

BIS

JOURNAL

ИНФОРМАЦИОННАЯ
БЕЗОПАСНОСТЬ
БИЗНЕСА

№2 (53) 2024

**Валерий
КОНЯВСКИЙ**
ОКБ САПР
«Изменяемая
архитектура
ИТ – новый этап
эволюции ИБ»
→ 28



**Виталий
ТЕРЕНТЬЕВ**
HeadHunter
«Мы живем в доме
со стеклянными
стенами...»
→ 72



ТЕМА НОМЕРА

Планирование цифровых прорывов — 2

Екатерина РАЧКОВА
BIS Journal
Парад законов
в первом квартале
→ 68

Светлана ГАЗИЗОВА
Positive Technologies
Что получит бизнес,
внедрив безопасную
разработку? → 108

Андрей ЖАРКЕВИЧ
Start X
Вымогатели
и человеческий
фактор → 114



SOC Tech

Технологии SOC киберзащита

*** 15 ОКТ 2024**

▾ Москва, LOFT HALL



SOC Tech 2024 – это мероприятие нового типа
Оригинальные форматы и возможности
сверхэффективного взаимодействия для всех
участников, спикеров и партнёров

Регистрация: ib-bank.ru/soctech



Елена ПОКАТАЕВА
обозреватель
BIS Journal

Тема планирования цифровых прорывов, начатая в прошлом номере BIS Journal, получила подтверждение своей высокой значимости в обращении Президента РФ Владимира Путина к Федеральному собранию 29 февраля 2024 г.

Это президентское Послание, направленное в будущее — до 2030 г., зафиксировало не только требование технологической независимости российской экономики, но и ряд ключевых направлений движения к этой цели:

1. Развитие отечественной науки как основы технологического развития России.
2. Подготовка кадров, способных работать в условиях технологического прорыва.
3. Технологический суверенитет как сквозная технология верхнеуровневого управления экономикой.
4. Реализация идеи технологического суверенитета на базе высокотехнологичных отраслей промышленности и повышение производительности труда в различных секторах экономики за счёт цифровизации.

«Проекты технологического суверенитета должны стать мотором нашей промышленности», — подчеркнул В. Путин. Цель понятна. Однако движение в сторону глобального технологического лидерства в условиях рушащегося старого экономического порядка и идущего ему на смену многополярного мира — это серьёзный вызов. Успех задуманного предприятия зависит от ряда существенных факторов, включая запуск цифрового производства на базе отечественных технологий и обеспечение информационной безопасности на всех уровнях работы предприятия: от контроллеров технологических процессов до интернет-коммуникаций с предприятиями-смежниками. При этом опора на достижения суверенной научной мысли говорит о необходимости прокладывать новые пути как в разработке новых технологий и видов продукции, так и в методах обеспечения безопасности бизнеса российских компаний и предприятий.

Задача требует нетривиальных организационных подходов: технологический прорыв должен интегрироваться в стратегии развития не только нынешних лидеров в своих секторах рынка, но и менее крупных компаний. Впрочем, необходимые ресурсы, в первую очередь интеллектуальные, для решения этой большой задачи «на вырост» есть. Главное — правильно организовать совместные усилия российской науки, государства и рыночных игроков.

РЕДАКЦИОННАЯ КОЛЛЕГИЯ

Батранков Д. В. — руководитель направления сетевой безопасности Positive Technologies
Былевский П. Г. — шеф-редактор, доцент департамента ИБ Финансового университета при Правительстве РФ, доцент кафедры международной ИБ МГЛУ, кандидат философских наук
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. — старший научный сотрудник ФГУП «ЦНИИХМ»
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)
Калашиников А. И. — управляющий директор Центра информационной безопасности дочерних и зависимых обществ Газпромбанка (АО)
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
Одувалов М. В. — директор службы Управления по обеспечению информационной безопасности ДБ Банка ВТБ (ПАО)
Окулесский В. А. — вице-президент по информационной безопасности ЦМРБанка, кандидат технических наук
Пазизин С. В. — заместитель начальника Управления по обеспечению информационной безопасности ДБ Банка ВТБ (ПАО), кандидат физико-математических наук
Филипчук А. А. — технический директор ГК ЦРТ
Хайретдинов Р. Н. — заместитель генерального директора ГК «Гарда»
Шумский Л. С. — руководитель службы информационной безопасности Яндекс Банка
Янсон И. А. — бизнес-партнёр по информационной безопасности, Департамент безопасности ПАО «Сбербанк России», кандидат физико-математических наук

РЕДАКЦИЯ ЖУРНАЛА

Главный редактор: **Некрасов И. В.**
 Директор по развитию: **Минаков А. В.**
 Арт-директор: **Мельников Н. С.**
 Руководитель интернет-проектов: **Воробьёва А. А.**
 Обозреватели: **Бродская М. А.**, к. т. н., **Покатаева Е. Н.**
 Иллюстрация на обложке: **Виктор Миллер Гаусса**
 Фото в номере: **Freerick**
 Цветокорректор: **Науменко М. В.**

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) как «BIS Journal — Информационная безопасность банков».

Зарегистрирован 11 июля 2023 года Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) как «BIS Journal — Информационная безопасность бизнеса». Свидетельство ПИ № ФС77-85487 от 11.07.2023 г.

Все права на материалы, опубликованные в номере, принадлежат журналу «BIS Journal — Информационная безопасность бизнеса». 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. Возрастная категория 16+.

Подписан в печать 12.04.2024. Тираж 5000 экз. Заказ № 1532024.

Цена договорная. Отпечатан в типографии «Московский Печатный Двор», 123298, г. Москва, 3-я Хорошевская 18, корп. 1, офис 21А

АКТУАЛЬНОЕ МНЕНИЕ

- 4 **Атаки на цепочки поставщиков**
Игорь Некрасов (BIS Journal)
Рыжие собаки с Севера
- 6 **Дипфейки**
Марина Бродская (BIS Journal)
Новая напасть...
- 8 **Экспертиза**
Евгений Царёв (RTM Group)
От роста к хаосу и обратно
- 10 **СМС**
Денис Калемберг (SafeTech)
Время отказаться от СМС

НОВОСТИ

- 12 **Тенденции и прогнозы, в России, криминал**

ТЕМА НОМЕРА: ПЛАНИРОВАНИЕ ЦИФРОВЫХ ПРОРЫВОВ

- 16 Елена Покатаева (BIS Journal)
Не многоточие, а точки прорыва
- 28 Валерий Конявский (ОКБ САПР)
«Подход, который позволяет менять архитектуру компьютера во времени, дает возможность избавиться от многих видов уязвимостей»
- 35 Сергей Новиков (Станкоинструмент)
«Нас ожидает метрологическая революция»
- 38 Олег Выголов, Андрей Лаврентьев, Андрей Духвалов (Лаборатория Касперского)
Российские нейроморфные технологии – на острие мирового прогресса

- 43 Ренат Юсупов (Kraftway)
«Для реального прорыва нам не хватает системного подхода к развитию»
- 48 Захар Кондрашов (НИИМА «Прогресс»)
«Без прорывных технологий и продуктов невозможно движение в будущее на уровне мировых лидеров»
- 52 Ольга Пестерева (АО «Микрон»)
«Для реализации технологического суверенитета нет чудесных решений. Есть постоянная работа над развитием того, что уже создано»
- 55 Сергей Иващенко (UMNO digital)
Как «среднему классу» промышленности с низким уровнем цифровой зрелости массово подключиться к цифровой трансформации?
- 61 Иван Чернов (UserGate)
«Гонка в лабиринте: мы не всегда видим, как и куда бежит наш соперник»

РЕГУЛЯТОРЫ

- 64 **ФСТЭК России**
Анна Катанкина (BIS Journal)
«Актуальные вопросы защиты информации»
- 68 **Нормотворчество**
Екатерина Рачкова (BIS Journal)
Парад законов

ИБ В ОТРАСЛИ

- 72 **Собеседник**
Виталий Терентьев (HeadHunter)
«Мы живём в доме со стеклянными стенами...»
- 76 **Промышленные системы**
Андрей Стрелков (Лаборатория Касперского)
Не выбираем, а сочетаем
- 79 **Ассоциация ФинТех**
Александр Товстолип (Ассоциация ФинТех)
В данных обстоятельствах

УГРОЗЫ И РЕШЕНИЯ

- 81 **Ботнеты**
Данила Чежин (Servicerpipe)
Эволюция плохих ботов
- 84 **Сканеры**
Давид Ордян (METASKAN),
Владимир Соловьев (ДиалогНаука)
Что не так с периметром?
- 86 **Zero Trust**
Евгения Лагутина
(Лаборатория Касперского)
«Нулевое доверие»: ключевые принципы...
- 89 **Аудит**
Олег Нестеровский (ARinteg)
ARinteg спешит на помощь
- 92 **Защита приложений**
Кирилл Салов (NGENIX)
ИБ в облаке: поиск компромисса



94

ИНФРАСТРУКТУРА

- 94 **Деловые мероприятия**
Марина Бродская (BIS Journal)
Магнитка 2024
- 99 **Деловые мероприятия**
Анна Катанкина (BIS Journal)
ТБ Форум 2024
- 103 **Деловые мероприятия**
Алёна Николаева (BIS Journal)
Crypto Summit 2024

БЕЗОПАСНАЯ РАЗРАБОТКА

- 105 **Security Champions**
Рустам Гусейнов (РАД КОП)
Найти нельзя создать
- 108 **Экономика**
Светлана Газизова
(Positive Technologies)
Что получит бизнес, внедрив безопасную разработку?

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

- 111 **Опыт VK**
Максим Бронзинский (VK)
Сети, ловушки, засады, капканы...
- 114 **Вымогатели**
Андрей Жаркевич (Start X)
Вымогатели и человеческий фактор

ЗА РУБЕЖОМ

- 119 **Дайджест ИноСМИ**
Марина Бродская (BIS Journal)
Грань всё тоньше
- 123 **Законодательство**
Александр Виноградов (ФГУП «ЦНИИХМ»), Сергей Меньшиков (Belarusian InfoSecurity Community), Андрей Ситнов (независимый эксперт), Валерий Соколенко (ICBC)
ОДКБ. Кыргызская Республика

СУБЪЕКТЫ

- 129 **История**
Борис Столпаков
(историк криптографии)
«Мы прибыли сюда с надеждой и решимостью»
- 136 **Заметки безопасника**
Александр Игонин (BIS Journal)
Тёмная сторона силы... знаний

РЫЖИЕ СОБАКИ С СЕВЕРА

ГЛАВНУЮ УГРОЗУ ЭТОГО ГОДА ЗНАЛИ, ЖДАЛИ, НО, КАК ВСЕГДА, ПРОЗЕВАЛИ...



Игорь НЕКРАСОВ
главный редактор
BIS Journal

По итогам 2023 года атаки на цепочки поставок стали настоящим бедствием для компаний и специалистов по кибербезопасности. Согласно данным исследований, хакеры активно эксплуатируют вопросы доверия при проведении атак типа компрометации поставщиков ПО (Software Supply Chain Compromise) или доверия третьих лиц (Third-party Risk), которые принято объединять под общим названием атаки на цепочку поставок/поставщиков. Эта тенденция сохраняется в 2024 году и, похоже, становится его главным трендом.

THIRD-PARTY RISK

Атака на цепочку поставщика — тип атак, который реализуется через компрометацию сторонних компаний — партнёров, клиентов или подрядчиков. По данным НКЦКИ, атаки на «цепочки поставок» возглавляют топ-3 векторов проникновения в ходе наиболее опасных компьютерных атак, выявленных в России в 2023 г. Следом за ними идёт эксплуатация уязвимостей в ПО на периметре (что подпадает под атаки типа Software Supply Chain Compromise) и фишинг. Реализация всех видов атак через цепочку поставок стала главной тенденцией про-

шлого года как в России, так и в мире. И этот тренд только усиливается.

По данным исследования «Атаки на подрядчиков. Эксплуатация доверия» компании «Инфосистемы Джет», лишь 20 % компаний определяют набор мер, исходя из специфики взаимодействия и профиля риска поставщика, менее 10 % проводят мероприятия по оценке уровня ИБ поставщика услуг. «Оценка проводится в основном с использованием опросных листов и зачастую носит формальный характер — не влияет на дальнейшее решение о выборе поставщика или архитектуры подключения к ресурсам компании. 80 % компаний используют защитные меры в отношении подрядчиков/поставщиков услуг, аналогичные удалённым работникам», — говорится в исследовании.

Чаще всего злоумышленники попадают в инфраструктуру к слабо защищённому поставщику, а затем двигаются по ней, получая доступ к более крупной жертве, отмечают эксперты по безопасности. Например, так злоумышленники из группировки LockBit, взломавшие системы консалтинговой компании Infosys McCamish Systems (IMS), получили доступ к данным клиентов Bank of America. Другой пример — «популярные» у хакеров взломы поставщиков медицинских услуг в Северной Америке. В результате взлома компании Shields Health Care Group злоумышленники получили данные 2 млн пациентов.

Кибератака вымогателей на компанию Change Healthcare, входящую в группу UnitedHealth Group, привела к отключению сервисов и, как следствие, нарушила систему взаиморасчётов и оборота лекарств, работу страховых компаний, врачей

и больниц, аптечных сетей по всей территории США. Инцидент привёл к увеличению нагрузки на всю систему здравоохранения страны, вмешательству регуляторов, финансовым убыткам. Появлялись сведения, что Change Healthcare выплатила крупный выкуп хакерам, которые заявили, что в ходе атаки получили данные клиентов компании. Также целями атак становятся финансовые и ипотечные компании, юрфирмы и ретейлеры, которые хранят конфиденциальную информацию, включая персональные данные клиентов и партнёров.

Из российских инцидентов наибольшую огласку получила утечка архива учётных записей более 60 тыс. пользователей компании «ИнфоТекС», которая произошла на стороне подрядчика, ответственного за разработку нового сайта. Хакеры эксплуатировали неизвестные уязвимости в системе «1С-Битрикс: Управление сайтом».

По мнению отечественных регуляторов, для обеспечения безопасности цепочек поставок необходимо управлять подключениями привилегированных пользователей из числа подрядчиков, следить за появлением сведений о компьютерных инцидентах в подрядных организациях, требовать от них отчёты о принятых мерах по реагированию на кибератаки. Иностранные регуляторы добавляют к этим советам рекомендации по сегментации сети и использованию многофакторной аутентификации для всех делегированных администраторов.

КОМПРОМЕТАЦИЯ ЦЕПОЧКИ

В 2022 г. компания Sonatype, которая занимается управлением цепочки поставок ПО, в ежегодном

исследовании, посвящённом программному обеспечению с открытым кодом (OpenSource Software – OSS), разработке приложений на его основе, а также безопасности цепочки поставок такого ПО, отмечала рост числа атак на репозитории OSS. Чаще всего разработчики не подготавливали о внедрении вредоносных пакетов в свои продукты в процессе сборки: одна из восьми загрузок OSS сопряжена с риском, говорится в исследовании.

По состоянию на осень 2023 г. Sonatype зарегистрировала более 245 тыс. подобных атак, это втрое больше, чем годом ранее. Устранение последствий такого числа инцидентов обошлось компаниям в \$ 46 млрд. Исследователи отметили, что число атак на цепочки поставок за 2023 г. в два раза превышает суммарные показатели 2019–2022 годов.

По данным отчёта Application Security Posture Management 2024 компании Sycode, которая специализируется на обеспечении безопасности и управлении исходным кодом в области разработки ПО, 77 % из 500 опрошенных CISA в США считают безопасность цепочки поставок ПО слепым пятном для AppSec. При этом разработчики приложений чаще сосредоточены на устранении критических уязвимостей, чем на исследовании безопасности используемого ПО. Только 21 % разработчиков и безопасников понимает, что несёт солидарную ответственность за OSS. 2023 год показал, что экспоненциальный рост атак на цепочки поставок, связанный с вредоносным ПО, затормозил рост числа эксплоитов.

Исследователи отмечают активное внедрение ВПО в репозитории OSS. Северокорейская группировка Lazarus в рамках кампании PaperPin активно атакует репозиторий Python. Так, целью пакетов VMConnect является дальнейшая загрузка ВПО с URL-адресов, контролируемых злоумышленниками, при использовании библиотек Python. В феврале 2024 г. о внедрении пакетов rusrpctoenv и rusrpctoconf, которые схожи с библиотекой инструментов шифрования rusrpcto для Python, сообщил CERT Японии. При загрузке лжепа-

По данным НКЦКИ, атаки на «цепочки поставок» возглавляют топ-3 векторов проникновения в ходе наиболее опасных компьютерных атак, выявленных в России в 2023 г.

кетов происходит дальнейшее заражение трояном Comebacker.

Уязвимость в компоненте с открытым исходным кодом Redis, который использовала компания OpenAI, привела к утечке данных пользователей ChatGPT. Несколько крупных атак на цепочки поставок зарегистрировано на PyTorch – платформу машинного обучения. Атака на разработчика VoIP-решений 3CX и его клиент 3CXDesktopApp могла скомпрометировать миллионы клиентов, этим решением пользуются более 600 тыс. организаций, включая транснациональные корпорации.

Некоторые из наиболее значительных Supply Chain Attack включают эксплуатацию уязвимостей популярных инструментов. Атака на ПО для управляемой передачи файлов MOVEit Transfer привела к цепочке взломов, затронув более тысячи предприятий и 60 млн частных лиц. Общий ущерб превысил \$ 9,9 млрд. Серию примеров можно продолжать до бесконечности.

По данным Sonatype, почти 96 % загрузок компонентов с известными уязвимостями можно избежать, если обращать внимание на версии релизов. До сих пор четверть всех загрузок библиотеки журналирования Log4j приходится на версию, содержащую уязвимость нулевого дня Log4Shell и закрытую в декабре 2021 г.

ЧТО ДЕЛАТЬ?

