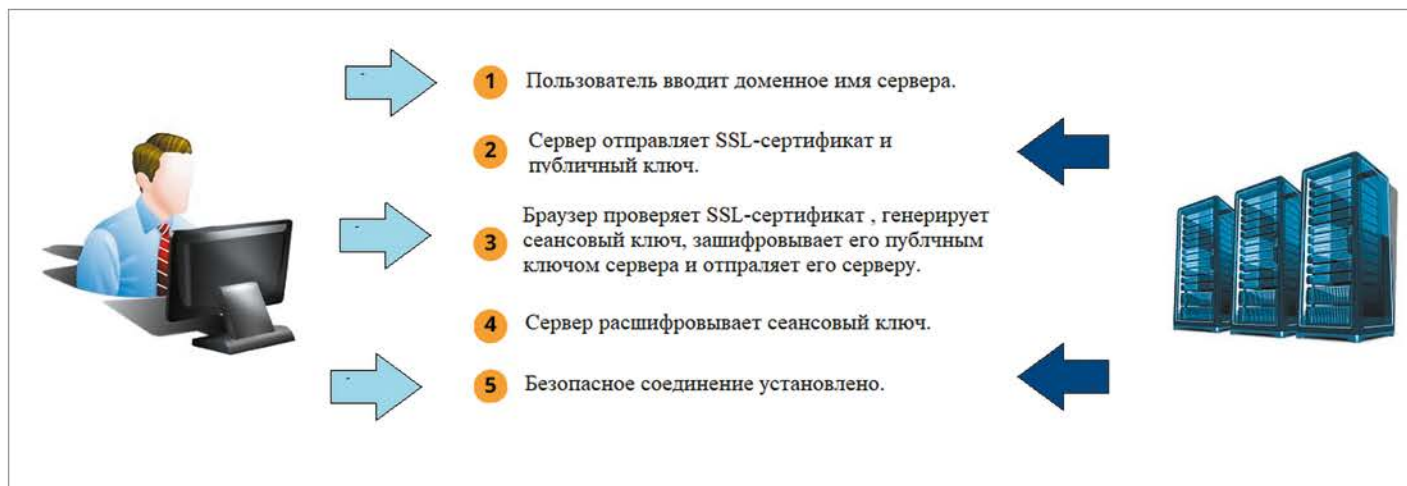


Рисунок 3. Процесс установления HTTPS-соединения

наиболее популярных браузерах отсутствуют, а в отечественных браузерах отечественные издатели могут появиться не в результате выполнения общепринятых требований, а на основе собственных российских подходов к доверию издателям SSL-сертификатов.

Если SSL-сертификат является доверенным для браузера, браузер генерирует сеансовый ключ, зашифровывает его публичным ключом веб-сайта и отправляет на сервер. Сервер расшифровывает сообщение и сохраняет сеансовый ключ. После этого между браузером и сайтом устанавливается безопасное соединение через протокол HTTPS.

Процесс можно сравнить со звонком в домофон. Когда вы слышите звонок, спрашиваете, кто пришёл. Скорее всего, вы не откроете дверь, пока не убедитесь, что это ваш знакомый. У SSL-сертификата похожий принцип работы: браузер не настроит безопасное соединение с сайтом, пока не убедится, что сертификат не поддельный.

Процесс установления HTTPS-соединения представлен на рисунке 3.

РАЗНОВИДНОСТИ SSL-СЕРТИФИКАТОВ

SSL-сертификаты выдаются удостоверяющими центрами, аккредитованными на соответствие принципам и требованиям Web Trust, и имеют следующие разновидности:

1. DV SSL-сертификат — для физических лиц.
2. OV SSL-сертификат — для среднего бизнеса.
3. EV SSL-сертификат — для крупного бизнеса.
4. Wildcard SSL-сертификат — для сайтов с большим количеством поддоменов.
5. Multi-Domain SSL-сертификат — для защиты нескольких доменов.

БЛОКИРОВАНИЕ РАНЕЕ ВЫДАННЫХ SSL- СЕРТИФИКАТОВ ГЛОБАЛЬНЫМИ УДОСТОВЕРЯЮЩИМИ ЦЕНТРАМИ

Первые попытки блокирования SSL-сертификатов на постсоветском пространстве имели место ещё в 2013 году, когда разработчики популярного тогда браузера Mozilla Firefox рассматривали вопрос блокирования нового корневого SSL-сертификата удостоверяющего центра телекоммуникационной компании TeliaSonera, одного из крупнейших поставщиков доступа к магистральным каналам связи на постсоветском пространстве. В процессе обсуждения заявки на добавление в список центров сертификации, которым доверяет Firefox, нового корневого сертификата TeliaSonera всплыли претензии, указывающие на то, что TeliaSonera продаёт технологии, позволяющие отслеживать приватные коммуникации граждан по требованиям спецслужб. Утверждалось, что подобные технологии использовались спецслужбами для анализа транзитного голосового и веб-трафика в сетях TeliaSonera в Азербайджане, Казахстане, Грузии, Узбекистане и Таджикистане.

Суть метода по перехвату зашифрованного HTTPS-трафика сводится к классической MITM-атаке (man-in-the-middle), реализованной на уровне провайдера и использующей подчинённый сертификат своего SSL-издателя для расшифровывания перехваченного SSL-трафика. Подчинённые сертификаты позволяют создать корректный и не вызывающий подозрения сертификат для любого сайта в сети, без привлечения корневого SSL-издателя, авторизованного на выполнение подобных операций. При установке SSL-соединения реальный SSL-сертификат целевого сайта подменяется сгенерированным на лету новым сертификатом, который отдаётся клиенту и не вызывает подозрения, так как данный сертификат связан

Тяжёлые последствия отзыва WebTrust SSL-сертификатов у российских сайтов, сделавшие их функциональность в значительной степени недоступной, заставили решать задачу создания отечественного SSL-корня в оперативные сроки

цепочкой доверия с реальным центром сертификации. При каждом HTTPS-сеансе пользователь изначально доверяет всем имеющимся центрам сертификации, поэтому сертификаты, сгенерированные с использованием подчинённых SSL-издателей, рассматриваются браузерами как валидные и не приводят к выводу предупреждений.

В случае если бы разработчики Mozilla приняли решение по прекращению доверия новому сертификату TeliaSonera, пользователи Firefox начали бы получать предупреждение об отсутствии доверия для HTTPS-сеансов со всеми сайтами, на которых используются SSL-сертификаты, купленные у удостоверяющего центра TeliaSonera и заверенные новым корневым сертификатом. Действия TeliaSonera нарушали принятые в Mozilla правила установки доверия сертификатам, которые запрещают выдачу сертификатов без ведома лиц, информация о которых содержится в сертификате.

Представители TeliaSonera были обеспокоены подобным ходом событий и утверждали, что имеют чистую репутацию, но, как и любой другой оператор связи, обязаны выполнять требования по санкционированному перехвату трафика, исходящие от правительств стран, где они работают. По заверению TeliaSonera, новый корневой сертификат планировалось использовать для генерации публичных SSL-сертификатов только для граждан Швеции и Финляндии, а все процессы сертификации соответствовали требованиям Mozilla и подтверждены ежегодным аудитом глобальной системы доверия удостоверяющим центрам Webtrust.

Завершая данный исторический экскурс, следует отметить, что решение о блокировании сертификата SSL-издателя TeliaSonera тогда так и не было принято.

ЧЕМ РОССИЙСКИМ ОНЛАЙН-РЕСУРСАМ ГРОЗИТ ОТЗЫВ SSL-СЕРТИФИКАТОВ?

2 марта 2022 года стало известно о досрочном отзыве SSL-сертификатов, выданных иностранными SSL-издателями для сайтов банка ВТБ и

Центробанка. Из вышеизложенного понятно, что лишение (отзыв) SSL-сертификата создаёт проблемы для сайтов, на которых осуществляется приём платежей, — банки, онлайн-магазины, сайты для бронирования билетов и пр.

Создать в России собственный глобальный удостоверяющий центр теоретически возможно, существует регламентированная процедура, которая стоит от полумиллиона долларов «на входе» и занимает от полугода времени. Вопрос о создании такого доверенного отечественного SSL-издателя поднимался в России очень давно. Но это не было сделано.

Для внутреннего употребления, т.е. в России, обеспечить SSL-сертификацию своими силами несложно, удостоверяющие центры уже есть. В соответствии с законодательством РФ для криптозащиты трафика по SSL-сертификатам, выданным в России, применяются отечественные криптографические алгоритмы. Это существенно ограничивает возможность использования таких сертификатов вместо прежних, выданных глобальными SSL-издателями. Отечественные криптографические алгоритмы без установки отечественных средств криптографической защиты информации ни Google Chrome, ни Microsoft Edge, ни Safari, ни другие западные браузеры не поддерживают. Поддержка отечественных SSL-сертификатов есть в «Яндекс.Браузере» и в поисковой системе «Спутник». Также их принимает Единый портал госуслуг (ЕПГУ).

Тяжёлые последствия отзыва WebTrust SSL-сертификатов у российских сайтов, сделавшие их функциональность в значительной степени недоступной, заставили решать задачу создания отечественного SSL-корня в оперативные сроки. Минцифры России в течение нескольких дней после указанных событий анонсировало создание отечественного SSL-издателя в рамках Государственного удостоверяющего центра и возможность получения SSL-сертификатов юридическими лицами через портал Госуслуг. Авторам данной статьи оперативно получить и протестировать такой сертификат к моменту написания статьи не удалось. Заявленный срок изготовления сертификата через ЕПГУ составляет 5 дней. Будем надеяться, что данное решение оперативно обеспечит возможность реализовать описанные выше задачи безопасности в российском сегменте сети Интернет, а в обозримом будущем позволит отечественному SSL-издателю стать настоящим глобальным доверенным удостоверяющим центром, которому будут доверять производители всего популярного ПО в мире, на всех платформах. Надеемся, что у Минцифры теперь такие планы есть.

НОВЫЙ СТАТУС: ДОВЕРЕННЫЕ ЛИЦА

ПЕРВЫЕ РЕЗУЛЬТАТЫ ОБНОВЛЁННОГО ЗАКОНА «ОБ ЭЛЕКТРОННОЙ ПОДПИСИ»

Как известно, законом 476-ФЗ от 27.12.2019 был внесён ряд значимых изменений в закон 63-ФЗ от 6.04.2011 «Об электронной подписи». В том числе существенно изменилось распределение ответственности в части выпуска квалифицированной электронной подписи (КЭП) для юридических лиц (ЮЛ) и индивидуальных предпринимателей (ИП). С 01.01.2022 выпуск квалифицированных сертификатов КЭП для лиц, действующих без доверенности от имени ЮЛ, и ИП осуществляется только уполномоченными государственными удостоверяющими центрами (УЦ), а именно УЦ ФНС России, УЦ Казначейства и УЦ Банка России. Согласно новой редакции закона помощь в выпуске квалифицированных сертификатов КЭП для ЮЛ и ИП для УЦ ФНС России могут оказывать его доверенные лица. Институт доверенных лиц УЦ ФНС России (далее Доверенные лица) был предусмотрен для расширения территории предоставления государственной услуги, а также для обеспечения возможности сохранения привычного клиентского пути для предпринимателей. В данной статье мы расскажем о первых результатах деятельности доверенных лиц УЦ ФНС и об опыте ПАО «Сбербанк» как доверенного лица УЦ ФНС России.

ПОРЯДОК ПОЛУЧЕНИЯ СТАТУСА И НОРМАТИВНОЕ РЕГУЛИРОВАНИЕ ДЕЯТЕЛЬНОСТИ ДОВЕРЕННЫХ ЛИЦ

Порядок получения статуса доверенного лица УЦ ФНС определён Постановлением Правительства РФ от 02.12.2020 № 1987 «О порядке определения доверенных лиц удостоверяющего центра федерального органа исполнительной власти, уполномоченного на осуществление государственной регистрации юридических лиц» (далее Постановление № 1987). Заключение об определении Доверенных лиц формирует Комиссия ФНС России по определению доверенных лиц. Причём согласно Постановлению № 1987 Доверенное лицо должно соответствовать требованиям к доверенным лицам, определённым

Постановлением Правительства РФ от 31 декабря 2020 г. № 2409 «О дополнительных требованиях к доверенным лицам удостоверяющего центра федерального органа исполнительной власти, уполномоченного на осуществление государственной регистрации юридических лиц» (далее Постановление № 2409), а также Приказом ФСБ России от 1 мая 2021 г. № 171 «Об утверждении организационно-технических требований в области информационной безопасности к доверенным лицам удостоверяющего центра федерального органа исполнительной власти, уполномоченного на осуществление государственной регистрации юридических лиц» (далее приказ № 171).

Постановлением № 2409 определён перечень видов организаций, которые могут быть Доверенными лицами. В частности, Доверенными лицами могут быть российские банки, организации федеральной почтовой связи, операторы подвижной радиотелефонной связи, «Ростелеком», дочерние компании корпорации «Ростех», которые имеют точки присутствия в не менее чем двух третьих всех субъектов Российской Федерации. Кроме того, возможность стать Доверенным лицом (без требования по охвату той или иной доли субъектов РФ) есть у операторов электронных торговых площадок, дочерних компаний субъекта РФ г. Москвы и Газпромбанка.

Кроме того, на Доверенные лица Постановлением № 2409 и Приказом № 171 накладываются ряд организационно-технических требований и требований по защите обрабатываемой информации и информационного взаимодействия с УЦ ФНС России. Например, согласно Постановлению № 2409 Доверенное лицо должно:

- ♦ обеспечивать круглосуточную бесплатную консультативную поддержку клиентам с помощью ряда сервисов (телефонная связь, электронная почта, сервис обмена мгновенными сообщениями);
- ♦ обеспечивать защиту каналов связи и обрабатываемой информации согласно требованиям порядка реализации функций УЦ ФНС России;



Иван ЯНСОН
бизнес-партнёр
по информационной
безопасности,
Департамент
безопасности
ПАО «Сбербанк
России»,
кандидат физико-
математических
наук

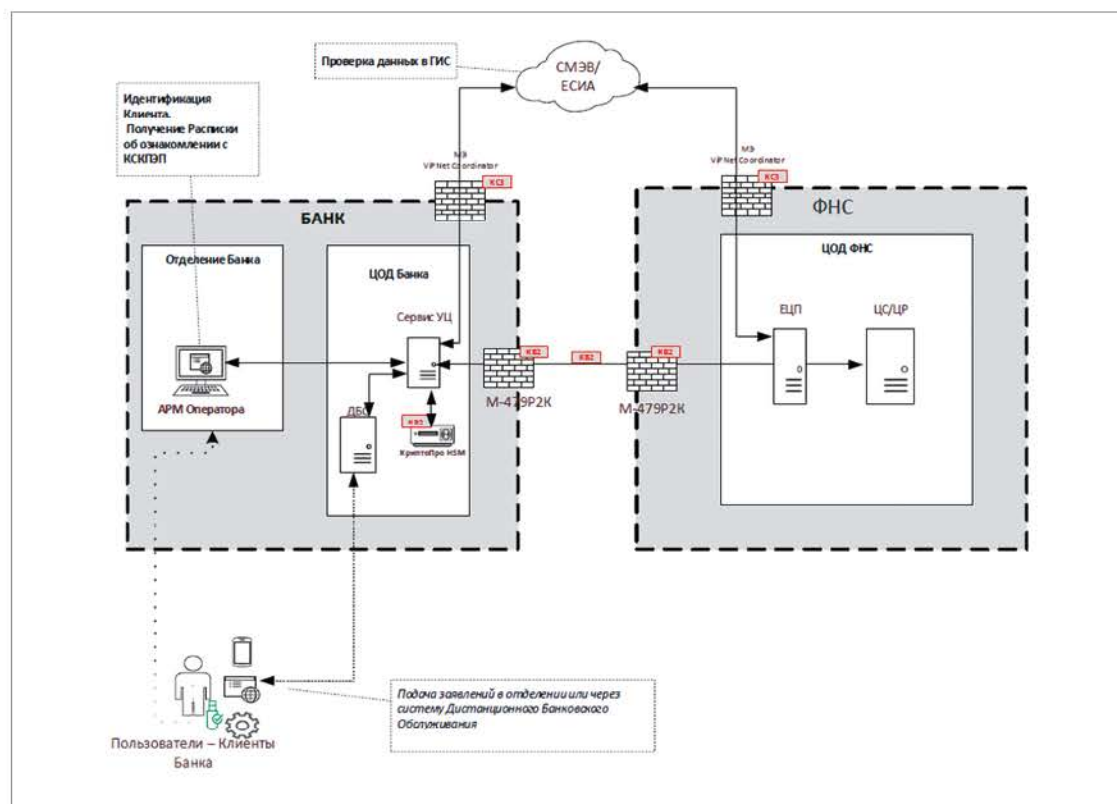


Рисунок 1. Схема Доверенного лица УЦ ФНС России на примере Банка

- ♦ реализовывать типовую схему доставки заявления на получение квалифицированного сертификата в УЦ, утверждённую ФСБ России;
- ♦ а также обеспечивать исключение возможности доступа своих сотрудников к ключам электронных подписей заявителей.

Упомянутый в Постановлении № 2409 порядок реализации функций УЦ ФНС России был утверждён приказом ФНС России от 30.12.2020 № ВД-7-24/982@ (далее Порядок реализации функций УЦ ФНС).

Также важным документом, определяющим требования к работе самого УЦ ФНС России и его Доверенных лиц, является регламент Удостоверяющего центра ФНС России (далее Регламент УЦ ФНС) утверждённый приказом ФНС России от 05.07.2021 № ЕД-7-24/636@ «О вводе в промышленную эксплуатацию Удостоверяющего центра ФНС России в целях обеспечения юридических лиц, индивидуальных предпринимателей и нотариусов квалифицированными сертификатами ключа проверки электронной подписи».

ЕДИНАЯ ЦИФРОВАЯ ПЛАТФОРМА УЦ ФНС РОССИИ И ТРЕБОВАНИЯ К ВЫПУСКУ КВАЛИФИЦИРОВАННЫХ СЕРТИФИКАТОВ

Взаимодействие информационных систем Доверенных лиц с УЦ ФНС осуществляется

через программный интерфейс Единой цифровой платформы Удостоверяющего центра Федеральной налоговой службы (далее — ЕЦП УЦ ФНС России). Данная система также предоставляет веб-интерфейс операторам УЦ ФНС России, выполняющим функции по выдаче квалифицированных сертификатов ключа проверки электронной подписи (КСКПЭП) заявителям.

Запросы на выпуск КСКПЭП заявителей при передаче в ЕЦП УЦ ФНС должны подписываться ключом ЭП Доверенного лица.

Согласно п. 8 Приказа № 171 Доверенное лицо должно создавать свои ключи ЭП с помощью средств ЭП класса не ниже КВ2, причём после создания ключей Доверенное лицо должно хранить, использовать и уничтожать свои ключи ЭП в том же средстве ЭП, в котором они были созданы. Другими словами, это означает, что Доверенное лицо должно использовать для подписания запросов, отправляемых в УЦ ФНС России, средства ЭП класса КВ2 с неизвлекаемым хранением ключей ЭП (средства типа HSM).

Что касается защиты канала связи между Доверенным лицом и ЕЦП УЦ ФНС России, то он должен быть защищён средствами криптографической защиты информации (СКЗИ) класса не ниже КВ (рис. 1).

Также согласно п. 2.6 Приказа № 171 информационная система Доверенного лица,

используемая для передачи запросов в ЕЦП УЦ ФНС России, должна быть аттестована на соответствие требованиям о защите информации, содержащейся в государственных информационных системах, утверждённым приказом ФСТЭК России от 11.02.2013 № 17.

Согласно пп. 4.1 и 5.1.1 Регламента УЦ ФНС России заявители обязаны предоставлять как в точки выдачи УЦ ФНС, так и в точки Доверенных лиц для создания ключей КЭП ключевые носители, имеющие действительный сертификат соответствия, выданный ФСБ России или ФСТЭК России. Приказ № 171 также предписывает использовать для записи ключей КЭП заявителей ключевые носители, исключающие несанкционированное копирование ключей КЭП.

Запросы на выпуск КСКПЭП согласно п. 4.3.6. Регламента УЦ ФНС России могут подаваться дистанционно через информационные системы ФНС России или Доверенных лиц. В этом случае запрос должен быть подписан квалифицированной ЭП.

Также согласно п. 5.2.7 Регламента УЦ ФНС России допускается передача в УЦ ФНС России, в том числе через Доверенное лицо, расписки об ознакомлении с информацией, включённой в квалифицированный сертификат, в форме электронного документа, подписанного квалифицированной электронной подписью.

Таким образом, при наличии у заявителя действующей квалифицированной ЭП возможен полностью дистанционный выпуск квалифицированного сертификата в УЦ ФНС России через Доверенное лицо.

Обратим внимание на одну особенность при выпуске сертификата в УЦ ФНС России. Согласно п. 3.1.10 Регламента УЦ ФНС России последний обязан отказать в создании квалифицированного сертификата КЭП, если УЦ ФНС России установлено наличие у владельца действующего квалифицированного сертификата, за исключением случаев, когда заявителем одновременно подаётся заявление на прекращение данного действующего сертификата. Другими словами, у представителя юридического лица, действующего без доверенности, и индивидуального предпринимателя может быть только одна квалифицированная ЭП. Данная мера нацелена на минимизацию мошеннического использования ЭП предпринимателей.

ДОВЕРЕННЫЕ ЛИЦА УЦ ФНС РОССИИ

В настоящее время статус доверенных лиц УЦ ФНС получили три организации:

1. ПАО «Сбербанк России», Приказ ФНС России от 04.08.2021 № ЕД-7-24/717@

2. АО «Аналитический центр», Приказ ФНС России от 04.08.2021 № ЕД-7-24/717@

3. Банк ВТБ (ПАО), Приказ ФНС России от 25.10.2021 № ЕД-7-24/929@

Информация о Доверенных лицах размещена на сайте ФНС России по ссылке https://www.nalog.gov.ru/rn77/related_activities/ucfns/

При этом деятельность по выпуску квалифицированных сертификатов электронной подписи для ЮЛ и ИП в УЦ ФНС России в пилотном режиме была начата ПАО «Сбербанк» (далее Банк) с конца 2020 года, на основании соглашения с ФНС России.

За прошедшее время Банк реализовал комплексную услугу по выпуску электронной подписи как для клиентов Банка, так и для ЮЛ и ИП, не имеющих расчётного счёта в Банке.

УСЛУГА ДЛЯ КЛИЕНТОВ В «СБЕРБИЗНЕСЕ»

Первой ещё в конце 2020 года была реализована услуга для клиентов Банка, которые используют сертифицированные токены Банка в интернет-банке «СберБизнес» (токены VPN-Key-TLS и Rutoken-TLS). Клиенты могут сформировать ключи квалифицированной электронной подписи от УЦ ФНС России непосредственно на своём USB-токене и заявку на выпуск сертификата электронной подписи с помощью сервиса «Документооборот» интернет-банка «СберБизнес». Если у клиента есть действующая КЭП, то клиент может пройти дистанционную идентификацию с помощью указанной КЭП, получить сертификат и активировать свою КЭП от УЦ ФНС полностью дистанционно. В целях безопасности Банком такая возможность ограничена: для дистанционной идентификации можно использовать только КЭП, сертификат которой выпущен либо УЦ ФНС, либо дочерним УЦ Банка для клиента Банка, который прошёл личную идентификацию в Банке согласно 115-ФЗ. Принимать другие КЭП для дистанционной идентификации Банк не готов, так как Банк, что называется, не видел таких клиентов и не может поручиться, что подпись была получена самим клиентом. Дистанционная процедура получения подписи от УЦ ФНС России через «СберБизнес» составляет не более 5 минут при условии, что предоставленные ранее клиентом в «СберБизнесе» сведения не изменились (паспортные данные, СНИЛС, ИНН).

Что касается клиентов, которые не имеют подходящих действующих КЭП, то они после отправки заявки через «СберБизнес» должны пройти личную идентификацию в любом



Рисунок 2. Примеры сертифицированных ключевых носителей (USB-токены).

отделении Банка, которое обслуживает юридических лиц и индивидуальных предпринимателей (более 2500 отделений во всех регионах страны). Идентификация обязательно должна быть пройдена лично руководителем юридического лица или индивидуальным предпринимателем, получение сертификата по доверенности запрещено. Составление заявки в «СберБизнесе» занимает около 10 минут, время посещения отделения составляет до 20 минут. Отметим, что токены Банка позволяют работать с КЭП от УЦ ФНС России с любыми сервисами и порталами, где можно пользоваться КЭП.

Далее для клиентов Банка в «СберБизнесе» была реализована возможность записи КЭП от ФНС на сторонние USB-токены. Подойдут «Рутокен Lite», «Рутокен ЭЦП 2.0», «Рутокен S», JaCarta LT, JaCarta-2 ГОСТ, ESMART Token, ESMART Token ГОСТ и другие сертифицированные USB-носители.

Так как согласно требованиям Регламента УЦ ФНС ключевой носитель должен быть в форм-факторе USB-токена/Туре-А и иметь сертификат соответствия, выданный ФСБ России или ФСТЭК России, то запись ключей КЭП от ФНС в реестр, на флеш-носители и на другие несертифицированные носители в «СберБизнесе» невозможна (рис. 2).

Возможность записи ключей КЭП от УЦ ФНС России на сторонние сертифицированные носители была реализована, так как большинство

клиентов ранее уже использовали в своей деятельности КЭП, сертификаты которых были получены в коммерческих удостоверяющих центрах, и, как следствие, у таких клиентов часто уже есть сертифицированные носители для КЭП, которые клиенты хотели бы продолжать использовать. Кроме того, некоторые клиенты явно выражали желание хранить КЭП от УЦ ФНС России и неквалифицированную ЭП для подписания платёжных документов в «СберБизнесе» на разных носителях (возможно, потому что ЭП для платежей руководители ЮЛ иногда доверяют использовать своим сотрудникам, а личную КЭП, очевидно, хотят иметь при себе).

Следующим шагом была реализована возможность выпуска КЭП ФНС для клиентов Банка, которые используют в интернет-банке «СберБизнес» СМС-способ защиты. Так как такие клиенты не применяют в «СберБизнесе» токенов Банка, для них была реализована возможность записи ключей КЭП от УЦ ФНС России на сертифицированные внешние носители из перечисленного выше перечня.

В дальнейшем клиентам для продления сертификатов КЭП от УЦ ФНС России уже не понадобится каждый раз посещать отделение Банка. Посещение отделения не потребуется, если своевременно перевыпускать сертификат через «СберБизнес» до истечения его срока действия. Срок действия сертификата от УЦ ФНС России сейчас составляет 15 месяцев.

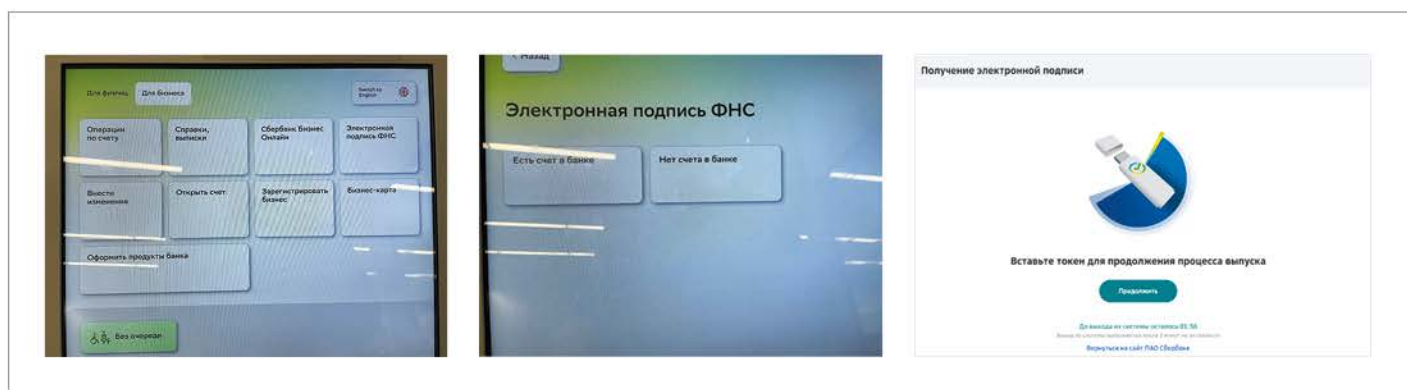


Рисунок 3. Получение талона на обслуживание у сотрудника отделения Сбербанка для получения услуги «Электронная подпись ФНС»

УСЛУГА ДЛЯ ЮРИДИЧЕСКИХ ЛИЦ И ИНДИВИДУАЛЬНЫХ ПРЕДПРИНИМАТЕЛЕЙ, НЕ ИМЕЮЩИХ РАСЧЁТНОГО СЧЁТА В БАНКЕ

Для ЮЛ и ИП, не являющихся клиентами Банка, услуга была реализована в декабре 2021 года, и на первом этапе было проведено её пилотное предоставление в отделениях Банка в городе Москве. Услуга сразу показала высокую востребованность со стороны предпринимателей, и с 1 марта 2022 года она была тиражирована в 96 городах в более чем 170 отделениях во всех регионах страны¹. Важно отметить, что руководитель ЮЛ или ИП может получить КЭП от ФНС в соответствующих отделениях, не открывая расчётного счёта. Сначала предприниматель проходит обязательную идентификацию у сотрудника отделения Банка, который заводит заявку на выпуск сертификата в автоматизированной системе Банка. Далее Доверенным лицом проводятся проверки предоставленных в заявке сведений в государственных информационных системах, после чего запрос на выпуск сертификата по защищённому каналу отправляется в УЦ ФНС России, а в ответ возвращается сертификат КЭП (рис. 3).

Так же, как с клиентами Банка, формирование ключей КЭП согласно Регламенту УЦ ФНС проводится только на сертифицированные USB-носители. При этом перечень поддерживаемых носителей является достаточно широким. После формирования ключей КЭП и запроса на выпуск сертификата руководитель ЮЛ или ИП подписывает у сотрудника Банка в отделении печатную форму выпущенного квалифицированного сертификата и правила безопасности использования электронной подписи. В целом процесс получения электронной подписи составляет около 30 минут.

Во II квартале 2022 года планируется ввод в эксплуатацию для клиентов, не имеющих расчётного счёта в Банке, сервиса по саморегистрации заявок на выпуск сертификатов КЭП от УЦ ФНС России. В данном случае руководитель ЮЛ или ИП сможет сам сразу дистанционно завести заявку на выпуск сертификата, сформировать ключи КЭП от ФНС и направить запрос на выпуск сертификата. Далее ему понадобится только прийти в отделение для идентификации и для подписания печатной формы сертификата и правил безопасности использования электронной подписи.

ИЗМЕНЕНИЕ ЛАНДШАФТА ВЫПУСКА КВАЛИФИЦИРОВАННЫХ СЕРТИФИКАТОВ КЭП

До изменения закона основная часть квалифицированных сертификатов для ЮЛ и ИП выпускалась операторами электронного документооборота (в 2021 году топ-4 оператора ЭДО выпустило 50,3% квалифицированных сертификатов). Это означало, что клиент обычно выпускал и использовал КЭП в одной и той же организации, и если у клиента возникали вопросы по использованию КЭП, то он преимущественно обращался в техподдержку той же организации, которая ему выпустила квалифицированный сертификат.

Изменение закона привело к возникновению разрыва между выпуском и использованием КЭП: выпуск осуществляется клиентами в одном месте — через УЦ ФНС и через Доверенные лица, а использование осуществляется в других местах — в системах ЭДО операторов ЭДО, для отправки отчётности в госорганы, для участия в торгах, для регистрации касс, для использования госсервисов (рис. 4).

Как следствие, изменился состав обращающихся в техническую поддержку Банка клиентов и тематики их обращений. Раньше в Банк звонили только клиенты Банка и только по вопросам использования КЭП в системе

¹ Кроме Республики Крым и г. Севастополь

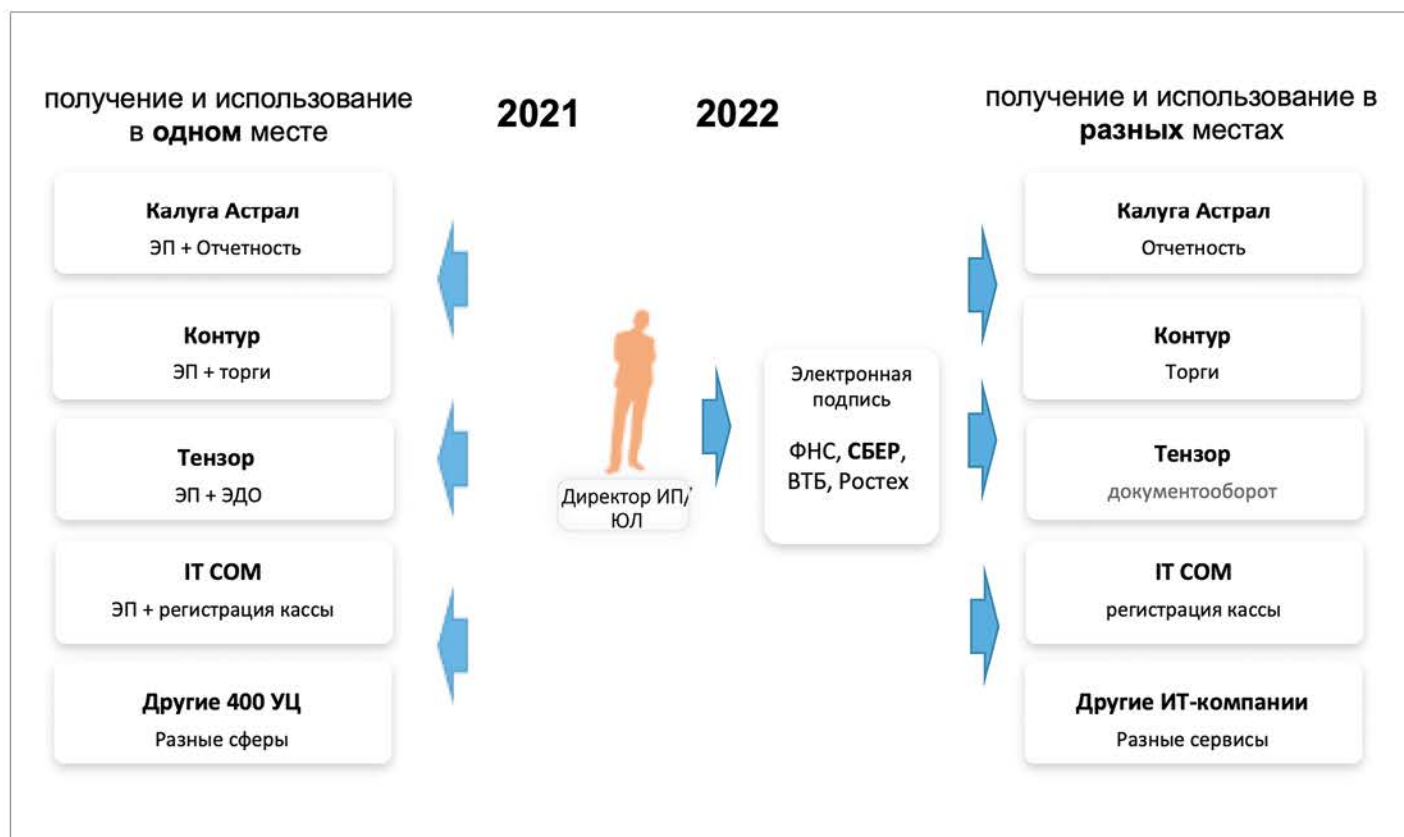


Рисунок 4. Получение и использование КЭП в 2021 и 2022 году

ЭДО Банка. Теперь же состав обращающихся следующий:

- ◆ 52% обратившихся ЮЛ и ИП — это клиенты Банка, у которых ранее была КЭП от Банка;
- ◆ 28% обращающихся — это клиенты Банка, которые ранее не имели КЭП Банка;
- ◆ 20% — это ЮЛ и ИП, которые ранее не имели расчётного счёта в Банке.

То есть видно, что добрая половина обращающихся раньше в Банк по вопросам формирования и использования КЭП не обращалась.

Изменения состава обращающихся клиентов повлекло за собой и то, что кардинально поменялся состав вопросов, с которыми обращаются клиенты. По данным февраля 2022 года топ-3 вопросов в техподдержку следующий:

- ◆ 50% — выпуск КЭП на небанковские токены;
- ◆ 14% — выпуск КЭП на токены Банка;
- ◆ 14% — работа с КЭП от УЦ ФНС России на сторонних ресурсах.

Приведённые цифры говорят о том, что более двух третей поступающих в техподдержку вопросов относятся к незнакомым Банку тематикам.

Кроме того, с начала 2022 года существенно вырос объём обращений по сравнению с 2021 годом. Число обращений в декабре 2021 года составило порядка 9 тыс. обращений,

а в январе и феврале 2022 года трёхкратно выросло и составило порядка 30 тыс. обращений ежемесячно.

Таким образом, Банку в роли Доверенного лица пришлось столкнуться как с возросшими объёмами, так и с совершенно новыми тематиками вопросов. Для разрешения указанных вызовов оперативно был проведён ряд мероприятий, в том числе:

- ◆ внесены изменения на сайте Банка — размещена информация для ЮЛ и ИП, которые не имеют счёта в Банке;
- ◆ переработаны инструкции для клиентов — добавлена информация по настройке рабочих мест для работы КЭП от УЦ ФНС России с внешними ресурсами;
- ◆ переработана база знаний службы техподдержки Банка;
- ◆ проведено обучение операторов службы техподдержки Банка по новым тематикам вопросов.

РЕЗУЛЬТАТЫ ПО ВЫПУСКУ КЭП ОТ УЦ ФНС РОССИИ И ПРЕДСТОЯЩИЕ ЗАДАЧИ

В 2021 году основная масса КЭП от УЦ ФНС России была выпущена для клиентов Банка. Услуга для ЮЛ и ИП, не имеющих расчётного счёта в Банке, была запущена только в декабре



Диаграмма 1. Статистика выпуска квалифицированных сертификатов в 2021 году.

2021 года, поэтому она не оказала сильного влияния на общую статистику.

В 2022 году услуга для неклиентов Банка была тиражирована на все регионы страны. И сейчас доля сертификатов КЭП, выданных неклиентам Банка, стала довольно заметной. На данный момент множество ЮЛ и ИП, получивших в 2022 году сертификаты КЭП от УЦ ФНС России через Доверенное лицо — «Сбербанк», — распределяется следующим образом:

- ◆ 76% — клиенты Банка, которые получили КЭП с очной идентификацией в отделении Банка;
- ◆ 7% — клиенты Банка, которые получили КЭП дистанционно;
- ◆ 17% — руководители ЮЛ и ИП, которые не имели расчётного счёта в Банке.

По нашей оценке, доля получателей КЭП, которые ранее не обслуживались в Банке, будет увеличиваться.

В целом вклад Банка в выпуск КЭП от ФНС России следующий: в 2021 году из 415 000 сертификатов КЭП, выданных УЦ ФНС России, 98 000 было выдано через Сбербанк (24%), в 2022 году по данным на конец февраля из 434 000 сертификатов, выданных УЦ ФНС, 61 850 была выпущена через сервисы Сбербанка (14%).

Но следует отметить, что пока что большая часть работы по переводу ЮЛ и ИП на КЭП от УЦ ФНС России ещё впереди. По оценкам ФНС России в стране порядка 6 миллионов ЮЛ и ИП должны получить КЭП от УЦ ФНС России. Это означает, что УЦ ФНС России и Доверенным

лицам предстоит обслужить не менее 5 миллионов предпринимателей, то есть более 80% работы ещё впереди.

Причём потребность по выпуску квалифицированных сертификатов КЭП от УЦ ФНС России будет нарастать неравномерно, впереди будут своего рода пики потребности в выпуске сертификатов КЭП. О таких пиках можно судить по статистике выпуска квалифицированных сертификатов для ЮЛ и ИП аккредитованными УЦ в 2021 году. Согласно данным ситуационного центра СМЭВ такие пики были в 2021 году в апреле, июне, октябре и в декабре. По мере истечения срока действия сертификатов КЭП, выпущенных в 2021 году, в аналогичные периоды времени можно ожидать роста потребности и в 2022 году (диаграмма 1).

В завершение статьи отметим, что Доверенное лицо «Сбербанк» готово внести достойную лепту в выполнение данной важной государственной задачи и оказать услугу по выпуску КЭП от УЦ ФНС как своим клиентам, так и предпринимателям, не имеющим расчётного счёта в Банке, быстро, просто, безопасно и с высоким уровнем сервиса. Услуга от Банка будет развиваться, клиентам будут предложены новые интересные возможности. За соответствующими новостями следите на сайте Банка в разделе «Электронная подпись от ФНС России».



Олег ХНЫКОВ
эксперт группы
по исследованию рынка ИБ
Positive Technologies

УЯЗВИМОСТИ В ФИНТЕХЕ

ОТ ПРОСТОГО СКАНИРОВАНИЯ К УПРАВЛЕНИЮ УЯЗВИМОСТЯМИ

Финтех-компании предлагают, как правило, целую экосистему продуктов и услуг: у них налажен полный цикл разработки приложений и сервисов, есть настроенная сетевая инфраструктура. Для всего нужно обеспечить высокий уровень информационной безопасности. Поэтому одним из ключевых условий киберустойчивости финтеха выступает vulnerability assessment — процесс выявления, оценки и приоритизации уязвимостей.

В 2021 году мы провели анализ защищённости банков¹, чтобы проверить, можно ли получить доступ к критически значимым для банков системам (АРМ казначейства, серверам обмена платёжными поручениями) и вывести денежные средства с корпоративных счетов. Интересно то, что во всех тестовых проектах заявленные риски удалось реализовать. Кроме того, получилось выполнить ряд действий, способных нарушить бизнес-процессы банка и повлиять на качество оказываемых услуг. В каждой организации были выявлены множественные уязвимости, позволявшие внешнему нарушителю проникнуть во внутреннюю сеть компании.

Чтобы узнать, насколько хорошо защищена финтех-организация, специалисты по ИБ исследуют ИТ-инфраструктуру и код (Infrastructure-as-Code — инфраструктура как код)

на предмет уязвимостей. Для первого подходят сканеры оборудования и программного обеспечения. К ним относятся инструменты для проверки сети и системы анализа защищённости, некоммерческие инструменты. Для второй задачи предназначены сканеры кода, которые находят в нём ошибки с помощью статического и динамического анализа, а также проверяют уже запущенное приложение в интерактивном режиме.

Давайте рассмотрим, в каких случаях классических сетевых сканеров будет недостаточно бизнесу, когда ему стоит задуматься о построении процесса vulnerability management (VM — управление уязвимостями), а также с какими сложностями сталкиваются специалисты по ИБ при организации этого процесса.

КАК СЕЙЧАС ПРОВОДЯТ АНАЛИЗ

По данным нашего опроса о процессе VM в российских компаниях², 26% специалистов по ИБ используют некоммерческие утилиты для сканирования сети. Такие инструменты подходят для проверки портов и служб на периметре, однако не дают информации о составе сети, об уязвимостях ПО, баз данных, а также не выявляют ошибки конфигураций. Коммерческими системами анализа защищённости пользуются 63% опрошенных компаний. Такие системы обычно поддерживают

сканирование в режиме белого ящика (audit) и чёрного ящика (pentest) и обеспечивают более качественную и полную проверку. В отличие от сканеров и утилит, они позволяют оценить общее состояние защищённости инфраструктуры и направлены на то, чтобы облегчить процесс устранения уязвимостей. Коммерческие системы дают возможность построить в компании полноценный процесс vulnerability management за счёт автоматизированной работы с активами и найденными уязвимостями, а также за счёт экспертизы вендоров.

Четверть респондентов, согласно тому же опросу, не используют специализированное ПО для выявления уязвимостей. Возможно, эти компании предпочитают заниматься ручной проверкой систем либо заказывают тестирование на проникновение у сторонних исполнителей. Однако такие подходы не способны полностью заменить регулярную проверку систем.

Лишь 4% респондентов указали, что используют сразу несколько систем анализа защищённости. Это позволяет выявить больше уязвимостей. В каждой системе разработчики дополняют общую базу данных собственной информацией об уязвимостях, которая регулярно обновляется на основе исследований.

КАКИЕ МОГУТ БЫТЬ СЛОЖНОСТИ

Сложность № 1. Нет регламента взаимодействия ИТ и ИБ. Ещё до внедрения системы управления уязвимостями

¹ Исследование «Кибербезопасность 2021-2022. Тренды и прогнозы»

² Исследование Positive Technologies «Как выстроен процесс управления уязвимостями в российских компаниях»



важно, чтобы ожидания от неё совпадали у обеих команд. Когда всё прозрачно и понятно, участники процесса работают продуктивней.

Между отделами ИТ и ИБ часто может возникать недопонимание. Приведём пример. Служба ИБ отправляет результаты сканирования в ИТ и требует устранить уязвимости как можно скорее. ИТ воспринимает этот отчёт как огромный список для патч-менеджмента, который требует усилий. А ведь, помимо этого, у ИТ-специалистов есть ещё и другие задачи: поддержка текущей инфраструктуры, оптимизация рутинных задач, мониторинг загрузки серверов. В то же время специалисты по ИБ не могут однозначно сказать, какие из уязвимостей наиболее опасны для бизнеса, какие нужно устранить в первую очередь. Так у ИТ может пропадать энтузиазм: бреши, обнаруженные ИБ, долго остаются незакрытыми.

Классические инфраструктурные сканеры безопасности помогают автоматизировать сбор информации с узлов и их проверку, но не решают проблему совместной работы департаментов ИБ и ИТ. Поэтому важно, чтобы в компании были заранее зафиксированы чёткие сроки устранения уязвимостей для каждой группы активов, другими словами, чтобы был выстроен патч-менеджмент.

В свою очередь, системы управления уязвимостями должны регистрировать такие договорённости и показывать отклонения. Так ИБ сможет

контролировать актуальность данных об активах и соблюдение сроков патч-менеджмента, а ИТ будет видеть фронт работ и понимать, что нужно делать. Всё становится прозрачно и понятно, количество вопросов у обеих служб друг к другу сводится к минимуму. Проблема длинных непонятных для ИТ отчётов исчезает. При таком контроле со стороны средств защиты подразделения могут договориться об оптимальных сроках патч-менеджмента, отслеживать возникающие трудности и при необходимости проводить ревизию сроков или самого процесса.

Сложность № 2. У команд нет общей задачи. Какие задачи ИТ и ИБ выполняют в тандеме? Оба подразделения служат общей важной цели бизнеса — обеспечению стабильности и защищённости инфраструктуры. При построении процесса управления уязвимостями об этом не стоит забывать. КРІ департамента ИБ завязан на то, чтобы не допустить реализации неприемлемых сценариев. У ИТ-службы свой КРІ, который зависит только от выполнения SLA по доступности инфраструктуры. Сделать компанию устойчивой к киберугрозам оба подразделения могут только сообща. При этом специфика компании отходит на второй план. Для формирования общей задачи нужно:

1) знать, какие активы есть в компании, и собирать с них максимум информации;

2) знать, насколько важен актив для бизнеса;

3) договориться о приоритетном устранении уязвимостей на важных активах.

Сделать это с помощью сканеров можно, если попытаться собрать узлы в группы, но здесь есть два момента.

♦ Статические группы быстро теряют актуальность. Их сложно администрировать на большой динамичной инфраструктуре, в которой постоянно меняется количество активов. Привязываться к статическим группам — неперспективно.

♦ Критерии для динамических групп ограничены. Большинство сканеров уязвимостей собирают крайне мало информации об активах; сложно составить группы по определённым параметрам.

В системах управления уязвимостями, как правило, уже есть необходимый набор функций, способный сформировать общую задачу для ИТ и ИБ. Решение такого класса способно собрать всю информацию об активе и классифицировать её по степени важности для бизнеса. MaxPatrol VM, например, показывает, какие конкретно уязвимости в данный момент актуальны для компании. Это возможно за счёт полного покрытия инфраструктуры сканированием, сбора и хранения информации об активе и его изменениях, а также импорта дополнительных данных о нём из сторонних источников.

Полная информация важна каждой из команд: ИТ не всегда знает актуальное состояние инфраструктуры, а ИБ это необходимо для поиска уязвимостей и запуска процесса vulnerability management на всей инфраструктуре. Если задача понятна каждому подразделению, выполнять её гораздо проще.

Сложность № 3. Нет единого интерфейса для команд. Система vulnerability management может служить единым окном для специалистов ИТ и ИБ. Для контроля зафиксированных и обеспокоенных сроков на патчинг специалисты могут настраивать дашборды системы под себя. Так ИБ будет проводить мониторинг, а ИТ — следить за соблюдением дедлайнов.

Те, кто привык работать с тикетницами, могут настроить интеграцию с системами анализа защищённости через API. Главное, чтобы заявка падала не по каждой выявленной уязвимости, а выставление приоритетности не отдавалось на откуп ИТ.

Сложность № 4. Непонятно, как приоритизировать уязвимости. Как понять, какие уязвимости самые опасные для компании? У сетевых сканеров и утилит по анализу защищённости ответа на этот вопрос нет. Максимум — такие решения проставляют оценку по метрике CVSS. Но она даёт лишь отдалённое представление об опасности. Логично, что оценка 10.0 по метрике CVSS говорит о большей опасности, чем оценка 5.5. Но не всё так просто. Опираясь только на метрику CVSS, сложно, а порой и невозможно определить минимальную оценку, при которой стоит устранять уязвимость максимально быстро. Работая только с метрикой CVSS, специалисты по ИБ могут получить вопросы от ИТ. Почему именно эта уязвимость с оценкой 9.5 самая опасная? А что делать с уязвимостями с оценкой 9.0 и 8.5? Где доказательства, что уязвимость действительно опасна? После таких вопросов ибэшник может долго думать над ответами. Такое взаимодействие непродуктивно.

Некоторые производители систем анализа защищённости прибегают к самостоятельной оценке уязвимостей. Каждая метрика имеет довольно

понятную формулу. В неё входят такие значения, как срок существования уязвимости, наличие эксплойта, упоминание в СМИ и других источниках, данные о вредоносном ПО. Часто мы видим, что все уязвимости просто пересчитываются по метрике вендора, и результат ничем не отличается от оценки по CVSS, а иногда может только всё усложнять. Например, уязвимость имеет оценку 9.5 по CVSS, а производитель назначает ей низкий уровень опасности.

В MaxPatrol VM есть понятие «трендовые уязвимости». Это уязвимости, которые используются злоумышленниками в реальных атаках на бизнес. Для ИБ они имеют высокий приоритет. Как правило, их количество невелико — не более 100. Такое ограничение даёт возможность ИТ успеть устранить их все, главное — договориться о дополнительном регламенте, чтобы такие уязвимости обрабатывались вне очереди. Разобравшись с трендовыми уязвимостями, ИТ-команда может переходить к обычному циклу патч-менеджмента, который контролируется системой и отслеживается командой ИБ.

Сложность № 5. Искать уязвимости — это долго. Задача любого сканера — сбор информации об узлах и поиск максимального количества уязвимостей. Все решения такого типа, представленные на рынке, справляются с этой задачей по-своему. Какие-то лучше, какие-то хуже.

Для поиска уязвимостей нужно проводить регулярное сканирование инфраструктуры. Запустить его можно не всегда. Нужно выбрать технологическое окно, проверить доступы к узлам, а после сканирования обработать его результаты. Если инфраструктура небольшая (до 1000 узлов), обычного сканера хватит, то есть он сможет проанализировать такой пул за один раз либо за отведённое, оптимальное для процессов компании, время. Но если компания большая, у неё несколько физических площадок и её инфраструктура динамическая, а количество активов постоянно меняется, то сканирование может занять несколько дней. При этом не стоит забывать и о пользователях сервисов кредитно-финансовых организаций. В пик высоких нагрузок никто не

разрешит проводить сканирование инфраструктурными сканерами.

Эту ситуацию классические сканеры безопасности решают тремя способами:

- ♦ сканируют не все узлы или только небольшие группы узлов;
- ♦ ищут определённые уязвимости;
- ♦ горизонтально масштабируются.

Горизонтальное масштабирование — хороший вариант, но требует дополнительных ресурсов и подходит не всем. Поиск конкретных уязвимостей в инфраструктуре спасает ситуацию. Он занимает в разы меньше времени.

MaxPatrol VM может выявить уязвимости без повторного сканирования. Что это означает? Система анализа защищённости в автоматическом режиме пересчитывает применимость уязвимостей к узлам сети при обновлении базы знаний либо при изменении параметров активов. При этом сканеру не нужно активно взаимодействовать с каждым узлом. Система должна уметь собирать и хранить информацию обо всех активах сети (о конфигурации железа, об операционных системах и установленном ПО), а также уметь в процессе пассивного сканирования получать информацию о новых активах, брать информацию о них из других источников, например из решений SIEM и NDR/NTA. Также важной является корректная идентификация или «склейка» активов, которая позволяет избежать дублирования систем.

Помимо этого, MaxPatrol VM умеет делать точечные проверки или проверки на группу уязвимостей, что существенно снижает время сканирования.

При выборе систем анализа защищённости нужно понимать, какие задачи стоят перед компанией, смогут ли службы ИТ и ИБ грамотно использовать внедряемые инструменты и позволит ли новая система решить основные задачи процесса vulnerability management:

- ♦ установить прозрачное взаимодействие служб ИТ и ИБ;
- ♦ выстроить чёткие приоритеты: что устранять вне очереди, а что стандартным патч-менеджментом;
- ♦ быстро выявлять уязвимости.

Эти критерии помогут построить эффективный процесс и увидеть, что работа с уязвимостями приносит результат.



Павел КОВАЛЕНКО
директор центра
противодействия
мошенничеству компании
«Информзащита»

МЕЖДУ СУПЕРМАРКЕТАМИ И ПОКУПАТЕЛЯМИ

ТОРГОВЫЕ СЕТИ ТЕРЯЮТ МИЛЛИОНЫ
ИЗ-ЗА МОШЕННИЧЕСТВ С ПРОГРАММАМИ ЛОЯЛЬНОСТИ



По данным центра противодействия мошенничеству компании «Информзащита», в 2021 году количество злонамеренных действий с бонусными картами выросло более чем в два раза по сравнению с 2020 годом. Эксперты считают, что эта тенденция будет

сохраняться в связи с распространением программ лояльности по всем возможным направлениям, начиная от финансовой области и банковских карт и заканчивая ритейлом и туризмом, где развитие идёт семимильными шагами. В зоне риска находятся прежде всего супермаркеты

и онлайн-магазины, так как создание программ лояльности является одним из ключевых средств для привлечения потребителя.

По статистике, три четверти взрослого населения России пользуются бонусными картами различных торговых сетей. Стоит отметить, что данный тип

взаимоотношений выгоден для обеих сторон — и для клиентов, и для ритейлеров. Первые получают возможность накапливать и тратить бонусные баллы, приобретая товары по более выгодной цене. Магазинам, в свою очередь, удаётся удерживать клиентов, стимулировать первичные и повторные покупки и накапливать сведения о покупателях (например, какие продукты пользуются спросом в определённом районе), благодаря чему корректируются поставки и тем самым выстраиваются эффективные схемы продаж.

Киберпреступникам тоже нравятся программы лояльности — благодаря им мошенники собирают личные данные и информацию о накоплениях, бонусах и другие подробности, то есть они могут направить атаку как на самого клиента, так и на ритейлера, который владеет данной программой. В результате торговые сети только ежемесячно теряют не менее 2–3 млн рублей.

КИБЕРАТАКИ С РАЗНЫХ СТОРОН

Первым фронтом атаки являются внешние киберпреступники, которые взламывают личные кабинеты клиентов, в том числе путём перебора учётных данных. Что они могут сделать с кошельком бонусной карты, зависит от самой программы лояльности — и тут есть несколько вариантов. Первый — расходование баллов для покупки товара, который потом можно легко сбыть на торговых площадках либо использовать для личных нужд. Также можно собрать все баллы на одном кошельке, если, конечно, программа лояльности это позволяет.

Вторым способом мошенничества является продажа как самих бонусных баллов, так и скидки, которую накопил клиент. Зачастую мошенники сбывают всё это посредством публичных телеграм-ботов.

Ещё один вариант: перевод накопленных баллов в реальные деньги, опять же при условии, что программа лояльности позволяет сделать это. В данном случае хакеры используют анонимные электронные кошельки или моментальные карты, чтобы скрыть следы.

Однако доступ к данным киберпреступники получают не только для

использования баллов — его применяют и для захвата персональных данных клиентов, которые понадобятся для дальнейших кейсов, связанных с социальной инженерией. Знание личной информации о жертве поможет мошеннику втереться в доверие и вывести денежные средства уже с реальных счетов. Самих способов получения доступа к кошелькам у хакеров огромное количество — начиная от рассылки фишинговых писем и заканчивая покупкой в даркнете ранее слитых баз данных, которые мог выставить как обиженный сотрудник, так и нечистый на руку администратор. Кроме того, очень часто сам клиент может использовать одни и те же данные аутентификации на разных сайтах, в том числе в личном банковском кабинете, что тоже будет огромным полем для дальнейших действий кибермошенников.

Следующее направление атаки может исходить от собственных клиентов бренда, которые могут воспользоваться лазейками в программе, например, создать несколько учётных записей для получения вознаграждения. Они могут долго пользоваться своими преступными схемами, не рассказывая об этом никому, а затем в какой-то момент выдать эту информацию в каком-нибудь телеграм-канале, чтобы похвастаться перед публикой, и тут-то обман вскроется. Злоупотребление условиями программ лояльности часто может быть незаметно в течение длительного времени и обнаружено только с помощью случайно найденной закономерности в результате анализа.