В 2022 г. Агентство ЕС по кибербезопасности (ENISA) назвало компрометацию цепочек поставок ПО новой главной киберугрозой. Признавая последствия для национальной безопасности и экономической стабильности, США и ЕС создают нормативные базы и разрабатывают рекомендации по усилению защиты от эскала-

ции киберрисков. Комплексный подход к проблеме включает требования к критически важной инфраструктуре, национальные стратегии кибербезопасности, законы о защите данных и расширение международного сотрудничества в борьбе с киберпреступностью. Аналогичные меры принимает Канада, Quad – стратегический союз Австралии, Индии, США и Японии по проблемам безопасности в Индо-Тихоокеанском регионе. Частные компании, занимающиеся вопросами управления цепочками поставок ПО, разрабатывают и продвигают на рынок платформы и экосистемы – закрытые среды, предлагающие доверенную разработку ПО. Также рекомендуется учитывать вопросы безопасной разработки на всех этапах жизненного цикла ПО, повышение уровня зрелости его разработчиков и потребителей.

В России в 2022 г. с целью повышения безопасности под эгидой ФСТЭК на базе ИСП РАН создан Технологический центр исследования безопасности ядра ОС Linux, в его работе принимают участие ведущие вендоры страны. Главная задача центра – повышение уровня безопасности отечественных Linux-систем. Также планируется создание испытательных полигонов и защищённых репозиториях доверенного ПО и программно-аппаратных комплексов, типовых решений, предназначенных для разработки, тестирования, хранения, распространения, развития и технической поддержки отечественного ПО. Работы ведутся в рамках нацпрограммы «Цифровая экономика» и войдут в нацпроект «Экономика данных».

А пока эти работы ведутся, атаки через поставщиков продолжают множиться...

НОВАЯ НАПАСТЬ...

ПОХОЖЕ, 2024-Й СТАНЕТ ЕЩЁ И ГОДОМ ДИПФЕЙКОВ



Марина
БРОДСКАЯ
обозреватель
BIS Journal

Доступность онлайн-инструментов и улучшенных инструментов ИИ открывает мошенникам новые возможности. Похоже, 2024-й станет ещё и годом дипфейков (deepfake, от англ. deep – глубокий и fake – подделка) – такой прогноз дали аналитики компании Onfido, специализирующейся на сервисах онлайн-проверки личности.

Согласно отчёту Identity fraud report 2024, в прошлом году число попыток мошенничества с использованием дипфейков выросло на 3000 % к показателям 2022 г. Менее изощрённые виды мошенничества выросли всего на 7,4 %. Рост числа дипфейков связан с широкой доступностью онлайн-инструментов и инструментов ИИ, что влияет на векторы атак по всем направлениям – от манипулирования цифровыми документами до дипфейков, отметили исследователи. Количество мошенничеств с биометрическими данными удвоилось. Число подделок цифровых документов выросло на 18 %, основными целями являются национальные

удостоверения личности (46,8 %) и заграничные паспорта (26,7 %). В 80 % случаев мошенники пытаются подделать видеоизображение.

СЛУЧАЙ В ГОНКОНГЕ

События начала 2024 г. подтверждают выводы экспертов. В конце января одна из транснациональных корпораций потеряла \$ 25,6 млн в результате мошенничества с использованием технологии дипфейк.

С заявлением в полицию обратился сотрудник гонконгского филиала корпорации. Он сообщил, что получил электронное письмо от финансового директора компании из Великобритании, в котором тот требовал провести секретную транзакцию. Поскольку послание вызвало у служащего сомнения, он пригласил финансового директора на групповую видеоконференцию с участием других сотрудников, знакомых работнику. Во время видеозвонка представители головного офиса в основном давали указания, а не общались между собой. В какой-то момент встреча оборвалась, что не смутило работника. Он осуществил 15 переводов на пять банковских счетов в Гонконге на общую сумму \$ 25,6 млн. Весь эпизод – с момента первого контакта с жертвой до её запроса в штаб-квартиру и обнаружения факта мошенничества – занял около недели.

Такие же методы злоумышленники использовали для общения ещё с несколькими сотрудниками компании, они поддерживали связь с жертвами

через мессенджеры, электронную почту и видеозвонки.

Полиция Гонконга не раскрывает название корпорации и продолжает расследование. Это первое подобное дело в Гонконге, отмечают следователи, и потому ему уделяется особое внимание. Установлено, что участники видеовстречи были воссозданы злоумышленниками в цифровом виде на основании общедоступных видео- и аудиозаписей этих людей.

СЛУЧАЙ В НИДЕРЛАНДАХ

В инциденте в Нидерландах финтех-банк Bunq избежал финансовых потерь. Али Никнам, генеральный директор Bunq, сообщил, что его сотруднику поступил видеозвонок от имени босса с просьбой срочно перевести крупную сумму денег. «Признаюсь, я был искренне удивлён, насколько убедительным оказался мой дипфейковый двойник», – написал Никнам в соцсети LinkedIn, отметив, что в организации есть процессы, которые обеспечивают безопасность в подобных ситуациях. В компании смогли быстро обнаружить мошенничество и в считанные минуты предупредить сотрудников о новой схеме обмана.

ПО ВСЕМУ МИРУ

Сегодня по всему миру известны многочисленные случаи, когда жертвы мошенничества были обмануты во время видеозвонков один на один или после просмотра роликов на сайтах и в соцсетях, в которых дипфейки знаменитостей предлагают незадачливым инвесторам вложиться в криптовалюты и удвоить свои деньги за считанные дни. В США используют образы Тейлор Свифт, Илона Маска и Брайана Армстронга, в Индии – известных финансистов и инвесторов, в России – актёров, якобы разбогатевших на крипте, или знакомых, попавших в затруднительную ситуацию. В Гонконге полиция арестовала нескольких граждан, которые использовали дипфейки и поддельные удостоверения личности при

В прошлом году число попыток мошенничества с использованием дипфейков выросло на 3000 % к показателям 2022 г. Менее изощрённые виды мошенничества выросли всего на 7,4 %

подаче заявок на кредиты и открытие счетов, они пытались обмануть программы распознавания лиц путём создания дипфейков людей, изображённых на украденных документах.

Как отмечают специалисты в США, пока ни один федеральный закон чётко не запрещает дипфейки. Девять штатов приняли законы, криминализирующие «глубокую порнографию без согласия». В марте во Флориде был принят законопроект, ограничивающий использование ИИ в политических кампаниях и обязывающий создателей рекламы извещать зрителей об использовании генеративного ИИ при изготовлении ролика. За нарушение требований вводится уголовная ответственность.

В ЕС дипфейки регулируются Законом об ИИ, который требует

от создателей и распространителей материалов раскрывать их искусственное происхождение и предоставлять информацию об используемых методах. Ещё один шаг — инициатива «Техническое соглашение по борьбе с мошенничеством использованием ИИ на выборах 2024 года», принятая на Мюнхенской конференции по безопасности. Это попытка противостоять вызовам, создаваемым дипфейками в избирательных процессах на фоне многочисленных кампаний этого года.

Крупные технологические платформы и соцсети уже выразили готовность маркировать контент, созданный ИИ.

В России на правительственном уровне идёт обсуждение вопросов правового регулирования техноло-

гии подмены личности (дипфейк) в целях недопущения её использования в противоправных целях. Сегодня в российском законодательстве отсутствуют отдельные категории преступлений, связанные с дипфейками. Правительство России планирует ввести наказание за использование таких технологий в противоправных целях. Предложения по этому вопросу должны проработать и предоставить Минцифры России совместно с МВД РФ и Роскомнадзором до 1 ноября 2024 г.

На итоговой пресс-конференции Level Up with Kaspersky в январе Сергей Голованов, главный эксперт «Лаборатории Касперского», заявил: «Все опасаются прямого эфира, в котором появится злоумышленник». «Это будет проблема, — сказал эксперт, — и ожидается она даже не в 2025 году, а уже в 2024-м».

BIS-КОММЕНТАРИЙ



Сергей ГОЛОВАНОВ
главный эксперт
«Лаборатории
Касперского»

Если злоумышленники обладают записями выступления человека, они с помощью нейросетей могут создать на их базе аудио- или видеозапись с необходимым содержанием, то есть имитировать голос и мимику этого человека. Инструменты для этого существуют, в том числе в открытом доступе. Причём изображение может быть с достаточно высокой детализацией, невооружённым глазом будет сложно отличить, настоящая это запись или нет. Такие методы могут применяться в много-

одного из этапов атаки: злоумышленники начинают переписку с жертвой в мессенджере, выдавая себя за знакомого или сотрудника. Для убедительности присылают видео- или аудиосообщение, а потом предупреждают, что в скором времени с жертвой свяжутся якобы из банка или правоохранительных органов, или требуют срочно перевести средства на определённый счёт. После чего следует уже стандартная схема, цель злоумышленников — украсть деньги.

Однако в режиме реального времени создавать подобную запись всё ещё крайне сложно. Несмотря на возможности современных нейросетей, действительно качественный дипфейк в реальном времени остаётся дорогостоящей и непростой задачей, требующей высокого уровня подготовки. В первую очередь речь идёт о больших вычислительных мощностях, продвинутых навыках и времени на сбор данных. Описанный случай [в Гонконге] скорее можно назвать единичным, однако не ис-

ключено, что на горизонте нескольких лет такие ситуации могут стать более массовыми.

Судя по описанию инцидента, большая часть роликов была создана заранее, в удобный для злоумышленников момент связь обрывалась.

Если говорить о том, как не попасться в руки мошенников, эксплуатирующих дипфейк-технологии, то основной способ — повышать цифровую грамотность и критически подходить к любым сообщениям в сети. Необходимо проверять информацию, которой с вами делятся, даже если она от знакомых. Стоит обращать внимание на качество видео- или аудиоконтента: возможны дефекты в изображении или помехи в голосе. Если вы говорите в реальном времени, попросите собеседника покрутить головой из стороны в сторону, поднести руки к лицу, задайте внезапный вопрос, на который нет очевидного ответа. Если собеседник просит сделать что-то в срочном порядке, пугает возможной ответственностью или последствиями — это повод насторожиться.

ОТ РОСТА К ХАОСУ И ОБРАТНО

ЗАЧЕМ ПРОВОДИТЬ ЭКСПЕРТИЗЫ ПРИ ПРИЁМКЕ ИТ-ПРОЕКТОВ?



Евгений ЦАРЁВ
управляющий
RTM Group

В последние несколько лет государство очень заметно инвестирует в ИТ-сектор, открывает различные инициативы, даёт льготы ИТ-компаниям, предоставляет субсидии. Эта активность запустила цепочку производства более качественных и дорогих услуг и продуктов. Казалось бы, самое время, чтобы ИТ-сектор совершил качественный скачок и создаваемые системы с внедряемыми продуктами работали эффективно, без сбоев. Однако на деле получается так, что средства вкладываются огромные, а ИТ-решения в полную силу не работают. Почему это происходит и как можно было бы исправить ситуацию?

СНИЖЕНИЕ ВМЕСТО ПОВЫШЕНИЯ

Сегодня российская отрасль ИТ, по мнению многих, переживает свой золотой век. В крупных компаниях зарплатой разработчика в 500 тыс. рублей никого не удивишь. Увеличилось количество игроков, продуктов, да и число проектов кратно выросло. По данным Минцифры, валовая добавленная стоимость ИТ-отрасли возросла с 319 млрд руб. в 2012 году до 1898 млрд руб. в 2022 году. Притом что количество людей в отрасли если и увеличилось, то не в разы. Да и уехавших специалистов нужно учиты-

вать: далеко не все они продолжили работать с российскими организациями на удалёнке. По нашим оценкам, сейчас больше всего начинающих и среднеуровневых специалистов, а старших экспертов с опытом не хватает. Всё это спровоцировало дополнительную нагрузку ИТ-повесткой на руководителей разных уровней. При этом менеджмент предприятий, как и системы закупки, существенно не изменились.

И вместо повышения эффективности ИТ в целом мы наблюдаем её снижение. Если раньше условное государственное учреждение вкладывало по 10 млн руб. в год в свои ИТ-сервисы, то теперь, получив субсидию, может потратить на них 200 млн руб. за год. Это же хорошо? Конечно. Но, как говорится, есть нюанс. Если раньше был один подрядчик, теперь их может быть десяток, если раньше вопрос интеграции разных компонентов не вставал, теперь он появился, если раньше собственное ИТ-подразделение успевало осуществлять управление проектами, то теперь есть сбой, и так далее.

КАК ПОТРАТИТЬ, НЕ ПОЛУЧАЯ РЕЗУЛЬТАТА

Показательно в этом смысле одно из судебных разбирательств. Имён по понятным причинам раскрывать не будем, но о сути расскажу. Государственное предприятие, входящее в промышленную группу, реализовывало большой комплексный проект. Происходило внедрение двух независимых систем автоматизации и целого перечня средств обеспечения информационной безопасности. Общее количество автоматизированных рабочих мест (АРМ) в сети — более 5 тыс. штук. Проекты были поделены на 5 договоров, четыре из которых — контракты на поставку

и внедрение. А вот пятый был растянут на два года и содержал два этапа: проектирование и приёмосдаточные испытания. Фактически интеграция всех решений в итоговое по этому договору была на стороне подрядчика. Проблемы начались на этапе, когда все решения были поставлены и по документам внедрены. И осталось лишь провести приёмосдаточные испытания. При этом ни одна из систем автоматизации не работала, как и часть средств защиты информации. Судебный иск был подан к подрядчику по пятому договору. Логично, ведь это он не мог осуществить сдачу последнего этапа. В результате экспертизы выяснилось, что в течение двух лет от создания проектного решения до испытаний заказчик осуществил переход на новую ОС, а часть технических решений была адаптирована к работе на предыдущем производителе и версии операционки. Плюс на этапе экспертизы выявились проблемы с системами автоматизации (они не были адаптированы под деятельность заказчика). Получается, деньги, время и усилия специалистов потрачены зря. Часть руководителей и сотрудников уволились или были уволены, также параллельно с судебным процессом шла проверка компетентными органами.

Приведённый пример не является чем-то из ряда вон выходящим, в последнее время таких кейсов становится всё больше. Быстрый рост сопряжён с существенными рисками контроля расходования. Государство стремится не просто потратить деньги, а потратить их с пользой. Поэтому надзорные мероприятия необходимы. Учитывая, что субсидирование подразумевает особое внимание контролирующих структур и необходимость отчитываться перед ними, внутренней



ИТ-службе и юридической службе, которые обслуживают весь этот резкий рост инвестиций, требуется какая-то страховка от неминуемых ошибок.

СТРАХОВКА ОТ ОШИБОК

В таких проектах важно всё документировать. Бумаги, к слову, могут также послужить доказательствами в ходе возможных судебных разбирательств. В рамках прокурорского надзора, который происходит очень часто, и контроля ФСБ также проверяются именно формальности (хронология проекта, наличие отчётных документов по всем этапам, право подписи ответственных и т.д.). И если обнаруживаются несоответствия, это может повлечь за собой иные проверки и даже возбуждение уголовного дела. Особенно если речь идёт о государственных деньгах.

При этом специалисты понимают реалии, например, разработки программных продуктов или поставки многокомпонентных серверных решений. Нюансы могут возникнуть на любом этапе. Например, были задержки в поставке отдельных компонентов для оборудования ЦОДа, а приёмка осуществляется для всего комплексного проекта, и некомплект быть не должно. При этом самому заказчику необходимо потратить деньги, например, до 31 декабря. И проект закрывается, а компоненты «довозятся» с задержкой

в несколько месяцев. В зависимости от проекта такое действие представителей заказчика может быть расценено как преступление. Правда, иногда всё можно оформить посредством подписания дополнительного соглашения или через иное оформление гарантийных обязательств поставщика. Важно, чтобы в итоге обе стороны договора были удовлетворены результатом, деньги были потрачены не зря и результат получен.

В этом сегменте особая ответственность лежит на руководстве, и это притом, что проектов очень много, а технических знаний и навыков для оценки ситуации и результатов работ не хватает. И любая поставка сложного ИТ-продукта, требующего длительного и сложного внедрения и адаптации, может стать проблемой. А это как раз более 90 % всех подобных проектов, ведь даже покупка обычного антивируса на крупном предприятии — непростое дело. Риски таких проектов чрезвычайно велики, особенно когда существует текучка кадров в ИТ- или ИБ-службах предприятия. И несут их подписанты при приёмке, а это обычно руководители служб ИТ и ИБ, а также первое лицо предприятия.

И СНИЖЕНИЕ РИСКОВ

Одним из вариантов радикального снижения рисков является привлечение независимой третьей стороны,

которая не только принимает участие в составлении договора, но и участвует в приёмке результата выполненных работ или поставки, оценивая фактическое выполнение услуг, например, по внедрению информационной системы. Что, в свою очередь, поможет снизить риски приёмки стороной заказчика и, как ни странно, исполнителя.

Если возникнут какие-либо вопросы со стороны проверяющих органов или судебного дела, эксперты третьей стороны могут дать свои пояснения и подтвердить соответствие или несоответствие техническому заданию. Регуляторная и судебная системы не могут игнорировать заключения экспертов.

Таким образом, участие третьей экспертной стороны в приёмке сложных и комплексных проектов будет направлено на снижение рисков руководителей организаций и позволит им быть уверенными в эффективном расходовании государственных средств. В то же время надзорные органы могли бы оперативно получать отчётность по крупным проектам, избегая привлечения собственных ресурсов. И снизить нагрузку по последующим разбирательствам. В итоге все могут оказаться в плюсе, а средства будут расходоваться действительно эффективно, что позволит вывести отрасль и крупные российские компании на качественно иной уровень.

ВРЕМЯ ОТКАЗАТЬСЯ ОТ СМС



**Денис
КАЛЕМБЕРГ**
генеральный
директор
SafeTech

Отказ от привычных способов подтверждения транзакций для банков в виде кодов из СМС и push – необходимость. И не только из-за нормативных документов ЦБ. Множащиеся атаки на клиентов банков требуют повышения уровня безопасности. Кроме того, грядущее увеличение штрафов за отказ от перехода на безопасное подтверждение операций делают излишний консерватизм слишком дорогим в финансовом плане. К счастью, на рынке есть решения, позволяющие обеспечить безопасное подтверждение операций в соответствии с требованиями законных и подзаконных актов.

В начале апреля в СМИ был вал публикаций о мошеннических схемах, в которых социальные инженеры убеждали граждан называть им код из СМС, и в результате получали доступ к мобильному банку и выводили деньги со счета жертвы. Скрипты были разные. Например, абонентов сотовой связи, ссылаясь на теракт в «Крокус Сити Холл», про-

сили подтвердить номер телефона. Объединяло все эти схемы одно – деньги выводились из банков, в которых транзакции подтверждались кодами из СМС или push-сообщений. То есть из тех кредитных организаций, кто фактически нарушал требования регулятора.

ЧТО СКАЗАЛ ЦБ?

Еще 18 февраля 2022 года ЦБ указанием № 6071-У внес изменения в Положение 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». Тогда и были конкретизированы требования по подписанию электронных сообщений. В документе появилась норма – «в целях обеспечения целостности электронных сообщений и подтверждения их составления уполномоченным на это лицом кредитные организации должны обеспечивать реализацию мер по использованию усиленной квалифицированной электронной подписи, усиленной неквалифицированной электронной подписи или СКЗИ, реализующих функцию имитозащиты информации с аутентификацией отправителя сообщения» (пункт 5.1 положения № 683-П). В марте 2023 года мегарегулятор еще раз подтвердил свое желание усилить безопасность электронных сообщений, указав в разъяснительном письме: «исполь-

зование ПЭП в указанных целях возможно только совместно с СКЗИ, реализующими функцию имитозащиты информации с аутентификацией отправителя сообщения».

ЗАЧЕМ СКАЗАЛ? ОЧЕВИДНОЕ

Причины, по которым ЦБ ужесточит требования к подтверждению финансовых транзакций, очевидны. Коды из СМС или push-сообщений уязвимы во время всего своего жизненного цикла. Начнем с того, что одноразовый код известен банку до момента отправки клиенту, что может стать аргументом в конфликтной ситуации (например, когда было хищение, платеж был подтвержден кодом из смс и клиент утверждает, что он СМС не получал). Кроме того, в передаче кода задействована третья сторона, уязвимость инфраструктуры которой может привести к массовым хищениям со счетов клиентов. Есть вопросы и по каналу связи. В документации Google прямо прописан запрет на передачу банковских кодов через канал PUSH. Канал передачи СМС является небезопасным из-за уязвимости протокола SS 7. Это уже привело к массовым хищениям у клиентов немецких банков и запрету на использование смс кодов в Европе (платежная директива PSD 2) и Сингапуре. Помимо этого, перевыпуск SIM-карты по поддельной доверенности позволяет мошенникам получить код вместо клиента. А код, доставленный в смартфон, может быть перехвачен вредоносным ПО, введен на фишинговом сайте или выведен при помощи социальной инженерии.

НЕОЧЕВИДНОЕ

Неочевидно другое – почему многие кредитные организации до сих пор не выполняют требования регулятора – пункт 5.1 положения № 683-П вступил в силу еще в октя-

Причины, по которым ЦБ ужесточит требования к подтверждению финансовых транзакций, очевидны. Коды из СМС или push-сообщений уязвимы во время всего своего жизненного цикла

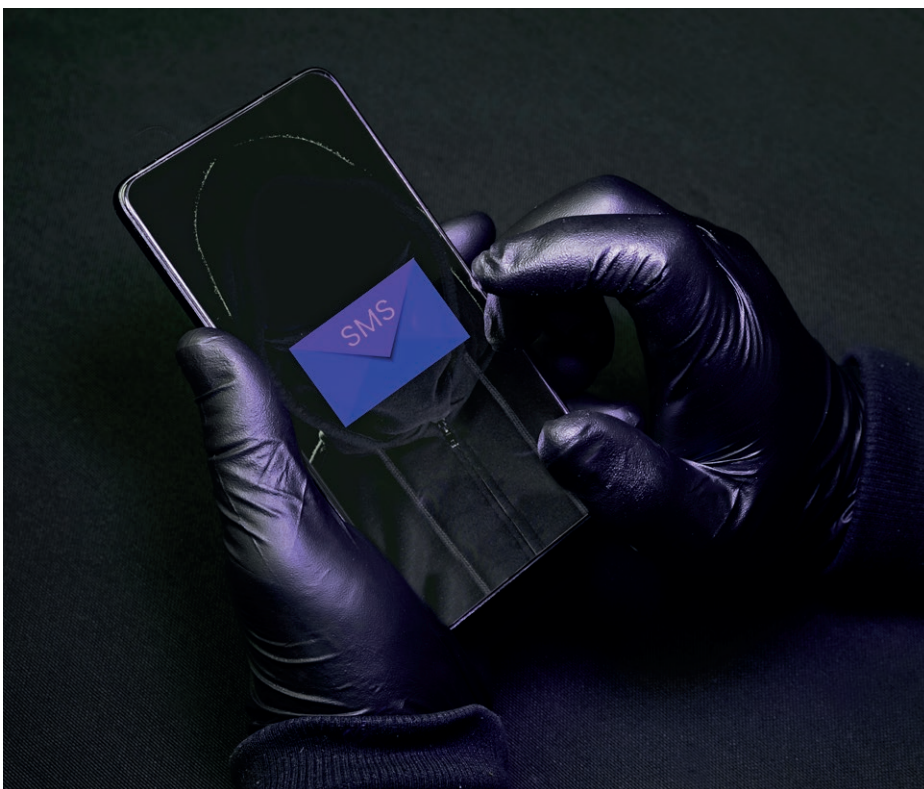
бре 2022 года. Тем более что на рынке есть решения, которые могут обеспечить безопасное подтверждение транзакций в соответствии с требованиями положения 683-П.

ЧЕТЫРЕ ВАРИАНТА

Для этого могут использоваться решения, основанные на симметричной или асимметричной криптографии, аппаратные или программные. Пример решений, основанных на симметричной криптографии – аппаратные криптокалькуляторы и программные генераторы кодов подтверждения для смартфонов. Минус первых – неудобство (необходимо руками вбивать пин код, номер счета, сумму, генерировать код, вбивать его в поле подтверждения) плюс стоимость от 10 долларов. Генераторы кодов – это мобильные приложения, ими удобнее пользоваться и удобнее распространять, но есть вопросы при возникновении спорных ситуаций с клиентами. На асимметричной криптографии основаны аппаратные USB токены и мобильная электронная подпись. У первого решения минусом также является стоимость и отсутствие возможности работать с мобильными устройствами (за исключением новых моделей с NFC). Мобильная электронная подпись – это приложение для смартфона, она имеет преимущества решений на асимметричной криптографии (закрытый ключ только у клиента, отображение документа на экране перед подписанием, нет кода, который можно было бы ввести на фишинговый сайт или сообщить мошеннику и т.д.) плюс удобство.

ОПТИМАЛЬНЫЙ ВАРИАНТ

Очевидно, что из всех четырех вариантов оптимальным является именно мобильная электронная подпись, совмещающая низкую стоимость, простоту распространения и юридическую значимость. Например, PayControl ГОСТ, который является средством для формирования усиленной неквалифицированной электронной подписи в смартфоне. Решение работает с использованием сертифицированных СКЗИ КриптоПро CSP и JCP, что позволяет сформировать и проверить усиленную неквалифи-



цированную электронную подпись в соответствии с государственными стандартами ГОСТ Р 34.11–2012 и ГОСТ Р 34.10–2012. Использование PayControl ГОСТ не только повышает защищенность операций, снижая уровень фрода в ДБО (в том числе и с использованием социальной инженерии), но и повышает usability для клиента. PayControl ГОСТ позволяет «превратить» мобильное устройство в аналог USB-токена с таким же высоким уровнем безопасности и очень простым пользовательским сценарием. Происходит подтверждение транзакций следующим образом – клиент создает операцию в DIGITAL-канале, информация об операции отображается в мобильном приложении, клиент нажимает «Подтвердить», операция подписывается, вся процедура может занять до 3,5 секунд. Создается подпись путём криптографических преобразований подтверждаемой информации в сочетании с уникальными характеристиками конкретного смартфона. PayControl ГОСТ работает на ОС Android и iOS.

О ВЫГОДЕ

Подтверждение финансовых транзакций в соответствии с требованиями

ми регулятора несет кредитной организации и финансовую выгоду. Если взять небольшой розничный банк с клиентской базой в 200 тыс. чел, то траты его на смс будут порядка 420 руб. на клиента в год, то есть более 80 млн руб. по банку в целом. Если это банк с корпоративными клиентами, то расходы на смс могут быть и 800 млн руб. в год, так как юрлица проводят больше операций. Переход на PayControl ГОСТ позволит сэкономить от 60 млн руб. ежегодно (если банк розничный), и сотни миллионов руб. в банке для юрлиц.

Кроме того, законодатели обсуждают возможность повышения штрафов для кредитных организаций за неисполнение требований нормативных документов ЦБ, в том числе и положения 683-П. Размер санкций предлагают увеличить в 10 раз, до 1 % от собственных средств (капитала) вместо 0,1 % сейчас. Поэтому подтверждение транзакций кодами из смс или push-сообщений в будущем может обернуться для банков ощутимыми штрафами. Так что самое время переходить на PayControl ГОСТ, позволяющий выполнить требования нормативных документов ЦБ и при этом сэкономить на стоимости смс.

ОПЫТ СБЕРА

На портале Сбера «Кибрарий» опубликована книга «Аналитическая платформа Кибербезопасности. Опыт Сбера».

Сегодня Платформа кибербезопасности является ключевым элементом системы управления киберрисками Сбера и обеспечивает real-time поток более 500 млрд событий в сутки, обработку 535 уникальных источников событий, основу для 25 внутренних продуктов и сервисов SOC и АнтиФрода, базу для обучения AI-моделей и многое другое.

В книге раскрывается архитектура, принципы построения, состав функциональных компонент платформы, а также сравниваются различные платформенные решения. По мнению авторов, эти материалы могут стать основой для создания открытого сообщества разработчиков систем кибербезопасности с применением технологий прикладной, продвинутой, прогнозной и предиктивной аналитики.

MICROSOFT СЛЕГКА ПРИТОРМОЗИЛ

В Softline рассказали, что Microsoft обсуждает перенос срока приостановки доступа к облачным сервисам для российских корпоративных клиентов с 20 марта на апрель.

Компания уточнила, что отсрочка не отменит планируемые ограничения, но даст время сделать бэкапы и настроить работу альтернативной инфраструктуры.

Ранее о прекращении доступа к облачным сервисам Microsoft сообщила всем причастным с помощью рассылки официальных уведомлений — под блокировку вероятнее всего попадут Teams, OneDrive, Azure, Office 365, а также другие сервисы и образовательные продукты. Речь, по-прежнему, идёт о юрилицах — физлиц ситуация пока не коснётся.

Подготовила Яна Белобрагина

ПОЛИТИЧЕСКИЕ АТАКИ: РАЗМИНКА ОКОНЧЕНА

Компания Servicepipe, специализирующаяся на обнаружении и фильтрации автоматизированных кибератак на онлайн-ресурсы, выявила четырехкратный рост объема атак хактивистов за год.

Так, на конец I квартала 2023 г. средняя пиковая мощность всех DDoS-атак, сгенерированных политически мотивированными хакерами, составляла 13 Гбит/с. На конец I квартала 2024 г. средняя пиковая мощность выросла до 47 Гбит/с. Увеличилась и длительность атак. В I квартале 2023 г. средняя DDoS-атака длилась 12 часов. В I квартале 2024 г. — не менее суток.

Изменился и выбор целей. Год назад атаки шли четко по отраслям, основными целями были финансовые организации, госсектор и СМИ. Сейчас нет отраслей, которые в той или иной степени не интересны злоумышленникам.

«В 2024 г. хактивисты могут атаковать даже безобидный онлайн-кинотеатр под лозунгом «Мы создаем ущерб российской экономике!», а это значит, что угроза есть почти для любой российской компании, от работы сервисов которой зависят другие лица», — указывает владелец продукта DosGate Даниил Бобрышев.



ПРОГНОЗ УГРОЗ ДО 2030 ГОДА

Агентство по сетевой и информационной безопасности ЕС (ENISA) опубликовало прогноз угроз кибербезопасности до 2030 года. Главными угрозами считаются:

- ◆ кибератаки на цепочки поставок ПО;
- ◆ нехватка навыков и дефицит квалифицированной рабочей силы;
- ◆ человеческие ошибки и устаревшие ИТ-системы;
- ◆ использование устаревшего и непропатченного ПО в рамках перегруженной межотраслевой ИТ-экосистемы;
- ◆ потеря конфиденциальности и увеличение числа случаев цифровой слежки за людьми;

- ◆ уязвимость трансграничных поставщиков ИТ-услуг как единой точки отказа;
- ◆ широкие высокотехнологичные кампании по дезинформации;
- ◆ рост числа высокотехнологичных гибридных угроз;
- ◆ неправомерное использование технологий ИИ;
- ◆ воздействия природного характера на объекты КИИ.

Несмотря на некоторое снижение общего показателя компрометации ПО в цепочке поставок, исследователи отмечают расширение самих цепочек за счет интеграции поставщиков и партнеров, что приводит к появлению новых уязвимостей.

ИИ ОСВАИВАЕТ СИБИРЬ

Сбер, Правительство Иркутской области и Иркутский национальный исследовательский технический университет (ИРНИТУ) подписали меморандум о сотрудничестве, предполагающем синергию усилий сторон в создании Байкальского центра



изучения искусственного интеллекта и цифровых технологий.

Документ был подписан в ходе рабочего визита зампреда правления Сбера А. Ведяхина в регион. Он сам прокомментировал событие так: «Центр, об открытии которого мы договорились, позволит значительно расширить применение технологий искусственного интеллекта в Иркутской области, повысив качество сервисов для жителей региона. Главными направлениями его научно-исследовательской деятельности станут климатические изменения, безопасность, энергетика и гуманитарные технологии. В этом году центр займется проектом по сохранению озера Байкал, созданием сервиса по работе с обращениями жителей области, а также сервиса по получению субсидий для производителей сельхозпродуктов. Еще одно важное направление — прогнозирование лесных пожаров, паводков и других стихий».

САНКЦИИ НА ПРОВАЙДЕРОВ ЦОД

Минфин США включил в новый санкционный пакет российских провайдеров ЦОД. Ранее такие ограничения не вводились.

Под санкции попали следующие операторы дата-центров: 3data (5900 стоек, по оценке iKS-Consulting); Oxygen (1700 стоек); «Миран» (561 стойки); SafeData (21 400 стоек); «ТрастИнфо» (1200 стоек; ГК «Айтеко»); Региональный ЦОД «ИнфоТех Балаково»; «Стек Телеком» (1400 стоек) и др.

Для самих участников рынка включение в санкционный перечень стало неожиданностью. Многие из них закупали импортное серверное оборудование и лицензии на софт, но теперь могут этого лишиться.

Ограничения США скажутся на бизнесе компаний, работа которых завязана на технологическом оборудовании западных стран, уверены эксперты.



АССОЦИАЦИЯ
БАНКОВ
РОССИИ

XXIV Всероссийская банковская конференция «Банки и институты развития в России: формат взаимодействия и сотрудничества»

Среди спикеров конференции - руководители Банка России, Минфина, других федеральных министерств и ведомств, Госдумы, Совета Федерации, ведущих кредитных организаций, рейтинговых агентств, представители экспертного сообщества.

Темы конференции:

- Академический взгляд на состояние российской экономики. От теории к практике
- Стройка и ипотека. Как «не сломать» драйвер роста
- Технологический суверенитет и адаптация экономики. Банки и институты развития
- Региональный взгляд на экономику, МСП, региональные институты развития

23 мая 2024 года

Москва + онлайн

Контакты: +7 (495) 785-29-93, +7 (495) 785-29-88
event@asros.ru, <https://asros.ru>

Подробная
информация



НЕХОРОШИЙ МАЛЬЧИК

Джозеф Гаррисон, 19-летний подросток из США, признал вину в организации масштабной атаки на букмекерский сервис DraftKings. Методом Credential Stuffing он взломал 60 тыс. аккаунтов на этом ресурсе.

Гаррисон с сообщниками привязывал в личном кабинете новый платёжный метод, вносил на счёт пять долларов для верификации, а затем наоборот — выводил с него все имеющиеся средства. Так злоумышленникам удалось похитить около 600 тыс. долл.

При инспекции компьютера обвиняемого было обнаружено около 40 млн строк учётных данных, которые могли использоваться в атаках методом подбора. А в телефоне нашли переписку с остальными фигурантами, где обсуждались способы взлома DraftKings и монетизацию схемы.

ЧЕРЕЗ «САЙТЫ ГОСОРГАНОВ»

Полиция задержала петербуржца, создававшего фишинговые сайты — копии официальных страниц различных госорганов.

При попытках воспользоваться сервисами жертвы привычно вводили данные своих аккаунтов, зарегистрированных на портале госуслуг, предоставляя преступнику доступ к своим учётным записям. Мошенник менял пароли и подавал через угнанные аккаунты заявки в микрокредитные организации. Средства выводил через анонимные электронные кошельки. Когда лимит на получение кредита исчерпывался, учётная запись удалялась вместе с информацией об её использовании.

Пострадали более 130 граждан. Возбуждено уголовное дело по ст. 272 УК РФ («Неправомерный доступ к компьютерной информации»).