И наконец, внутренний мошенник — самый опасный нарушитель, которого сложнее всего выявить. Эксперты сходятся во мнении, что большинство утечек данных и обманов с картами лояльности приходится на самих сотрудников торговых сетей. Имея доступ к базам данных, можно без особых усилий заполнять в свою пользу балансы вознаграждений, пользоваться невостребованными бонусами из бездействующих учётных записей, особенно тех, у кого количество баллов накоплено в больших количествах, а также красть персональные данные клиентов. Сотрудники, работающие с самими бизнес-процессами

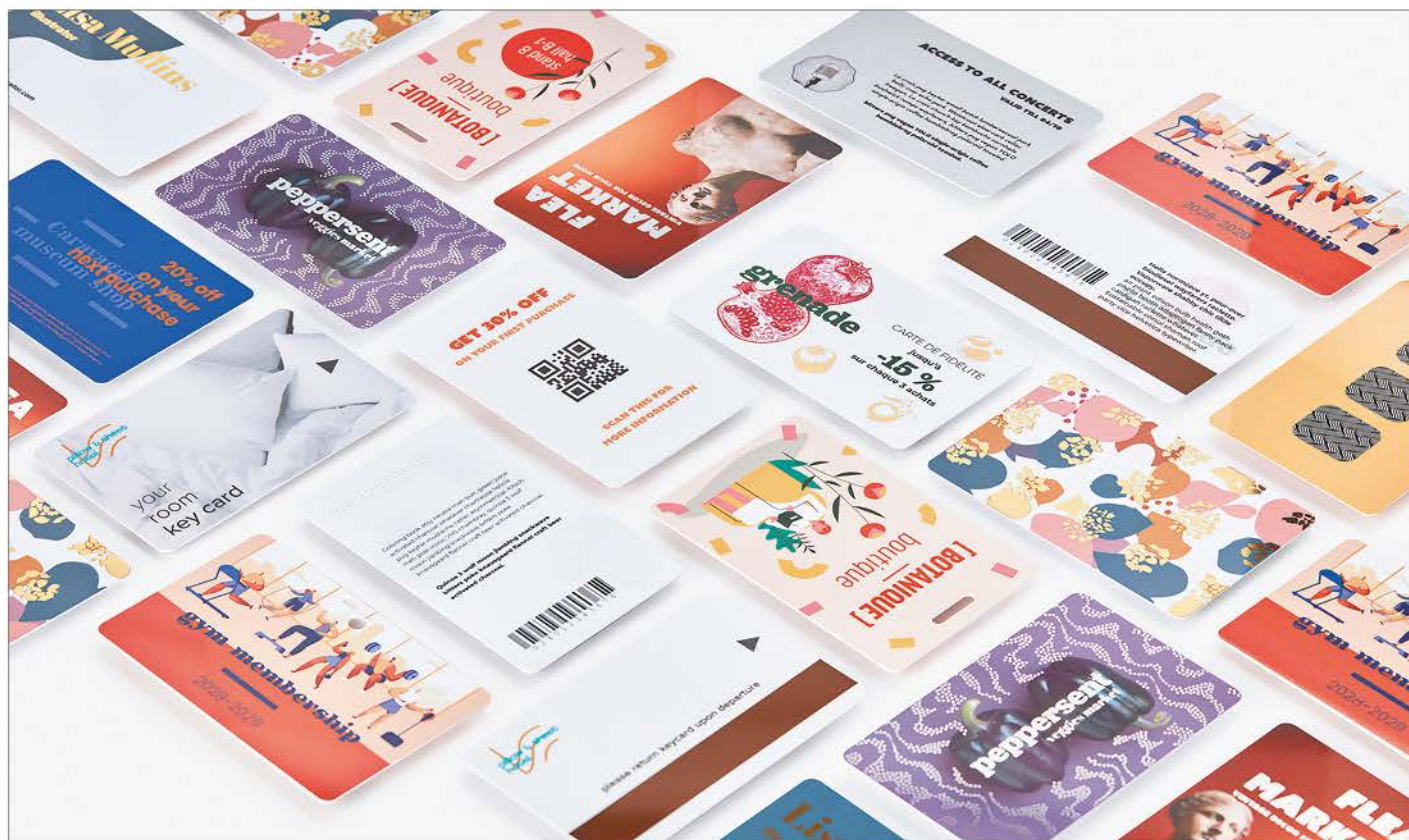
программ лояльности, прекрасно знают все уязвимости и нередко пользуются ими, заодно подчищая за собой следы после совершённых действий. Также у них есть KPI, которые необходимо выполнить, поэтому они могут выпускать карты лояльности для нецелевого использования, чтобы закрыть план.

КАК ПРЕДОТВРАТИТЬ?

Мошенничество с программами лояльности обходится дорого, но сами ритейлеры неохотно говорят на эту тему, вероятно, остерегаясь возможных репутационных потерь. Все риски, как правило, уже бывают заложены в суммы товаров и возможные операционные потери.

Одним из вариантов является многофакторная аутентификация. Добавление дополнительного контроля для входа в личный кабинет или при расходовании баллов поможет значительно уменьшить количество несанкционированных применений программы лояльности как со стороны внешнего нарушителя, так и со стороны внутреннего. Также одним из способов борьбы с мошенничеством является установка лимитов на использование баллов, но данное решение можно настроить только после запуска программы лояльности и анализа на большом периоде. Стоит отметить, что оба варианта могут как снизить количество мошенничеств, так и увеличить число жалоб клиентов и уменьшить их лояльность в целом, что, в свою очередь, понесёт за собой отток покупателей, а следовательно, лишение части прибыли.

Если смотреть в сторону внутренних мошенников, то самым действенным способом всегда являлось внедрение управления доступом на основе ролей и отслеживание сетевой активности сотрудников на наличие признаков нелегитимных действий. Любые избыточные права доступа работников ведут к увеличению риска утечки информации. Также необходимо проводить постоянную инвентаризацию прав доступа, чтобы контролировать необходимые права, которые требуются для выполнения должностных обязанностей, возложенных на сотрудника в настоящий момент.



БЕЗ АНТИФРОДА НЕ ОБОЙТИСЬ

Но в случае если система программы лояльности является громоздкой, то более выгодным решением может оказаться внедрение комплексной системы антифрода, которая закроет многие проблемные зоны. Сегодня современные системы позволяют собирать большое количество событий из разных источников (поведенческих, сессионных и транзакционных метрик) со стороны клиентов, сотрудников, кассиров и других лиц, участвующих в программе лояльности.

НЕ ОБОЙТИСЬ И БЕЗ АУДИТА

При этом любое построение системы антифрода или введение других необходимых контролей неразрывно связано с проведением качественного и многогранного аудита бизнес-процессов, которые задействованы в программе лояльности. Детальный анализ следует проводить не только в плоскости бизнес-процессов. Помимо того, что нужно понимать, где именно проблема, необходимо знать, какие существуют уязвимости, в том числе в коде и периметре. Такой аудит лучше всего выполнять

внешними компаниями, что позволит получить независимую и объективную оценку текущего состояния систем, в которых могут быть реализованы мошеннические схемы, а также выявить уязвимости и потенциально возможные сценарии фрода.

Кроме того, такой аудит поможет повысить эффективность работы бизнес-процессов, в которых есть место для хакерских действий, что, в свою очередь, поможет увеличить прибыль от программы лояльности, созданной ритейлером. Особенно отметим, что все векторы атак и последующие сбыт/использование программ лояльности в мошеннических схемах отличаются в зависимости от того, чья это система поощрения. И каждый отдельно взятый вид мошенничества может иметь свои особенности: для ритейла — анализ площадок, где идёт реализация бонусов или товаров, для заправочного бизнеса — изменение оборота на каких-либо АЗС по бензину или использованию баллов отдельным лицом, для тревел-области — корректность начисления миль и так далее. Но нужно понимать, что в любой области без качественного аудита не удастся выявить

весь спектр уязвимостей, а некоторые более хитрые схемы останутся без внимания и могут приносить ощутимый убыток компании.

Подведём итог вышесказанному: мошенничество в программах лояльности не просто увеличивается, а растёт в геометрической прогрессии в связи с развитием данного типа взаимоотношений между супермаркетами и покупателями и привлечением всё большего количества клиентов. Негативные комментарии, которые возникают в соцсетях и СМИ после появления новостей о каких-либо утечках, мошенничестве или хитростях использования баллами, отрицательно сказываются на репутации как самой программы лояльности, так и всего бренда. Поэтому каждый ритейлер, который предоставляет подобную систему поощрения, должен выбрать подходящий именно его бизнесу метод борьбы с охотниками за бонусными счетами, однако понять, какой именно, можно только после оценки потерь.



Тамара ДЕМЕНКОВА
эксперт департамента
финансового комплаенса
ГК «ЦИБИТ»

СЛОЖНЫЕ ВОПРОСЫ

ПРО СООТВЕТСТВИЕ ТРЕБОВАНИЯМ НОВЫХ ПОЛОЖЕНИЙ БАНКА РОССИИ

С конца февраля специалисты финансового сектора фиксируют новую масштабную волну DDoS-атак на ключевые российские компании банковской отрасли: атакам подверглись в том числе Сбербанк, ВТБ, Газпромбанк. Соответствие требованиям информационной безопасности становится приоритетным вектором и самым острым вопросом.

За последние три года Банк России выпустил целый ряд положений в области информационной безопасности (683, 747, 719, 757). Наиболее трудоёмким требованием новых документов является оценка соответствия требованиям ГОСТ Р 57580.1–2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер», который включает в себя требования к восьми процессам защиты информации, требования к защите информации на этапах жизненного цикла АС, а также требования по направлению процессов защиты информации (планирование, реализация, контроль и совершенствование) — всего 667 требований.

ОЦЕНКА СООТВЕТСТВИЯ ТРЕБОВАНИЯМ ГОСТ Р 57580.1–2017: СЛОЖНЫЙ И ТРУДОЁМКИЙ ПРОЦЕСС

Перед началом оценки соответствия организациям необходимо понять определение контуров безопасности. Малым организациям рекомендуется рассматривать единый контур безопасности, который будет включать в себя всю внутреннюю инфраструктуру организации, за исключением сегментов SWIFT и PCI DSS, так как данные сегменты оцениваются в рамках проведения отдельных аудитов. Оценку платёжного сегмента Банка России рекомендуется провести в рамках оценки единого контура безопасности с учётом того, что данный сегмент является выделенным во внутренней инфраструктуре организации.

Описание контуров рекомендуется оформить документально. Кроме того, для каждого контура необходимо составить ведомость применимости требований ГОСТ, для неопределяемых параметров необходимо составить обоснование исключения их из оценки. Таким обоснованием может являться то, что некоторые технологии могут

не использоваться в данных контурах (беспроводные сети, виртуализация серверов и рабочих станций, удалённый доступ).

По нашим оценкам, в крупных финансовых организациях может выделяться 4–5 контуров безопасности, включая контур обработки биометрических персональных данных. Простой математический подсчёт показывает, что при рассмотрении пяти контуров безопасности оценивать необходимо будет 3335 требований.

Оценка контуров безопасности требованиям ГОСТ Р 57580.1–2017 — трудоёмкий процесс, что связано с большим количеством оцениваемых параметров, а также с удалённым режимом работы сотрудников организаций. Из-за этого усложняется сбор свидетельств, подтверждающих выполнение того или иного требования.

СОВРЕМЕННЫЕ РЕШЕНИЯ В ОБЛАСТИ ФИНАНСОВОГО КОМПЛАЕНСА

Эксперты департамента финансового комплаенса ГК «ЦИБИТ» разработали сервис оценки, который позволяет загружать свидетельства выполнения требований аудиторами и сотрудниками оцениваемых организаций, сохранять все данные аудита в удобном формате, формировать список рекомендаций по повышению уровня оценки соответствия. Кроме того, сервис предоставляет возможность копирования полученных данных для проведения последующего аудита.

По нашим оценкам, в крупных финансовых организациях может выделяться 4–5 контуров безопасности, включая контур обработки биометрических персональных данных



Данное решение позволит сосредоточиться на проверке выполнения рекомендаций, которые были даны при предыдущих оценках соответствия, а также выработке дальнейших рекомендаций по совершенствованию выполнения требований.

Пример. При первой оценке соответствия была дана рекомендация по отслеживанию неактивных (в течение 45 дней) учётных записей пользователей в Active Directory. При следующей оценке соответствия аудитор проверяет, каким образом была выполнена данная рекомендация, и формирует рекомендацию, которая усовершенствует выполнение данного требования — отслеживание неактивных учётных записей пользователей

в конкретных приложениях, которые попадают в оцениваемый контур безопасности.

Сервис позволяет сохранять данные оценок соответствия в течение пяти лет, а также копировать информацию по предыдущему аудиту для проведения текущей оценки. Это позволяет «обогащать» свидетельства выполнения требований новыми данными, а также удалять неактуальные свидетельства и добавлять актуальные.

Для доступа ко всем данным оценки соответствия в целях интеграции с другими приложениями у сервиса оценки разработано API.

Таким образом, новый сервис позволяет проводить оценку соответствия более комплексно, формировать рекомендации с учётом опыта предыдущих аудитов и постоянно совершенствовать выполнение требований к ИБ, что в конечном итоге означает соответствовать запросам времени.



ГРУППА КОМПАНИЙ
ЦИБИТ

КОНТАКТЫ

Телефон: +7 (495) 792-80-80
E-mail: info@cibit.ru
Сайт: www.cibit.ru



Сергей ВИХОВ
эксперт BIS Journal,
советник генерального
директора
ООО «ИТ-Экспертиза»

Филармонический концерт. Слушатель,
обращаясь к соседу справа: «Это не Вы
сказали: „Да“?» — «Нет!». Обращаясь к соседу
слева: «Это не Вы сказали: „Да“?» — «Нет!».
Сам себе: «Значит, музыкой навеяло...»
Анекдот

ИНФОФОРУМ-2022, ТБ-ФОРУМ-2022

ЭССЕ НЕ О МЕРОПРИЯТИЯХ, А О ТОМ, ЧТО НАВЕЯЛО...

Февраль оказался богатым на ИБ-шные мероприятия. Сначала Инфофорум, потом ТБ-форум. И если первое мероприятие — пафосное, парадное, то второе — скорее камерное. Мне больше импонирует именно ТБ-форум. Правда, он охватывает многие аспекты безопасности, но я буду говорить о том, что ближе: об информационной безопасности. В чём камерность? По своей сути ТБ-форум — это совокупность разных конференций, каждый может найти себе нужную проблематику. А ещё это гибридный формат (ну куда же деваться в эпоху пандемии).



*Налево пойдёшь — в санкции попадёшь.
Направо пойдёшь — в отставание
отечественных технологий упрёшься.
Прямо пойдёшь — и куда бедному
крестьянину податься — деньги потеряешь*

не рассчитывайте, впрочем, как и на какие-то рекомендации по их решению, но проблемы обозначу.

ИМПОРТОЗАМЕЩЕНИЕ

Говорим об импортозамещении уже давно, а воз двигается медленно. Разговоров много, эффекта — не очень. Итак, налево пойдёшь — в санкции попадёшь. Направо пойдёшь — в отставание отечественных технологий упрёшься. Прямо пойдёшь — и куда бедному крестьянину податься — деньги потеряешь. Ищи компромисс, а он невелик: либо используешь пиратские копии, как в старые 90-е, потом платишь по искам обладателей, либо берёшь наш недоделанный продукт и потом платишь за его доделку и кастомизацию. Думайте сами, решайте сами — иметь или не иметь.

Конечно, надо начинать с элементной базы. Но технологии наши, к сожалению, не позволяют реализовать все задумки. Что делать? Думаю, надо искать международное сотрудничество. Да, возможности из-за напряжённой международной обстановки небольшие, но они всё-таки есть. Это и Китай, и Индия, и другие восточные страны. Так, может, стоит посмотреть на Восток?

АПОЛОГЕТИКА

Это немного о нашей нормативке. Направо пойдёшь — куда прёшь! Иди по центру! Налево пойдёшь — я тебе попереключаю! На первый, по центру! По центру пойдёшь — в штрафы упрёшься. Да, без репрессий в нашем обществе не всегда управишься. Но! Репрессии не защищают, а только создают иммунитет. Это как с ковидом: прививка — это иммунитет, а где лекарство? Прививкой не вылечишься, но и лекарством не защитишься, нужен комплекс. Нужны не только штрафы, но и цельные, грамотные, обоснованные с точки зрения экономики рекомендации. Вот на это и надо направлять наши

ИБ-шные мероприятия. Я уже много писал и про БДУ, и про стандарт по архитектуре СОБИ, и про методику категорирования. Вроде всё есть, но как-то далеки они от народа... Неувязочка. Никак их не соединишь и не получишь целостную картину. И проблема здесь, на мой взгляд, в отсутствии единой теории построения систем безопасности информации. Книг много, и даже в вузах читают курсы (сам читал), но единой теории — нет. Вот, как мне кажется, достойная тема для ГНИИ ПТЗИ. А отсутствие единой теории порождает разрозненные нормативные документы.

И ещё о нашем менталитете. К сожалению, если всё отдать на откуп хозяину информационной системы, никакой защиты не будет. Убеждать, что это важно, нужно, необходимо — это хорошо, но неэффективно. Российский человек, если его не заставлять, делать не будет. Раньше, в стародавние времена, все требования были обязательны (но и время было такое). Потом была определённая вольница (вспомните хотя бы эпопеи с профилями защиты, когда каждый хозяин хотел сделать свой профиль). Так, может, настало время, когда надо совместить два эти подхода?

ВЕНДОРСТВО

Плох тот менеджер, который не умеет продать свой продукт. Поэтому налево пойдёшь — тебе продукт впендюрят, потому что он есть, и при этом убедят, что жить без него нельзя, ну, как без БАДов. Направо пойдёшь — обесчуждают важность и целесообразность, забыв рассказать о стоимости внедрения. Прямо пойдёшь — как в сказке: чем дальше, тем страшнее. Купите наших слонов, наши слоны самые лучшие слоны в России! Мы можем всё и сразу! Мы решим все ваши проблемы! Но ведь ещё древние сказали, что панацеи нет. Кремлёвская таблетка есть только в теории. Комплексность — это «Хед энд Шолдерс», три в одном, это сложнее.

Что общего в этих форумах? Чего не хватило? А как-то маловато нового. К сожалению, идут перепевки уже отговорённого. Ну понятно, и нормативки сейчас новой особо нет, да и то и это — всё уже не раз обсуждалось. Поэтому я не буду давать отчёт с форумов, кому это интересно, в интернете можно найти много отзывов. Я хочу поговорить о том, что навяли эти мероприятия, о чём захотелось поразмышлять, поделиться своими мыслями, может, и не совсем правильными.

ТРИ ДОРОГИ

Почему-то вспомнились русские сказки. Там всегда есть перепутье: три дороги. Куда идти — тебе решать. Вот и я прикинул те проблемы, которые обсуждались на форумах. На глубокий анализ



Валерий КУЛИКОВ
обозреватель BIS Journal

НУЖНА ЛИ ВАВИЛОНСКАЯ БАШНЯ НА ЦИФРОВОМ ФУНДАМЕНТЕ?

ЭТО БЫЛО БЫ УМЕСТНО ОБСУДИТЬ ЕЩЁ В ФЕВРАЛЕ
НА УРАЛЬСКОМ ФОРУМЕ — 2022

Бесшовная интеграция разнообразных информационных систем для «прозрачного» обмена данными — тема не новая, если речь идёт о масштабах предприятия или ведомства. Новые «аккорды» зазвучали в этой теме лет пять назад в связи с идеями «цифровой трансформации», «цифровой экономики» и «цифрового» «государства как услуги». Применительно к кредитно-финансовой сфере, инвестиционным технологиям и страховому бизнесу тема «прозрачного» и «бесшовного» обращения информации была поднята в ходе декабрьской 2021 года конференции Finopolis-2021 на пленарной дискуссии «Бесшовные рельсы цифровизации: возможно ли это?» и на нескольких специализированных секциях.

При этом основной упор делался на якобы выгоды свободного обращения персональных данных (ПД) о собственности граждан, их покупательной активности и прочем подобном.

Уместные слова об «обезличивании» этих данных, их обработки только «для заявленных целей» и только «после получения согласия владельца данных»

дежурно произносились. Но кто из нас не сталкивался с возникающими «ниоткуда» потоками профильного рекламного спама в разных каналах персональных коммуникаций после того, когда ты, казалось бы, только подумал о покупке кондиционера или посещении сауны? Да, потом вспоминаешь, что сделал пару звонков или несколько поисковых запросов в интернете, но ведь без вхождения в аккаунт или с телефона, оформленного на другого члена семьи!

Но сейчас речь даже не о мифах «обезличивания».

А ОНО НАМ НУЖНО?

К анализу дискуссий Finopolis-2021 ставят вернуться новостные ленты последних дней прошлого года и января года нынешнего. Недоступность в течение нескольких дней объединённой информационной системы одного из силовых ведомств России и что-то вроде блэкаута объединённой энергосистемы трёх азиатских лимитрофов на постсоветском пространстве заставляют в очередной раз задуматься об угрозах безопасности при реализации «бесшовных» и «прозрачных» интеграционных

мегапроектов. Тех, что строятся на основе интеграции и без того мегасистем, к которым относятся ряд государственных ИТ-«долгостроев» и «новостроев» ИТ-систем маркетплейсов и суперприложений так называемого бизнеса, который, по собственным признаниям его представителей, мыслит на глубину пары-тройки лет от силы.

На пленарной дискуссии «Бесшовные рельсы цифровизации: возможно ли это?» Минцифры представило «допиливание» ЕБС всероссийского уровня (министр считает, что подтверждать личность — одна из корневых функций государства). Намерение довести уровень цифровизации процессов до уровня, достигнутого в российских банках, обозначили на Finopolis-2021 несколько представителей страхового бизнеса. Чиновница Центробанка безапелляционно заявляла о востребованности обществом проектов по СБП, ЕБС, цифровому профилю.

Но ни разу не было приведено объективных доводов в пользу востребованности результата упомянутых работ населением страны или необходимости этого результата для населения.

Более того, когда министр рассказывал о «прикручивании» к ЕБС интерфейсов, призванных «упростить процесс сдачи биометрии», он обосновал эту доработку так: «Чтобы у пользователя возникла мотивация сдавать свою биометрию». Тем самым министр косвенно признал непопулярность ЕБС в массах, а позже уже прямым текстом упомянул о «пробуксовках ЕБС», хотя в целом и выразил уверенность в будущем успехе системы с неоднозначно оцениваемыми специалистами характеристиками ИБ.

О ДИАЛЕКТАХ И ГОВОРАХ ИТ-ИНФРАСТРУКТУР

А когда представитель страхового сообщества, пришедший в эту систему на осознании факта недоохоженности страхового бизнеса цифровыми технологиями а-ля «финтех», поделился перспективами автоматизации страхования на основе «бесшовного» использования данных Росреестра, то за кадром осталось качество данных в ЕГРН (об этом можно судить, например, по многочисленным комментариям на специализированных юридических ресурсах) и продолжающиеся процессы «допиливания» информационных систем ведомства.

И «допиливание» ИТ-инфраструктуры, и точность и полнота информации, обращающейся в ней, — это проблемы не только Росреестра!

Современные процессы разработки ИТ-систем практически исключают понятие «стабильной платформы». И если на внутриведомственном (внутрикорпоративном) уровне поддержание должного уровня ИБ теоретически возможно при переходе от принципов DevOps к DevSecOps, то на уровне межведомственной интеграции широко используемая практика такого рода пока не описана.

Также «бесшовная» и «прозрачная» цифровизация обострила проблему качества данных (и «унаследованных», и тех, что в режиме широкомасштабного «чёса» собираются сегодня).

О какой достоверности цифрового профиля можно говорить, если смартфоны на всю семью нередко оформлены на главу семейства, в компаниях стихийно организуются «колхозы» бонусных и скидочных карт, а в на-

«Бесшовная» и «прозрачная» цифровизация обострила проблему качества данных (и «унаследованных», и тех, что собираются сегодня в режиме широкомасштабного «чёса»)

стройках смартфона, используемого в Краснодарском крае, вполне «штатно» используются настройки Танзании?!

«Безопасники» общего профиля, ответственные за внедрение СКУД на основе «интеллектуального» видеонаблюдения, честно делятся своими наблюдениями об уровнях ошибок первого и второго рода таких систем в повседневной эксплуатации. Уровнях, которые хуже тех показателей, на которые ссылаются бенефициары внедрения ЕБС. Уровнях, которые заставляют «по месту» подбирать частоту актуализации данных биометрии в локальных системах СКУД на основе «интеллектуального» видеонаблюдения.

ЦИГЕЛЬ, ЦИГЕЛЬ, АЙ-ЛЮ-ЛЮ?

И ЕБС, и СБП, и «цифровой профиль» выглядят, мягко говоря, ещё сыровато. А некоторые представители финансового регулятора уже мыслят на перспективу, практически обсуждая в реальном времени на Finopolis-2021 необходимость создания «Платформы управления согласиями» [граждан на передачу своих персональных данных]. И времени на создание такой платформы отводится один год (цитата: «Рынку надо не через 10 лет, максимум через год»).

А понимает ли рулевой финансовыми потоками, что «Платформа управления согласиями», как, впрочем, и ЕБС, и СБП, и «цифровой профиль» — это системы, а не «железо» и «софт» для поддержки ядра системы? А ведь надо ещё подумать о самой возможности создания удобной для граждан периферии, на основе которой ядро системы будет общаться с владельцами персональных данных.

И для работ этих государственных систем надо не только освоить бюджет на программные разработки и закупки аппаратных платформ, но и разработать идеологию «Управления согласиями» (включая её правовые аспекты), а до этого понять, намерены ли граждане

управлять своими согласиями во имя решения неочевидных задач и достижения неочевидных целей. О результатах оперативной реализации «благих намерений» мы уже можем судить по социальным QR-потрясениям в Канаде и Европе.

Но буде идеология государственной ИТ-платформы «Управления согласиями» разработана, смогут ли «9 женщин родить ребёнка за 1 месяц»? Здесь использовано образное описание требования «рынку надо не через 10 лет, максимум через год» в контексте объективного многолетнего опыта инженерных разработок системного уровня, когда только проведение НИОКР требует около года (с отклонениями и в плюс и в минус), а устранение «детских болезней» — от нескольких лет до тех 10 лет, через которые «рынку не надо».

А к упомянутым срокам, объективность которых подтверждена практикой, следует добавить и необходимость обсуждения аспектов информационной и кибербезопасности, связанных с отсутствием на данный момент единых взглядов на архитектуру кибербезопасности государственных систем для «потребительских» целей и перспектив реализации этой архитектуры на платформах, отвечающих требованиям «импортозамещения». О необходимости и неизбежности разработки таких архитектур и платформ говорилось и на конференции в ходе работы киберполигона Сбера в 2021 году, и на РНД 2021, но есть ли решение на нынешний день? И имеет ли смысл городить государственные ИТ-мегапроекты без решения этих вопросов?

Очень жаль, что поспешное решение об отмене февральского 2022 года Уральского форума «Информационная безопасность финансовой сферы» не позволило обсудить в широкой аудитории упомянутые проблемы. А ведь времени на раскачку нет!



Павел БЫЛЕВСКИЙ
доцент Департамента
информационной
безопасности
Финансового
университета при
Правительстве РФ

«ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ». ИСПРАВЛЕНИЕ ИМЕНИ

ОПЫТ БОРЬБЫ С ВРЕДОНОСНОЙ
ГУМАНИТАРНОЙ ЗАКЛАДКОЙ

С 24 февраля 2022 года остро встал вопрос о реальном, а не декларативном суверенитете цифровизации, об отечественных прорывных разработках так называемого искусственного интеллекта. «Копирующей локализации» зарубежных решений не получится, придётся критически переосмыслить зарубежные подходы, выявить и устранить вредоносные «закладки».

РИСКИ ЛИХОРАДОЧНОЙ ЦИФРОВИЗАЦИИ

Так называемый искусственный интеллект считается центральной «сквозной технологией», локомотивом «ускоренной цифровизации», лихорадочно начатой в России несколько лет назад.

Вопрос, что теперь с этим делать, не менее актуален, чем приостановка в России работы международных платёжных систем Visa и MasterCard, всё более серьёзные угрозы отключения отечественных банков от SWIFT.

Под вопросом не только перспективы «цифровизации», но и просто дальнейшее функционирование российских автоматизированных информационных систем и сервисов, государственных и банковских. Можно ли по-прежнему говорить о «цифровой экономике» в финансовой сфере или же «не до жиру, быть бы живу»? Лишь бы обеспечить устойчивость того, что есть? Перед лицом угрозы ограничений или полной блокировки использования привычных

зарубежных решений российскими государственными органами, корпоративными и индивидуальными пользователями?

Развилка, на которой мы оказались, требует непростых решений и долгого тяжёлого труда. Ускоренное обеспечение цифрового суверенитета и импортозамещение не могут быть сведены к копированию зарубежных решений и созданию их локальных аналогов. Необходим критический пересмотр наличных подходов для альтернативных отечественных разработок, способных обрести опережающий характер.

Пересмотр базовых подходов к «искусственному интеллекту» открывает перспективы решений, «перпендику-

ПРЕДСТАВЛЕНЫ 43 ПРОЕКТА НАЦИОНАЛЬНЫХ СТАНДАРТОВ В ОБЛАСТИ ИИ

На сайте Технического комитета по стандартизации № 164 «Искусственный интеллект» (ТК 164) опубликованы¹ первые редакции 43 проектов национальных стандартов в области применения искусственного интеллекта.

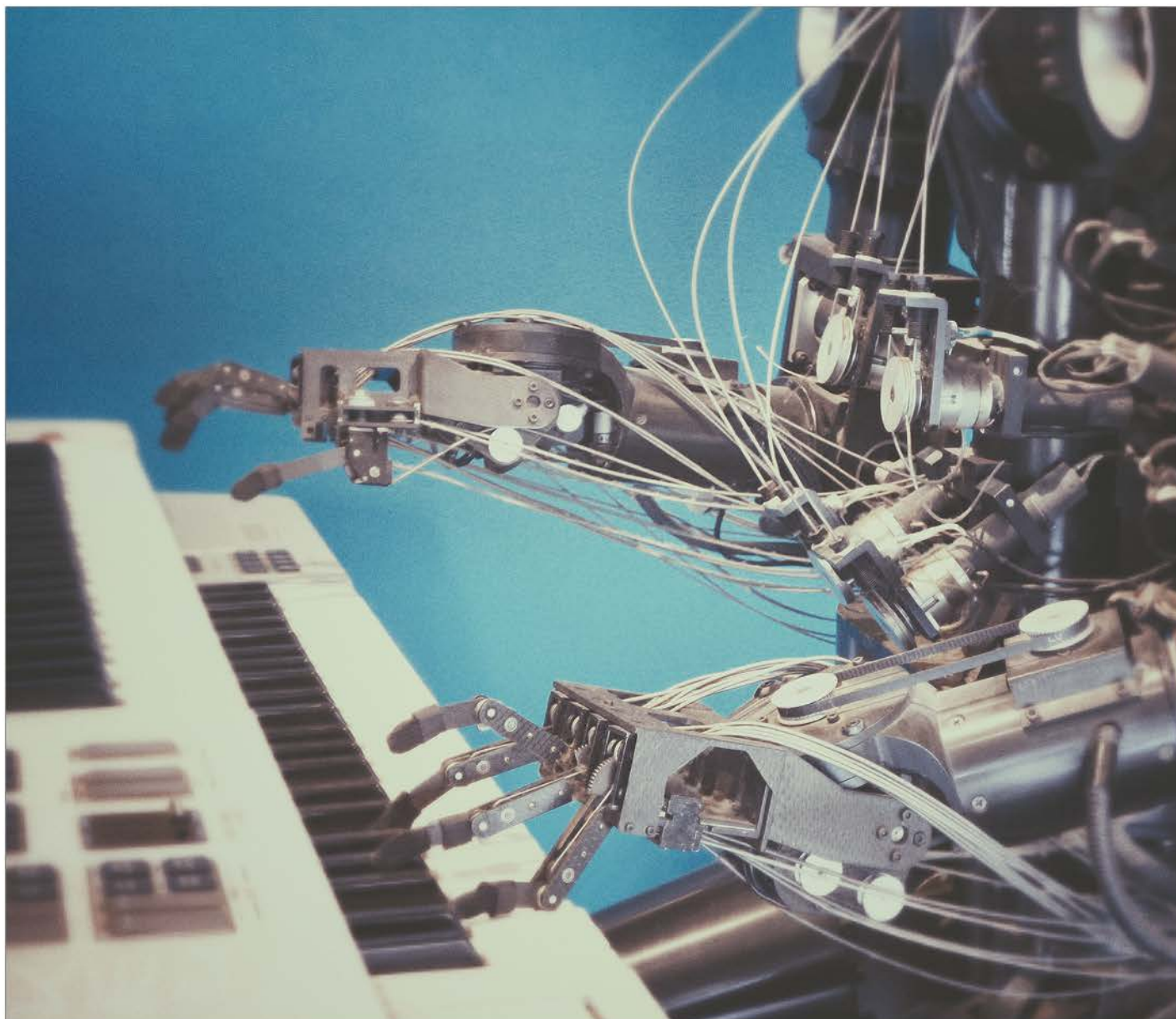
Напомним, Технический комитет «Искусственный интеллект» создан в 2019 году по инициативе РВК при поддержке Минпромторга РФ и Росстандарта. Работы по стандартизации в области ИИ в ключевых отраслях экономики проводятся ТК 164 в соответствии с Национальной стратегией развития искусственного интеллекта на период до 2030 года.