Подготовила Александра Миронова

ВЫМОГАТЕЛЕЙ К ОТВЕТУ!

Канадский суд вынес приговор одному из администраторов хак-группы LockBit. 34-летний Михаил Васильев, гражданин России и Канады, признал себя виновным по восьми пунктам обвинения и получил четыре года тюрьмы. Также его обязали выплатить 860 тыс. долларов пострадавшим.

Среди прочего Васильев признан виновным в кибервымогательстве. Подсудимый нанес серьёзный ущерб



трём канадским компаниям в 2021–22 гг. Судья охарактеризовала мужчину как кибертеррориста и отметила, что его действия были мотивированы личными финансовыми интересами.

Задержание хакера произошло в октябре 2022 года в канадском Брэдфорде — в рамках международной операции с участием властей Европы, США и Канады. Сейчас М. Васильев согласен на экстрадицию в Штаты, где он также обвиняется по нескольким статьям (включая заговор с целью умышленного повреждения защищённых компьютеров и передаче требований о выкупе). В случае признания виновным в США ему грозит до пяти лет лишения свободы.

Там же ожидает суда Руслан Астамиров, другой известный член группировки LockBit, — он использовал вымогательское ПО против жителей Кении, Франции, Японии и США.

РОССИЯ — БЕЛАРУСЬ: ДИАЛОГ ДРУЗЕЙ

Главное управление цифрового развития Следственного комитета Республики Беларусь совместно с ГУБОПиК МВД РБ и Управление по борьбе с противоправным использованием информационно-коммуникационных технологий МВД РФ провели успешную операцию по задержанию лиц, причастных к деятельности международной ОПГ. Офисы группы находились в Минске и Москве.

Злоумышленники четыре года осуществляли масштабную мошенническую схему, предлагая гражданам разных стран ложные инвестиционные возможности с обещанием высокого заработка. Использовали фейковые ресурсы. После перевода денег на эти площадки, мошенники исчезали.

В Беларуси под стражу взяты 48 человек, среди которых руководитель Минского офиса и граждане

разных стран. После обысков изъяты компьютеры, мобильные устройства, документация, автомобили и наличные валюты. Арестованы преступные счета.

В Москве задержан один из организаторов группы, а в его квартире обнаружено более 30 млн рублей.

Разоблаченные преступники дали признательные показания и помогли выявить новые факты. Поиски других участников ОПГ продолжаются.



Международный фестиваль по кибербезопасности Positive Hack Days 2

от **positive technologies**



23-26 мая 2024,
Лужники, Москва

Positive Hack Days — фестиваль, объединяющий экспертов по кибербезопасности, этичных хакеров со всего света и всех, кто хочет погрузиться в мир инфобеза и отлично провести время!

На четыре дня спортивный комплекс «Лужники» превратится в настоящую киберарену. На площадке соберутся эксперты, представители министерств и ведомств, топ-менеджеры разных компаний, а также рядовые пользователи цифровых товаров и услуг.

Будет интересно всем:

- **Все желающие** смогут **бесплатно** посетить открытую часть фестиваля — мегаполис с интерактивными образовательными инсталляциями, которые расскажут о цифровом мире и в игровой форме помогут прокачать киберграмотность.
- **На кибербитве Standoff** каждый сможет увидеть грандиозное противостояние этичных хакеров и защитников, сражающихся за ресурсы виртуального государства, и понаблюдать, что будет, если хакеры доведут свои атаки до конца.
- **Для экспертов индустрии, представителей министерств и ведомств, топ-менеджеров, студентов** и всех интересующихся информационной безопасностью свои доклады на самые актуальные темы ИБ представят более 250 специалистов в технических и бизнес-треках закрытой части фестиваля*.
- В **молодежном треке** студенты смогут узнать все о самых востребованных профессиях, послушать истории успеха и увлекательные лекции, найти единомышленников и завести полезные знакомства.



В Telegram-канале PHDays Media вы сможете найти все подробности о том, что ждет гостей киберфестиваля в этом году.

* Для входа на закрытую часть фестиваля необходимо приобрести билет. Все собранные средства будут переданы в фонд «Подари жизнь»

До встречи на Positive Hack Days 2 в «Лужниках»!

НЕ МНОГОТОЧИЕ, А ТОЧКИ ПРОРЫВА

ТЕХНОЛОГИЧЕСКИЙ СУВЕРЕНИТЕТ ЭКОНОМИКИ
НАПРЯМУЮ ЗАВИСИТ, ВО-ПЕРВЫХ, ОТ ДЕРЗНОВЕНИЙ
ОТЕЧЕСТВЕННЫХ УЧЁНЫХ И, ВО-ВТОРЫХ,
ОТ ОПЕРАТИВНОСТИ ВНЕДРЕНИЯ ИХ РАЗРАБОТОК



Елена ПОКАТАЕВА
обозреватель
BIS Journal

Словосочетание «технологический суверенитет» появилось в лексиконе руководителей страны в 2022 году. Его главное содержание — ускоренное развитие различных отраслей экономики на базе отечественных высокотехнологичных разработок мирового уровня. Сегодня мы проходим этап, образно говоря, «эскизного проектирования» той большой технико-организационной системы, которая должна обеспечивать устойчивое функционирование технологически суверенной экономики.

Базовые целевые очертания этой системы описал Президент РФ Владимир Путин в послании Федеральному собранию 29 февраля 2024 г.: доля отечественных высокотехнологичных продуктов в экономике должна увеличиться за шесть лет в полтора раза, а доля импорта — снизиться до 17% ВВП. При этом перед рынком поставлены чёткие задачи:

- ♦ создавать глобально конкурентные продукты на основе уникальных отечественных разработок;
- ♦ формировать долгосрочный заказ на российскую технологическую продукцию минимум на 10 лет вперёд;
- ♦ наращивать объёмы частных инвестиций в высокотехнологичные разработки.

Александр Шойтов, заместитель министра цифрового развития, связи и массовых ком-

муникаций РФ, рассказал в интервью BIS Journal (№ 1/2024), что для решения поставленных задач «нужна хорошая кооперация, в первую очередь науки с государством и бизнесом». Создание такой кооперации сегодня является приоритетной задачей Минцифры.

Общая ситуация выглядит достаточно благоприятно. Так, ко Дню российской науки (8 февраля) Институт статистических исследований и экономики знаний НИУ ВШЭ опубликовал исследование актуальных тенденций развития в России области исследований и разработок. Оно показало, что наша страна входит в число мировых лидеров по масштабам ресурсной обеспеченности и результативности деятельности данного сектора. В частности, страна занимает пятое место в мире по численности персонала, занятого исследованиями и разработками (в эквиваленте полной занятости), шестое место по численности ключевой категории научного персонала — исследователей и десятое место по объёму финансирования R&D. При этом достижения отечественных учёных воплощаются в виде готовых технических систем, работающих буквально на самом острие прогресса в области высоких технологий. Приведем некоторые примеры.

НЕЙРОСЕТИ КАК ДВИЖУЩАЯ СИЛА

Сегодня весь мир проходит этап взрывообразного роста математических методов построения искусственных нейронных сетей (ИНС). Мир современных ИНС — это настоящий космос, в котором постоянно вспыхивают «сверхновые звёзды» новых математических алгоритмов, оперативно воплощаемых в тех или иных практических задачах.

Одна из них — импульсные (спайковые) нейронные сети, появившиеся как ответ на голо-

вокругительный рост сложности нейросетевых моделей на существующих аппаратных платформах. Рассказывает Михаил Киселёв, руководитель Лаборатории нейроморфных вычислений Чувашского госуниверситета имени И. Н. Ульянова: «Число синаптических связей в мозге человека составляет приблизительно 10^{14} , а количество параметров в самых сложных современных нейросетевых моделях достигает 10^{12} , так что обучение такой модели требует месяцев счёта на самых мощных современных суперкомпьютерах». Отдельный вопрос — энергетические затраты на такие вычисления: они становятся предельно критичными, если ставится вопрос «малой интеллектуализации», то есть создания миниатюрных автономных интеллектуальных устройств, например медицинских роботов или элементов интернета вещей.

Импульсные нейронные сети позиционируются как биологически правдоподобные: информация, которая передаётся от нейрона к нейрону ИНС, — это аналог нервного импульса или спайка, который в мозге человека передаётся от нейрона к нейрону через синаптическую связь (рис. 1).

А команда учёных из Нижегородского государственного университета им. Лобачевского под руководством профессора Сусанны Гордлеевой пошла ещё дальше: предложила новую — нейрон-астроцитарную — сетевую модель, подходящую для эффективной реализации нейроморфного искусственного интеллекта в «железе».

Учёные взяли за основу модель спайковой нейронной сети и построили ИНС, которая воспроизводит передачу сигналов не только между нервными клетками, но и между нейронами и астроцитами — вспомогательными клетками мозга, которые, в частности, защищают нейроны от перевозбуждения, «очищают» передаваемые сигналы от лишних шумов, а также участвуют в регуляции нейронной динамики. Фактически речь идёт о том, что учёные сделали серьёзный шаг вперёд в понимании того, как в мозге человека кодируется информация, связанная с конкретными сенсорными стимулами.

В модели есть пирамидальные нейроны, воспринимающие сигналы, вставочные нейроны, которые распространяют сигналы по сети, и астроциты. При этом между искусственными нейронами передаются сигналы, подобные электрическим импульсам, а между астроцитами и нейронами — сигналы, моделирующие выделение определённых химических веществ клетками естествен-

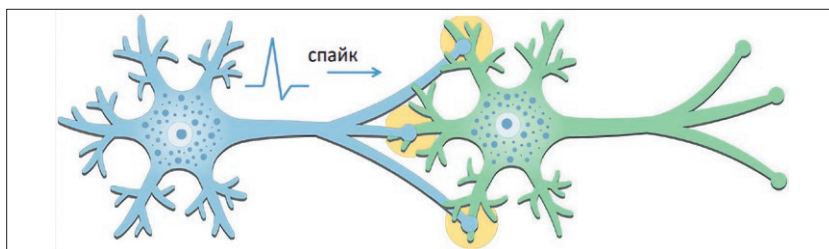


Рисунок 1. «Биологически релевантная» модель спайка искусственной нейронной сети

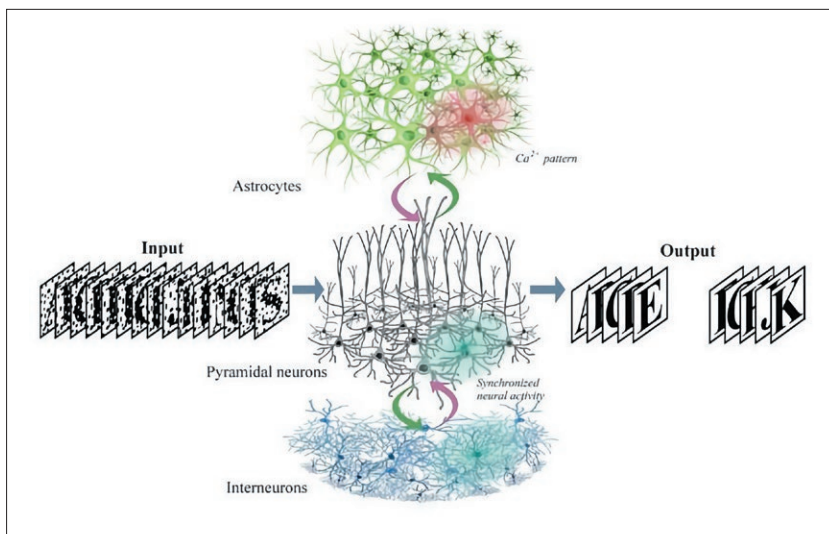


Рисунок 2. Схема работы нейрон-астроцитарной сетевой модели. Источник: статья С. Гордлеевой с соавторами, опубликованная в IEEE Transactions on Neural Networks and Learning Systems, <https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=5962385>, декабрь, 2023 г.

ного головного мозга. Оказалось, что нейросеть с астроцитами обучалась на 20% лучше, чем спайковая сеть без астроцитов (рис. 2).

Продвинутая математика нейронных сетей — это горячая точка мировой конкуренции в области искусственного интеллекта: там идёт битва за создание высокопроизводительных, энергоэффективных и недорогих нейроморфных процессоров, которые найдут применение во множестве компьютерных систем, реализующих алгоритмы ИНС. Аналитики IDC выделяют три группы такого «железа»: до 40 трлн (40×10^{12}) операций в секунду, от 40 до 60 и свыше 60 трлн. По их оценкам, в настоящее время американские процессорные лидеры — Qualcomm, AMD, Intel — серийно выпускают процессоры первого поколения, а на второй уровень планируют перейти в нынешнем году.

При этом в конце прошлого года китайские учёные из университета Цинхуа представили полностью аналоговый фотоэлектронный чип ACCEL, который в лабораторных условиях показал производительность 4,6 PFLOPS ($4,6 \times 10^{15}$ операций с плавающей точкой). Этот

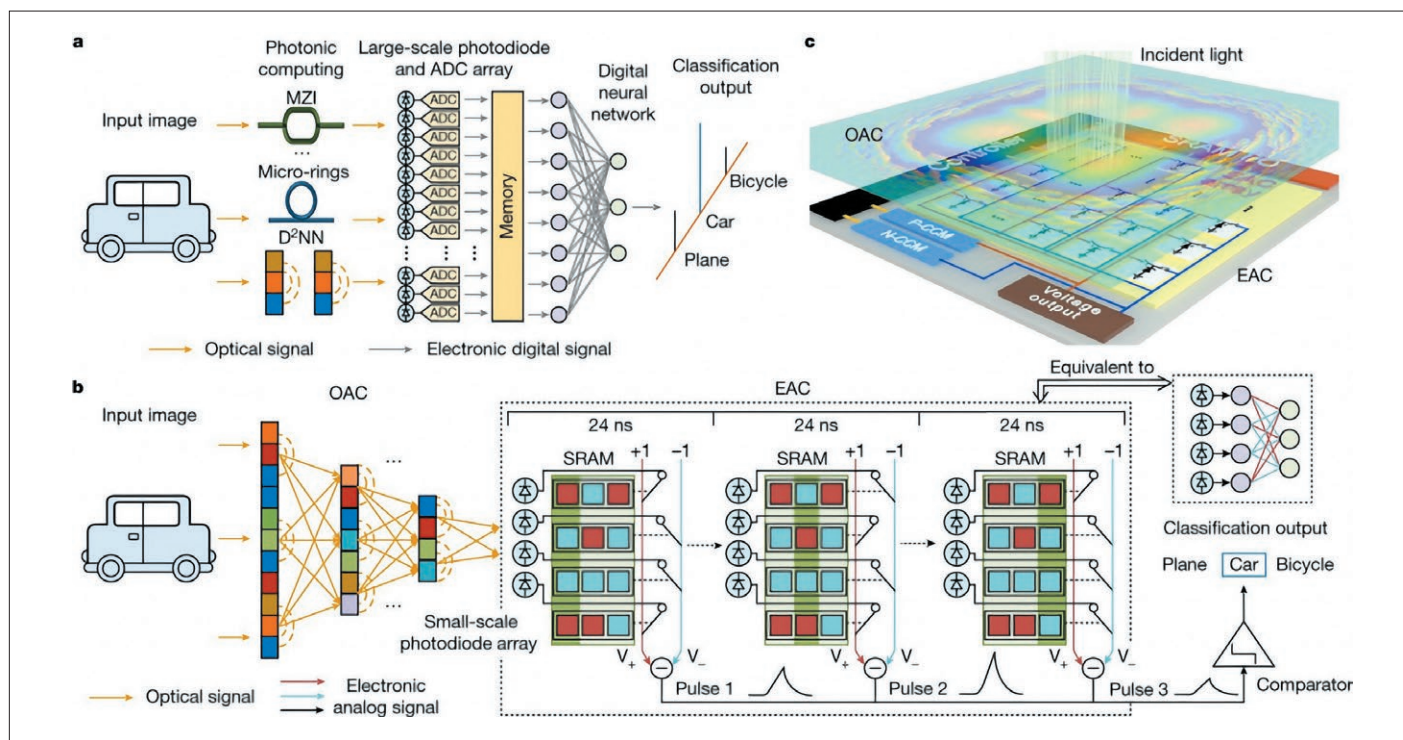


Рисунок 3. Архитектура чипа ACCEL. Источник: Tsinghua University, 3dnews.ru

чип использует управление световыми волнами посредством дифракции для кодирования и обработки информации, а вычисления производятся аналоговым способом при помощи интерференционных паттернов, создаваемых светом, поясняет Сергей Сурабекянц в своей статье на ресурсе 3dnews.ru. Эксперты отмечают, что этот процессор, который продемонстрировал хорошие результаты в задачах машинного зрения, в 3000 раз быстрее нынешнего лидера рынка – видеокарты Nvidia A100, а по энергоэффективности превосходит современный графический процессор в 4 млн (!) раз. Причём произвели его на китайской микроэлектронной фабрике SMIC по технологическим нормам 180 нм. Иными словами, это совсем недорогой в производстве микроэлектронный блок (рис. 3).

Свои разработки в области нейроморфных чипов ведёт также «Лаборатория Касперского». Сотрудники рассказывают, что такой чип, состоящий из 8 тыс. нейронов, потребляет 4 мВт электроэнергии, и он может работать в составе автономного робота или БПЛА, используя стандартную батарейку. А при совместном использовании этого нейроморфного процессора с нейроморфной камерой сможет вести обработку весьма динамичных картинок со скоростью 1250 кадров в секунду. По образному выражению сотрудников компании, можно будет посчитать песчинки, которые падают

в песочных часах, или капли падающего дождя на стекле.

Ещё одно «горячее» направление нейросетевых технологий – решение проблем с безопасностью данных, используемых в ИНС-моделях. Так, в МФТИ идут разработки в области так называемого федеративного обучения (federated learning). Речь идёт о том, что обучающая выборка распределённо хранится на локальных устройствах пользователей (телефонах, планшетах, персональных компьютерах), рассказывает Александр Безносовиков, заведующий лабораторией фундаментальных исследований «МФТИ-Яндекс», а модель обновляется на сервере путём агрегации обученных моделей с различных устройств. Поскольку данный подход нацелен в первую очередь на оптимизацию внутренних коммуникаций данных, которые осуществляются в ходе параллельных и распределённых вычислений в рамках реальных задач машинного обучения, он базируется на глубоко проработанных методах математической оптимизации.

Сотрудники лаборатории нейроморфной фоники МГУ под руководством профессора Андрея Федянина ведут разработки в области нейроморфных систем, которые обладают кратковременной и долговременной памятью, что имеет значение для решения когнитивных задач. Они разработали оптоэлектронные структуры, которые реализуют

ют идею спайков и нейронов человеческого мозга. В частности, искусственный синапс создаётся на основе нанокристаллической плёнки оксида цинка.

А НЕ ЗАМАХНУТЬСЯ ЛИ НАМ... НА КЛАССИЧЕСКИЙ ПК?

Многочисленные опыты с созданием аппаратных блоков традиционных ПК на новых физических принципах или с применением новых принципов организации вычислений активно идут по всему миру. Большие ожидания от реализации в «железе» нейросетевых подходов привели к появлению нового класса устройств — так называемых мемристоров (memory + resistor). В отличие от классического пассивного компонента электрической цепи, они обладают некоторой памятью: мемристор способен изменять уровень сопротивления при прохождении через него электрического заряда разной мощности. Так, при использовании низкого напряжения с него можно считать информацию, а с помощью более высокого напряжения — записать. Причём циклы смены состояния мемристора происходят на порядки быстрее, чем у популярной сегодня флеш-памяти.

Поскольку мемристор способен не только хранить информацию, но и выступать в качестве логического элемента, меняющего своё состояние в ходе вычислений, появилась новая парадигма вычислительных систем — вычисления в памяти. Ещё одно интересное свойство мемристора заключается в том, что в отличие от классических бинарных транзисторов, у которых есть два состояния: «0» или «1», он может находиться в большем количестве состояний. Это свойство, называемое пластичностью, позволяет мемристору запоминать большее количество информации. Например, мемристоры, созданные в Курчатовском институте, запоминают не менее 16 различных значений, что соответствует 4 битам информации, в то время как ячейки классической компьютерной памяти могут хранить только 1 бит данных.

Для создания этих мемристоров слой термопласта поли-п-ксилилена толщиной 100 нм размещается между двумя проводящими электродами: инертным и активным, сделанным из металла — меди или серебра. Резистивное переключение осуществляется за счёт создания «проводящего моста» между двумя электродами. По мнению учёных, такие конструкции хорошо подходят

для создания, например, энергонезависимой компьютерной памяти или встраиваемых микрочипов, которые можно будет даже имплантировать в тело человека.

Международный российско-итальянский научный коллектив (НИЦ «Курчатовский институт», Пармский университет и др.) создал образец органического запоминающего энергонезависимого мемристора с возможностью самообучения на основе токопроводящего полимера полианилина. Учёные говорят, что это первый опыт реализации многоуровневых нейронных сетей с высокой плотностью записи на основе многослойных технологий. Предполагается выпускать соответствующие изделия микроэлектроники в рамках техпроцесса 10 нм.

Ещё один вариант многослойного мемристора создали российские учёные из Нижегородского госуниверситета имени Н. И. Лобачевского. Они применили многослойную структуру «металл — оксид — металл», которая включает слои тантала, оксида тантала TaOx, оксида циркония, допированного иттрием $ZrO_2(Y)$, оксида тантала (V) Ta_2O_5 , диоксида титана TiO_2 и нитрида титана TiN.

Специалисты рассказывают, что сегодня наиболее популярный способ получения эффекта резистивного переключения — туннельная структура «металл — изолятор — металл». Учитывая нанометровые размеры слоёв, наиболее подходящими технологиями производства таких структур является атомно-слоевое осаждение (АСО) и магнетронное формирование гетероструктур в едином вакуумном цикле. Эти технологии дополняют процесс создания высокоэффективных СБИС и позволяют на конечной стадии изготовления кристалла добавить в него мемристорную память.

Совместные исследования учёных Института физики полупроводников им. А. В. Ржанова СО РАН (ИФП СО РАН), ОИЯИ и Новосибирского государственного технического университета (НГТУ НЭТИ) идут в направлении создания энергонезависимой памяти для гибкой электроники. Специально для этих целей разработан новый композитный материал из наночастиц оксида ванадия, покрытых фторированным графеном. Такие мемристоры обеспечивают пути протекания электрического тока по графеновым квантовым точкам. Причём время переключения элемента, то есть время, требуемое для перезаписи информации, составляет 30–40 нс, что приблизительно в 1000 раз быстрее, чем у современной флеш-памяти. При этом они

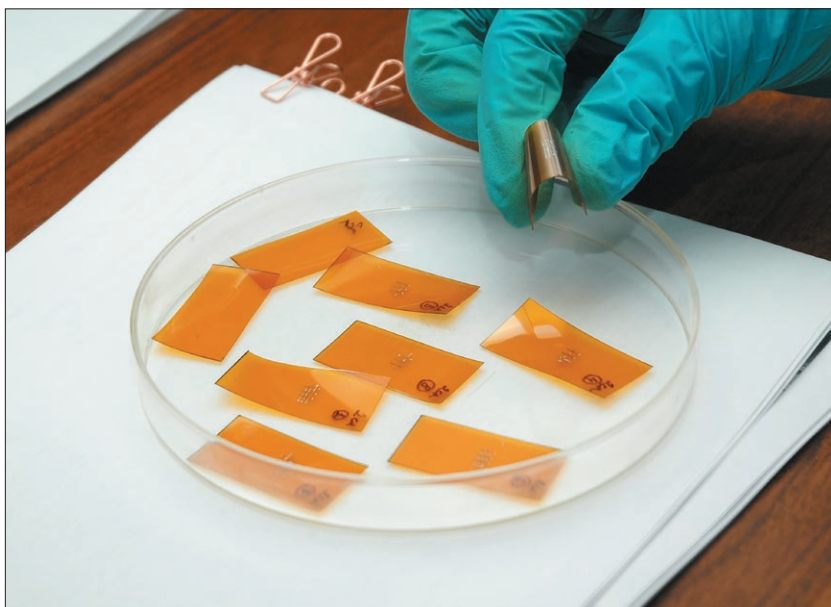


Рисунок 4. Гибкие мемристорные структуры, напечатанные на полимерном материале. Источник: Институт физики полупроводников им. А. В. Ржанова СО РАН

демонстрируют рекордные характеристики перезаписи — выдерживают миллионы циклов подачи тока. Изготавливаться они будут методом печати на 2D-принтере (рис. 4).

Опыты с новыми физическими средами ведут учёные Санкт-Петербургского государственного электротехнического университета ЛЭТИ. Они разработали модель химической реакции, с помощью которой можно будет создать первый резервуарный компьютер, работающий на реагентах: серная кислота, малоновая кислота, вода и ферроин. Идея нового подхода базируется на постулатах известной реакции Белоусова — Жаботинского: после смешивания реагентов в течение определённого времени ряд параметров раствора меняется колебательно, причём частота колебаний зависит от концентрации химических реагентов. Таким образом, гипотетически появляется возможность с помощью управления подобной реакцией реализовать новый тип компьютерных вычислений.

Таким образом, архитектуре фон Неймана объявлена война. Точнее, она сама уже сдаёт позиции под натиском требований к производительности и энергоэффективности со стороны высоконагруженных задач обработки цифры. «Узким горлышком» этой архитектуры стал обмен данными между процессором и оперативной памятью. «Архитектура фон Неймана крайне не оптимальна для современных задач обработки больших данных, — отмечает Геннадий Красников, президент РАН, научный руководитель АО «НИИМЭ». —

Сегодня для реализации памяти на 1 бит информации приходится шесть (!) комплементарных транзисторов». По его оценкам, во всём мире есть не менее десятка компьютерных архитектур, которые планируют прийти на смену устаревшему «фон Нейману».

СЛУХИ О КВАНТОВОМ ПРЕВОСХОДСТВЕ ОКАЗАЛИСЬ НЕСКОЛЬКО ПРЕУВЕЛИЧЕННЫМИ

В последние годы ожидания компьютерной индустрии в части резкого роста производительности связывались с появлением серийно производимых квантовых компьютеров.

В поисках наилучшего решения учёные разных стран создают квантовые компьютеры на основе различных физических принципов: фотонные, ионные, системы на нейтральных атомах, СКВИД (сверхпроводящий квантовый интерферометр), полупроводники. В числе наиболее значительных исследовательских проектов следует упомянуть создание твердотельных кубитов (кремний) и реализации так называемого конденсата Бозе — Эйнштейна. Его учёные образно называют пятым состоянием вещества.

По сути, это агрегатное состояние вещества, основу которого составляют бозоны, охлаждённые до температур, близких к абсолютному нулю. В таких условиях большое количество атомов оказывается в минимально возможных квантовых состояниях и ведёт себя как одна частица, то есть квантовые эффекты начинают проявляться на макроскопическом уровне.

Это экзотическое квантовое явление впервые наблюдалось в 1995 году в разреженных атомных газах, а сегодня стало предметом активных исследований. Например, различные организации (Сколтех, СПбГУ, ФТИ имени Иоффе) экспериментируют с поляритонным лазером — прибором, внутри которого находится Бозе-конденсат светожидкости (экситонных поляритонов), а наружу выходит когерентный свет определённой длины волны, то есть лазерный свет, рассказывает Алексей Кавокин, руководитель научной группы «Квантовая поляритоника» Российского квантового центра, на научном интернет-ресурсе «N+1». Он говорит, что на основе таких лазерных структур планируется создать полупроводниковую платформу для квантовых вычислений.

Второе большое направление исследований — магноны, то есть электронные спинные волны, которые могут управляться магнитным полем. Магнитное упорядоче-

	GPU	ASIC	Future Quantum
I/O Bandwidth	10,000 Gbit/s	10,000 G/s	1 Gbit/s
Operation throughput			
16-bit floating point	195 Top/s	550 Top/s	10.5 kop/s
32-bit integer	9.75 Top/s	215 Top/s	0.83 kop/s
binary (Boolean logical)	4,992 Top/s	77,000 Top/s	235 kop/s

Рисунок 5. Сравнительный анализ характеристик пиковой производительности популярного чипа GPU, микросхемы ASIC и квантового компьютера. Источник: Disentangling Hype from Practicality: On Realistically Achieving Quantum Advantage, By Torsten Hoeffler, Thomas Häner, Matthias Troyer, Communications of the ACM, May 2023, Vol. 66 No. 5, Pages 82–87.

ние можно рассматривать как аналог сверхтекучести: конденсат выглядит как излучение монохроматических микроволн, которые настраиваются с помощью приложенного магнитного поля.

Дальше всех по пути превращения квантового компьютера в рабочий инструмент ИТ-специалистов продвинулась корпорация IBM. В середине января она представила модульную квантовую систему IBM Quantum System Two, которая включает квантовые процессоры Quantum Heron (каждый состоит из 133 кубитов с фиксированной частотой) и программные средства коррекции ошибок. Учёные Российского квантового центра создали 20-кубитный квантовый компьютер на ионной платформе, 25-кубитный компьютер — на атомной платформе. В нынешнем году запланировано получение компьютера на 50 кубитов, а следом — 100 кубитов, рассказывает Руслан Юнусов, советник генерального директора госкорпорации «Росатом».

В связи с высокими ожиданиями общества от грядущих квантовых компьютеров важно мнение Геннадия Красникова: «Специалисты понимают, что в ближайшее десятилетие квантового превосходства не будет».

Это мнение эксперта подтверждают данные, приведённые в статье «Отделяем шумиху от практичности: о реалистичном достижении квантового преимущества» («Disentangling Hype from Practicality: On Realistically Achieving Quantum Advantage»), которая была опубликована в мае 2023 г. в авторитетном научном журнале Communications of the ACM. «Из-за ограничений пропускной способности входа и выхода квантовые компьютеры будут практичны для задач «больших вычислений» на небольших данных, а не на больших данных», — говорится в статье.

Авторы сравнили производительность классического чипа типа популярного гра-

фического процессора NVIDIA A100 с гипотетическим квантовым компьютером самого оптимистичного уровня, который может быть достигнут в ближайшее десятилетие: 10 тыс. логических кубитов с исправлением ошибок, временем работы логических операций 10 мкс, способностью одновременно выполнять операции со всеми кубитами и подключением «все ко всем» для реализации отказоустойчивости двухкубитных вентилей (рис. 5).

Получилось, что результирующая производительность квантового компьютера оптимистичного будущего в 10 тыс. раз меньше, чем у сегодняшнего классического чипа. «Очевидно, что любая задача уровня поиска в базах данных будет быстрее решена классическими компьютерами», — делают вывод исследователи. По их оценкам, получить практическую ценность от применения перспективных квантовых компьютеров удастся только для некоторых классов расчётных задач, например, теоретической физики или материаловедения.

«Квантовый компьютер в лучшем случае будет не альтернативой, а дополнением существующих классических универсальных компьютеров», — говорит Геннадий Красников.

Так что корпорация IBM логично включила в состав программной платформы для работы с квантовыми компьютерами Qiskit новый модуль: Qiskit Patterns даёт возможность трансформировать задачи в классической постановке в квантовые схемы и выполнять их на квантовом компьютере или в режиме имитации обрабатывать результаты.

Тем временем в НИЦ супер-ЭВМ и нейрокомпьютеров в Таганроге в рамках научной программы НЦФМ российские учёные создают терагерцевый фотонный суперкомпьютер, работающий на частоте 1 трлн Гц. Потенциально скорость его работы будет в 300 раз выше, чем у самых быстрых нынеш-



Рисунок 6. Проект «Сфера». Источник: НИИМА «Прогресс»

них процессоров, сообщил ТАСС проф. Илья Левин, директор НИЦ супер-ЭВМ и нейрокompьютеров: «Мы занимаемся синтезом архитектуры суперкомпьютеров, разрабатываем облик цифровой фотонной машины и вычислительные элементы: арифметико-логические устройства, системы синхронизации и коммуникации». Правда, фотонный компьютер не способен иметь собственную фотонную память, поэтому необходимо сопрягать медленную память обычного электронного компьютера с фотонными высокоскоростными средствами обработки информации.

Какая именно из многочисленных научных идей «выстрелит» на практике, зависит от целого комплекса окружающих задач. С одной стороны, важны параметры соответствующих производственных процессов и возможность организовывать их на различных площадках для запуска массового производства. С другой стороны, столь же важны характеристики новых видов компьютерной техники с точки зрения их встраивания в существующую ИТ-инфраструктуру предприятий и особенно в части поддержки уже работающего прикладного программного обеспечения.

ВЫЗОВЫ КОСМИЧЕСКОГО УРОВНЯ

«Слепое копирование зарубежных достижений должно быть полностью исключено при

реализации масштабных проектов в отечественной космической отрасли», — заявил глава госкорпорации «Роскосмос» Юрий Борисов на общем собрании Российской академии наук в декабре 2023 г. и подчеркнул: «Крайне важно при принятии решений о реализации масштабных проектов фокусироваться на будущем». Для решения таких задач задуман госпроект, детализация которого должна быть подготовлена к 1 июля 2024 года. Президент России Владимир Путин характеризует задачу его создания как формирование мощной и суверенной отечественной индустрии космических сервисов, технологий и продуктов, в которой реализовано эффективное частно-государственное партнерство. Оно подразумевает, в частности, доступ частного бизнеса к государственной инфраструктуре и испытательным полигонам, а также формирование долгосрочного государственного заказа на космические услуги, в котором могут принимать участие частные компании.

В русле этой идеи в начале января 2024 г. Новосибирский госуниверситет анонсировал создание в рамках проекта Передовой инженерной школы фабрики, выпускающей малые космические аппараты. Компания «Бюро 1440», которая входит в «Икс холдинг», сообщила о планах запуска в 2027 г. коммерческого сервиса спутникового интернета на базе 250 спутников. А к 2030 г. размер спутнико-



Рисунок 7. Источник: Презентация «Квантовое распределение ключей через атмосферные каналы связи», Сергей Кулик, Центр квантовых технологий МГУ имени М. В. Ломоносова, Конференция «РусКрипто, 25 марта 2021 г.

вой группировки превысит 700 аппаратов. Силами государства выполняется масштабный проект создания глобальной сети спутников коммуникации и мониторинга «Сфера». Проект охватит пять спутниковых группировок связи («Ямал», «Экспресс-РВ», «Экспресс», «Скиф», «Марафон») и пять спутниковых группировок дистанционного зондирования Земли («Беркут-Х», «Беркут-О», «Беркут-ВД», «Беркут-С», «Смотр»). Предполагается, что наблюдение в различных диапазонах длин волн поможет решать разнообразные задачи для различных отраслей экономики России (рис. 6).

Масштаб задуманного космического «строительства» ставит перед российскими учёными и конструкторами немало вызовов. Один из самых очевидных — низкий уровень защищённости современных навигационных технологий. К ним можно применить подавление навигационного сигнала либо его подмену (так называемый спуфинг), рассказывают в НИИМА «Прогресс». Компания видит свою задачу в том, чтобы дать рынку такую технологию, которая обеспечит на объектах критической инфраструктуры надёжный устойчивый навигационный сигнал, неподвластный подделке или зашумлению. Соответствующий продукт — локальная система навигации «КОНСУЛ». У неё, по оценке специалистов НИИМА «Прогресс», есть только одна конкурирующая система на мировом уровне, которая уступает отечественной разработке по степени помехозащищённости.