Документы сгруппированы по темам: «Информационные технологии. Искусственный интеллект»; «Системы искусственного интеллекта в естественных и искусственных источниках излучения»; «Системы искусственного интеллекта в клинической медицине» и т. д. Их разработкой занимались различные коллективы, среди них НИУ ВШЭ, МГУ, Научно-практический клинический центр диагностики и телемедицины ДИТ Москвы и пр.

Как говорится на сайте комитета, ТК 164 является «зеркальным» по отношению к международному подкомитету SC 42 «Artificial Intelligence» объединённого технического комитета ISO/IEC JTC 1 «Information Technologies» и выполняет функции постоянно действующего национального органа в ISO.

Принятая в декабре 2020 года перспективная программа стандартизации по приоритетному направлению «Искусственный интеллект» на период 2021–2024 годов, утверждённая Росстандартом и Минэкономразвития, предусматривает разработку 217 стандартов в области ИИ.

¹ <https://www.tc164.ru/первые-редакции>



лярных» по отношению к имеющимся разработкам в нормативной и организационно-технической сферах, вплоть до принципов архитектуры и прикладных решений. Зарубежным подходам к разработкам так называемого искусственного интеллекта присущи базовые критические ошибки, подобные смысловым вредоносным закладкам. Двусмысленные основные понятия, начиная с некорректного термина «искусственный интеллект», способны дезориентировать и ввести в заблуждение кого угодно.

Авторы термина «искусственный интеллект» изначально заложили в него не просто двусмысленность, а многозначность, включая противопо-

речащие друг другу смыслы. «Искусственный» — это и рукотворный, и имитационный (создающий всего лишь иллюзию), и поддельный (обманный).

Специфика переживаемого переломного момента, как и в сказке Г.Х. Андерсена про голого короля, помогает внезапно узреть излишний балласт изначально неверных, ошибочных подходов. Сразу обратим внимание на неверность, метафоричность, вводящую в заблуждение формулировку понятия «искусственный интеллект». В отличие от отечественной формулировки «автоматизированные системы управления технологическими процессами» — прямой, однозначной и конструктивно-рациональной.

ОТ САМООБМАНА ДО МОШЕННИЧЕСТВА

Разработчики «искусственного интеллекта» не только сами путают человека с машиной и сетевыми решениями, но и вносят лишнюю сумятицу в нормативное регулирование, техническое и правовое. Или же наводят тень на плетень в простом вопросе отличия людей от других людей, от живых организмов — животных и растений, от неживых предметов и процессов, механизмов. Некорректное использование двусмысленного термина «искусственный интеллект» можно разделить на невольное, по общей инерции — и злонамеренное.

Добросовестно заблуждаются создатели, разработчики практических

направлений автоматизации: перевода с одного языка на другой, цифровизации физических параметров и аналоговых образов предметов и процессов, продвинутой робототехники. Чего стоит приписывание машинам без каких-либо оговорок человеческих умений!

Не более чем метафорический характер носит обозначение функциональности программно-аппаратных устройств «зрением», «слухом», «речью», «распознаванием», «обучением», «решением задач». Для описания работы машин, автоматизированных механизмов лишь весьма условны формулировки таких способностей биологических организмов, как ощущения и чувства.

Весьма сомнителен и термин «нейронные сети», как и «нейротехнологии». Приставка «нейро...» означает вовсе не мыслительные способности и даже не мозг, а нервное волокно — ткань, её клетку-нейрон. «Подобие» электронно-вычислительных сетей нервной системе, тем более мозгу, носит более чем условный характер. «Моделирование» мышления на них не более похоже на оригинал, чем работа на экскаваторе напоминает копание лопатой или конструкция самолёта — бионике птицы или летающего насекомого.

«Копируется» недействительная функциональная работа человеческого организма, включая нервно-мышечную систему и мозг. «Воспроизводится»... обратная проекция на человека архаической схематики, механистической традиции в западной науке и технике.

Те, кто создали и употребляют термин «искусственный интеллект», могут просто добросовестно заблуждаться. Но изначальная двусмысленность может использоваться и как орудие мошенничества, как коммерческого, так и политического. Учитывая, что обманывать других легче всего неподдельной искренностью, когда мошенник искренне впадает в сладостный самообман.

«Вёсны» искусственного интеллекта выражались в инвестиционных бумагах на волне очередной версии обещания создать «сверхразум, способный

решить все проблемы». Тема столь же регулярно обновляющаяся, как и «таблетка бессмертия» от фармацевтов, а также различные версии «решений» от трансгуманизма, создателей киборгов, генных инженеров и биотехнологов.

Финансовые спекулянты, используя учёных и разработчиков высоких технологий, регулярно провозглашали очередные утопические посулы: создать «добрый сверхразум», способный принести инвесторам невиданные прибыли. С другой стороны — антиутопические угрозы, что такие разработки раньше создадут конкуренты — коммерческие или политические. Финансовый пузырь надували, играя на повышение, а потом тихо схлопывали, уводя на время отыгранную тему в тень.

Западному праву исторически присуща дискриминация: ограничение прав групп граждан на основе ошибочных и лженаучных теорий. Правовые системы колониализма обосновывались социал-дарвинизмом и расовыми концепциями о якобы неполноценных расах и «сверхлюдях». Современное движение BLM (Black Lives Matter), по сути, является расизмом наизнанку.

Аналогичные псевдонаучные конструкции положены в основу движения ЛГБТК+ — деструктивного перформативного гражданского права на основе замены мужского и женского полов десятками «гендеров» — произвольных «социальных конструкторов». Подобным образом «бракосочетание» может быть распространено не только с однополыми гражданами, но также с животными и предметами — тем же «искусственным интеллектом».

Попытки превратить «искусственный интеллект» в субъект права совершаются для выстраивания серых схем оптимизации налогообложения, снятия ответственности за ущерб его применения с разработчиков, производителей и эксплуатирующих лиц. Есть «позиция» и для политиков — уйти от ответственности за негативные последствия собственных решений и действий путём ссылок на «правосубъектность» программно-аппаратных комплексов, обеспечивающих «машиночитаемый» и «машиноисполняемый» деловой документооборот.

ФИЛОСОФСКАЯ АРХАИКА И ТЕХНОСУЕВЕРИЯ

Механистический подход к жизни и человеку — одна из стародавних тенденций западноевропейского мировоззрения. Философ-математик Рене Декарт считал животных механизмами-автоматами, способными лишь на «рефлексы», и немногим выше он ценил человека. В основе современного понятия «искусственный интеллект», совершенно нестрогого, если не сказать ошибочного, лежит вульгарное «картезианство». Дополненное тем, что можно назвать «техносуевериями», схожими с первобытным фетишизмом — наделением предметов воображаемыми сверхъестественными качествами.

Людям первобытной культуры свойственно обожествление стихий природы, животных. Подобные архаичные формы сознания могут воспроизводиться и в нашу технотронную эру, когда современную технику называют «умной» не в фигуральном смысле. Тогда легко представить, что появятся машины «умнее человека», которые будут ему «служить», а потом «захотят поработить».

Можно воспринимать автоматизированное автономное программно-аппаратное устройство как «умное», подобно тому, как человеку первобытной культуры с непривычки может показаться, что внутри «говорящего» радио спрятан другой человек.

Проверочный вопрос на засыпку: способен ли телеграфный столб мыслить, переживать эмоции, чувствовать? Наверное, да: для богатого воображением ребёнка, в детской сказке или юмореске. Возможны и другие варианты: для адепта секты техносуеверий или человека, у которого не всё в порядке с головой.

Пойдём дальше: может ли мыслить шагающий экскаватор или роботизированная линия пошива изделий нижнего белья? В состоянии ли ощущать и чувствовать государственная публичная библиотека, архив документов? Какие человеческие возможности присущи манекену для одежды на витрине магазина?

Эти детские вопросы с очевидными ответами подводят к теме, отчего и зачем в наши дни сложные программно-аппаратные решения называют

«искусственным интеллектом». В том числе там, где наиболее точно звучит обозначение АСУ ТП — автоматизированные системы управления технологическими процессами.

ПРИВЕТ ИЗ СССР

Понятие «искусственного интеллекта» является философско-идеологической метафорой, маскирующей неприглядные социально-политические аспекты развития автоматизации технологических процессов с помощью программно-аппаратных средств. Современные концепции «искусственного интеллекта» ведут отсчёт с 1940–1950-х годов, включая дискуссии в СССР о кибернетике, которые разграничили, с одной стороны, действительный потенциал электронно-вычислительного и роботизированного оборудования, с другой — необоснованные претензии на создание технотронного «сверхчеловека».

Преднамеренное и невольное смешивание человека и машины, путаница понятий и терминов — черта глобального научно-технического мышления. Далеко не только в научной фантастике и массовой культуре, но также в философии и методологии науки, в нормативно-правовом регулировании вплоть до научно-исследовательских и опытно-конструкторских разработок. Остаётся размытым, неопределённым ответ на вопрос, в чём отличие людей друг от друга, от животных, от неодушевлённых предметов.

Манипуляции с понятием «интеллект» крайне обманчивы: человеческое мышление можно свести к одному из его узкоспециализированных проявлений. Если свести интеллект к навыку счёта или раскапыванию земли, его трудно «воспроизвести» и «победить» с помощью механических орудий. Тех же простых бухгалтерских счётов, не говоря о логарифмической линейке, арифмометре. Несомненно, что в выполнении вычислений, формализованных и алгоритмизированных операций электронно-вычислительные устройства более производительное орудие, чем человек. Точно так же, как экскаватор в выкапывании больших объёмов грунта заменяет сотни землекопов.

Многие действия человека можно выполнять с помощью инструментов,

орудий труда. Однако не все: человеку приходится выполнять как собственно человеческие, так и не обязательно свойственные ему функции. Критерием неотъемлемо человеческих действий служит невозможность их алгоритмизации, «неисчислимость».

Действия человека, которые можно формализовать, свести к набору заранее заданных правил, шаблонов, можно выполнять при помощи автоматизированного орудия труда — машины. Но и в этом случае действующим лицом остаётся человек — создатель и пользователь машины.

Самого человека можно свести к «говорящему орудию труда», так в Древнем мире называли рабов. Лбом можно забивать гвозди вместо молотка, кость выдержит; но не наоборот: молотком нельзя думать. Можно усовершенствовать компьютерные алгоритмы так, чтобы выигрывать партии в шахматы у чемпионов мира. Однако будущие гроссмейстеры смогут побеждать сегодняшние шахматные алгоритмы и базы данных; это извечное состязание щита и меча.

ИСПРАВЛЕНИЕ ИМЁН

Некритически перенесённые из-за рубежа в высшей степени неточные термины широко используются в национальных нормативных актах, начиная с самого высокого уровня. Например, в «Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года», утверждённой Правительством РФ Распоряжением от 19 августа 2020 г. № 2129-р.

Между тем в этой сфере называть вещи своими именами — значит говорить об автоматизированных системах управления технологическими процессами при помощи компьютерно-телекоммуникационных технологий. Называть это традиционное для отечественных научно-технических разработок направление «искусственным интеллектом» не только ошибочно, но и вредно.

Рациональное содержание «искусственного интеллекта» подразделяется на следующие направления автоматизации систем управления технологическими процессами.

1. Самообслуживание работы с базами данных (экспертные системы, поддержка принятия решений, перевод), включая возможности предварительной обработки (упорядочивания и «аналитики»).

2. «Оцифровка» и перекодировка в разные форматы чувственно воспринимаемых характеристик объектов (статических и динамических изображений; звуков и речи; формы, размеров и взаимного расположения; других физических параметров — температуры, влажности, свойств поверхности, упругости и т.п.).

3. Программирование и контроль работы роботизированных устройств, комплексов и систем.

4. Отдельная тема — внешний дизайн, «имитация», «человекообразность» робота в зависимости от исполнения: в объёме (металл и пластик), как изображения (статического или видео), в голосовом или текстовом исполнении ввода-вывода.

Путаница в понятиях, зачастую преднамеренная, снижает эффективность создания новых решений и облегчает ловлю рыбки в мутной воде. «Исправление имён» в ходе импортозамещения и цифровой суверенизации поможет повышению не только эффективности разработок и нормативно-правового регулирования, но и восприятию гражданской общественностью. Чтобы избежать самообмана, напрасной траты времени и ресурсов, разработчикам лучше использовать верный и однозначный понятийно-терминологический аппарат.

Очистка при помощи правильной методологии нормативной документации от вредоносных концептуальных «закладок» так называемого искусственного интеллекта поможет эффективной оптимизации нормативного технического и правового регулирования в России. «Исправление имён», коррекция двусмысленностей и ошибок в понятийно-терминологическом аппарате поможет эффективному развитию отечественных АСУ ТП, в том числе их конкурентному преимуществу на международных рынках.



Елена ПОКАТАЕВА
научный обозреватель BIS Journal

РАЗНЫЕ ГРАНИ ОДНОЙ МЕЧТЫ

КАК РАЗЛИЧАЮТСЯ ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И МАШИННОЕ ОБУЧЕНИЕ

70 с лишним лет развитие математических методов, объединяемых зонтичным понятием «искусственный интеллект», проходит практическую проверку на тесте Тьюринга. Похоже, пришло время его модернизировать.

Начало истории искусственного интеллекта (ИИ) связывают с публикацией в 1950 г. статьи английского математика Алана Тьюринга Computing Machinery and Intelligence, а также с

появлением теста его имени, призванного оценивать «интеллектуальность» мыслящих машин. Что такое тест Тьюринга? В переписке на естественном языке между человеком, компьютером и третьим участником — независимым арбитром — компьютер должен успешно выдать себя за человека. С тех пор огромные усилия математиков и специалистов в когнитивных науках были вложены в практическую реализацию тезиса «вести себя как человек».

И на этом пути регулярно встречаются точки завышенных ожиданий с последующими разочарованиями, за которыми следуют новые повороты в научных исследованиях.

ИИ: ЗНАНИЯ И ЛОГИКА МОГУТ ВСЁ

Летом 1956 г. во время знаменитого семинара в Дартмутском колледже четыре столпа ИИ — Джон Маккарти, Марвин Минский, Натаниэль Rochester и Клод Шеннон — решили в течение двух месяцев совместной работы в стиле мозгового штурма создать механизмы формализации интеллектуальной деятельности человека и воплотить на программном уровне распознавание текстов на естественном языке, формирование абстрактных понятий и концепций с тем, чтобы компьютер мог имитировать человека в сфере интеллектуальных действий. Поставленной цели они, конечно, не достигли, но положили начало практическим реализациям систем искусственного интеллекта в виде систем, основанных на знаниях и соответствующих правилах логического вывода (рис. 1).

Такой подход был понятен не только математикам, но и заказчикам ИИ-систем: это ведь фактически реализация метода Шерлока Холмса с его логическими рассуждениями на базе



Рисунок 1. База знаний в формализме семантической сети описывает происходящее в сказке

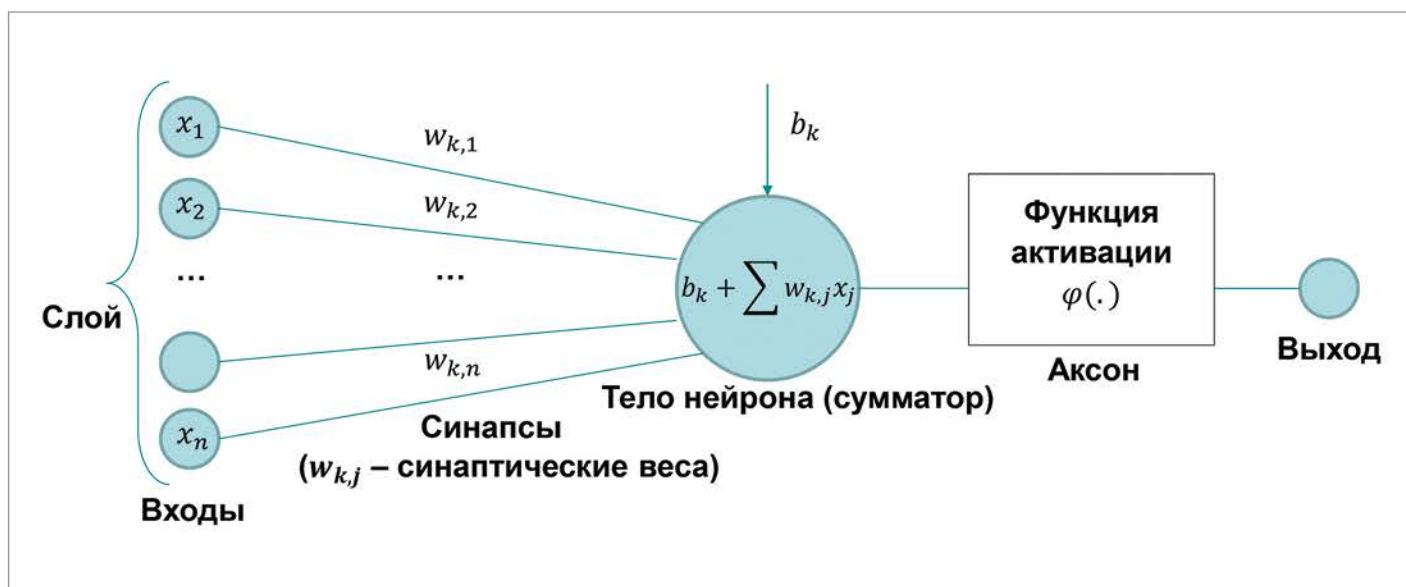


Рисунок 2. Схема обучения нейронов в классической схеме перцептрона Розенблатта. Источник: образовательный курс «Многослойные полностью связанные сети», Нижегородский государственный университет им. Н. И. Лобачевского, 2018 г.

доступных знаний о ситуации загадочного убийства, которые приводят в итоге к выявлению убийцы и всех обстоятельств криминального происшествия. Достаточно подробно описать все детали конкретной предметной области и отношения между её элементами, и можно находить неявные связи между объектами, определять действующих лиц и причины их поведения.

Первая волна завышенных ожиданий принесла с собой множество теоретических исследований и практических реализаций в области систем логического ИИ, но мечта о создании «мыслящей машины», имитирующей интеллект человека, так и осталась мечтой.

МАШИННОЕ ОБУЧЕНИЕ: ТАК ДУМАЕТ ЧЕЛОВЕК?

В 90-е годы прошлого века интерес исследователей сместился на машинное обучение: этому направлению работы с данными дали старт исследования американского учёного Фрэнка Розенблатта, впервые предложившего в 1957 г. модель перцептрона как упрощённую модель приобретения знаний живыми «познающими системами».

Она получила наибольшее распространение в задачах распознавания аудио и изображений. В первую очередь потому что именно там эффективно работает механизм отделения «похожих» и «непохожих» сущностей. Классическая задача тут — выбрать

фотографии с котиками из общей массы предъявленных фото, которые промаркированы с помощью двух пометок: «есть котик» или «нет котика».

В ходе обучения нейросети множество специально размеченных фотографий поступают на вход перцептрона. Это нейроны входной последовательности, над которыми совершаются математические действия с помощью специально подобранной функции активации. Её задача — обеспечить разделение всех данных на две группы: «есть котик» либо «нет котика», а потом на обученной сети рассчитать, к какой группе относится неизвестное фото (рис. 2).

В классическом варианте у перцептрона — один вспомогательный уровень. Однако уже сам Фрэнк Розенблатт изучал свойства перцептронной модели из трёх слоёв, добиваясь улучшения качества распознавания. Настоящий бум сегодняшнего дня наступил, когда

разработки исследователей в области многослойных нейронных сетей (то самое глубокое обучение, Deep Learning) объединились с возможностями современной вычислительной техники, позволяющей быстро обрабатывать мегабайты и даже терабайты данных.

МНОГОСЛОЙНАЯ НЕЙРОННАЯ СЕТЬ

Как из рога изобилия посыпались перспективные варианты DL-сетей, показывающие отличные результаты на задачах различного типа: сверточные сети и автокодировщики, рекуррентные сети, порождающие состязательные сети, обучение с подкреплением и т.д. Реальным прорывом в практическом использовании DL стало появление в 2018 г. моделей машинного обучения, ориентированных на задачи обработки текстов на естественном языке (NLP, Natural Language Processing), в первую очередь модель глубокого обучения BERT.

Первая волна завышенных ожиданий принесла с собой множество теоретических исследований и практических реализаций в области систем логического ИИ, но мечта о создании «мыслящей машины», имитирующей интеллект человека, так и осталась мечтой

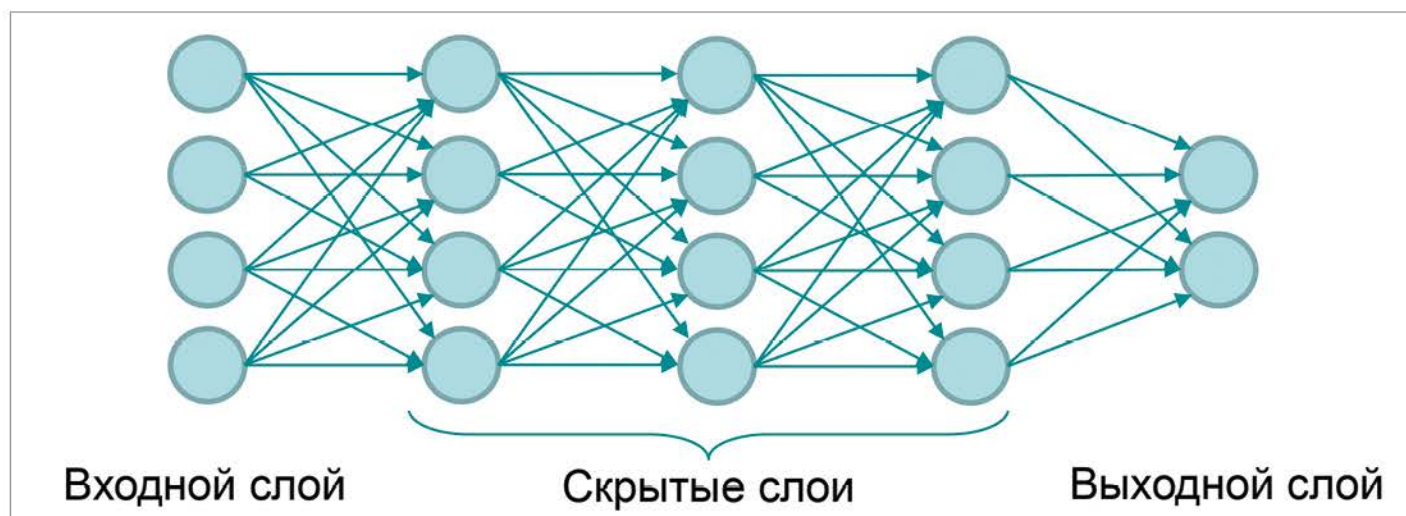


Рисунок 3. Схема многослойной нейронной сети

Дело в том, что к распознаванию ЕЯ-текста сводится большое количество задач, реализуемых на практике в ИТ-системах: от автоматического анализа неструктурированных документов до распознавания тематики в разговоре оператора контакт-центра с клиентом и автоматического перевода. И вдруг оказалось, что нейросети в практических задачах лучше справляются с задачей распознавания текстов, чем классические семантические конструкции типа семантической сети. Например, раньше исследователи полагали, что наилучший способ осуществления машинного перевода — использование языково-независимого представления текстового содержания в виде некоторой семантической схемы, но на практике этого не получилось. «Оказалось, что предложить единый семантический формализм для всего разнообразия текстов чрезвычайно трудно», — отмечает Наталья Лукашевич, профессор кафедры теоретической и прикладной лингвистики МГУ. Но повысить качество перевода удалось за счёт использования нейронной сети, которая преобразует последовательность на входном языке в последовательность слов на другом языке с помощью некоторой внутренней обработки (чистая вычислительная математика), которая вообще не поддается интерпретации.

На уровне поверхностных рассуждений получается, что нейросетевые модели обошли классический ИИ в решении задач, свойственных

человеческому интеллекту? Такой вывод подняли на щит маркетологи, устроившие хайп глубокого обучения такого уровня, что многие далёкие от математики люди стали всерьёз считать глубокое обучение единственным проявлением искусственного интеллекта.

МАЯТНИК КАЧНУЛСЯ В ОБРАТНУЮ СТОРОНУ

«Хотя современные модели машинного обучения и делают множество потрясающих вещей, постепенно превосходя человека во многих ранее недостижимых для компьютера областях, до «универсального чёрного ящика», который мог бы самостоятельно обучиться действовать в новой обстановке, как это делает человек, пока ещё очень, очень далеко. Несмотря на все успехи, у машинного обучения всё ещё впереди», — говорят авторы монографии «Глубокое обучение. Погружение в мир нейронных сетей» (С. Николенко, А. Кадушин, Е. Архангельская, Спб: Питер, 2019).

В целом книга развенчивает ключевой миф о глубоком обучении: о том, что на свалку истории можно отправить всё остальное, потому что для решения любой интеллектуальной задачи «...нужно просто придумать удачную архитектуру нейронной сети, начать обучать её градиентным спуском, и при достаточно большом датасете и достаточно мощной видеокарте всё получится». Нет, это не так. «Хотя сейчас революция глубокого обучения в самом разгаре и в этой науке расцветают все цветы, мы полагаем, что будущее — за

байесовскими методами и слиянием вероятностных моделей с нейронными сетями... В результате глубокие нейронные сети будут делать то, что они делают лучше всего: служить универсальными аппроксиматорами для очень сложных функций, и функции эти будут, например, плотностями интересующих нас распределений», — говорят авторы.

Иными словами, для математиков, работающих «на земле», работы непочатый край. И где в ней находит место тот самый пресловутый сильный AI? Пора признать, что это ещё одна давняя мечта человечества, которой не суждено сбыться. Системы ИИ не способны ничего самостоятельно «понимать» в том смысле, как это свойственно человеку. Они лишь моделируют решение конкретных задач, которые связаны с принятием тех или иных решений. И уже не столь важно, просматривается или нет конкретная цепочка логического вывода, если на практическом уровне механизм глубокого обучения даёт адекватный результат. Да, и семантическая сеть, если вдуматься, сама по себе ничего не «понимает». Так что в утиль надо сдать попытки имитировать человеческий интеллект в полном масштабе, согласившись с тем, что речь идёт о различных подходах к компьютерному моделированию его отдельных проявлений.

Ну а тест Тьюринга заменить более работоспособным механизмом классификации и сравнения моделей интеллектуальных систем.

DLP 2022

ФОРУМ



1 июня



Цифровое деловое
пространство

ПРОТИВОДЕЙСТВИЕ ВНУТРЕННИМ УГРОЗАМ КОРПОРАТИВНОЙ БЕЗОПАСНОСТИ

#dlpplus



ОРГАНИЗАТОР



Ростелеком
Соляр

ОПЕРАТОР



АВАНГАРД



Антон НЕЧИПОРЕНКО
начальник отдела информационной безопасности, СПАО «Ингосстрах»



Андрей ЭЛИ
начальник отдела контроля и анализа информации, СПАО «Ингосстрах»

ДУМАЙТЕ САМИ, РЕШАЙТЕ САМИ...

КАК УСИЛИТЬ ЗАЩИТУ, НЕ НАРУШИВ БИЗНЕС-ПРОЦЕССОВ

Начать мы хотели бы с ключевого совета, который был дан одним из топ-менеджеров: «Если вы чего-то не знаете, то это исключительно ваша проблема». Этот совет применим ко многим областям ИБ, но давайте рассмотрим его с позиции влияния средств защиты информации на бизнес-процессы. Данная статья будет интересна специалистам, которые недавно погрузились в вопросы информационной безопасности или имеют небольшой опыт работы.

ВЛИЯНИЕ СРЕДСТВ ИБ НА БИЗНЕС

В любом учебнике по ИБ можно найти описание ключевых параметров безопасности: доступность, целостность, конфиденциальность. Мы специально не будем рассматривать три дополнительных параметра из гексады Паркера, чтобы не усложнять статью. Итак, начнём. Если конфиденциальность и целостность в любой компании являются незыблемыми авторитетами, то в части доступности всегда будут прения с бизнесом, особенно если вы работаете в коммерческой организации. Бизнес всегда будет недоволен вводимыми ограничениями и всегда будет пытаться их обойти или снять. «Выложенная в интернет база со свободным доступом» всегда будет удобнее для бизнеса, чем использование построенных вами систем безопасного

доступа, и тут стоит искать здравый компромисс. При построении любой системы доступа к информации нужно изучать бизнес-процессы и оценивать влияние средств защиты на них.

ЗАЩИТА ВНЕШНЕГО ПЕРИМЕТРА И СЕО-ОПТИМИЗАЦИЯ

Возьмём известный всем процесс построения периметральной системы защиты для вашего интернет-ресурса, в первую очередь сайта компании. Чтобы защитить доступный из сети ресурс, понадобятся: Firewall (межсетевой экран), Web application firewall, IPS/IDS (системы предотвращения вторжения) и система защиты от DDoS (на канале провайдера или систем очистки трафика сторонней компанией).

А как это всё влияет на отклик сайта? И как отклик влияет на поисковый рейтинг? Если закрутить гайки проверок на этих средствах на максимум, то каждый пакет будет проверяться довольно долго, а значит, влияние окажется значительным. Давайте попробуем рассмотреть настройки IPS и как можно их подкрутить под изученный бизнес-процесс. Как известно, есть трафик пользовательский, а есть серверный, и для них существуют разные угрозы. Очевидно, если речь идёт про защиту сайта, это серверный трафик, а значит, постарайтесь сделать настройки средства защиты информации так, чтобы проверки пользовательского трафика на него не

распространялись. Вам незачем включать проверки, относящиеся к пользовательским рабочим станциям, угрозы для пользовательских операционных систем для вас неактуальны. Отключив проверки трафика для пользовательского сегмента, вы не уменьшите уровень защиты, но проверка трафика будет проходить в разы быстрее.

Допустим, у вас есть сервис получения различных файлов от клиентов, а проверку файлы проходят в песочнице. Постарайтесь понять, в каких процессах у вас участвует сбор информации от клиентов. Какая это информация? В каких форматах? Чем больше вы узнаете о сервисе, тем проще вам будет настроить профиль защиты, а главное, что у вас будет описание того, что проверяется и почему и что может проходить свободно без проверки. Добавьте к этому аргументы по минимизируемым рискам, и бизнес будет доволен.

Посмотрите на построенную вами систему защиту для предотвращения вторжения. Поговорите с владельцем бизнеса, и, может быть, у вас появятся преднастроенные правила, такие как превентивная блокировка трафика по геопозиции. Это позволит сделать собираемые сигнатуры более чистыми. Не вносите таких изменений без изучения процесса, иначе вы можете заблокировать валидный трафик, а значит, будет много жалоб на ваше средство защиты и зайдёт речь о том, что оно скорее мешает, чем помогает.

ПЕРЕХОД ОТ МОНИТОРИНГА К БЛОКИРОВАНИЮ

О превентивных способах защиты информации. В мире ИБ большинство компаний предпочитают использовать средства защиты информации как системы мониторинга. Таким образом, они не предотвращают внешние или внутренние угрозы, а разбирают уже совершившиеся инциденты и после пытаются «залатать» дыры. Указанный подход не должен применяться в среднем и крупном бизнесе, а также в государственных и муниципальных структурах.

Приведём несколько примеров обязательных блокировок. Утечка информации — одно из важнейших направлений. Сейчас мы живём в эпоху облачных технологий (хранение файлов, мессенджеры, почта и т.д.), ограничивать весь поток информации во внешний мир представляется невозможным, а на тонкие настройки могут уйти месяцы, в то время как ситуация может меняться каждые несколько дней. Необходимо ввести «ответственность за передачу»: если сотрудник отправляет информацию во внешний мир и система DLP выдаёт заключение об инциденте ИБ, сотруднику приходит ответное письмо, указывающее, что сотрудник, возможно, нарушает политику безопасности и должен подтвердить «уверен ли он, что хочет отправить файл».

Вы удивитесь, но результаты на нашем примере оказались следующими: за квартал до внедрения системы было порядка 200 инцидентов, после введения ограничений в первый месяц — около 40, а во второй и третий — всего несколько. Таким образом можно мягко помочь бизнесу понять, что ответственность за утечку данных носит индивидуальный характер и подтверждения отправки документов являются дополнительным мотиватором не совершать инциденты.

Конечно, придётся погрузиться и изучить несколько бизнес-процессов, а может быть, и внести в них коррективы, которые не отнимают времени и сил у представителей бизнес-подразделений, но серьёзно повышают уровень защищённости. Например, внедряя портал по обмену конфиденциальной информации с клиентами/партнёрами, интегрируйте его с SIEM, DLP, песочницей. Это не внесёт серьёзных корректив в

работу бизнеса, но позволит вам знать всё про движение информации и получать больше информации для расследований, а в дальнейшем и для построения правильных блокировок.

Внедрение систем управления ИТ-инфраструктурой (например, SCCM от Microsoft) позволит сотрудникам выбрать необходимое им ПО из разрешённого списка и в пару кликов установить необходимые инструменты для работы. Это позволит вам избежать ненужных загрузок из интернета и использовать уже предназначенные инструменты. Автоматическая классификация документов (файлов) позволит более точно контролировать движение значимой информации без участия пользователей. Система позволяет защитить документы как с юридической точки зрения (проставления грифов/меток), так и со стороны ИБ (шифрование, ограничение доступа и т.д.).

СЕГМЕНТАЦИЯ СЕТИ И ГРУППИРОВКА СЕРВИСОВ

Время — деньги. Сегментация сети — один из самых старых механизмов защиты внутренней сети. Есть примеры компаний с одним-единственным сегментом, а есть и те, у кого каждый узел — в своём сегменте. Любая сегментация будет вызывать аллергическую реакцию ИТ и бизнеса, если она не формализована и нет правил её использования. Постарайтесь посмотреть на сегментацию с точки зрения бизнеса.

Сколько времени у бизнеса занимает вывод нового сервиса в разделённой среде? Написание матриц доступов к нему? Консультаций с рабочими группами и т.п.? Если вы формализовали правила использования сегментов, то вывод нового сервиса в правильный сегмент займёт минимальное время. Старайтесь знать все процессы, которые существуют в компании, — это поможет сразу делать корректную сегментацию, а вновь появляющиеся системы и процессы должны лишь корректировать вашу модель. Правильно сгруппированные сервисы дадут возможность найти оптимальный баланс между требованиями ИБ и скоростью работы бизнеса.

Вообще, вопрос «группировки сервисов» намного более тяжёлый, чем кажется. Нужно очень хорошо отдавать себе отчёт, в каких процессах участвует сервис,

какие сервисы являются техническими/обслуживающими основной бизнес-процесс. Можно ли создавать маленькую экосистему вокруг одной бизнес-системы или проще разделить по техническим критериям. Здесь нет «таблетки от всех болезней», каждый случай будет уникальным. И так как ответа на вопрос «как правильно сегментировать сеть, чтобы защитить и не навредить?» не найти в интернете, то нужно на него ответить самому. Сможете придумать устраивающие вас критерии группировки — выделяйте сегмент. Не можете — дробите мельче, но всегда имейте единый план, понятный бизнес-заказчикам и ИТ.

ЗАКЛЮЧЕНИЕ: ВСЕГДА ДУМАЙТЕ И ПРОСЧИТЫВАЙТЕ

Мы постарались показать несколько примеров, не нарушающих бизнес-процессы компании. Очевидно, что в наше время развитие ИТ является важнейшим залогом ведения успешного бизнеса. Средства информационной безопасности влияют на множество вещей, начиная от простого доступа к сайту, заканчивая правилами, как работать за компьютером в офисе. Для многих не будет секретом, что другие подразделения «недолюбливают» подразделения безопасности, так как безопасность закрывает доступы, «мешая» работе или «пристают со своими рекомендациями и правилами». Ведь неверно настроенный межсетевой экран или система контроля доступа в интернет могут остановить работу всей компании.

К сожалению, множество наших коллег стараются следовать стандартам безопасности или указаниям регуляторов, не предлагая никаких альтернатив бизнесу. Подобное поведение заставляет сотрудников нарушать политики компании, «лишь бы выполнить» свою работу, за которую они получают деньги, а если сотрудник имеет процент от продаж, то его мотивация в нарушении политик безопасности увеличивается в разы. Выполняя свою работу, подумайте, как сделать так, чтобы собственноручно не подтолкнуть сотрудников к нарушениям.

А НЕ ПЕРЕБОР?

НЕОЖИДАННЫЕ ПОСЛЕДСТВИЯ ИЗБЫТОЧНОГО ИНФОРМИРОВАНИЯ



**Андрей
ЖАРКЕВИЧ**
редактор
ООО «Антифишинг»

Телефонные аферисты, опустошающие банковские счета граждан РФ, стали одной из самых громких проблем 2021 года. Федеральные и региональные СМИ непрерывным потоком освещали мошеннические инциденты, банки атаковали своих клиентов мощным валом оповещений по всем каналам взаимодействия от рассылок по электронной почте, СМС-предупреждений и посланий в мессенджерах до «историй» в банковских приложениях и всплывающих окон на сайтах онлайн-банкинга. Даже Банк России не остался в стороне и создал не только раздел об информационной безопасности на своём сайте, но и целый портал, посвящённый повышению финансовой грамотности и противодействию мошенникам.

Кажется, что после такого беспрецедентного многоканального информирования о мошенниках должны знать буквально все жители нашей страны. И не только знать, но и ни в коем случае не поддаваться на уловки. Однако, как показывает статистика, количество хищений средств с банковских карт и не думает уменьшаться. Так, например, «Альфа Страхование» сообщает, что в 2021 году 92% обращений по страховым событиям с банковскими картами пришлось на случаи несанкционированного доступа к счёту, причём больше половины из них были связаны с телефонным мошенничеством. А по данным МВД, ущерб от телефонного мошенничества в России за одиннадцать месяцев 2021 года составил 45 млрд рублей.

Напрашивается довольно неудобный вывод: слишком интенсивное информирование мешает решению проблемы? Разберёмся в возможных причинах такого явления.

При поступлении слишком большого количества данных включается фильтр восприятия. Сознание отсекает информацию, которую считает известной, поскольку её обработка уже не приносит практической пользы

ИНФОРМАЦИОННЫЙ ШУМ

Человеческое сознание устроено таким образом, что при поступлении слишком большого количества данных включается фильтр восприятия. Сознание отсекает информацию, которую считает известной, поскольку её обработка уже не приносит практической пользы.

Задача этого механизма — защитить человека от информационной усталости, которая возникает при обильных потоках входящей информации, перегружающих мышление.

Если провести параллель с компьютерными технологиями, интенсивное информирование напоминает распределённую атаку на отказ в обслуживании — DDoS. При таких атаках на целевой хост в интернете направляется поток входящих запросов от разных источников, обработка которых истощает ресурсы сервера, и его работа парализуется.

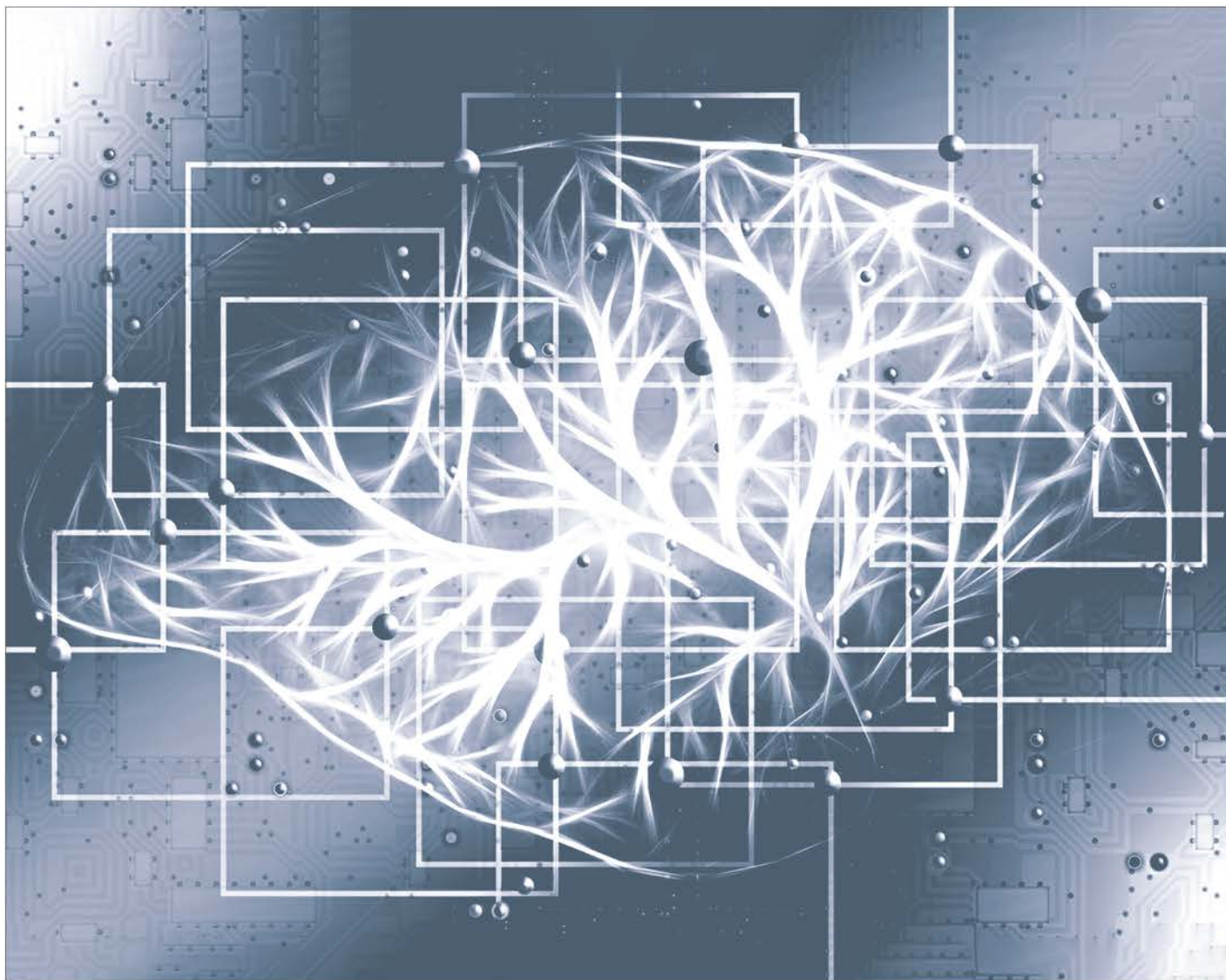
В случае с информированием человек точно так же получает входящие пакеты данных: плакат на улице, оповещение в банковском приложении, электронная рассылка, баннер в интернете, видео на YouTube и даже объявление в подъезде. И везде примерно одно и то же: не сообщайте код мошенникам, не переводите деньги, не нажимайте кнопку, перезвоните в банк...

Постепенно эта, в общем-то, важная и полезная информация превращается в информационный шум, который остаётся где-то за гранью восприятия. Примерно так сознание курильщиков отфильтровывает страшные картинки на пачках сигарет. Они существуют где-то в параллельной реальности, не поднимаясь на уровень осознания.

АНАЛИТИЧЕСКИЙ ПАРАЛИЧ

Банки, регулятор, правоохранительные органы и ИБ-компании стремятся максимально глубоко разобрать мошеннические сценарии, проанализировать и классифицировать их. Появляются обучающие курсы, видеоролики и буклеты, порталы и сервисы, посвящённые борьбе с мошенниками. Они содержат много полезной информации, и это опять порождает проблемы:

♦ далеко не все считают угрозу мошенников настолько важной для себя, чтобы специально выделять время на изучение способов защиты;



♦ решившие погрузиться в тему тонут в потоке достаточно сложных сведений, впадая в аналитический паралич.

Состояние аналитического паралича — это проблема, напрямую связанная с перегрузкой знаниями. Изучив несколько курсов о борьбе с мошенниками, человек пытается найти идеальное решение, но боится ошибиться. В результате выбор затягивается до тех пор, пока в конце концов его не делают на основе поспешного суждения или интуитивной реакции.

Приступ аналитического паралича приводит к тому, что страх выбрать неоптимальное решение отключает здравый смысл. Эта комбинация особенно опасна при реальных мошеннических инцидентах, поскольку все сценарии используют в качестве завязки удар по базовым эмоциям, который также отключает рациональное мышление.

Выведенный из равновесия звонком аферистов человек судорожно пытается вспомнить

правильную рекомендацию из пройденных курсов, но никак не может это сделать. Страх удваивается: к угрозе потерять деньги, о которой его известили мошенники, добавляется страх выбрать неправильную схему действий. Чаще всего в такой ситуации жертва позволяет убедить себя и теряет деньги.

ЭФФЕКТ СПЯЩЕГО НА СЛУЖБЕ МОШЕННИКОВ

Ещё одна проблема избыточного информирования связана с интересной особенностью психики, известной как эффект спящего. Смысл этого эффекта состоит в том, что, даже если человек в момент получения информации точно знает, что её источник не заслуживает доверия, с течением времени сведения об источнике забываются, а сама информация уже воспринимается как правдивая.

Рассмотрим, как это происходит в случае с мошенническими кампаниями. В качестве

Все усилия по проработке сценариев улучшают информированность не только потенциальных жертв, но и заказчиков банкета — мошенников

примера возьмём известную многоходовку с «преступниками из банка».

В этой схеме мошенники используют довольно распространённое среди граждан РФ недоверие к банкам, которое подпитывается многочисленными роликами и статьями в стиле «как меня обманули в отделении банка Х». Даже после разъяснений и опровержений этих эпизодов у людей остаётся стойкое убеждение, что мошенники в банках встречаются довольно часто. А информирование о реальных мошеннических инцидентах окончательно закрепляет ассоциацию.

На этом фоне звонок от «сотрудника безопасности», который просит помочь поймать мошенника из банка, попадает на благодатную почву. Жертва с готовностью соглашается прийти в офис банка, оформить кредит и перевести деньги на «спецсчёт в ЦБ», чтобы вывести неблагонадёжного банкира на чистую воду. И разумеется, не верит настоящим сотрудникам банка, которые пытаются отговорить клиента от странных действий.

ШПАРГАЛКА ДЛЯ АФЕРИСТОВ

Организаторы мошеннических кампаний изучают рекомендации по борьбе с собой даже более внимательно, чем потенциальные жертвы. Появление методик для борьбы с самыми эффективными сценариями обмана — повод для разработки новых.

Например, после того как в инфополе стали массово говорить о том, что нельзя сообщать по телефону код, поступивший в СМС, вежливых собеседников с южно-российским акцентом сменил «робот-помощник ВТБ», который вежливо предлагал ввести поступивший код на клавиатуре телефона. Отсутствие «живого» собеседника, который требовал назвать код, сработало: многие поддались обаянию электронного мошенника и потеряли деньги.

Когда примитивная схема со «службой безопасности банка» была разобрана буквально во всех СМИ, мошеннические сценаристы разработали многоходовку, которые начинаются со звонка представителя силовых ведомств. Поскольку все эксперты рекомендовали «не доверять и проверять», «силовик» представлял фамилией и именем реального сотрудника

органов и даже сам предлагал проверить свою подлинность на сайте.

Таким образом, все усилия по проработке сценариев улучшают информированность не только потенциальных жертв, но и заказчиков банкета — мошенников, которые используют эти сведения для совершенствования имеющихся и создания новых способов обмана.

В контексте «информационной помощи» мошенникам стоит упомянуть ещё один источник их «всемогущества» — украденные из банков и других организаций базы данных, содержащие сведения о клиентах, паспортные данные, номера телефонов и даже остатки по счетам. Обо всех таких утечках оперативно сообщают профильные СМИ, что позволяет приобретать «свежие базы» на киберпреступных форумах сразу после публикации предложений.

КАК ЗАЩИТИТЬ ЛЮДЕЙ

Складывается довольно непростая ситуация: с одной стороны, информирование граждан о мошенниках и способах противодействия необходимо, с другой — способно нанести реальный вред, если проводится слишком интенсивно.

Для решения проблемы всем заинтересованным сторонам необходимо объединить усилия, привлечь экспертов из ИБ-компаний, психологов и специалистов по социальной инженерии, чтобы разработать единые стандарты информирования и последовательно реализовывать их, не превращая важные сведения в информационный шум.

Разумеется, одного информирования недостаточно. Чтобы научить людей вести себя безопасно, правильно действовать в потенциально проблемных ситуациях, необходимо добавить к информированию адекватную систему тренировки навыков. Способы реализации такой системы могут быть самые разные — от онлайн-тренажеров и приложений для смартфонов до телеграм-ботов или даже телефонных имитированных атак, максимально приближённых к реальным.

И ещё одна, безусловно, необходимая мера для ликвидации массового телефонного мошенничества — это последовательная борьба с утечками данных о банковских счетах граждан. Если не решить эту проблему, то мошенники будут продолжать свою преступную деятельность, и остановить их с большой вероятностью не поможет ни блокировка подмены номеров, ни требование дополнительного подтверждения при переводе денег.

ВЫШЛИ НА МЕЖДУНАРОДНЫЙ УРОВЕНЬ!

ЗАВЕРШИЛСЯ ФИНАЛ V ЮБИЛЕЙНОГО КЕЙС-ЧЕМПИОНАТА
ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ RISC

В марте состоялся финал пятого — юбилейного — кейс-чемпионата по информационной безопасности RISC, прошедший полностью в онлайн-формате. По традиции конкурсные задания участников оценивали руководители служб ИБ крупнейших российских и международных компаний.

Кейс-чемпионат по ИБ RISC — состязание для студентов и аспирантов в формате ситуационного анализа. Участникам предлагается исследовать ситуацию, разобраться в сути проблем и предложить решения за ограниченное время. Уникальность мероприятия в том, что кейсы для него составляют и проверяют действующие директора по ИБ крупных российских и международных компаний. Это помогает достичь главной цели — сформировать у будущих специалистов по ИБ практические навыки и опыт решения реальных управленческих задач.

В ходе V кейс-чемпионата команды решали два кейса. В рамках первого из них необходимо было расследовать инцидент ИБ на крупнейшем в регионе предприятии топливно-энергетического сектора. Второе задание было посвящено усилению защиты ИТ-инфраструктуры страховой компании, которая за последний месяц неоднократно подвергалась фишинговым атакам со стороны внешних злоумышленников.

ПОБЕДИТЕЛИ

Первое место в конкурсе заняла команда «Рост» из Сибирского государственного университета науки и технологий им. академика М. Ф. Решетнева (Красноярск, Россия). Второе место — у команды LAMERS из Иркутского национального исследовательского технического университета (Иркутск, Россия). Третье место заняла команда Kryptonite из Евразийского национального университета имени Л. Н. Гумилёва (Нур-Султан, Казахстан).

В конкурсе капитанов победителем стала Варвара Палагутина, капитан команды «Системщики» — Балтийский федеральный университет имени Иммануила Канта (Калининград, Россия).

МЕЖДУНАРОДНЫЙ УРОВЕНЬ

Призёры конкурса отметили интересный формат заданий, который помог им раскрыть практические навыки и знания. По мнению участников, по качеству и масштабу мероприятие, безусловно, достигло международного уровня. В первом отборочном туре приняла участие 131 команда из четырёх стран (Россия, Беларусь, Казахстан, Киргизия) и 25 городов. Шесть команд дошли до финала.

ЖЮРИ И ПАРТНЁРЫ

Победители кейс-чемпионата были награждены почётными кубками и меда-

лями, а также призами от организаторов и партнёров конкурса. Ассоциация RISC выражает огромную признательность всем членам жюри, ведущему конкурса, а также спонсорам и партнёрам проекта — компаниям BI.ZONE, Альтирикс Групп, Deiteriy, TerraLink, RTM Group — за доверие и поддержку V юбилейного кейс-чемпионата по ИБ RISC.

Рустэм Хайретдинов, директор по росту компании BI.ZONE:

— Не первый год участвую в этом чемпионате и с радостью отмечаю рост по всем направлениям: количеству участвующих команд, расширению географии, качеству подготовки соревнующихся и актуальности кейсов. Молодцы все — и студенческие команды, и профессиональное жюри, и, конечно, энтузиасты-организаторы.

Лев Шумский, член жюри, CSO Yandex Bank:

— Не скрою, в этом году судить было сложнее, поскольку команды, вышедшие в финал, были примерно одного уровня, и члены жюри разошлись в своих оценках. Своим уровнем удивили ребята из Казахстана: несмотря на то что это студенты 1–2-го курса, они обладают серьёзным практическим опытом! Желаю участникам и организаторам нескончаемого позитива и по-настоящему весеннего настроения. До встречи на VI кейс-чемпионате по ИБ RISC!

ОБ ОРГАНИЗАТОРЕ

Russian Information Security Club (RISC) — некоммерческая ассоциация специалистов по информационной безопасности, основанная в мае 2014 года. RISC работает в нескольких форматах — проведение очных семинаров на различные актуальные темы по информационной безопасности; организация и проведение очных и онлайн-мастер-классов с известными экспертами; выпуск различных методических документов, подготовка экспертных материалов и аналитических отчётов, основанных исключительно на практике работы в области информационной безопасности.



Марина БРОДСКАЯ
обозреватель BIS Journal

ПРИЁМНАЯ КАМПАНИЯ — 2022

В СФЕРЕ ИБ НЕГАТИВНЫЕ ТЕНДЕНЦИИ ОЧЕВИДНЫ

В российских вузах станет больше бюджетных мест, понизится проходной балл, а победителям олимпиад придётся сразу выбирать будущую специальность. Об этих и других новшествах в Правилах поступления — в данной статье.

НОВЫЙ ГОД — НОВЫЙ ПОРЯДОК

В «Порядок приёма на обучение по образовательным программам высшего образования» (утверждён приказом от 21.08.20 № 1076) внесены изменения, которые начали действовать с 1 марта 2022 г. Ожидается, что они продержатся до 1 сентября 2027 г.

Согласно новой редакции, вторая волна приёма, отказ от которой в 2021 г. стал причиной многих проблем с поступлением у абитуриентов, не вернётся.

Уточнён п. 18 Правил, который уточнил, что при наличии нескольких оценок ЕГЭ по одному и тому же предмету (но за разные годы) вуз автоматически учитывает наивысший по баллам результат, «но не менее установленного минимального количества баллов, в соответствии с установленными на основании пунктов 15–17.1 Порядка перечнем и формой вступительных испытаний».

Выпускники на базе среднего общего образования (после 11-го класса) потеряли возможность поступления в университеты без ЕГЭ, по итогам вступительного экзамена. Вступительные

испытания становятся всего лишь дополнительными баллами к баллам ЕГЭ.

Для выпускников колледжей с дипломами о среднем специальном образовании (СПО) возможность учесть либо ЕГЭ, либо вступительные испытания, проводимые вузом, сохраняется. Как при этом учитываются максимальные баллы при наличии и результатов ЕГЭ, и диплома СПО, не уточняется. Как и раньше, порядок поступления вуз определяет самостоятельно. Он может установить, что формой вступительного испытания на базе СПО является ЕГЭ, и не проводить свои вступительные экзамены, а может провести внутренние экзамены с учётом профиля образовательных программ СПО, родственных программам бакалавриата или специалитета, на которые ведётся приём.

Ограничили в возможностях и победителей олимпиад. По новым правилам они имеют право на приём без вступительных испытаний только в один вуз и только на одну образовательную программу по выбору поступающего (вне зависимости от количества оснований, обуславливающих соответствующее особое право). Списки олимпиад и конкурсов, дающих дополнительные баллы, а также особые права описаны в Порядке приёма, утверждённом министерством, и регулируются правилами приёма вуза.

Уточнён порядок целевого приёма. На места в пределах целевой квоты по общему правилу проводится

однопрофильный конкурс. В случае если целевая квота не детализирована, возможно провести многопрофильный конкурс, предварительно распределив контрольные цифры приёма между специальностями или направлениями подготовки. В противном случае абитуриент участвует в конкурсе по одной детализированной квоте по конкретной специальности или направлению подготовки.

Изменена и процедура приёма. В 2022 г. будут действительны результаты ЕГЭ 2018–2022 гг.

Сроки основного этапа зачисления пройдут с 3 по 9 августа.

Предусмотрены три способа подачи документов: дистанционная в электронной форме, очная и почтовая. Вуз обязан предоставить абитуриентам возможность подавать документы всеми тремя способами.

По-прежнему можно подать документы только в пять вузов. Университеты самостоятельно устанавливают максимальное количество специальностей и направлений подготовки, по которым абитуриент сможет участвовать в конкурсе, таких направлений может быть от 2 до 10.

В некоторых университетах могут потребовать медицинскую справку 086/у, что должно быть указано в перечне документов на официальном сайте вуза.

Победители школьных олимпиад могут подать заявление о поступлении без вступительных испытаний только

в один вуз только на одну образовательную программу по своему выбору. Спортивные достижения учитываются только при поступлении на профильные направления обучения. Каждый вуз устанавливает собственные правила учёта индивидуальных достижений абитуриентов.

Изменились и сроки подачи документов и зачисления.

Не позднее 20 июня 2022 г. начнётся приём заявлений и документов у абитуриентов.

27 июля будут опубликованы конкурсные списки.

28 июля завершится приём заявлений о согласии на приоритетное зачисление, 30 июля должны быть изданы приказы о приоритетном зачислении.

До 3 августа осуществляется приём заявлений о согласии на основное зачисление. И 9 августа должны быть изданы приказы об основном зачислении.

При наличии вакантных мест, в том числе бюджетных, вуз может объявить дополнительный набор абитуриентов.

БЮДЖЕТНИКОВ СТАНЕТ БОЛЬШЕ

В 2022 году более 580 тысяч человек смогут поступить в вузы РФ на бюджетные места, заявил вице-премьер РФ Дмитрий Чернышенко на пресс-конференции в ТАСС, которая прошла в январе 2022 г. Это на 11,5 тыс. мест больше, чем было в предыдущую приёмную кампанию.