В решениях компании также используются передовые методы повышения точности навигации с использованием дифференциальных поправок. В результате достигается высокоточная навигация, которая используется, например, в точном земледелии, речной навигации на сложных фарватерах и т.д.

Большой потенциал просматривается у беспроводной квантовой связи, в частности, защищённой космической связи на базе технологии с квантовым распределением ключей. Первые эксперименты такого рода российская компания QRate начала проводить ещё в 2017 г., тогда был создан атмосферный оптический канал связи. А в начале января стало известно об успешном совместном эксперименте по передаче сообщений, защищённых с помощью квантовой криптографии, между Россией и Китаем, в котором приняла участие команда учёных из МИСИС, Российского квантового центра и компании «КуСпэйс Технологии». Для передачи ключа шифрования на расстояние более 3,5 тыс. км использовался китайский спутник квантовой связи «Мо-цзы». Он используется в Китае как доверенный узел, обеспечивающий распределение ключей на расстояние 7800 км. В ходе эксперимента исследовался обмен закодированными изображениями размером 256×64 пикселей (рис. 7).

Защищённые системы связи такого рода жизненно необходимы, в частности, для активно развивающейся сферы беспилотного транспорта разного вида. Компания QRate

начала три года назад исследовать возможности интеграции системы квантового распределения ключей с управлением беспилотным транспортом в Иннополисе.

БЕЗ ПИЛОТА, НО НА «ЦИФРЕ»

Нацпроект по беспилотникам должен быть запущен в текущем году. Очевидно, что управление развитием сегмента «беспилотии», как его окрестил Василий Шпак, заместитель министра промышленности и торговли, — сложнейшая задача, которая включает ряд больших направлений: от формирования единой технологической политики до управления финансово-экономическими процессами внедрения беспилотников в практическую жизнь отраслей и конкретных предприятий, например, в виде лизинговых схем.

Значительная роль на старте мегапроекта принадлежит технологической части: предстоит утвердить нормативные требования к беспилотникам в части ключевых технологий. В их числе — технологии точной автономной посадки, динамической маршрутизации, обнаружения и дистанционной идентификации беспилотного воздушного судна, автоматического предотвращения столкновений беспилотных и пилотируемых воздушных судов. А специалисты АО «ГЛОНАСС» выполняют уникальный в мировом масштабе проект — создают «Цифровое небо». По сути, в интересах безопасного применения гражданских авиабеспилотников идёт создание цифрового двойника небесного пространства. По аналогии с цифровыми двойниками интеллектуальных автотрасс, по которым должны перемещаться беспилотные автомобили, цифровой двойник неба России будет агрегировать всю информацию: от метеоданных до специфических прикладных применений. Алексей Райкевич, генеральный директор АО «ГЛОНАСС», называет эту комплексную разработку уникальным эталонным проектом опережающего развития, который обеспечит глобальное лидерство и технологический суверенитет России. Важная составная часть проекта — надёжная связь всех элементов «небесных трасс», создаваемая целиком на отечественных технологиях и спутниковом оборудовании.

ПРОМЫШЛЕННОСТЬ — НА ОСТРИЕ ТЕХНОЛОГИЧЕСКОГО СУВЕРЕНИТЕТА И ЦИФРОВОЙ ТРАНСФОРМАЦИИ

В сентябре 2023 г. Правительство РФ утвердило обновлённую сводную стратегию раз-

вития обрабатывающей промышленности России до 2030 г. и 2035 г., в которой сделан акцент на достижение технологического суверенитета. Денис Мантуров, министр промышленности и торговли России, пояснил, что под этим понимается последовательное обеспечение технологической независимости в сфере цифрового проектирования, испытаний, самого производства и управления жизненным циклом, а также послепродажного обслуживания промышленной продукции.

Летом прошлого года Минпромторг провёл оценку уровня цифровой зрелости предприятий промышленности, который составил 45%. Правда, эта цифра — некая «средняя температура по больнице», ведь уровень цифровой зрелости промышленных компаний существенно различается в зависимости от отрасли и размера бизнеса.

Так, на предприятиях «Северстали» работают нетривиальные интеллектуальные цифровые решения, позволяющие добиться ускорения непрерывного производства. Например, программные решения, написанные специалистами компании, управляют напрямую прокатным станом 5000, который производит листовой прокат для изготовления труб большого диаметра, и непрерывно-травильным агрегатом НТА-3, который выполняет травление свариваемых встык полос и лент из рулонов стали. На базе имеющихся цифровых моделей ИТ-специалисты «Северстали» создают цифровых двойников технологических агрегатов. «В результате можно улучшить производственное планирование — задавать последовательность рулонов на входе таким образом, чтобы прокатывать ещё больше стали», — рассказывает Борис Воскресенский, директор по развитию цифровых технологий компании «Северсталь».

Группа НЛМК перешла на современную информационную систему управления производственными процессами (MES-систему) в сталеплавильном производстве. Она помогает тысячам сотрудников управлять обработкой более 85 плавков на 30 агрегатах в сутки: отслеживается и оптимизируется свыше 100 технологических параметров, например температура и химический состав металла, время обработки, дозировка материалов и т.д. а также более 50 показателей эффективности работы. Так, математическая модель прогнозирует химический состав поступающего из доменных цехов чугуна, а затем рассчитывает номенклатуру и оптимальное количество лома, который

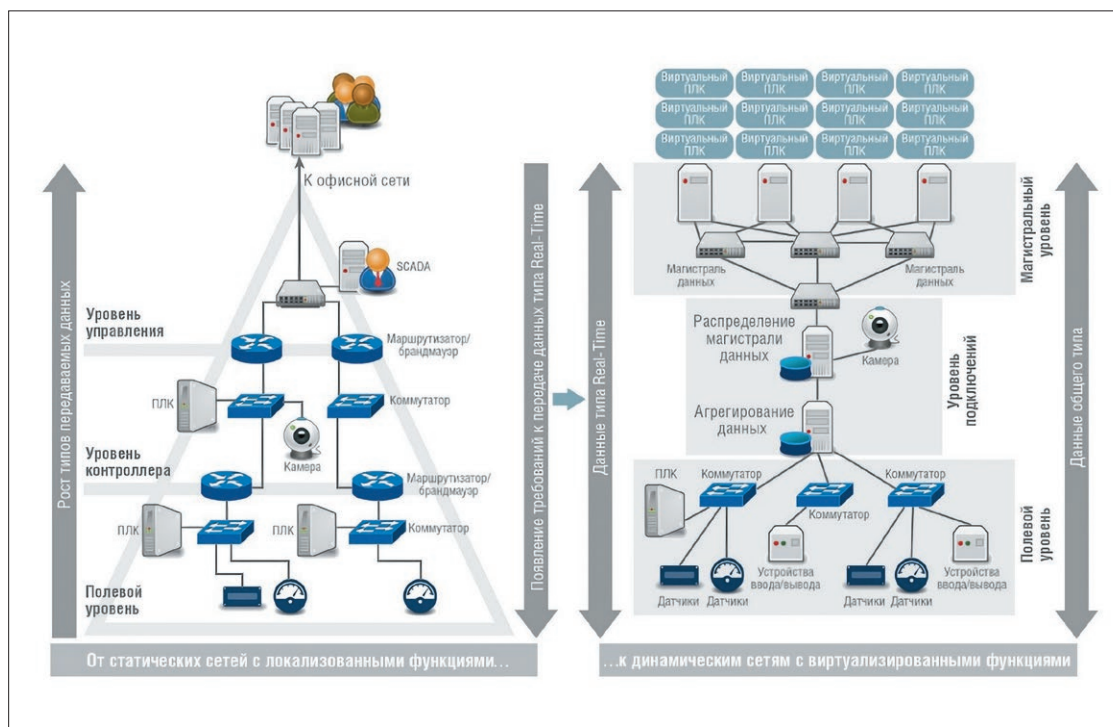


Рисунок 8. Возможный вариант трансформации АСУ ТП на базе открытых стандартов. Источник: «Северсталь», апрель 2023 г.

нужно добавить в плавку для получения стали нужных параметров.

Но это штучные примеры активности действующих отраслевых лидеров мирового уровня. Текущий уровень цифровизации менее крупных предприятий чаще всего ограничивается базовой автоматизацией уровня АСУ ТП, возможно, произведённой достаточно давно и на базе устаревших технологий. По оценкам Минпромторга, по состоянию на август 2023 г. производством промышленных роботов занималось семь отечественных компаний, которые за 2022 год отгрузили заказчикам 120 единиц продукции...

Масштаб предстоящей технологической трансформации российской промышленности поражает воображение. Минпромторг со своей стороны поддерживает 96 комплексных проектов по созданию отечественного промышленного ПО. А в части программно-аппаратных решений технологические заделы цифровой модернизации формируются в специализированных индустриальных центрах компетенций (ИЦК). Всего по линии Минпромторга одобрено 53 проекта таких центров.

Со своей стороны российские промышленники из нескольких ИЦК объединились для создания открытой архитектуры АСУ ТП, способной составить достойную конкуренцию мировым лидерам: Siemens и General Electric. Работы предстоит много:

- ♦ создать открытый стандарт промышленной автоматизации, охватывающий все отрасли промышленности и различные виды производств (непрерывные, дискретные и гибридные);

- ♦ создать единую информационную модель АСУ ТП (уровни 0, 1, 2, 3);

- ♦ сформулировать требования и получить аппаратные разработки в части микропроцессоров (MIPS, RISC-V, ARM), устройств для протоколов автоматизации (EtherCAT, ProfiBUS, ProfiNET), модулей рефлексивной памяти (ReflectiveMemory), модулей сбора и анализа данных процесса и т.д.;

- ♦ сформулировать требования и разработать ПО в части IoT-платформы для управления объектами промышленной автоматизации, распределённой системы управления, интегрированной среды разработки, «открытого программного ПЛК» (программируемого логического контроллера, OpenSoftPLC), а также требования к ОС реального времени для работы в АСУ ТП и открытые протоколы внутренней и внешней шины ПЛК и т.д.;

Особые группы требований относятся к ПО диагностики и предиктивной аналитики работы оборудования и процессов, а также задачам информационной безопасности в Open АСУ ТП, включая создание открытой АСУ ТП на объектах КИИ (рис. 8).

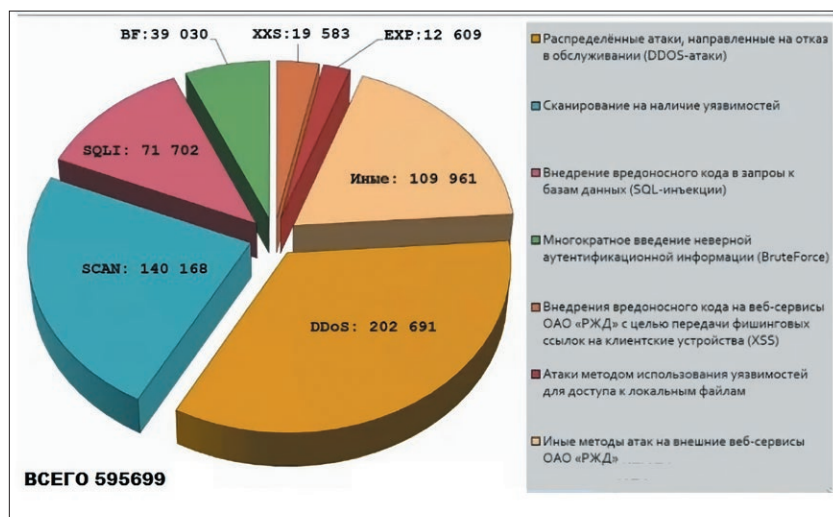


Рисунок 9. Структура атак на внешний периметр инфраструктуры ОАО «РЖД». Источник: ОАО «РЖД», «Инфофорум-2024», февраль 2023 г.

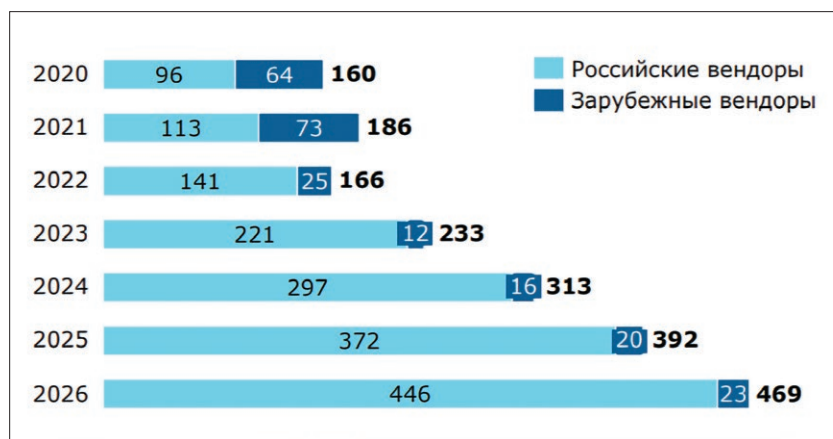


Рисунок 10. Динамика роста российского рынка ПО для информационной безопасности, 2020–2026, млрд руб. Источник: Обзор российского рынка инфраструктурного ПО и перспектив его развития, Strategy Partners, сентябрь 2023 г.

ЗАЩИЩЁННАЯ РЕАЛИЗАЦИЯ ТЕХНОЛОГИЧЕСКОГО И ЦИФРОВОГО ПРОРЫВА

Информационная безопасность — сквозная технология, которая пронизывает все технологические и цифровые продукты, внедряемые на предприятиях и в организациях. Степень агрессивности внешней среды продолжает нарастать. Например, количество кибератак на ИТ-инфраструктуру РЖД выросло в 2023 году на 36% по сравнению с предыдущим годом (рис. 9).

Как рассказал на конференции «Инфофорум-2024» Юрий Ногинов, начальник департамента управления информационной безопасностью ОАО «РЖД», инфраструктура компании ранее была заявлена в качестве приоритетной цели для атак террористической кибергруппировкой «IT Армия Украины», которая представляет собой рас-

пределённую структуру, включающую добровольцев-«хактивистов».

Российские заказчики активно вкладывают средства в развитие корпоративной информационной безопасности. Однако объём угроз растёт не менее энергично. Согласно данным аналитического отчёта Центра информационной безопасности компании «Инфосистемы Джет» за 2023 г., у 72% компаний были найдены критические уязвимости на периметре, что может послужить точкой входа злоумышленника в инфраструктуру компании. «В 2023 году индустрия кибербезопасности столкнулась с необходимостью пересмотра своих стратегий и приоритетов, — говорит Андрей Янкин, директор центра информационной безопасности компании «Инфосистемы Джет». — Компании вынуждены активно анализировать и контролировать информацию за пределами своих внутренних сетей, чтобы обеспечить системный контроль защищённости постоянно модернизируемой ИТ-инфраструктуры» (рис. 10).

В связи с появлением огромного количества новых угроз, говорят специалисты, применение стандартных средств защиты (межсетевые экраны, виртуальные частные сети, средства защиты от НСД) является необходимым, но недостаточным условием для построения надёжной комплексной системы защиты информации. Индустрия информационной безопасности активно экспериментирует с различными нетривиальными подходами к борьбе со вторжениями. Например, компания UserGate реализовала в своём устройстве класса NGFW решение для защиты масштабных и географически распределённых сетей с поддержкой концепции Zero Trust Network Access.

Специалисты кафедры «Информационная безопасность компьютерных систем» Санкт-Петербургского политехнического университета Петра Великого называют в качестве главной сегодняшней проблемы отсутствие согласованности и разобщённость существующих средств защиты, функционирующих на различных уровнях, — это и позволяет вредоносному ПО активизировать компоненты разных уровней и манипулировать данными для обхода механизмов анализа и контроля безопасности.

Перспективный способ выхода из сложившейся ситуации, по мнению ряда исследователей, заключается в использовании адаптивного управления безопасностью. Например, в петербургском Политехе его предлагается

реализовывать на основе модели гомеостаза. Гомеостаз при этом понимается как свойство безопасности — способность информационной системы обеспечивать необходимое значение объема функциональных возможностей путём внесения архитектурных изменений в ответ на деструктивное воздействие (динамическая защита).

По мнению Евгения Павленко, доцента Института кибербезопасности и защиты информации, именно такой подход способен учесть специфические проблемы безопасности, свойственные киберфизическим системам (КФС): «Прямой перенос понятий информационной безопасности в виде конфиденциальности, доступности и целостности в КФС невозможен в силу того, что, в отличие от информационных процессов, физические процессы являются необратимыми, и для них невозможно реализовать такой же уровень контроля и управления. Для них на первый план выходит соблюдение корректного протекания технологических процессов». В этих условиях для обеспечения информационной безопасности КФС предлагается методология динамического переконфигурирования параметров и структуры системы с использованием принципа гомеостаза.

ОРГВЫВОДЫ

Очевидно, что в контексте общей картины мировой технологической эволюции каждая компания, работающая в высокотехнологичной сфере, должна совершить свой рывок на уровень глобальной конкурентоспособности. Причём их действия должны быть согласованы и объединены общей целью — включить в общий план прорыва и все предприятия различной отраслевой принадлежности. Им также предстоит свой рывок на уровень мировой конкурентоспособности за счёт технологической модернизации и цифровой трансформации.

Такую масштабную амбициозную задачу можно решить исключительно с опорой на принципы государственного планирования. Только так можно гармонизировать «внутривидовую» конкуренцию, стимули-

рующую рыночное развитие, с необходимостью коллективных усилий. Этот подход и реализуется сегодня на практическом уровне: разрабатываемая концепция цифрового «Госплана 2.0» охватывает все отрасли экономики России.

«Государство правильно реагирует на появившиеся вызовы, — говорил Геннадий Красников в интервью журналу «Стимул» в ноябре 2023 г. — Во-первых, оно придерживается комплексного подхода, когда запускает базовые отрасли. И во-вторых, фактически каждое министерство, каждая большая корпорация стали заново рассматривать возможности академических институтов, возможности фундаментальных исследований для получения востребованных промышленностью научных результатов».