Число бюджетных мест увеличивается ежегодно. При формировании контрольных цифр приёма учитываются запросы рынка, показатели государственных программ, проектов и потребности регионов в профессиональных кадрах. Важно, чтобы студенты могли получить доступное и качественное образование в своём регионе и в нём же продолжили трудовую деятельность, считают в правительстве.

По количеству бюджетных мест в лидерах, помимо Москвы, Санкт-Петербурга и Ленинградской области, оказались Свердловская, Ростовская, Новосибирская области, Республика Татарстан, где располагаются крупные инновационные, промышленные, научные центры страны.

На 2023/24 учебный год планирует распределить между вузами уже свыше 590 тыс. бюджетных мест.

Увеличение числа бюджетных мест на 2022/23 учебный год затронет и магистратуры, и аспирантуры. Во второй половине марта 2022 г. глава Министерства образования и науки РФ Валерий Фальков отметил, что «в этом году было выделено 17,5 тысячи аспирантских мест против прошлогодних 16,5 тысячи». Этот шаг позволит повысить качество подготовки научных кадров.

«Замысел состоит в том, чтобы были исследовательские магистратуры и чтобы дать места вузам, где есть возможность предложить своеобразные предтечи аспирантуры», — заявил Валерий Фальков на сессии все-российского форума «Педагогическое образование в российском классическом университете», который прошёл 18 марта 2022 г.

При этом министр отметил низкие цифры по итогам окончания аспирантуры — 5–8%. «К сожалению, это всё следствие сложных лет и инерция, которую наследовали, когда учёная степень, учёное звание были модным аксессуаром», — считает Фальков.

Вопрос о выделении дополнительных мест окончательно не решён, решение должно быть оформлено в течение ближайших двух недель, уточнял ТАСС.

ПРОХОДНОЙ БАЛЛ СНИЖАЕТСЯ

Специалисты НИУ ВШЭ зафиксировали снижение среднего проходного балла ЕГЭ для поступления на бюджетные места на очную форму обучения в российских вузах. «Средний балл поступления в вузы постоянно повышался с 2010 г. Максимальный балл был зафиксирован в 2020 г. и составил 70,8. В 2015 г. он составлял 66,1. В 2021 году проходной балл впервые снизился и составил 70,3 против 70,8 по бюджетным местам и 68,6 (68,7) по совокупному приёму», — говорится в исследовании НИУ ВШЭ. Это объясняется значительным увеличением числа бюджетных мест на очную форму обучения в региональных вузах.

При расчёте баллов не учитывалась статистика по творческим и военным

вузам, где итоги Единого государственного экзамена не являются ключевыми параметрами.

По статистике самих региональных высших учебных заведений, в прошлом году наблюдалось снижение проходных баллов от 1 до 12%. Снижение зафиксировали и в некоторых федеральных университетах. Это позволило большему числу абитуриентов со средними баллами по ЕГЭ поступить в университеты.

ВЫПУСКНИКИ ИТ-СПЕЦИАЛЬНОСТЕЙ ПОЛУЧАТ ЛЬГОТЫ

В рамках поддержки ИТ-отрасли на фоне санкционных ограничений, введённых на фоне специальной военной операции на Украине, Правительство РФ ввело налоговые льготы для отечественных компаний.

«На три года все ИТ-компании будут освобождены от уплаты налога на прибыль и от проверок контрольными органами, они смогут на выгодных условиях взять кредиты на продолжение работы и новые проекты по ставке, не превышающей 3%», — заявил глава правительства Михаил Мишустин на заседании кабинета министров, передаёт ТАСС.

Важно не допустить снижения темпов развития ИТ-отрасли в нашей стране, заявил премьер-министр. Поэтому правительство предоставит сотрудникам таких компаний возможность оформить льготную ипотеку, а специалисты до достижения ими возраста 27 лет получат отсрочку от призыва на военную службу на время их работы в российских ИТ-компаниях.

В ВУЗЫ БЕЗ ЭКЗАМЕНОВ

В 2022 г. абитуриенты из Донецкой и Луганской народных республик (ДНР и ЛНР) смогут поступать в российские вузы по квотам для иностранных студентов, пройдя лишь собеседование. Экзамены, как остальным иностранным студентам, им сдавать не придётся.

Сейчас большого потока обращений с вопросами о переводе в российские вузы от студентов из ДНР и ЛНР не наблюдается, сообщает ТАСС со ссылкой на источники в Минобрнауки.

Специальность	2022		2021		2020		2019		2018		2017		2016	
	б	пл	б	пл	б	пл	б	пл	б	пл	б	пл	б	пл
10.03.01	34	266	48	198	62	256	40	224	40	184	36	156	24	62
10.05.01	60	150	60	128	77	85	70	78	70	70	70	119	70	63
10.05.02	60	150	60	23	72	79	70	58	70	68	70	127	60	66
10.05.03	60	150	60	40	72	60	70	86	70	59	60	57	25	16
10.05.04	44	76	39	20	43	52	30	52	35	44	30	26	25	19
10.05.05	43	77	39	37	42	55	25	80	35	59	30	51	20	24
Итого	301	869	306	446	368	587	305	578	320	484	296	536	224	250

Таблица 1. Статистика приёма в МИРЭА на специальности в сфере ИБ (б — число абитуриентов, зачисленных на бюджет, пл — на платные места)

В 2022–2023 г. в российских вузах появятся 5 тыс. мест для иностранцев. В общей сложности в рамках предоставления квот будет создано 23 тыс. мест для обучения иностранцев. По данным ведомства, в приёмной кампании 2021/22 учебного года наибольшее количество заявок поступило из Китая, Вьетнама, Таджикистана, Узбекистана и Афганистана.

В начале марта на ректорском совещании проректор Санкт-Петербургского государственного университета (СПбГУ) Александр Бабич предложил зачислять в вуз без вступительных экзаменов участников военной операции на Украине. Эта идея была поддержана всеми участниками совещания. Соответствующее обращение было направлено министру науки и высшего образования Валерию Фалькову.

Новая редакция Порядка закрепила возможность приёма граждан Беларуси на основании результатов проводимого в их стране централизованного тестирования. Эти результаты приравниваются к результатам ЕГЭ, если абитуриент не сдавал таковой. Важно, чтобы результаты тестирования были не старше 1 года. Порядок признания результатов белорусского централизованного тестирования в качестве результатов общеобразовательных вступительных испытаний вуз устанавливает сам.

О НАБОЛЕВШЕМ

Несмотря на растущую потребность в молодых кадрах на фоне непрекращающегося

роста кибератак, запрос в поисковике на тему «в университете открылась новая специальность по направлению информационная безопасность» выдаёт только старые новости: университеты не хотят расширять имеющийся набор специальностей. Ведущие обучение по направлениям бакалавриата (10.03.00) и специалитета (10.05.00) университеты, как кажется, сохраняют контрольные числа приёма на прошлогоднем уровне и даже незначительно увеличивают число бюджетных мест за счёт внутреннего перераспределения ресурсов. Эти места, по опыту предыдущих лет, в основном заполняются медалистами, победителями олимпиад и поступающими по квотам. Желающих учиться на платных местах тоже достаточно. Однако, сделав сводную таблицу по итогам прошлых лет с учётом планов на нынешний год, можно увидеть другую картину. Например, изучим статистику приёма МИРЭА (таблица 1), где открыто большинство из интересующих нас специальностей по ИБ (информация взята с официального сайта университета).

Из таблицы видно, что пик интереса к специальностям 10.00.00 «Информационная безопасность» как со стороны руководства, так и абитуриентов, пришёлся на 2020 г. И, несмотря на солидные цифры приёма на 1-м курсе, уже на 3-м курсе на специальности 10.05.01 есть 8 вакантных бюджетных мест, а на 4-м и 5-м таких мест уже по 12 (данные приведены на сайте учебного заведения по состоянию на март

2022 г.). Учитывая, что всегда есть возможность перейти с платного отделения на бюджет, можно предположить, что желающих по тем или иным причинам не нашлось. И в очередной раз отметим, что контрольных цифр выпуска ни один из университетов, и МИРЭА в том числе, не даёт.

Из негативных тенденций, которые можно ожидать в этом и последующих годах, — снижение числа платных студентов. Это связано и с ростом стоимости обучения (до 490 тыс. руб. в ВШЭ), и с негативными тенденциями в экономике и на рынке труда, где намечается сокращение работающих в связи с массовым уходом из России иностранных компаний. Ряд университетов уже несколько лет подряд держит цены на одном уровне, а кто-то даже незначительно снизил цену за обучение, но тенденция очевидна даже на примере МИРЭА. Число принятых на платной основе в 2021 г. снизилось примерно на 25 % по сравнению с 2020 г. А экономический кризис вынудит многих поднять цену за образование.

Конечно, можно ожидать перераспределения высококвалифицированных специалистов в области ИБ, покинувших старые места работы в иностранных компаниях, ушедших из России, и их перехода на новые должности. Однако кадровый голод в целом внутренняя миграция работников не решит.

БУДУЩЕЕ КИБЕРБЕЗОПАСНОСТИ — ЗА ЖЕНЩИНАМИ!

ТАК СЧИТАЮТ ПРОФЕССИОНАЛЬНЫЕ
СООБЩЕСТВА СТРАН АФРИКИ И АЗИАТСКО-
ТИХООКЕАНСКОГО БАССЕЙНА

CYBERGIRLS FELLOWSHIP

В конце февраля 2022 г. завершился приём документов на программу кибербезопасности CyberGirls Fellowship для девушек и женщин 18–28 лет, проживающих в Нигерии, Гане, Руанде, Египте, Замбии и ЮАР. CyberGirls Fellowship — годовая программа фонда CyberSafe Foundation, в рамках которой молодые женщины с опытом работы в ИТ или без такового приобретают навыки работы в области кибербезопасности. Предпочтение при отборе отдаётся выпускницам школ или магистратуры, в процессе обучения всем участницам выплачивается стипендия. Навыки работы в сфере кибербезопасности позволят жительницам Чёрного континента начать карьеру в области ИБ как на родине, так и по всему миру. Программа CyberGirls направлена на реализацию таких целей устойчивого развития, провозглашённых ООН, как ликвидация бедности, доступное образование, уменьшение гендерного неравенства.

Инициатива Фонда направлена на борьбу с киберпреступностью, нехваткой навыков в сфере кибербезопасности и гендерным неравенством в технологических отраслях. Сначала стипендиаты CyberGirls познакомятся с основами работы в сфере ИТ и кибербезопасности, узнают о возможностях карьерного роста в области ИБ. А после выбора направления обучения в сфере кибербезопасности получат теоретические и практические знания по выбранной специализации при поддержке наставников. Итогом обучения станет прохождение сертификации,

возможность получения оплачиваемой стажировки или трудоустройства по полученной специальности на должностях начального уровня. Проект реализуется CyberSafe Foundation при помощи благотворительных организаций и заинтересованных в получении квалифицированных кадров компаний-партнёров.

CyberSafe Foundation — ведущая африканская неправительственная организация в области цифрового развития. Её миссия — содействие изменениям, обеспечивающим инклюзивный и безопасный цифровой доступ в Африке. Фонд работает над повышением инклюзивности и безопасности использования цифровых технологий в Африке, особенно среди наиболее уязвимых слоёв общества. Так, с помощью программ Фонда повысили квалификацию сотрудников малых и средних предприятий в Нигерии; совместно с правительством Великобритании был запущен проект DigiGirls, который расширяет возможности женщин и девушек в возрасте от 15 до 40 лет, имеющих навыки работы с цифровыми технологиями. Также Фонд запустил кампанию по повышению осведомлённости о кибербезопасности, охватившую более 10 млн человек по всей Африке.

НАМИБИЙСКИЕ ХАКЕРЫ УЙДУТ НА ПОКОЙ

Сетевая академия компании Check Point Software Technologies, ведущего мирового поставщика решений для кибербезопасности, совместно с факультетом вычислительной техники и информатики Университета науки и технологий Намибии, компаниями

Salt Essential IT и Complete Enterprise Solutions (CES) решают проблему нехватки специалистов по кибербезопасности в этой африканской стране.

В рамках сотрудничества преподаватели университета пройдут курсы повышения квалификации по программе Check Point Certified Security Administrator, что позволит им начать преподавать ИБ студентам уже с нового учебного года. Помощь в подготовке новых программ будут оказывать все партнёры. Также планируется, что CES и Salt Essential IT как создадут возможности интегрированного обучения студентов, так и предоставят места для стажировок.

Координатор программы со стороны университета Мерси Читауро считает, что благодаря такому сотрудничеству происходит укрепление кибербезопасности в Африке. Лекторы будут передавать полученные ими кибернавыки новому поколению профессионалов. В свою очередь, представители ИТ компаний-партнёров университета отмечают, что работа Сетевой академии Check Point в Намибии — это важный шаг вперёд в воспитании кадрового резерва специалистов по ИБ, развитие устойчивой питательной среды для кадрового резерва в стране.

СТАРТОВЫЙ ПРЫЖОК

Сотрудничество намибийского университета и Сетевой академии Check Point расширяет возможности и другой программы Check Point — Cyber Security Jump Start. По этой программе учащиеся могут получить доступ к бесплатным онлайн-курсам из любой точки



мира, сдать по окончании экзамен и получить соответствующий сертификат. Курсы уже прошли более 20 тыс. студентов и специалистов по ИБ в Африке, повысив тем самым общий уровень кибербезопасности в Африке.

Панкадж Бхула, региональный директор по Африке в Check Point Software Technologies, отмечает стремление компании сделать образование в области кибербезопасности доступным для всех. В условиях кадрового дефицита и нехватки навыков по ИБ важно воспитать как можно больше профессионалов. Задача компании — повысить уровень специалистов не только в Намибии, но и по всему континенту, учитывая, что киберпреступность здесь находится на рекордно высоком уровне. Компании Намибии сталкиваются

с киберугрозами на 49% чаще, чем в среднем по миру.

ВОСХОД КИБЕРФЕМИНИЗМА

В Африке ширится движение, выступающее за ликвидацию гендерного неравенства и равный доступ к цифровым технологиям для мужчин и женщин.

Как философское течение киберфеминизм признаёт различия во власти между мужчинами и женщинами, особенно в отношении цифрового дискурса, и считает необходимым ликвидировать эти различия. Как общественное движение киберфеминизм сосредоточен на расширении прав и возможностей женщин. Это важно, учитывая, что африканские женщины заведомо подвержены риску в цифровом пространстве,

поскольку не овладели всеми навыками работы в интернете.

«У женщин не так много возможностей изучить потенциал цифровых технологий, особенно в Африке, — считает Анна Коллард, старший вице-президент компании KnowBe4 Africa. — Мир переходит на цифру, а женщины рискуют остаться в традиционно женских профессиях. Эта динамика должна измениться».

Женщины привносят неповторимый колорит в любую бизнес-среду. Их участие может коренным образом изменить инновационные процессы, считают сторонники киберфеминизма.

Однако жизнь пока противоречит тенденциям. Исследование Международного союза электросвязи показало, что женщины в Африке пользуются Интернетом значительно реже, чем мужчины. Одной из причин разрыва остаются установки и нормы, увековеченные патриархальным обществом. Это проявляется во всех сферах: от здравоохранения до занятости. Мужчины довлеют над женщинами и часто контролируют сайты, к которым должен получить доступ и слабый пол.

Опрос, проведённый KnowBe4 в 2020 году, показал, что цифровая грамотность и образование в области ИБ у населения в целом отсутствуют: 62% респондентов указали, что департаменты ИБ в их организациях недоукомплектованы, 57% — о кадровом голоде. 61% ответивших считают, что менее половины из всех претендентов на вакансии в области кибербезопасности подходят для этой работы. Только 3,7% опрошенных африканских учителей сказали, что они предлагают кибербезопасность как предмет для изучения.

При этом потребности в специалистах по ИБ на африканском континенте огромны. По данным на 2020 г., были заняты порядка 10 тыс. вакансий, ещё больше были свободны. Например, в Кении, где требуется порядка 1700 специалистов в области кибербезопасности, ежегодно готовят всего 100. И если в мире порядка 20% специалистов по ИБ — женщины, в Африке их не больше 9%. Только 1% женщин, работающих в отрасли, достигают позиций высшего менеджмента.

«Нужно изменить границы, изменить восприятие и принять идею киберфеминизма, — считает Коллард. — Мы должны сосредоточить усилия как отдельных лиц, так и организаций на укреплении прав женщин, на внедрении инноваций в цифровую грамотность и образование в области ИТ, обеспечении доступа к интернету для всех. Необходима национальная политика гендерного равенства в области информационно-коммуникационных технологий».

ИИ — ОН И В АФРИКЕ ИИ

Компании Codecademy и Black and Brilliant запускают программу изучения искусственного интеллекта в Африке. Эта программа предоставит африканским специалистам возможности обучения и практики в области ИИ в ведущих технологических компаниях мира. Полученный опыт африканцы смогут применить при внедрении инновационных технологий в своих регионах. Таким образом, планируется расширить возможности для привлечения и обучения новых кадров на континенте.

Сочетая повышение квалификации и наставничество, программы Codecademy и Black and Brilliant сосредоточатся на навыках, необходимых для построения успешной карьеры в области ИИ. За 10 учебных недель участники программы получают знания в сфере науки о данных и инженерии данных, научатся программировать с использованием платформы практического обучения Codecademy. Участники будут работать с группой преподавателей и наставников из компаний Shopify, Google и Etsy.

ИЩИТЕ ЖЕНЩИНУ!

Мир становится всё более цифровым, угроза киберпреступности — всё более очевидной. Только в 2020 году мировые потери бизнеса из-за цифровых угроз составили \$1 трлн 57% организаций на планете жалуются на нехватку кадров, глобальная потребность в специалистах по ИБ оценивается в 3,5 млн человек. Сегодня в отрасли работают 4,4 млн человек, таким образом, надо найти источники роста на 80%. «Где взять столько специалистов?» — задаётся вопросом аналитик Boston Consulting Group из Сингапура Шугер Чан.

Один из ключевых способов вырастить талантливую смену — привлекать и стимулировать интерес к профессиональной сфере с раннего возраста с помощью наставничества, знакомства и возможностей. И пример женщин-безопасников должен вдохновлять новичков

Хотя женщины составляют 47% от общей численности рабочей силы во всём мире, они составляют всего порядка 25% сотрудников в сфере кибербезопасности. Получение специализированного образования, сертификации и опыта в этой сфере требует времени и денег. Нехватка кадров в отрасли ИБ будет продолжать увеличиваться с каждым годом. Например, в период с 2020 по 2021 гг. разрыв вырос на 13%.

Эффективный и действенный способ быстро восполнить этот кадровый пробел — облегчить доступ женщин в область науки, технологий, инженерии и математики (Stem), в том числе для старта карьеры в области ИБ. Для этого надо изменить чисто мужское отношение к женщинам в сфере кибербезопасности. Слабый пол часто воспринимается как «недостаточно техничный», но это далеко не так. В последние годы такой сдвиг в мышлении происходит, и в технологическом секторе появляется всё больше женщин: с 2017 по 2020 г. в кибербезопасности их стало в два раза больше, и всё чаще они занимают руководящие позиции.

Один из ключевых способов вырастить талантливую смену — привлекать и стимулировать интерес к профессиональной сфере с раннего возраста с помощью наставничества, знакомства и возможностей. И пример женщин-безопасников должен вдохновлять новичков.

Опыт проведения мероприятий Capture the Flag, организованных сингапурским отделением Women in Security (WoSEC) в 2019 г., показал интерес девушек к кибербезопасности. Организация SG Women in Tech в 2021 г. нашла 18 школьниц и студенток, которые вошли в список «100 женщин в сфере технологий» Сингапура.

Многочисленные учебные программы служат платформами, на которых женщины-профессионалы в области ИБ делятся опытом со студентами, прежде чем они выйдут на работу. Поэтому можно сказать, что в Азиатско-Тихоокеанском регионе у женщин многообещающее будущее в сфере ИБ.

Согласно опросу, 82% студентов естественно-научных дисциплин выразили заинтересованность в получении дипломов в области кибербезопасности. Поэтому необходимо сделать карьеру в области ИБ более доступной и осуществимой для женщин. Это потребует от организаций расширения равных возможностей для женщин за счёт сокращения гендерного разрыва в оплате труда и активизации усилий DEI, а также внедрения политики и передового опыта для поддержки и расширения прав и возможностей женщин в области кибербезопасности. Правительства могут поддержать путём внедрения дополнительных инициатив по развитию экосистемы кибербезопасности и работать в тандеме с организациями и учебными заведениями. Это привело бы к более целостным инициативам по созданию надёжного канала кадров, от обучения до найма, удержания и продвижения по службе.

В конечном счёте привлечение женщин в сферу кибербезопасности не только уменьшит разрыв в возможностях. Оно обещает различные перспективы для инноваций и решений проблем, что только укрепит возможности кибербезопасности. Диверсифицированная рабочая сила будет способствовать инклюзивному и инновационному восстановлению экономики после пандемии COVID-19 и в итоге повысит эффективность бизнеса и национальной экономики.

ЗЛОНАМЕРЕННАЯ КИБЕРАКТИВНОСТЬ В ГЛОБАЛЬНОМ МАСШТАБЕ

МИР И КИБЕРИНЦИДЕНТЫ — ГЛАЗАМИ СТУДЕНТОВ МГЛУ

В IS Journal продолжает творческое сотрудничество со студентами-переводчиками МГЛУ. Их задача — выбрать в СМИ разных стран сообщения о киберинцидентах. В результате редакция получает сотни случаев, из которых после фильтрации формируется довольно насыщенный информационный коктейль.

ПО ВСЕМУ МИРУ

— Компьютерный сбой в системе железнодорожной сигнализации привёл к перебоям в движении поездов в ряде стран Европы и Азии, — заявил 17 марта французский железнодорожный гигант Alstom. — Причины сбоя обнаружены и устраняются, это не была кибератака, — отмечается в пресс-релизе.

По данным Итальянской государственной железной дороги, поезд на ключевой магистрали Рим — Флоренция задерживались на 2 часа или были отменены из-за проблем в централизованной системе управления.

— В Польше расследованием инцидента занята специальная команда, — заявил глава правительства по кибербезопасности Януш Цешински. Внезапное отключение произошло в 03:00 по Гринвичу 17 марта и затронуло 19 из 33 центров управления железными дорогами Польши, что привело к остановке движения поездов, в том числе были затруднены перевозки беженцев из районов, пограничных с Украиной.

Сбои в управлении также затронули железнодорожные системы Таиланда и Индии, где отмечались перебои на ряде маршрутов, сообщили информационные агентства.

ТОГО

Первый в Африке саммит по кибербезопасности прошёл в Ломе 23 и

24 марта. Мероприятие, организованное Республикой Того и Экономической комиссией ООН для Африки (ЭКА ООН), объединило официальных лиц государств Африки и частных лиц, работающих в сфере ИБ. Они обсудили множество вопросов по кибербезопасности и цифровому развитию.

Были затронуты вопросы биометрической идентификации, государственно-частного партнёрства и синергии между национальным CERT Того и SOC в Ломе, а также регионального сотрудничества в сфере ИБ.

В Того успешно функционируют Национальное агентство кибербезопасности (ANCy), Национальный центр реагирования на инциденты в области кибербезопасности (CERT), задачей которого является выявление, анализ и смягчение киберугроз, затрагивающих тоголезское государство, граждан, предприятия и организации. Страна заключила государственно-частное партнёрство с Asseco (Польша) для создания совместного предприятия Cyber Defense Africa, которое предоставит услуги по киберзащите Того и поможет госучреждениям и частным компаниям региона сделать их инфраструктуру безопасной.

ЕВРОПЕЙСКИЙ СОЮЗ

Эксперты предупреждают ЕС о необходимости принять дополнительные меры против российских кибератак, опасаясь, что Россия может использовать их в ответ на санкции.

В конце февраля лидеры ЕС призвали Россию и поддерживаемых ею хакеров остановить кибератаки на Украину, которые ведутся одновременно с военной спецоперацией. Заявление было сделано на фоне объявления санкций против российских чиновников и частных лиц.

Член Европарламента от Нидерландов Барт Гротуис после визита в страны Балтии отметил, что вредоносное ПО, атакующее критическую инфраструктуру Украины, также было обнаружено в Латвии и Литве. По его мнению, кибербезопасность должна быть вопросом иностранных дел ЕС, а не техническим вопросом, учитывая «стратегические издержки» кибератак.

Агентство ЕС по кибербезопасности выпустило руководство по усилению безопасности государственных и частных организаций в Европе, аналогичные руководства вышли в США и Великобритании. НАТО также приняло внутреннее руководство о том, какой тип кибератаки можно считать «вооружённым нападением», что приведёт к срабатыванию пункта о взаимной защите.

Также службы ЕС и национальные группы реагирования на киберинциденты разыграли вымышленный сценарий, в котором кибератака со стороны некоего государства Blueland приводит к сбоям в больницах и электростанциях по всей Европе. «Кибератака» приводит к жертвам, активизирует санкции ЕС, также начинает действовать пункт о взаимной защите в договоре ЕС, который в последний раз использовался после атаки террористов на Париж в 2015 г.

Технологические ассоциации из Румынии, Молдовы, Литвы, Словакии, Эстонии, Венгрии, Польши и Финляндии призвали лидеров ЕС создать «цифровой щит», усилив обучение и вложив значительные средства в кибербезопасность.

Интенсивность кибератак против Украины возросла за несколько недель до военной спецоперации России, заявил Александр Валентий, сотрудник по ИБ компании по кибербезопасности

Surfshark. По его словам, первые крупные атаки на компании и госучреждения на Украине были зафиксированы почти десять лет назад, в 2014 году. Сообщалось о значительных сбоях в работе интернета в нескольких городах. В 2022 году, по данным компании NetBlocks, на Украине были атакованы несколько веб-сайтов государственных организаций и банков.

АКЦИИ РАСТУТ В ЦЕНЕ

Биржи предсказуемо отреагировали на спецоперацию России на Украине. И если в России биржевые торги приостановлены, производители покидают рынок сбыта, а товары в магазинах дорожают, то на западных рынках растёт цена акций компаний, занимающихся ИБ.

Фонд кибербезопасности WisdomTree (WCBR) отслеживает индекс WisdomTree Team8 компаний, занимающихся кибербезопасностью и технологиями, ориентированными на ИБ. С началом спецоперации на Украине он вырос за неделю на 8,6%. Предполагается, что за месяц эта цифра будет ещё выше. WCBR уже доказал свою актуальность на фоне ситуации в Восточной Европе. Для сравнения, индекс S&P500 не показал такого роста.

23 февраля CrowdStrike — компания, работающая в сфере ИБ, сообщила в своём блоге о существовании нового вредоносного ПО DriveSlayer. Вредонос используется для атак на украинские системы. Это второе вредоносное ПО, обнаруженное за последнее время и нацеленное на конкретный регион. Первым вредоносом был WhisperGate. CrowdStrike Holdings (NASDAQ: CRWD) входит в число индексированных Фондом WCBR организацией, компания является шестой по величине капитала, её доля составляет 4,85%.

По оценкам западных экспертов, Украина является динамично развивающимся рынком аутсорсинговых услуг в области ИТ. Более 100 компаний из списка Fortune500 хотя бы частично используют услуги украинских ИТ-компаний. Объём экспорта информационных технологий с Украины увеличился на 36%, до \$6,8 млрд в 2021 г. по сравнению с примерно \$5 млрд в



Первый в Африке саммит по кибербезопасности прошёл в Того 23 и 24 марта

2020 г. И целевые атаки на компании региона могут привести к непредсказуемым последствиям.

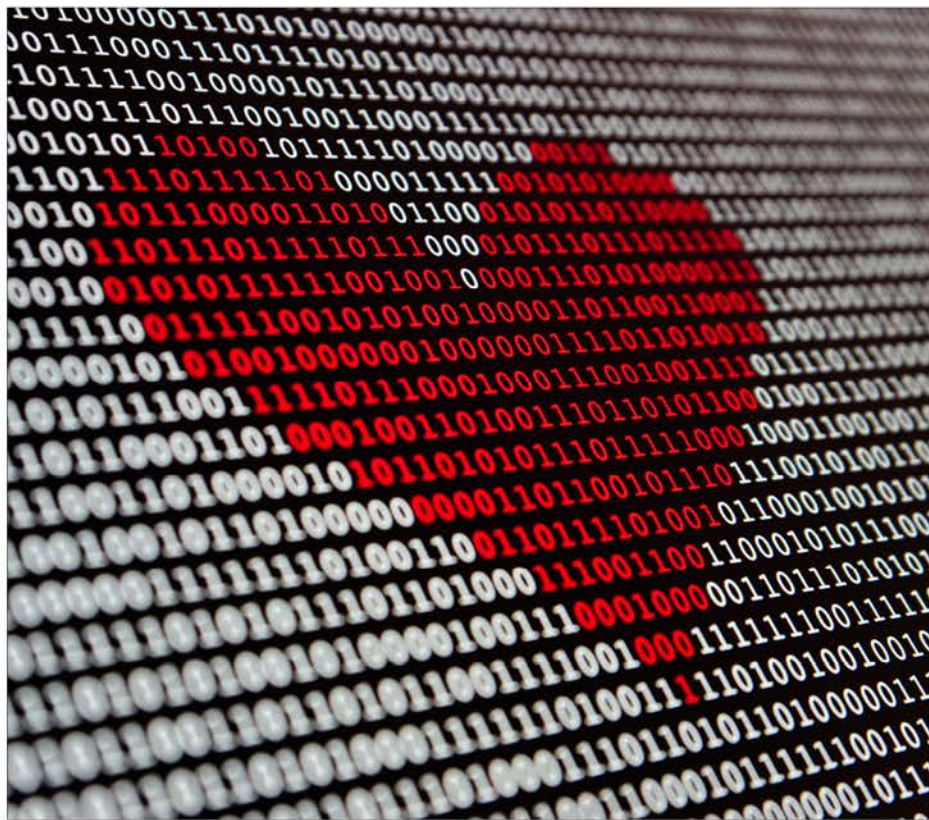
Время покажет, продолжит ли WCBR реагировать на геополитические действия в Европе. А эксперты считают, что на акциях конкретных компаний, занимающихся кибербезопасностью, можно будет неплохо заработать.

ИНДИЯ

В Патне (Индия) полицией был задержан подозреваемый в причастности к многочисленным преступлениям. При нём были обнаружены 33 банковские карты и более 1 млн рупий наличными.

По данным полиции, молодой человек является членом группы кибермошенников, обманом снимающих деньги с банковских счетов. Полиция изъяла у него также девять банковских сбер книжек, три чековые книжки и мобильный телефон.

Мошенник был задержан в тот момент, когда снял из банкомата 1 млн рупий с помощью двух банковских карт. На допросе он рассказал, как вместе с сообщниками обманывал людей и выводил деньги с их банковских счетов. На похищенные средства они покупали землю, брендовые вещи и роскошные автомобили.



По словам мошенника, в группе работают 25 человек. Они отправляют различные заманчивые сообщения на мобильные телефоны жертв, звонят им или связываются через электронную почту и соцсети. Бедные и нуждающиеся люди попадают в ловушку, веря поддельным документам, вкладывают деньги в якобы выгодный бизнес мошенников.

Задержанному полицией уже предъявлены обвинения по статьям «мошенничество и незаконное побуждение к передаче имущества», «подделка ценных бумаг, завещаний» и «подделка документов с целью мошенничества» Уголовного кодекса Индии и соответствующих разделов Закона об информационных технологиях, сообщает Times of India.

ГРЁЗЫ И СЛЁЗЫ

По данным Федеральной торговой комиссии США (FTC), за последние пять лет одинокие люди потеряли в приложениях для знакомств около \$1,3 млрд в результате мошенничества на основе романтических отношений, что делает последнее самым дорогостоящим видом мошенничества в стране.

Февральский документальный фильм «Мошенник из Тиндера» исследовал проблему и возобновил разговор о мошенниках, которые прячутся у всех на виду в приложениях для знакомств. Так, Шимону Хаяту запретили пользоваться платформами знакомств Tinder и Hinge после того, как он представился богатым продавцом бриллиантов и получил сотни тысяч долларов от женщин, которым рассказывал, что находится в опасности и нуждается в деньгах. Позже его заблокировали в социальных сетях.

В январе мужчина из Денвера рассказал изданию The Sun, что потерял \$1,6 млн после того, как на сайте ему посоветовали инвестировать эти деньги в пенсионный счёт. В феврале 24-летняя женщина по совету на портале знакомств отдала свои сбережения в размере \$300 тыс., чтобы инвестировать в сайт обмена криптовалютой, который оказался фальшивым. А супружеская пара была отправлена в тюрьму за участие в схеме мошенничества с несколькими пожилыми людьми на \$660 тыс.

Как защитить себя от кражи личных данных и финансового мошенничества? Марк Капчински, вице-президент

по стратегической кибербезопасности OneRep, советует удалить личную информацию (адрес, номер мобильного телефона и электронную почту) из результатов поиска Google, сохранять в тайне номер своего мобильного телефона и всегда выяснять, с кем вы собираетесь встретиться, прежде чем встретиться лично.

ХАКЕРЫ БЬЮТ ПО ЗДОРОВЬЮ

Отдел здравоохранения округа Ист-Уэнатчи обратился в прокуратуру штата Вашингтон и сообщил об инциденте кибербезопасности в марте 2021 г. Произошла утечка персональной и медицинской информации, затронувшая порядка 109 тыс. человек.

Клиника из Ораделле, штат Нью-Джерси, сообщила в Министерство здравоохранения США об инциденте с программами-вымогателями в ноябре 2021 г., затронувшем 92 тыс. пациентов.

Эксперты отмечают, что эти инциденты являются частью тревожных тенденций, которые угрожают критически важным секторам инфраструктуры. Майкл Гамильтон, директор по ИБ компании Critical Insight, отмечает, что использование программ-вымогателей может быть приравнено к терроризму. Кража записей и отказ в обслуживании становятся тактиками вымогательства. Учреждения здравоохранения также могут быть затронуты каскадными последствиями атак на другую критически важную инфраструктуру, например, электро-, водоснабжение и т.д.

Ранее об утечке данных сообщила государственная больничная система Broward Health, штат Флорида. Пострадали более 1,3 млн человек. Этот инцидент произошёл в октябре 2021 г. и пока является крупнейшим из обнаруженных в 2022 г. Министерство здравоохранения шт. Мэриленд в декабре 2021 г. подверглось атаке программы-вымогателя, которая в январе текущего года затронула различные ИТ-системы и приложения департамента.

В мае 2021 г. в результате атаки программы-вымогателя Conti вышла из строя система общественного здравоохранения Ирландии. Были нарушены работа ИТ-систем и обслуживания пациентов Управления



здравоохранения страны. На март 2022 г. стоимость восстановления системы уже достигла \$48 млн но может составить до \$110 млн. Особенно уязвимы медицинские учреждения в сельской местности, где нет специалистов-практиков, скудный бюджет, а управление советами здравоохранения осуществляется гражданами, не имеющими опыта ни в области здравоохранения, ни в сфере кибербезопасности.

Поскольку число атак на сектор здравоохранения продолжает расти, эксперты рекомендуют организациям внимательно следовать недавним указаниям федеральных и отраслевых органов.

НОВЫЕ ПРАВИЛА

Еврокомиссия вводит новые правила для установления общих мер кибербезопасности в учреждениях, органах, офисах и агентствах ЕС. Предложение направлено на повышение их устойчивости и увеличение потенциала реагирования на киберугрозы и инциденты, а также на обеспечение безопасной работы учреждений ЕС в условиях растущей злонамеренной киберактивности в глобальном масштабе.

Новые правила являются важной вехой в сфере кибербезопасности ЕС.

Они основаны на усиленном сотрудничестве и взаимной поддержке между институтами, органами, офисами и агентствами ЕС, а также на скоординированной готовности и немедленном реагировании. Это настоящее коллективное усилие ЕС.

Еврокомиссия предложила принять Регламент о кибербезопасности и Регламент об информационной безопасности. Устанавливая общие приоритеты и рамки, эти правила будут способствовать дальнейшему укреплению межведомственного сотрудничества, минимизации подверженности рискам и дальнейшему укреплению культуры безопасности ЕС.

Регламент о кибербезопасности создаст основу для управления рисками и контроля в области кибербезопасности. Это приведёт к созданию нового межведомственного совета по кибербезопасности, расширит возможности кибербезопасности, будет давать регулярную оценку качеству работы в области кибербезопасности организаций ЕС и рекомендации по улучшению кибергигиены. Регламент расширит полномочия Группы реагирования на компьютерные чрезвычайные ситуации для учреждений, органов, офисов

и агентств ЕС (CERT-EU) в качестве центра разведки угроз, обмена информацией и координации реагирования на инциденты, центрального консультативного органа и поставщика услуг. Согласно Регламенту кибербезопасности усилятся полномочия и финансирование CERT-EU, повысятся требования по кибербезопасности для учреждений, органов, офисов и агентств ЕС, они будут обязаны сообщать об инцидентах в CERT-EU без задержек. Появится новый межведомственный совет по кибербезопасности для управления и контроля за выполнением регламента, а также для управления CERT-EU.

Будет создана межведомственная группа по координации информационной безопасности, установлен общий подход к категоризации информации по степени конфиденциальности, модернизированы политики ИБ, включая цифровую трансформацию, удалённую работу и т.д.

Предложенные меры полностью согласованы с существующей политикой кибербезопасности ЕС и с действующим европейским законодательством.

Публикацию подготовила
Марина Бродская



Узел связи 138-й стрелковой дивизии
в подвальном помещении завода «Красный
Октябрь» в Сталинграде, 1942 год.
Фото: Григорий Зельма (РИА «Новости»)



Борис СТОЛПАКОВ
историк криптографии,
к. ф.-м. н.

ЗА БОЕВЫЕ ЗАСЛУГИ

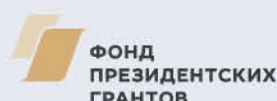
РАТНЫЙ ТРУД И ЗАСЛУЖЕННОЕ ПРИЗНАНИЕ ФРОНТОВОЙ РАДИОРАЗВЕДКИ

Уже 80 лет отделяют нас от начала Сталинградской битвы. Семь месяцев её непрерывных боёв, прервавших более миллиона человеческих жизней, стали

поворотным моментом всей Второй мировой войны. В победный итог битвы, а затем и последующих сражений значительный вклад внесли фронтовые радиоразведчики.

ПЕРВЫЕ УДАЧИ В ДОНСКИХ СТЕПЯХ

Нелёгкок был путь фронтовых частей радиоразведки к такому успеху. В период отступления от Харькова, с конца



Публикация подготовлена при поддержке гранта Президента Российской Федерации на развитие гражданского общества №21-1-009977, предоставленного Фондом президентских грантов

июня 1942 г., радиоразведка оказалась в сложном положении в донских степях. Тогда, согласно воспоминаниям ветеранов, «фронтовые части радиоразведки систему радиосвязи немцев в оперативном звене контролировали слабо, а в тактическом (дивизия — полк) вообще исключили из наблюдения». Некоторая стабилизация наступила в середине июля. «Фронтовые радиодивизионы стали располагаться в 40–50 км от линии фронта, что позволило вести наблюдение за дивизионными радиосетями немцев. Был организован более качественный анализ и обобщение получаемых ими разведывательных сведений.

К началу обороны Сталинграда 394-й и 561-й радиодивизионы ОсНаз Сталинградского фронта уже достаточно полно вскрыли и начали непрерывное наблюдение радиосвязи 6-й полевой и 4-й танковой армий противника». 394-й радиодивизион работал по войскам 6-й армии, а 561-й — по войскам 4-й танковой армии. «К 20 июля было точно установлено, что в помощь 6-й армии Паулюса прибыли два армейских корпуса — появились новые радиостанции, принадлежащие их штабам. В последующие два дня до радиомолчания снизилась активность радиосвязи противника. Это говорило о том, что враг готов к наступлению. 6-я армия ударила 23 июля, радиомолчание прекратилось».

Бывший старшина И.З. Захаров из 394-го радиодивизиона вспоминал, как знание характеристик вражеских радиостанций, а также скорости, чёткости и почерков работы на ключе немецких радистов позволило ему с товарищами отличать танковые и мотодивизии от пехотных и эсэсовских. «В дни наступления танковых соединений мы замечали каждое изменение пеленгов их радиостанций... В один из таких дней я принял радиограмму, переданную открытым текстом. В ней дивизионный радист сообщал в вышестоящий штаб, что «25 танков переправляются через Дон в районе Цимлянской». Эта же телеграмма была принята и старшим сержантом В.А. Ковалём. Содержание её доложили командующему фронтом К.К. Рокоссовскому. А он приказал лётчикам нанести бомбовый удар по переправе через Дон и танкам врага...

Коваль и я стали кавалерами ордена Красной Звезды».

Из наградного листа на начальника приёмного центра старшего лейтенанта А.К. Бушуева: «... под его руководством в боях за Сталинград были выявлены 6-я армия, 4-я танковая армия, 48-й танковый корпус, 24, 51, 17 и 8-й армейские корпуса, 44, 376, 113, 76, 295, 79, 305 и 386-я пехотные дивизии. Для повышения качества боевой работы предложил новые технические методы радиоразведки — спаренность приёмников, в результате которых намного повысилось качество добываемого материала о противнике».

ГЛАВНЫЕ ОРИЕНТИРЫ — ЗЕНИТЧИКИ И ЛЁТЧИКИ

Кроме радиосетей сухопутных, танковых войск, авиации, надёжным источником необходимых сведений стали радиосети зенитной артиллерии. «Зенитный дивизион придавался дивизии, и штаб зенитчиков всегда располагался рядом с её штабом. Обнаружив штаб зенитного дивизиона, «слухачи» твёрдо знали: там же находится и штаб дивизии».

В обороне немцы широко использовали проводные линии связи и режим радиомолчания. Но даже в такие моменты в авиации радиообмен продолжался. Ветераны вспоминали: «Наши специалисты по особенностям построения позывных бортовых радиостанций научились различать принадлежность самолётов к определённому роду авиации, эскадрам, группам, отрядам. Когда гитлеровцы ввели в действие новую таблицу позывных Е, начался трудный этап раскрытия этой таблицы. Нас выручил, во-первых, золотой фонд — опытные радисты-слежечники, способные запомнить едва уловимые особенности почерка вражеских радистов, и, во-вторых, более углублённая централизованная обработка материалов радиоразведки. Постепенно захватывались войсками и сами таблицы Е».

Неприятельская авиаразведка стала особенно ценным источником информации. Поэтому дивизионами были сформированы две группы для перехвата донесений авиаразведки противника на волнах УКВ, их разместили на КП фронтов.

Перехват сообщений немецких самолётов-разведчиков в 394-м радиодивизионе был поручен переводчику В.Д. Козлову. «Вооружённый приёмником УКВ, позволявшим обнаруживать вражеские самолёты с момента их вылета, он, расположившись на небольшой высоте, следил за их полётами. Обычно немецкий самолёт-разведчик вылетал рано утром. Лётчик связывался со своим аэродромом и штабом, запрашивал слышимость, сообщал метеосводку и облетал передний край наших войск. Он наблюдал за артиллерийскими батареями, скоплением пехоты, аэродромами и другими объектами. Глядя на карту, где все пункты были закодированы, он открытым текстом в микрофон передавал расположение наших войск. Эту же информацию с картой перед глазами и с карандашом в руках принимал и заносил на карту В.Д. Козлов. Он без промедления по телефону передавал информацию своему начальнику. Исходя из этого, командование фронта принимало меры по передислокации и маскировке войск».

ЖГУЧАЯ ОСЕНЬ И ГОРЯЧИЙ СНЕГ

В конце сентября бои шли уже в городе. «Стремясь завершить захват Сталинграда, немцы постоянно производили перегруппировку своих сил из-за больших потерь. Радиоразведчики докладывали о перемещении частей противника. Им удалось своевременно обнаружить выход итальянских и румынских частей к Дону: северо-западнее 6-й армии перешли к обороне 3-я румынская и 8-я итальянская армии, а южнее Сталинграда место убиавших в Сталинград немцев заняли части 6-го и 8-го румынских корпусов».

Как оказалось впоследствии, эта информация стала бесценной для командования, подарив идею будущей победной операции «Уран» по окружению вражеских войск. В радиодивизионы тогда оперативно прибыли переводчики с итальянского и румынского языков. «Радиосвязь итальянских и румынских войск явилась для капитана М. Пяткова и других офицеров оперативного отделения новым источником получения сведений не только о них, но

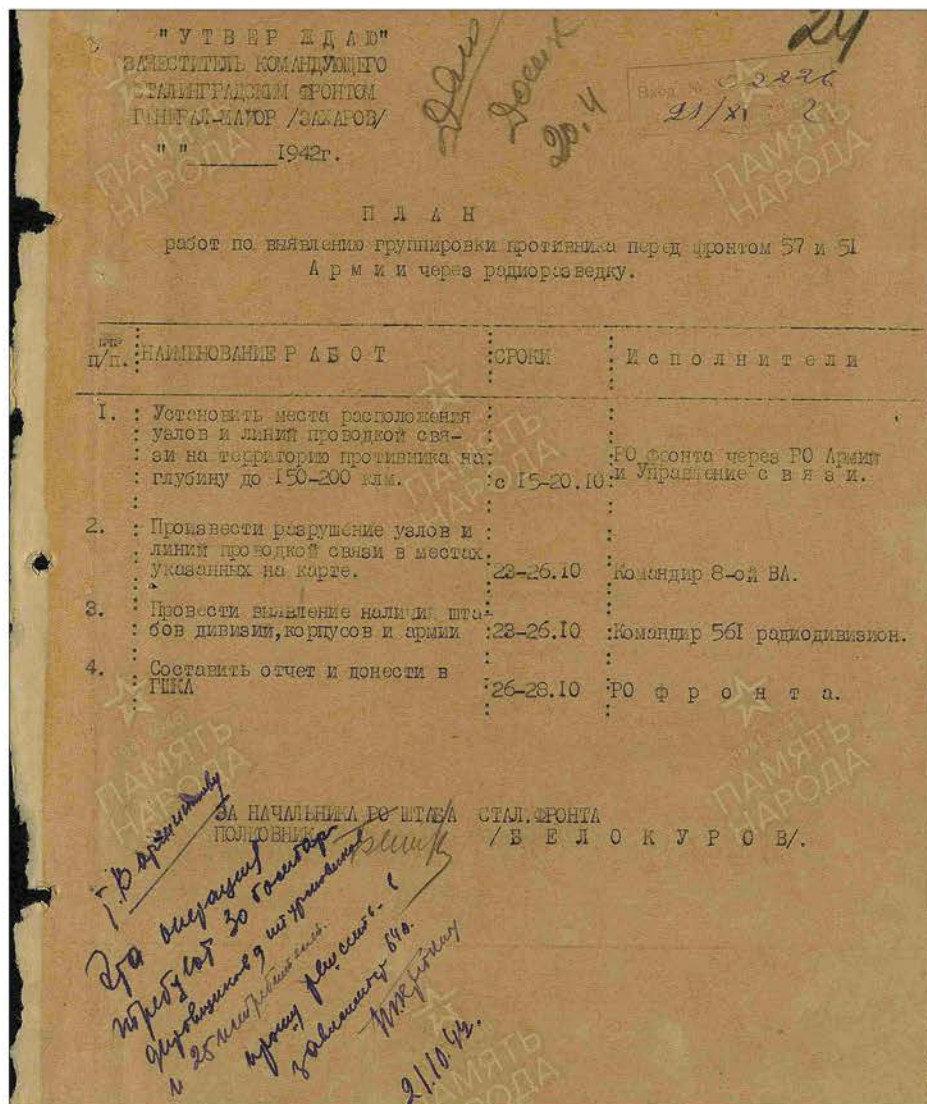


Иллюстрация 1. Директивы для радиоразведки при подготовке операции «Уран»

Sprechtafel Nr. 1					
Es folgen Grundzahlen	Es folgen Ordnungszahlen	Stop	röm.	Punkt	Komma
B	i	L	D	IV	V
Bindestrich -	Fragezeichen ?	Ausrufezeichen !	Klammer ()	von	an
A	Z	H	M	σ	T
laufenden Monats	vorigen Monats	Es folgen Rufzeichen	Es folgen kHz	Funkstellen-Nummer	Zahlenanfang
VI	VII	P	IX	E	C
Zahlende	Es folgen Auswertebegriffe	Blocknot	Chi-Nr.	Entzifferung	Decknamen
U	K	X	F	VIII	R
Koordinaten	NKWD	Rufz.-Ber. Tafel	Überschlüsselg. Reihen	Fernaufklärung	Nahaufklärung
U	W	S	I	J	O
Peilmeldung	Netzmeldung	5-Z.	i-Block	o-Block	z-Block
G	Q	II	N	V	III
8	3	4	2	5	9

Иллюстрация 2. Одна из германских переговорных таблиц

и о немецких частях, взаимодействующих с ними».

«К началу контрнаступления советских войск радиоразведка вскрыла группировку немцев и их союзников перед Юго-Западным, Донским и Сталинградским фронтами. В ходе контрнаступления радиоразведка фронтов достаточно полно освещала состояние и деятельность войск противника, вскрывала подготовку их контратак и переброску резервов». Так, «20-23 ноября радиоразведка засекла переброску из-под Сталинграда в район прорыва 24 танковой дивизии. 22-24 ноября доложено нашему командованию о переброске с Северного Кавказа на аэродром Тацинская 1-й штурмовой эскадры. 23 ноября кольцо окружения сомкнулось. Радиоразведка сообщила о штабах противника, попавших в окружение.

В декабре радиоразведка постоянно вскрывала состав сил, которые противник направлял для деблокирования 6-й армии. Радиоразведка выявила прибытие в деблокирующую армейскую группу командующего группой армий «Дон» генерал-фельдмаршала Маништейна. 394-му радиодивизиону была поставлена не совсем обычная задача: создавать помехи, срывать связь между штабом 6-й армии и штабом деблокирующей группировки, где находился тогда Маништейн. Помехи обеспечивали фронтовые связисты, а вот наводили и корректировали их по частоте радиоразведчики. Они использовали и дезинформацию окружённого противника, входя с ним в связь по выясненным позывным».

12 декабря немцы перешли в наступление из района Котельниково, но были остановлены. «Специалисты 561-го радиодивизиона в решающий момент добыли очень ценные сведения: немцы перебрасывают в район Котельниково с правого берега Дона 17-ю танковую дивизию. Навстречу устремилась 2-я армия Малиновского. 19 декабря противник был остановлен, а затем и разбит. А к 31 декабря деблокирующая группировка потерпела полное поражение». 9 января немцам предъявили ультиматум, на следующий день, 10 января, советские войска начали операцию «Кольцо». 2 февраля окружённый противник сдался.

ПЕРВЫЕ КРАСНОЗНАМЁННЫЕ ДИВИЗИОНЫ

В феврале 1943 г. за весомый вклад в общую победу и «образцовое выполнение боевых заданий командования» 394-й и 561-й радиодивизионы были награждены орденами Красного Знамени.

Вот некоторые из заслуг 394-го радиодивизиона, отмеченных в наградных документах:

- ♦ своевременно давались данные о передислокации дивизионных радиостанций противника при движении на Сталинград, движение дивизий налучине реки Дон, выход и действие их южнее Сталинграда;

- ♦ во время окружения 6-й армии и 4-й танковой армии у Сталинграда отражались все перегруппировки войск до полного разгрома данной группировки;

- ♦ выявлен подход танковых дивизий на Котельническое направление и в район Тормосин, а также отход данных дивизий под ударами Красной Армии на юго-запад от Сталинграда;

- ♦ в период подготовки к наступлению на Сталинград выявлена переброска из глубинных аэродромов 1-й штурмовой эскадры, 76-й бомбардировочной эскадры, 1-й учебной эскадры пикирующих бомбардировщиков на аэродромы в Тагинскую, Морозовский, Миллерово, Таганрог, Ростов.

На 1 января 1943 г. личный состав 394-го радиодивизиона насчитывал 215 человек, из них рядовых — 18.

«...УСТАНОВИЛ ДИСЛОКАЦИЮ И ДИНАМИКУ ПЕРЕД ПРАВЫМ ФЛАНГОМ»

После разгрома немцев под Сталинградом дивизион перебросили на Орловско-Курскую дугу в подчинение командованию Центрального фронта. Постоянное взаимодействие в эфире радиоразведчиков и радистов противника давало бесценный опыт и тем, и другим. В 1943 году в немецких войсках заметно изменился характер радиообмена. «Открытый текст в радиопередачах стал встречаться лишь в исключительных случаях. Передача и приём во многих радиосетях стали осуществляться на различных частотах, обычной стала радиосвязь без позывных.

От былого пренебрежения к советской радиоразведке не осталось и следа».

С осени 1943 года фронтовые дороги неудержимо приближали бойцов краснознамённого 394-го радиодивизиона к Берлину. Больше стало наградных документов. В одном из них, на начальника радиостанции старшего сержанта Д. И. Густова, записано: «...Своей непосредственной работой на аппаратуре установил дислокацию и динамику перед правым флангом фронта следующих войсковых соединений противника: 16-го армейского корпуса СС с входящей в него 15-й пехотной дивизией СС латышской, 7-й танковой дивизией СС. Из перехваченного открытого текста установил действие на Штеттинском направлении 14-го танкового корпуса. 18 февраля отметил перемещение радиостанций из состава 4-й мд СС «Полицай» из Ноймер в Браллентин».

«ДОСТОИН ПРАВИТЕЛЬСТВЕННОЙ НАГРАДЫ...»

Интересную информацию о радиоразведке и боевом пути радиоразведчиков содержат наградные листы, представленные на интернет-портале «Память народа». Конечно, их краткое содержание может вызвать вопросы и иногда нуждается в комментариях. Вот пример.

Ст. лейтенант Эсс Игорь Яковлевич, оперуполномоченный 6-го Полевого отдела 5-го Управления НКГБ СССР.

«Ст. лейтенант Эсс в Красной Армии с 1940 года. Участник боёв по обороне Ленинграда.

Весь период Отечественной войны находился в действующей армии. Находясь в 6 Полевом Отделе с 1942 г., тов. Эсс быстро овладел своей специальностью дешифровальщика и разработал за этот период более 3000 шифрованных радиogram противника.

После Отечественной войны тов. Эсс разработал около 2000 телеграмм переписки германских частей, сохранившихся после капитуляции Германии и возглавляемых штабом немецкой армии «Норд».

Тов. Эсс предан нашей Родине и партии и вполне достоин награждения правительственной наградой орденом «КРАСНАЯ ЗВЕЗДА» (илл. 3).

Согласно представлению к ордену, ст. лейтенант И. Я. Эсс занимался дешифрованием документов группы армий «Север». Так, с переводом на русский язык, ныне принято называть германскую военную группировку «Норд», обеспечивавшую блокаду Ленинграда, а в январе 1944 года отброшенную от города на Запад. К осени значительная её часть, упомянутая в наградном листе, закрепилась на обширном полуострове в западной части Рижского залива и стала именоваться советским военным командованием как Курляндская группировка. Несколько попыток её ликвидации, сопровождавшихся большими потерями в советских войсках, к успеху не привели. Немцы морем доставляли снабжение и пополнение через расположенные на Курляндском полуострове крупные порты Лиепая и Вентспилс. Краснознамённый Балтийский флот в основном был заперт тогда минными полями в восточной части Финского залива. Всё же 10 мая 1945 года началась сдача в плен отдельных немецких частей. Она затянулась до конца мая, иногда сопровождаясь попытками вооружённого прорыва. Всего сдались около 200 тысяч военнослужащих, приблизительно 25 тысяч сумели добраться морем до Швеции, попытки таких переправ продолжались до поздней осени. Значительная часть латышского легиона СС спряталась в лесах и болотах Курляндии, создав основу «лесных братьев».

Понятно, что в таких условиях боевая работа дешифровальщиков Полевого отдела затянулась надолго. Прежде всего требовалось провести разработку трофейных штабных документов. Разумеется, среди пленных организовали поиск всех причастных к шифровальной работе. Подобная работа уже давно была налажена и в Красной Армии, и у союзников.

Так, по заданию созданного союзниками «Комитета по целевой разведке» — TICOM (Target Intelligence Committee) в последние месяцы войны около двухсот германских криптографов были разысканы и тайно вывезены в Великобританию. С их помощью и на основе анализа захваченных германских документов союзники выяснили, какие из их собственных

НАГРАДНОЙ ЛИСТ

1. Фамилия, имя и отчество - ЭСС Игорь Яковлевич

2. Звание - старший лейтенант 3. Должность, часть - оперуполномоченный 6 Полевого Отдела 5 Управления НКГБ Союза ССР

Представляется к ордену "КРАСНАЯ ЗВЕЗДА"

4. Год рождения - 1922 5. Национальность - русский

6. Партийность - член ВКП/б/ с 1945 года

7. Участие в гражданской войне, последующих боевых действиях по защите СССР и отечественной войне - с июня 1941 года

8. Имеет ли ранения и контузии в отечественной войне - не имеет

9. С какого времени в Красной Армии - с 1940 года

10. Каким РВК призван - Смольненским РВК, г. Ленинград

11. Чем ранее награжден - медалью "ЗА БОЕВЫЕ ЗАСЛУГИ"

12. Постоянный домашний адрес представляемого к награждению и адрес его семьи -

=====

**I. КРАТКОЕ, КОНКРЕТНОЕ ИЗЛОЖЕНИЕ ЛИЧНОГО
БОЕВОГО ПОДВИГА ИЛИ ЗАСЛУГ**

Ст. лейтенант ЭСС в Красной Армии с 1940 года. Участник боев по обороне Ленинграда. Весь период отечественной войны находился в действующей армии. Находясь в 6 Полевом Отделе с 1942 года тов. ЭСС быстро овладел своей специальностью дешифровальщика и разработал за этот период более 3000 шифрованных радиোগрам противника. После отечественной войны тов. ЭСС разработал около 2000 телеграмм переписки германских частей, сохранившихся после капитуляции Германии и возглавляемых штабом немецкой армии "Норд".

Тов. ЭСС предан нашей Родине и партии и вполне достоин награждения правительственной наградой орденом "КРАСНАЯ ЗВЕЗДА".

НАЧАЛЬНИК РАЗВЕДЫВАТЕЛЬНОГО ОТДЕЛА
5 УДАРНОЙ АРМИИ
Полковник /СИНЯЕВ/ -

15 декабря 1945 г.

Иллюстрация 3. Наградной лист радиоразведчика

шифров немцам удалось вскрыть. В частности, оказалось, что в Германии успешно читали переписку, использовавшую «Шифр ВМС № 3», часто применявшийся союзными конвоями в Атлантическом океане. Вероятно, по этой причине конвои нередко становились жертвой неожиданных атак противника. Понятно, что немецкое командование тщательно скрывало такие успехи своих специалистов и стремилось отвести от них подозрение. Вполне возможно, что этим объясняются

высокие германские награды для руководителей финских дешифровальщиков, особенно после гибели конвоя PQ-17.

«...МЕДАЛЬ ЗА ГОРОД БУДАПЕШТ»

Приведём ещё несколько выписок из наградных листов завершающего периода ВОВ.

Ст. сержант Негреев Фёдор Васильевич, старшина-радист 5-го Отдельного дивизиона Спец. службы войск НКВД СССР.

«Тов. Негреев, находясь на фронтах с самого начала Отечественной войны, проявил себя способным и умным радиоразведчиком. Радиоразведчик I класса.