Таким образом, «земная твердь» технологического суверенитета держится на трёх «китах». Первый — финансовая поддержка государства (она охватывает широкий спектр вариантов). Второй — поступательное развитие фундаментальной и прикладной российской науки. Третий «кит» — организационные меры, превращающие красивую идею в исправно работающий механизм с отличными показателями КПД. В их числе — создание промышленных кластеров, которые должны повысить спрос реального сектора экономики на инновационные научные решения, а также поддержка малых технологических компаний — перспективных «единорогов».

При этом ключевым элементом задуманной мегатрансформации является организация массового перехода предприятий российской промышленности и других отраслей экономики на суверенные отечественные технологии и цифровые решения. Фактически речь идёт о «приземлении» на поле деятельности всевозможных российских компаний и предприятий из реального сектора экономики продвинутых технологий, решений и услуг, которые создаются в кабинетах научных сотрудников, а затем обретают «плоть и кровь» на рабочих местах инженеров-конструкторов радиоэлектронной аппаратуры и разработчиков ПО.

ОТ РЕДАКЦИИ

Об особенностях этого «приземления» BIS Journal попросил рассказать российских экспертов, имеющих опыт создания и внедрения технических решений мирового уровня.

«ПОДХОД, КОТОРЫЙ ПОЗВОЛЯЕТ МЕНЯТЬ АРХИТЕКТУРУ КОМПЬЮТЕРА ВО ВРЕМЕНИ, ДАЕТ ВОЗМОЖНОСТЬ ИЗБАВИТЬСЯ ОТ МНОГИХ ВИДОВ УЯЗВИМОСТЕЙ»



Валерий КОНЯВСКИЙ
научный руководитель
ОКБ САПР, заведующий
кафедрой защиты
информации МФТИ,
доктор технических наук

Увы, мы живем в эпоху победившего маркетинга. Он проник даже в такую деликатную сферу, как информационная безопасность, и иногда переворачивает с ног на голову представления потребителей о самих актуальных проблемах и рисках информационной безопасности. Яркий пример — угрозы со стороны будущих квантовых компьютеров. Скажу честно: я здесь угрозы не вижу. Реализуется обычная схе-

ма противостояния меча и щита — одни компьютеры получают способность быстрее подбирать ключи шифрования, а другие, соответственно, будут делать ключи еще более длинными. На моей памяти длина ключей, используемых в практических системах шифрования, выросла с 32 до 4096 бит и, очевидно, будет расти дальше. Другое дело — распределение ключей.

НАСТОЯЩИЕ И ВЫДУМАННЫЕ ПРОБЛЕМЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ

Есть такие алгоритмы, для которых доказаны теоремы о том, что расшифровать зашифрованный с их помощью документ без знания ключа просто нельзя. Пример — известный шифр Вернама, система симметричного шифрования, изобретенная в 1917 г. для задачи автоматического шифрования телеграфных сообщений. Она является одной из простейших

криптосистем, которая в то же время обладает абсолютной криптографической стойкостью. Автор метода — телеграфист Гильберт Вернам — тогда не знал, что использовал известный сегодня метод гаммирования (наложения гаммы на исходный текст), то есть сложение символов исходного текста и ключа по модулю, равному числу букв в алфавите. Достаточно взять длинную гамму — хорошие случайные числа, и сложить их посимвольно с тем материалом, который нужно зашифровать. Тогда на выходе получаем текст, который совершенно невозможно расшифровать, если не знать эту гамму.

Единственное препятствие для широкого применения таких шифров — чисто технологическая проблема передачи ключей. Когда то ключи передавались на бобинах перфоленга, что, конечно, очень усложняло все процедуры. В результате появились упрощенные варианты, например, взять короткую случайную последовательность (она и есть ключ), и этот ключ развернуть в гамму. Собственно, на этом допущении основана вся сегодняшняя блочная криптография.

Однако сегодня обычный флеш-носитель может содержать такое огромное количество случайных чисел, что исчезают любые проблемы с физическим перемещением криптографической гаммы. Так что длина ключа и скорость вскрытия зашифрованных данных — это вовсе не та проблема, о которой нужно беспокоиться «всем миром», особенно в русле подхода «щит и меч». Я не думаю, что механизмы и способы обеспечения информационной безопасности, которые используются у нас в стране, существенно отстают от решений, работающих в развитых странах Запада. Думаю, что как раз здесь у нас — приоритет, а по многим направлениям мы даже впереди.

ГДЕ РЕАЛЬНЫЕ УГРОЗЫ?

Главная проблемная точка нынешних угроз ИБ — это увеличение потоков атак, высокая плотность атак. Для нынешнего времени характерен существенно возросший уровень агрессивности внешней среды.

Надо сказать, что государство предпринимает усилия для противодействия этим угрозам. В частности, начинает реально действовать федеральный закон № 187 «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 г. Этот закон выделяет три типа значимых объектов КИИ: информационные системы, телекоммуникации, АСУ ТП. Но эти

три сферы находятся на разных уровнях проработки методологии защиты. Если в информационных и телекоммуникационных системах все аспекты ИБ неплохо разработаны, начиная с методологических вопросов, есть наработанные практики и компании, которые эффективно занимаются вопросами защиты, то с защищенностью АСУ ТП дело обстоит совсем плохо. Защищенных АСУ ТП очень немного. По крайней мере, незащищенные системы встречаются на порядки чаще. Мы слышим слова о защищенности и даже обещания показать соответствующий сертификат, но при реальном рассмотрении надежная защита секторов реальной экономики обнаруживается нечасто.

Я думаю, что сейчас самая актуальная задача для сферы ИБ — это защита АСУ ТП. Нужно защищать производство — то, что является основой экономики.

В условиях резко возросшей агрессивности внешней среды необходимо пересмотреть практически все политики информационной безопасности, модели угроз, модели нарушителей. Потому что все, что делалось раньше, исходило из предпосылок достаточно низкой агрессивности среды. При этом приоритетное внимание следует уделить специфике производственных систем, поскольку до сих пор системным образом безопасностью АСУ ТП мало кто занимался.

Это направление должно иметь наивысший приоритет среди всех задач, которые стоят сегодня перед сферой информационной безопасности страны. Признак сегодняшнего дня — смещение статуса самой большой проблемы в сфере ИБ с защиты персональных данных, чем многие профессионалы занимались многие годы, применяя стандартные механизмы и хорошо разработанные требования к информационным системам, на защиту АСУ ТП, где очень велика доля нестандартных методов и решений.

Причина нестандартности заключается в том, что системы АСУ ТП создавались на предприятиях в течение многих лет, по факту — затыкались наиболее вопиющие дыры, превращая системы в натуральное «лоскутное одеяло»: от отсутствия стандартных форм-факторов до неимоверно длинного списка используемых протоколов, который включает и такие, которые уже практически не используются в новых проектах и плохо поддаются попыткам обеспечения interoperability.

Для задачи создания защищенных производственных систем это состояние дел оз-

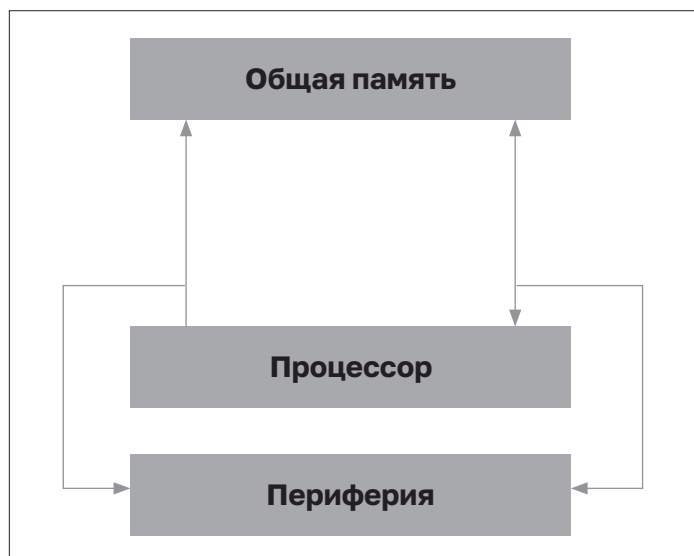


Рисунок 1. Архитектура фон Неймана. Команды и данные не разделяются, а передаются по единому общему каналу

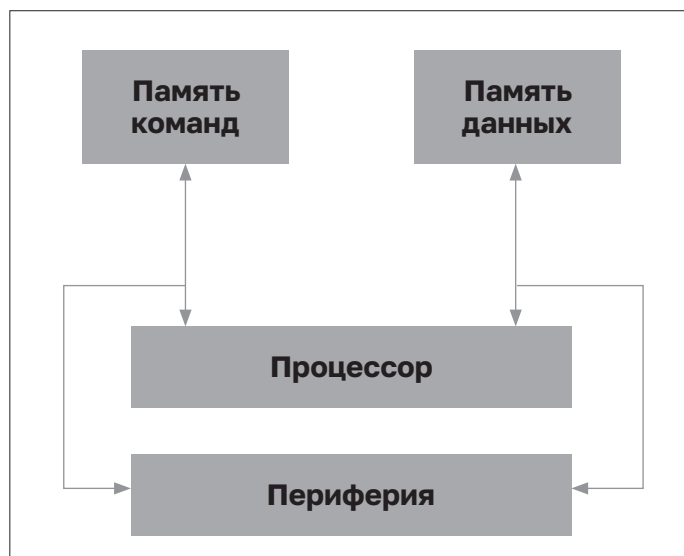


Рисунок 2. Гарвардская архитектура. Поток команд и данных параллельны и независимы

начает, как минимум, длительные сроки ее решения: на создание конкретного средства защиты уходит не менее года и еще два — на сертификацию. Если мы не найдем такого единого решения, которое позволяет успешно применять его в разных АСУ ТП, производственные системы рискуют еще долго оставаться беззащитными. И точно не стоит идти по сомнительному пути понижения уровня требуемой защищенности — это очень слабая позиция. Крайне важно, чтобы уровень защищенности был достаточен, начиная с самого первого документа — описания угроз, атак, системы защиты.

Но как получить единое универсальное решение для защиты производственных систем?

О СОЗДАНИИ НОВОЙ КОМПЬЮТЕРНОЙ АРХИТЕКТУРЫ

Стоит вспомнить, что подавляющее большинство нынешних компьютеров представляют собой ту или иную реализацию машины Тьюринга. Наибольшее распространение получили два конкурирующих варианта: архитектура фон Неймана, которая развивалась в лабораториях Принстонского университета, и гарвардская архитектура, связанная научными работами специалистов Гарварда (рис. 1, 2).

Принципиальный элемент архитектуры фон Неймана — совместное хранение программ и данных в памяти компьютера. Он же обусловил основной недостаток этой архитектуры: поскольку программа и данные не могут считываться одновременно, пропускная способность передачи данных по единому

каналу между памятью и процессором существенно ограничивает скорость работы процессора. И более важная с точки зрения ИБ особенность неразличимости команд и данных — она открывает хакерам огромные возможности для манипулирования такими системами.

В отличие от архитектуры фон Неймана гарвардская архитектура подразумевала разные хранилища для данных и инструкций, а также разные каналы их передачи. Это открывало возможности значительного роста производительности компьютера и создавало предпосылки для различимости данных и команд. Однако в силу того, что данная схема была сложнее конкурирующей, она проиграла в битве за массовое распространение архитектуре фон Неймана по стоимости решения: микроэлектроника в середине XX века была очень дорогой, и фон-неймановская архитектура оказалась гораздо эффективнее для того уровня развития техники. Кстати, сегодня, когда цена микроэлектроники резко понижается, начинает побеждать направление гарвардской архитектуры.

Но в целом обе эти архитектуры — это реализация идеи универсального вычислителя А. Тьюринга. Для машины Тьюринга известен тезис Черча-Тьюринга: такая машина может выполнить любую вычислительную задачу. Вот здесь и кроется проблема!

Ведь если компьютер может выполнить любую задачу, то он выполнит и вредоносную! Это очевидное следствие из тезиса Черча-Тьюринга, но для его осмысления и формирования понадобились многие годы. Отсюда же следует, что за универсальность

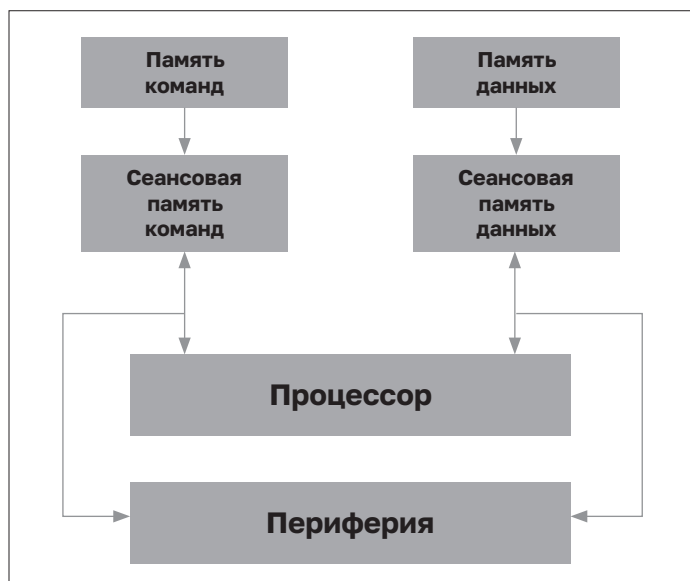


Рисунок 3. Новая гарвардская архитектура



Рисунок 4. Один из вариантов исполнения криптошлюзов семейства TrusT-in-Motion

архитектуры мы платим безопасностью, так как закрыть архитектурные уязвимости с помощью программных «заплаток», очевидно, невозможно. Нужно улучшить архитектуру.

Решение — использование новой компьютерной архитектуры. При этом не следует ставить знак равенства между архитектурой чипа и архитектурой компьютера. Есть, конечно, фактор привычных ассоциаций: процессор, который выпускает, например, компания Intel, и компьютер на его базе, который работает в архитектуре фон Неймана. Планшет или смартфон с процессорной архитектурой ARM, который работает в системе команд гарвардской компьютерной архитектуры. Но бывает ведь и по-другому!

Тут стоит также вспомнить оригинальные компьютерные разработки, которые велись, например, в Советском Союзе в Институте кибернетики под руководством В. М. Глушкова. С помощью доступной микроэлектроники серий K133 и K155, известных всем советским радиолюбителям, создавались высокоэффективные многопоточные вычислительные системы. Многие технические показатели тех прекрасных машин до сих пор не удалось превзойти. Паритетное развитие компьютерной науки было «успешно» остановлено переходом на копирование других разработок — IBM-360 и PDP-11. Темп развития был утрачен.

В 80-е годы прошлого века в Институте проблем управления (ИПУ) под руководством И. В. Прангишвили разрабатывались машины семейства «ПС», что означало «перестраиваемые структуры». Подразумевается, что архитектура машины перестраивалась в за-

висимости от того, что подавалось на вход: если на входе была программа на языке Алгол, она становилась Алгол-машиной, если же на Фортране, то она становилась Фортран-машиной и т.д. Иверий Варламович заложил основы понимания того, что архитектура может быть изменяемой.

НОВАЯ ГАРВАРДСКАЯ АРХИТЕКТУРА КОМПЬЮТЕРОВ

Новая гарвардская архитектура, разработанная ОКБ САПР, — это компьютерная архитектура, изменяемая в процессе работы. Мы не были первыми в этой области, но пошли своим путем, в том числе, в теоретическом обосновании нового архитектурного подхода. Раз уязвимость — в архитектуре, то бороться с ней можно именно на архитектурном уровне.

Действительно, если контролировать неизменность компьютерной среды нельзя программными средствами (программа может быть изменена), то контролирующие процедуры должны быть вынесены из этой модифицируемой среды в другую среду — немодифицируемую и легко проверяемую, то есть простую и небольшую по объему, которая выполняется аппаратным устройством, независимым от компьютера, который оно проверяет. Фактически мы создали решение, которое меняет архитектуру компьютера на некоторый период времени. При включении компьютера он выполняет только достаточные контрольные процедуры, включая идентификацию, контроль целостности и т.д. И только после того, как все контрольные процедуры выполнены, загружается проверенная опе-

рационная система, и компьютер с этой проверенной ОС становится доверенным, способным при этом выполнять любые задачи. Это привычный способ обеспечения доверенности компьютера с изначально недоверенной архитектурой — установка в него аппаратного средства защиты, работающего до старта ОС.

Но если мы можем не использовать уже существующую архитектуру, улучшая ее аппаратными СЗИ, а внести в нее изменения сразу, создать ее сразу, без установки дополнений — изменяемой? То самое независимое аппаратное устройство, которое проводит контрольные процедуры, станет частью архитектуры по умолчанию, только и всего. Примерно так и выглядит Новая гарвардская архитектура, если не вдаваться в подробности.

Это структура, перестраиваемая во времени. Но также есть решения, перестраиваемые в пространстве, например, защищенный смартфон, работающий по-разному в зависимости от того, где он находится.

Но новая архитектура требует переделки всего ПО. Мы подумали и об этом — Новая гарвардская архитектура включает неизменяемую память и блоки сеансовой памяти для исполнения программ. Сеансовая память и обеспечивает возможность исполнения ранее разработанного ПО (рис. 3).

Речь идет о том, что мы создали технологическую базу, которая позволяет создавать различные решения, изменяющие архитектуру в соответствии с заданной логикой. В частности, такой подход дает возможность избавиться от компьютерных вирусов и многих других видов узависимостей.