За время наступательных действий войск фронта тов. Негреев дал много ценных сведений о противнике. Во время контрнаступления противника в январе и феврале 1945 г. тов. Негреев обеспечил перехват материала от окружённой группировки в Будапеште. Работал на самом ответственном участке спец. задания.

За образцовое выполнение спецзаданий командования тов. Негреев заслуживает Правительственной награды — медали «ЗА БОЕВЫЕ ЗАСЛУГИ».

Сержант Миненко Александр Сергеевич, старшина-радист.

«Тов. Миненко находится в радиоразведчастях с 1940 г. и на фронтах Отечественной войны с самого её начала. За это время тов. Миненко дал много ценных сведений о противнике. Радиоразведчик I класса.

Во время боёв в районе Секешфехервар и оз. Балатон тов. Миненко обеспечил перехват ценного материала от 5 ТД СС «Викинг», 3 ТД СС «Тотенкопф». ...Заслуживает Правительственной награды — медали «ЗА БОЕВЫЕ ЗАСЛУГИ».

Мл. сержант Коломиец Мария Ананьевна, старший радист.

«Тов. Коломиец, находясь на фронте Отечественной войны с мая месяца 1942 г., проявила себя умелой и способной радиоразведчицей.

За это время тов. Коломиец много вскрыла сетей противника, тем самым дала много ценного материала, особенно о дислокации частей и соединений. Во время контрнаступления противника ею были вскрыты сети 5 ТД СС «Викинг» в полном составе, 3 ТД СС «Тотенкопф», а также наличие 1 ТД в районе озера Балатон. ...Заслуживает Правительственной награды — медали «ЗА БОЕВЫЕ ЗАСЛУГИ».

В ту пору, когда утверждались представленные здесь наградные документы, на венгерских просторах вступала в свои права весна. Победная весна 1945 года.

РЕЛИКВИИ КРИПТОГРАФИЧЕСКОГО ФРОНТА

РАДИОГРАММЫ ИЗ ЭПИЦЕНТРОВ СОБЫТИЙ

С недавних пор благодаря сайту «Память народа» появилась возможность ознакомиться с документами, запечатлевшими напряжённую борьбу в эфире в годы Великой Отечественной войны, а также проблемы Криптографической службы, возникавшие в незримом противоборстве с могучим противником.

ACHTUNG! ПРОТИВНИК ЗАХВАТИЛ...

Уже в первые недели войны германское командование издавало приказы, свидетельствовавшие об активизации действий советской радиоразведки.

«Секретно! 26 пехотная дивизия. Командный пункт дивизии 7.8.41. Оперативный отдел/отделение связи.

Русские радиостанции пытались различными способами вступить в связь с немецкими радиостанциями с целью установить месторасположение немецких соединений и их обстановку. Это обстоятельство говорит о том, что противник ведёт за немецкой радиосвязью тщательное наблюдение и имеет представление о планах немецкой радиосвязи.

Следует предполагать, что противник захватил «Войсковую таблицу условных сигналов», а также таблицу «Основные сокращения для ведения радиопереговоров».

Для того чтобы на вопросы противника немецкие радиостанции не давали никаких ответов, приказывается:

1. Снабжать все радиোগраммы отдельных дивизионов, полков и соответствующих штабов, передающиеся вышестоящим инстанциям, подписью командира данной части или штаба.

2. Проверять каждую радиোগramму с целью выяснения, известен ли позывной передающего указанной командной инстанции.

3. На радиোগramмы, начиная от полков, отдельных батальонов и выше, закодированных по таблице условных сигналов, ответа не давать.

4. Если принимаются передачи, в которых использованы «Основные сокращения для ведения радиопереговоров», то следует проверять, применимы ли они для данной передачи и употребляются ли они вообще в проведении радиопереговоров.

5. Всем радистам докладывать своему начальнику обо всех замеченных отступлениях в порядке радиосвязи, допускаемых известными им корреспондирующими радиостанциями.

6. Обо всех подозрительных случаях в разрезе пунктов 1–5 докладывать немедленно по команде в 26 ПД — отдел разведки и начальнику связи дивизии.

За командира дивизии подписал Первый офицер штаба».

Этот документ переведён и прочитан в 1-м отделе 2-го Управления ГРУ Генштаба Красной Армии 23 октября 1942 г.

«РАДИОПЕРЕХВАТОМ УСТАНОВЛЕНО...»

Следующий документ (илл. 1) датирован 23 июня 1941 г. Он подтверждает, что в самом начале боёв на западных рубежах советская радиоразведка внимательно отслеживала и передвижения войск пока ещё нейтральной Финляндии.

«По данным радиоразведки, радиосеть, работавшая ранее в районе Коувала на 22.6, передвинулась в восточном направлении в район Лаппиенранта, в районе Коувала дислоцировался 2 Арм. Корпус. Радиоперехватом установлено движение танков в восточном направлении, предположительно из

Иллюстрация 1. Донесение о радиоперехвате

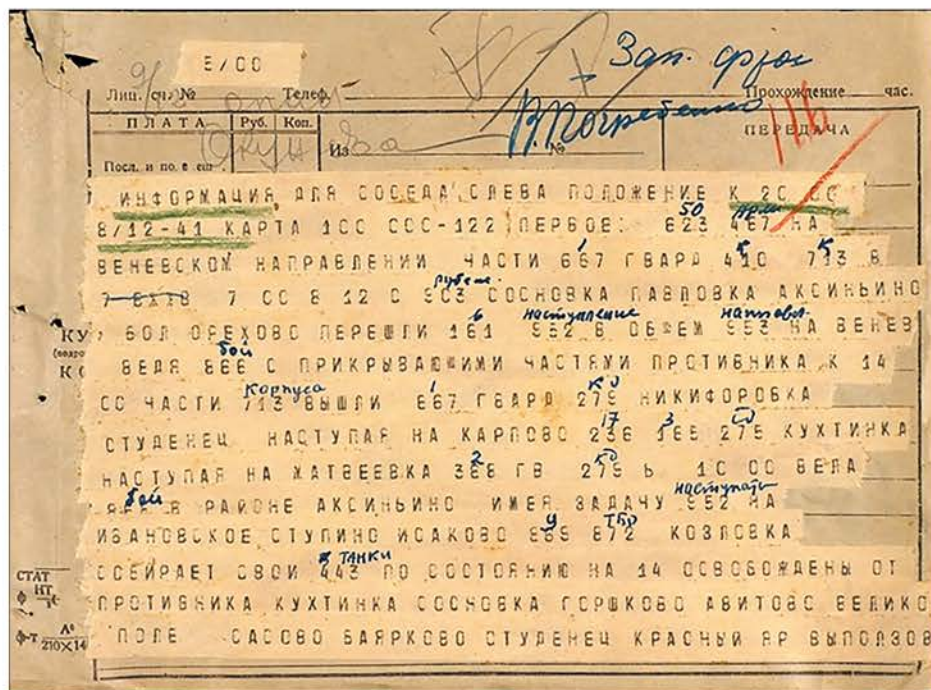


Иллюстрация 2. Кодограмма с раскодировкой

района Коувала. Зам. начштаба ЛВО генерал-майор Тихомиров. Получена 4.00 23.6.41».

Уточним, что финский город Лаппиенранта расположен близ Карельского перешейка, в 30 км от нынешней российско-финской границы. Город Коувала лежит в 83 км к западу от Лаппиенранта.

«ИНФОРМАЦИЯ ДЛЯ СОСЕДА СЛЕВА»

На илл. 2 можно видеть очень редкий документ — кодограмму с её раскодировкой. Такие документы обычно не сохранялись. Здесь наглядно продемонстрировано существо применяемого кодирования (цифровые замены слов и обозначений воинских частей). Обратим внимание на дату — 8 декабря 1941 г. Это один из первых дней советского контрнаступления под Москвой. Кодограмма живо передаёт напряжённость обстановки и содержит такие долгожданные признаки грядущей победы. Вероятно, это объясняет и сохранение документа.

«Информация для соседа слева. Положение к 20.00 8/12-41. Первое: 50 Арм. на Венёвском направлении части 1 Гвард. КК (Кавалерийского Корпуса) в 7.00 8 12 с рубежа Сосновка, Павловка, Аксиныно, Бол. Орехово перешли в наступление общим

направлением на Венёв, ведя бой с прерывающимися частями противника. К 14:00 части корпуса вышли: 1 Гвард. КД Никифоровка, Студенец, наступая на Карпово, 173 СД Кухтинка, наступая на Матвеевка, 2 Гв. КД в 10:00 вела бой в районе Аксиныно, имея задачу наступать на Ивановское, Ступино, Исаково. 9 ТБр Козловка собирает свои танки. По состоянию на 14 освобождены от противника Кухтинка, Сосновка, Горшково, Авитово, Великое поле, Сасово, Баярково, Студенец, Красный яр, Выползово».

Город Венёв расположен в 45 км от Тулы в северо-восточном направлении. 24 ноября 1941 г. танковая армия Гудериана сломала его оборону, но 9 декабря Венёв был освобождён частями 1-го гвардейского кавалерийского корпуса генерал-майора П.А. Белова. Группа войск под командованием генерала Белова в конце ноября остановила под Каширой немецкое наступление на Москву с южного направления. 26 ноября 2-й кавалерийский корпус заслужил право именоваться 1-м гвардейским кавалерийским корпусом. В начале декабря, получив пополнение, части корпуса перешли в контрнаступление. Его подготовку удалось скрыть даже от высшего германского командования.

«ОБОРОНА ПРОТИВНИКА НАХОДИТСЯ НА ГРАНИ СВОЕГО КРИЗИСА»

Так оценил состояние фронта перед началом контрнаступления Красной Армии под Москвой командующий группой армий «Центр» генерал-фельдмаршал Ф. фон Бок. Вот перевод трофейного документа.

«Секретно! Телеграмма.

Из штаба Центральной Группы Армий. 2.12.41

1. 2 Танковой Армии
2. 4 Армии
3. 4 Танковой Группе
4. 3 Танковой Группе

Точно установлено, что в последнее время противник пытается облегчить своё положение, перебрасывая целые дивизии или части дивизий с наименее угрожаемых на наиболее угрожаемые участки фронта. Прибытие нового пополнения было замечено только на одном участке и в небольшом количестве.

Из этого следует, что оборона противника находится на грани своего кризиса. Необходимо напрячь все силы, чтобы использовать эту слабость противника.

Я прошу немедленно ознакомить войска с настоящим приказом.

Фон Бок

ЦГА. Оперотдел, № 2799/41»

«ПЕРЕДАЁТСЯ ДЛЯ НЕУКЛОННОГО ИСПОЛНЕНИЯ»

Ещё один из документов начального периода ВОВ напоминает о вынужденном значительном обновлении личного состава связистов и вытекающих из этого сложностях в работе телеграфистов советской засекреченной связи (илл. 3).

«2801 приказал при передачах по Бодо боевых донесений, информации и при переговорах строго выполнять приказ НКО по кодированию. Донесения, нарушающие этот приказ, не принимать. — Передаётся для неуклонного исполнения. 3503 динамит».

КАК РАЗГАДАТЬ ЗАГАДКУ?

Известно, что на своих войсковых линиях связи немцы широко применяли трёхдисктовую шифровальную машину «Энигма» («загадка» — в русском переводе). Удельный вес переписки,

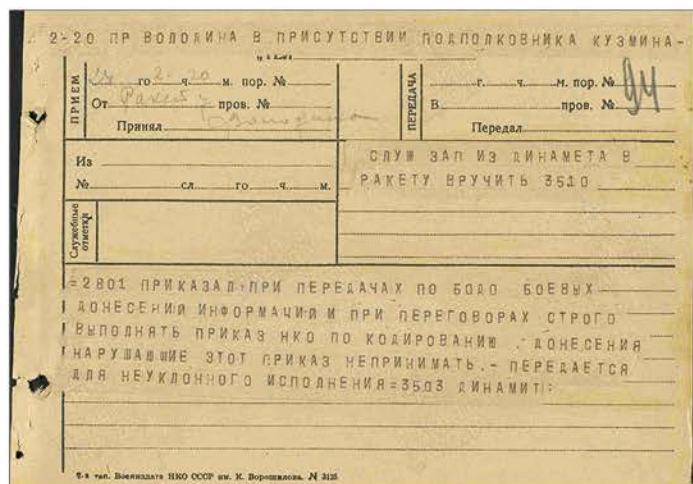


Иллюстрация 3. Директива командования

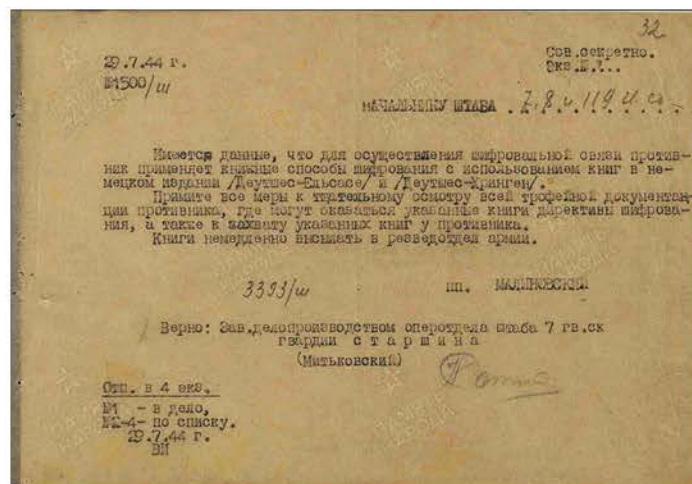


Иллюстрация 4. Задание на книжный поиск

зашифрованной этими аппаратами, составлял около 70%. В ходе боевых действий в руки советских специалистов попадали экземпляры «Энигмы», а также ключи к ней. Один из первых образцов — в начале декабря 1941 года во время наступления на Клин. В 1941 году в советский плен попали и несколько немецких шифровальщиков. Уже в ноябре 1942 года в представлении к наградам группы своих подчинённых начальник ГРУ генерал И. И. Ильичёв указал: «Научная группа Управления выявила возможность расшифровки немецких телеграмм, зашифрованных машинкой «Энигма», и приступила к конструированию механизмов, ускоряющих расшифровку». Тогда советские специалисты, используя трофейные аппараты и пояснения плененных шифровальщиков, сумели построить математическую модель немецкого шифратора. При этом выявили и слабости, которые могли способствовать процессу дешифрования. В дальнейшем эти сведения пригодились при создании советских шифрмашин, хотя в годы войны нашим специалистам не удалось добиться чтения немецкой переписки, зашифрованной на «Энигме». Тем не менее в январе 1943 года, уже высоко оценивая возможности советских дешифровальщиков, специалисты Управления связи немецких сухопутных войск пришли к выводу о необходимости усиления шифра «Энигмы». Несмотря на все трудности такой работы, после Сталинграда шифр «Энигмы» и правила её применения были значительно усложнены.

«ПРИНЯТЬ ВСЕ МЕРЫ...»

На сайте «Память народа» выложены и такие, неожиданные по содержанию, документы завершающего периода ВОВ.

«28.7.44 г. Нач. Развед. отделов и нач. 6 отделений 5, 129 и 169 СД.

По имеющимся данным немецкие штабы на фронте используют для шифрования телеграмм книги под названием «Деутшес Ельсасе» и «Деутшес Лотхринген». Принять все меры к тщательному осмотру всех захваченных у противника документов и при обнаружении указанных шифровальных книг немедленно направлять в штаб корпуса.

Дать указания войскам, чтобы в дальнейшем при разгроме штабов полков, дивизий и корпусов все захваченные документы тщательно осматривались. Мироненко».

«29.7.44 г. Сов. секретно Начальнику штаба 7, 8 и 119 гв. СД

Имеются данные, что для осуществления шифровальной связи противник применяет книжные способы шифрования с использованием книг в немецком издании /Деутшес Ельсасе/ и /Деутшес Хринген/.

Примите все меры к тщательному осмотру всей трофейной документации противника, где могут оказаться указанные книги директивы шифрования, а также к захвату указанных книг у противника.

Книги немедленно высылать в разведотдел армии.

пл. Малиновский (илл. 4).

Судя по номерам стрелковых дивизий и указанному времени, в первом

документе речь идёт о наступательной операции «Багратион» в Белоруссии, а во втором — об освобождении Латвии. Многие крупные воинские подразделения противника тогда оказались в окружении. Вероятно, с этим и была связана потребность в использовании книжных шифров в переписке немецких штабов. Можно предположить, что в июле 1944 г. обстановка на фронте затруднила доставку шифровальных ключей и штабы противника перешли на резервный вариант их выработки на местах.

Илл. 5 подтверждает, что розыск книги был успешным. Вероятно, и с применённым шифровальщиками противника книжным шифром тоже удалось разобраться. Возможно, это произошло уже после окончания войны.

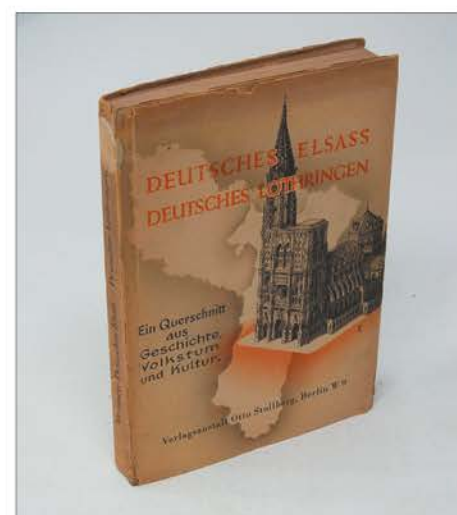


Иллюстрация 5. Книга «Немецкий Эльзас и немецкая Лотарингия», назначенная в розыск

«КАК НЕКУЛЬТУРНО!»

СВОБОДА СМИ И ПРИНЦИПЫ ИБ В КОНТЕКСТЕ ТРЕБОВАНИЙ ЗАКОНА №224-ФЗ

Реальной ценностью обладает не абстрактная, расплывчатая сущность, скрывающаяся за словом «информация», а знание — продукт, венчающий вершину пирамиды. Пирамиды, где основание — это передел «данных» в «информацию», выше — передел «информации» в «информационные модели» (ИМ), и уже наверху — знание, полученное на основании опыта использования упомянутых ИМ.

К сожалению, в финансовой сфере, страховом бизнесе и госуправлении качество такого передела и его конечного продукта оставляет желать лучшего. И причины тому — на уровне добычи и обработки данных.

ОБ УЩЕРБНОСТИ СОВРЕМЕННОЙ ИНФОРМАЦИИ

В упомянутых сферах деятельности сегодня на передний план в технологиях передела данных в информацию выходит Machine Learning. И в этой ситуации весьма важна корректность тех данных, что «скармливаются» алгоритмам машинного обучения. Но эти «данные» зачастую представляют собой набор как объективно измеряемых величин (возраст, цена и т.п.), так и субъективной или сознательно искажённой «информации».

И всё более очевидным становится тот факт, что такая «информация» (например, данные из социальных сетей) заслуживает специального названия,

для которого один из докладчиков форума «Банки России — XXI век» предложил особый термин — «мнения».

Не более надёжны и так называемые персональные данные в их расширенном варианте, когда речь идёт не о возрасте, поле или месте рождения, а о, например, потребительских предпочтениях, оцениваемых на основании «активности» платёжных карт, карт лояльности и иных изобретений современного финтех, формально индивидуализированных, но чаще используемых как «расшаренный» инструмент (например, для семейного использования или в рамках офисных «колхозов» карт лояльности).

Скептическое отношение к «данным» и продукту их передела высказывалось и на конференции Банка России «Противодействие инсайту и манипулированию рынком: в поисках новой парадигмы», где отмечалось, что «информации так много, что трудно определить, где она точная, а где сфабрикована».

Причём речь может идти как о ненадёжности информации, извлекаемой из нового класса «персональных» данных, описывающих состояние компаний, эмитентов ценных бумаг, так и о ненадёжности информации, тиражируемой СМИ на основании перепечаток сторонних источников или сознательных «вбросов» из «авторитетных источников». При этом уместно вспомнить, что в числе противников принятия закона № 224-ФЗ «О противодействии

неправомерному использованию инсайдерской информации и манипулированию рынком...» были и представители СМИ, считавшие закон инструментом для цензурирования журналистики и покушения на свободу слова.

КУЛЬТУРА КАК ЕДИНСТВЕННОЕ ПРИБЕЖИЩЕ ИБ

На ноябрьской конференции «Противодействие инсайту...» в качестве инструмента для реализации регуляторных задумок закона № 224-ФЗ было предложено развитие культуры рынка в виде системы табу и ограничений на недобросовестное поведение. Речь при этом велась об игроках, что называется, прямого действия — финансовых организациях и структурах-площадках для проведения торгов, и совсем не упоминались СМИ, хотя необходимость учёта их недобросовестного поведения понятна ещё со времён написания романа «Граф Монте-Кристо».

Безусловно, развитие культуры рынка необходимо всячески поддерживать, но при этом нельзя не включить в число окультируемых структур ещё и СМИ, а также попытаться оценить возможность использования метрик ИБ для управления таким окультированием. Это позволит, с одной стороны, формализовать список элементов культуры СМИ, а с другой — исключить СМИ из числа инструментов недобросовестной «социальной инженерии» как на финансовом рынке, так и в жизни общества в целом.

Не стоит сбрасывать со счетов и то, что эта работа позволит уточнить наши представления о метриках ИБ и их взаимосвязях.

ДОСТУПНАЯ И НЕВЕРНАЯ

На последнем форуме «Банки России — XXI век» ставился вопрос о влиянии на биржевые спекуляции качества

Весьма важна корректность тех данных, что «скармливаются» алгоритмам машинного обучения. Но эти «данные» зачастую представляют собой набор как объективно измеряемых величин (возраст, цена и т.п.), так и субъективной или сознательно искажённой «информации»

информации в контексте не только её объективности, но и своевременности ознакомления с ней рынка, т.е. **доступности** информации. В связи с этим упоминался, в частности, такой инструмент, как «высокочастотные» роботы для биржевой торговли.

Ещё одной ИБ-проблемой рынка биржевой торговли называлась проблема балансировки нагрузки на серверах в пиковых режимах работы бирж. А это значит, что, возможно, имеет смысл оптимизировать скорость предоставления информации с тем, чтобы интересы сиюминутного извлечения прибыли на быстро меняющемся рынке не вступили в конфликт с интересами устойчивой работы биржевых систем в течение всего торгового дня.

Применительно к СМИ доступность информации обеспечивается тотальным проникновением Интернета в работу редакций.

При этом СМИ, особенно в условиях их современной конкурентной многоканальности, грешат эстрадным подходом во взглядах на допустимые темпы информирования рынка и о рынке. «Утром в газете, вечером в куплете!» — это кредо политической эстрады начала прошлого века приходит сегодня на ум, когда за утренним кофе сталкиваешься с односторонней утренней радиозаписью, обеспеченной интернет-поисковиком, которым все как один пользуются ведущие радиоканалы. То же касается, впрочем, и утренней интернет-ленты СМИ.

Однако, помимо односторонности, ещё одной негативной обратной стороной лёгкой и быстрой доступности информации для СМИ стало заполнение эфира и газетных полос непроверенными сведениями, а то и откровенной ложью, используемыми нередко и для манипулирования рынками, и в интересах злонамеренной социальной «инженерии».

Соответствующие примеры легко можно было найти, анализируя освещённую так называемую пандемию SARS-CoV-2 или информационную атаку на Россию в связи с весенним санкционным обострением «коллективного Запада».

При этом, наряду с откровенной ложью ангажированных источников,

Клоном технологии недобросовестной дезинформации со стороны СМИ является и использование нескольких независимых, но некомпетентных источников

встречается «серая» дезинформация, основанная, «скажем так», на оперативном вбросе информации без надлежащей проверки добросовестности источника или системного анализа нескольких независимых источников.

КУЛЬТУРА ВЕРНОСТИ ДОСТУПНОЙ ИНФОРМАЦИИ

Стилистика с использованием современного речевого паразита «скажем так» использована для подчёркивания «некультурности» подобного поведения СМИ. И «некультурность» подобной природы при использовании для её описания метрик ИБ может быть связана с деградацией **целостности** информации.

Уместно заметить, что желание обеспечить целостность информационного потока в СМИ может конфликтовать с **конфиденциальностью** информации.

И в этом случае культурной проблемой для СМИ может стать противоречие — внимание! — между желанием обеспечить доступность актуальной для общества информации и объективной невозможностью обеспечить должное качество этой информации из-за прорех в её целостности, которые появляются в результате конфликта с требованиями конфиденциальности. Причём уровень академических требований к конфиденциальности на практике может доходить до грифа «Секретно» и выше.

КАК РАЗРЕШИТЬ КОНФЛИКТ?

Как разрешить такой конфликт? Решение этой задачи важно не только для СМИ в контексте повышения доверия к каналу поступления информации, но и применительно к упомянутой в начале статьи проблеме построения культуры рынка в виде системы ограничений на недобросовестное поведение.

Ещё одну проблему повышения культуры СМИ в контексте желания

исключить журналистику из числа инструментов недобросовестной «социальной инженерии» можно сформулировать, отталкиваясь от примеров недобросовестной дезинформации, использующих имитацию анализа многих источников («фактчекинга»), тогда как, по сути, все такие каналы дирижируются из одного центра.

Клоном технологии недобросовестной дезинформации со стороны СМИ является и использование нескольких независимых, но некомпетентных источников. Сегодня нередко можно услышать комментарии по теме, например, импортозамещения от лиц, формально «отягощённых» высокими должностями, но вскочившими на подножку «экспертности» из менеджеров по рекламе или с должностей помощников руководящих персон, не написав при этом ни строки кода и не пройдя на практике по технологической цепочке микроэлектронного производства.

ЧЕМ НЕ ПРИМЕР?

Проблема исключения журналистики из числа инструментов для манипулирования рынком и сознанием людей, равно как и задача использования журналистики для воспитания квалифицированного творца актуальны для современного общества. И объективная регуляторика в этой сфере, использующая метрики ИБ, могла бы сыграть тут свою роль.

Эту тему можно было бы обсудить на февральском Уральском форуме «Информационная безопасность финансовой сферы», но не случилось. И не случилось, в том числе и в связи с тем, что организатор опирался на устаревшие и неполные данные о состоянии угроз со стороны штаммов SARS-CoV-2.

«Как некультурно!» — сказала бы героиня Фаины Раневской.



Александр
ИГОНИН
эксперт BIS Journal

СЕМЬ АУДИТОВ НА СУНДУК БЕЗОПАСНИКА

Информационная безопасность — занятие непростое, особенно там, где она сталкивается с реальностью: печально известные Security Operations. Из-за постоянно меняющегося ландшафта угроз (а зачастую — и самой ИТ-инфраструктуры) отовсюду лезут и лезут проблемы: то логи перестали приходить, то инцидент неправильно отработали, то пентестеры опять поломали всю сеть. В общем, «то лапы ломит, то хвост отваливается», как в одном известном советском мультфильме.

После определённого количества серьёзных проблем высшее руководство обычно начинает искать пути их решения. На самый долгий, сложный и дорогой (нанять больше людей, выстроить процессы и автоматизировать по максимуму рутинные задачи) решаются немногие — что неудивительно, учитывая то, что собственный SOC — удовольствие и так недешёвое. И тут на помощь руководству спешат консультанты. Дорвавшись до высокой аудиенции, они демонстрируют простой и понятный план: давайте мы проведём аудит всего, напишем рекомендации — а вам только и останется воплотить их в жизнь и наслаждаться результатами.

Звучит, может быть, и здорово — но вот в реальности прекрасная идея оборачивается совсем другим. И без того заматанные текущими задачами подразделения безопасности вынуждены теперь тратить драгоценное время на внеплановые совещания и заполнение бесчисленных табличек в «Экселе», которые отправляются аудиторам на «проверку». И потом всё бумерангом возвращается в виде вопросов, уточнений и вороха рекомендаций. А вот дополнительного времени и ресурсов на эту активность, как правило, никто не даёт.

Я несколько лет работаю в SOC одной зарубежной компании, и мой личный рекорд на данный момент — это, кажется, четыре параллельно идущих аудита в один месяц. При этом

каждый аудитор клятвенно уверял, что его вопросы срочные и требуют немедленного внимания. Вот бы ещё и работать успевать при таких вводных...

В общем, если кто-то из читающих этот номер делает подобное у себя — не надо так. А вот как надо:

- ◆ перед принятием решения об аудите соберите обратную связь от команды — наверняка они сами назовут какие-то критичные проблемы, которые имеет смысл решить сразу же;
- ◆ чётко определите цели аудита (и, желательно, согласуйте их с подразделением, где он будет проходить);
- ◆ по возможности — обходитесь теми аудитами, которые являются обязательными (например, проводимыми в рамках PCI DSS), не плодите лишние сущности;
- ◆ обеспечьте достаточные ресурсы и временные рамки для устранения выявленных замечаний;
- ◆ в любом случае не допускайте нескольких аудитов, идущих одновременно. Расставьте приоритеты и оставьте какой-то один. Закончите его, отработайте замечания — и только потом переходите к следующему.

И операционная безопасность скажет вам спасибо.



XI симпозиум

«Современные тенденции в криптографии»

Тематика симпозиума включает следующие вопросы (но не ограничивается ими):

- исследование криптографических алгоритмов и протоколов, в том числе являющихся международными стандартами;
- эффективная реализация методов анализа криптографических алгоритмов и протоколов;
- оценка криптографической стойкости российских криптографических алгоритмов и протоколов;
- эффективная реализация российских криптографических алгоритмов и протоколов;
- математические аспекты криптографии;
- криптография в «Интернете вещей»;
- квантовая криптография и квантовые вычисления;
- постквантовая криптография;
- криптография и технология блокчейн;
- криптографическая защита биометрических данных;
- другие актуальные и перспективные направления криптографии



ОРГАНИЗАТОРЫ



TK26



МИАН

ПРИ ПОДДЕРЖКЕ



ФСРБ

ОРГПОДДЕРЖКА



Kaspersky Symphony XDR



Искусство киберзащиты
в одном решении



kaspersky