На этом принципе построены выпускаемые серийно микрокомпьютеры m-Trust, которые являются платформой для создания целой линейки разнообразных решений. Фактически это платформа СКЗИ-ready с заранее созданными условиями обеспечения среды функционирования криптографии на классы КС3 или КС2. Важно, что это именно платформа: на основе m-Trust строятся различные решения, причем, не только нами, но и партнерами-интеграторами или даже самими заказчиками. Например, на этой основе мы создали решение, которое работает с датчиками и понимает, когда нужно отключать внешние каналы. Это позволило произвести довольно интересные специализированные смартфоны, которые были упомянуты выше.

В инновационном проекте ВТБ «Криптоанклав» используется каналный шифра-

тор на базе специализированного компьютера m-Trust с аппаратной защитой данных. В станках с ЧПУ «Балт-Систем» решения m-Trust без корпуса установлены на специально разработанной для этого проекта интерфейсной плате. А в шкафах SCADA «Вега-газ» криптошлюзы m-Trust в корпусе монтируются на DIN-рейку.

На базе m-Trust выпускается Trust-in-Motion — крипто-шлюз для систем с подвижными объектами, который может поставаться либо с предустановленным СКЗИ или в виде СКЗИ-ready. Такие криптошлюзы применяются, например, в проектах «Сапсан», «Ласточка», «Иволга» компании «РЖД». Продукт fin-Trust — крипто-шлюз для банкоматов, а МЭ-Trust — межсетевой экран объектового уровня (рис. 4).

О ПРОЦЕССОРАХ ДЛЯ НОВОЙ ГАРВАРДСКОЙ АРХИТЕКТУРЫ

Конечно, мне как разработчику компьютерной архитектуры хочется получить процессор, который работает по принципу Новой гарвардской архитектуры. Но я думаю, что в данном случае неправильно начинать развитие всего направления с чипа. Правильнее сначала выпускать решения, соответствующие концепции Новой гарвардской архитектуры на любых существующих процессорах. Конкретная система команд к конкретному варианту реализации компьютера имеет очень малое отношение, и мы можем сделать свой компьютер на любой архитектуре процессора, включая x86, ARM. Я думаю, что будущее — за системой команд RISC-V, именно в этой схеме будет разрабатываться большая часть новых решений в ближайшем будущем.

Так что имеет смысл сначала накопить опыт создания компьютеров Новой гарвардской архитектуры, которые используют чипы, работающие в самых разных системах команд, а уже потом преобразовать его в конкретный чип процессора.

В то же время, как и для любого процессора, здесь возникает большой пласт работ, связанных с производством чипов, микропроцессорных средств и технических инструментов, а также разработкой операционных систем и прикладного ПО.

Как управлять этими процессами?

О СВЯЗКЕ ГОСУДАРСТВА И НАУКИ

Конечно, поддержка развития суверенной компьютерной архитектуры — это задача государства. Никакой рынок сам по себе этого не сделает. В определенной мере можно

было бы рассчитывать на отраслевое научное сообщество, но его фактически не существует. Вместо разрушенной цепочки, связывавшей науку с промышленностью, ничего не появилось.

Советская цепочка была выстроена логично. Фундаментальные задачи решались в учреждениях Академии наук. Эти решения подхватывались вузовской наукой, которую финансировала отраслевая наука. Фактически вузовская наука отработывала идеи, приходящие с фундаментального уровня, переводя их в формат прототипов прикладных задач. Эти предложения вузовской науки поступали в отраслевые НИИ, которые разрабатывали готовые изделия, основанные на достижениях фундаментальной и отраслевой науки, и предлагали их для запуска в серийное производство конструкторским бюро при производственных объединениях. И вот эти КБ превращали новые технические решения в производственные технологии, технологические карты, программы для станков с ЧПУ — АСУТП.

В результате административной реформы 90-х были уничтожены не только цепочки связей от фундаментальной науки до производства, но и отраслевая и вузовская наука. В отсутствие отраслевого научного сообщества соответствующую деятельность мы ведем сами, но только в рамках научно-технической поддержки собственного производства. Также поступают другие компании с научно-технологическими заделами. И вот что важно: эта деятельность не воспринимается на рынке как конкурентное преимущество, отделяющее компанию от остальных участников рынка. Уровень недоверия к научным проработкам коллег крайне высок! И это положение дел очень вредит общему делу создания суверенной высокотехнологичной экономики страны. Научно обоснованные прорывные решения должны объединять участников рынка!

Поправить положение может только государство. Но здесь я вижу большую организационную проблему. У нас есть отрасли, которые отвечают за программное обеспечение, и есть отрасли, которые занимаются микроэлектроникой и радиоэлектронной продукцией. Но никто не отвечает за готовые решения... Возможно, должен появиться новый регулятор. Или какие-то фонды, которые возьмут на себя риски научного поиска. Пока механизмов такого рода нет, об ускорении продвижения наукоемких идей до уровня промышленности, к сожалению, говорить не приходится.

Есть еще одна задача государства, важная для организации поступательного инновационного развития. Если воспользоваться известным философским парадоксом про Ахиллеса, догоняющего черепаху, как аналогией российской и мировой высокотехнологичной отрасли, нужно уметь выделять из тысяч «бегунов» тех, кто способен не только бегать, но и прыгать, чтобы мог перепрыгнуть черепаху и помчаться дальше по пути опережающего технологического развития.

А на практическом уровне нужно понимать, что у любой новой архитектуры обязательно возникнет вопрос миграции программ, ранее написанных для других известных архитектур. Мы в своих решениях используем специальные механизмы, которые позволяют на новой архитектуре выполнять все ПО, подготовленное для обычной гарвардской архитектуры. Для этого нам пришлось добавить в решение несколько микросхем, которые образуют так называемую сеансовую память.

А это значит, решение становится несколько дороже. Пусть немного, но условия для конкуренции на рынке ухудшаются. Это тоже задача государства — построить такую систему стимулирования нетривиальных разработок, которая не ведет к необходимости упрощать и ухудшать систему только для того, чтобы снизить ее стоимость. Пользоваться такими решениями должно быть выгодно!

О КРИТИЧЕСКИ ВАЖНЫХ НАПРАВЛЕНИЯХ СУВЕРЕННОГО ТЕХНОЛОГИЧЕСКОГО РАЗВИТИЯ В СФЕРЕ ИБ

Помимо защиты АСУ ТП, что является задачей наивысшего приоритета, есть ряд других направлений, где актуально ускоренное технологическое развитие:

- ◆ Интернет вещей, особенно в части промышленного варианта (IIoT). Главная проблема заключается в том, что системы такого рода существенно интегрированы с глобальными сетями передачи данных. Думаю, что нужно создавать специальное направление, которое будет прицельно заниматься безопасностью систем Интернета вещей.

- ◆ Так называемые «туманные технологии», связанные с глобальным объединением ресурсов отдельных компьютерных устройств — отдельных «капелек» тумана. Это будущее, которое наступит очень скоро и принесет целый пласт новых угроз, обусловленных тем, что, например, ваша личная информация будет размещаться в смартфонах людей,

которых вы никогда не видели. Проблемой «безопасности в тумане» уже нужно предметно заниматься.

♦ Семантика — огромная проблема нынешнего века. Современные компьютеры работают с формой, а не содержанием данных. В результате оказывается, что 90 % сегодняшних атак совершаются тогда, когда под влиянием среды сравниваются разные семантические понятия, и это, собственно, вызывает прерывания, которые обрабатываются внедренной закладкой, и т.д. Образно говоря, если попытаться из пяти метров вычестить пять помидоров, а на получившееся число разделить вчерашнюю дату, то точно возникнет прерывание — вот и успешная атака.

Компьютер работает с формой, а содержание результату дает приложение. И это неправильно. Если пятницу нельзя будет умножить на сентябрь, то исчезнет основная масса ошибок. А с ними и огромная масса компьютерных атак.

Столь же провокационным является популярный ныне подход Data Lake: в одно «озеро данных» сливается все, что можно, а потом из этой мешанины мы пытаемся восстановить семантику данных. Но семантику данных нужно поддерживать изначально, с того момента, когда они только появляются! Это позволит радикально сократить количество успешных атак злоумышленников на информационные системы.

Есть, конечно, подходы типа Semantic Web, и это направление весьма полезно. Однако датацентричность, связанные данные и семантическая интероперабельность — гораздо более продуктивные направления исследований. Нужно помнить, что ошибку, сделанную в архитектуре, поздно исправлять в Сети. Нужно сразу нужно делать хорошо. Но постановка задач здесь существенно шире:

♦ Новый термин «цифровые данные», появившийся в Конституции, дает возможность серьезно развивать методологию и решать задачи, которые раньше не поддавались решению, в том числе, из-за законодательных барьеров, например, в контексте 152-ФЗ «О персональных данных». Однако требуется дальнейшая методологическая и технологическая работа, например, по разделению понятий «обработка персональных данных» и «трансформация цифровых данных», что откроет зеленый свет целому мощному направлению — созданию моделей на основе искусственного интеллекта с хорошим предсказательным результатом.

О ПРОБЛЕМАХ МАССОВОГО ВНЕДРЕНИЯ ПРОРЫВНЫХ РЕШЕНИЙ

Областям реальной экономики — перерабатывающим отраслям, машиностроению и т.д. — предстоит решить сложную и дорогую задачу комплексной цифровизации и импортозамещения предприятий. В силу их нынешней незащищенности нужно также провести большую массовую работу по обеспечению информационной безопасности в этих отраслях. На мой взгляд, эти задачи НЕ должны решать сами отрасли. Не их задача — заниматься импортозамещением, да еще в ИТ-сфере, и выстраивать безопасность своих производственных технологий. Добывающие компании должны добывать, перерабатывающие — изготавливать продукцию, машиностроительные — строить станки и машины, а банки — заниматься кредитно-финансовой сферой, а не создавать решения ИБ. Поэтому понятно, почему организации пытаются порой обойти даже решения регулятора.

И такая «итальянская забастовка» будет длиться долго, до тех пор, пока не появится некоторая единая регулирующая сила, которая снизит интеллектуальную и финансовую нагрузку на предприятия в тех областях деятельности, которые не являются для них профильными, но важны для государства в целом.

Также нужны меры, стимулирующие деятельность высокотехнологичных компаний-стартапов, ведь именно они являются основной движущей силой инновационного технологического развития. Однако избытия свободных инвестиционных денег на нынешнем этапе развития нашей страны не замечено. Отраслевой разработки также пока нет. Опыт зарубежных стран показывает, что хорошим механизмом решения прорывной задачи является создание временных институтов. Этим специально созданным организациям под конкретный проект длительностью 3–5 лет государство выделяет серьезные средства, достаточные для того, чтобы полностью решить поставленную задачу. В рамках такого временного института находят применение команды стартапов.

После завершения работ данный институт завершает свое существование, а людей приглашают на другие проекты. Думаю, для нашей страны — это наиболее работоспособная модель решения крупных инновационных наукоемких задач. Бесспорно, она гораздо эффективнее той, что действует сегодня, когда коммерческие компании самостоятельно содержат собственное R&D направление.

«НАС ОЖИДАЕТ МЕТРОЛОГИЧЕСКАЯ РЕВОЛЮЦИЯ»



Сергей НОВИКОВ
главный редактор
журнала
«Станкоинструмент»,
кандидат технических
наук

Россия – страна с богатой историей настоящих прорывов в производственных технологиях. В их основе всегда лежат новые физические явления или принципы, что неоднократно было подтверждено практикой. Достаточно вспомнить электроискровой метод обработки материалов, который был разработан в СССР супругами Б. Р. Лазаренко и Н. И. Лазаренко. Они зарегистрировали открытие электроискрового способа обработки металлов 3 апреля 1943 г., а 12 августа 1945 г. вышло в свет постановление Совнаркома СССР о патентовании данного способа за рубежом. В течение 1946 г. этот способ был запатентован в ряде стран: Швейцарии, Франции, Великобритании, США, Швеции.

Значительный прогресс в обработке материалов был достигнут после изобретения лазера советскими учёными Н. Г. Басовым и А. М. Прохоровым. Данные технологии в настоящее время постоянно совершенствуются на основе использования современных информационных технологий. Например, бурно развивающиеся аддитивные технологии основаны на селективном лазерном сплавлении порошков, 3D-моделировании и программном управлении лазерным лучом. Мало кому известно, помимо узких профессионалов, что сама идея аддитивных технологий принадлежит советскому учёному. Ещё в 50-х годах XX века академик АН СССР, создатель роторно-конвейерных линий Л. Н. Кошкин

видел перспективы развития промышленного производства в технологиях выращивания детали путём сложения, а не путём удаления лишнего материала.

О ПРОБЛЕМЕ «ПРОРЫВОВ» В ПРОИЗВОДСТВЕННЫХ ТЕХНОЛОГИЯХ

Сегодня возможности традиционных технологий обработки материалов практически исчерпаны. Поэтому для «прорыва» необходимо проведение фундаментальных исследований поведения материалов при сверхвысоких скоростях нагружения и высокоэнергетических воздействиях. Например, в Национальном центре физики и математики в Сарове реализуется проект создания крупной научной инфраструктуры – Международного центра исследований экстремальных световых полей (ЦИЭС) на базе использования источников лазерного излучения с гигантской (экзаваттного уровня) пиковой мощностью. Проект базируется на значительных успехах, достигнутых в России и мире в последнее десятилетие по созданию петаваттных лазеров (1 петаВатт = 10^{15} Ватт) с интенсивностью до 1022 Вт/см², излучение которых сконцентрировано в импульсах сверхкороткой длительности (< 100 фемтосекунд = 10^{-13} с).

В основе планируемой инфраструктуры будет находиться новый уникальный источник света с мощностью 0,1–0,2 экзаватта, в сотни раз превосходящей имеющиеся сейчас лазеры (для сравнения, подобная мощность приблизительно в 10 000 раз больше мощности всех источников энергии, работающих на планете). Фундаментальные процессы взаимодействия такого излучения с веществом представляют совершенно новую область знания и могут стать основой новых технологий.

И только при таком подходе можно добиться реального технологического суверенитета для России и переместиться из положения догоняющей страны в опережающую позицию.



Рисунок 1. Точки роста цифровой трансформации ТМХ. Источник: <https://tmholding.ru>

О ВЫЗОВАХ «ИНДУСТРИИ 4.0» ДЛЯ ОТЕЧЕСТВЕННОЙ ПРОМЫШЛЕННОСТИ

Сегодня производственные предприятия всего мира увлечены идеей того, что принято называть концепцией «Индустрия 4.0» или цифровой трансформацией. Она предполагает включение всех единиц технологического оборудования в общую информационно-телекоммуникационную сеть, связывающую их функционально, а также регламентирующую все аспекты производства, включая 3D-проектирование, энергообеспечение технологических операций, последовательное пооперационное перемещение обрабатываемых деталей и сборочных единиц по необходимым маршрутам, а также последующий маркетинг и послепродажное обслуживание, и т.д. (рис. 1)

Данный подход характеризуется экспоненциальным ростом числа измерительных операций и, соответственно, различных данных, несущих информацию. При этом данные наравне с людьми, технологиями, капиталом становятся одним из основных активов корпораций, а зачастую самым главным. Но надо понимать, что взрывообразный рост количества измерений требует проведения гигантских работ в области метрологического обеспечения, разработки большого числа новых эталонов и др. Это необходимо для обеспечения достоверности данных и принятия правильных управленческих решений. По сути, это будет метрологическая революция.

Однако на практическом уровне наблюдается удивительный парадокс. Россия, которая по измерительным возможностям в послед-

ние годы занимает первое или второе место в мире, при этом практически не имеет своего приборостроения, то есть производства средств измерений и контроля. А это значит, что для достижения технологического суверенитета необходимо создание новой большой отрасли приборостроения.

Отдельно следует остановиться на проблемах информационной безопасности. Здесь возникают большие риски, связанные с появлением огромного количества умных устройств, включённых в большие сети, а значит, множество новых точек рисков ИБ. Эти данные стремятся интегрироваться друг с другом, поступают на другие уровни производства — риски нарастают. И это уже не просто DDoS-атаки, это и кибердиверсии. Достаточно вспомнить о вирусе Stuxnet на центрифугах обогатительного завода в Иране.

«ГОРЕ ОТ УМА»

Новые серьёзные проблемы связаны с внедрением интеллектуальных счётчиков электроэнергии. Такой прибор, по сути, представляющий собой мини-компьютер, подвержен новым моделям угроз, с которыми раньше отрасль не сталкивалась. Изменение хранимых данных, корректирование внутренних метрологических настроек счётчика и резидентного программного обеспечения, атаки на коммуникации, перехват, подмена, незаконное считывание данных со счётчика, подача несанкционированных команд на счётчик — всё это может не только привести к искажению данных об энергопотреблении, но и стать причиной отключения многомиллионных городов.

Помимо новых угроз, проекты по внедрению интеллектуального учёта сталкиваются и с необходимостью решения новых задач в области обработки и анализа получаемых данных. Подобные проблемы известны и за рубежом. Так, ИТ-специалисты из американской компании Digital Assurance обнаружили многочисленные недостатки в трёх видах счётчиков, которые используются, например, для учёта использования газа и электричества. Как правило, эти устройства используют беспроводное подключение к поставщику по стандартному протоколу, поэтому хакеру не составит труда внедриться в беспроводную связь и отправить ложные данные или команды счётчику.

Специалисты специально приобрели несколько образцов счётчиков на интернет-аукционах и обнаружили, что в некоторых

из них уровень защиты ниже, чем в игровых консолях Xbox. «Счётчики — это по существу плохие компьютеры в плохих коробках» — так охарактеризовали состояние безопасности умных счётчиков американские специалисты.

В целом во всём мире сейчас наблюдается повышенный интерес к защите объектов критически важной инфраструктуры, использующих проводные компьютерные сети, в то время как возможностям беспроводного взлома уделяется гораздо меньше внимания. Здесь точно нужны опережающие разработки отечественных специалистов для того, чтобы производственные сети российских промышленных предприятий, которым Правительство РФ «прописало» технологическую модернизацию на базе передовых технологий, не оказались беззащитными перед лицом киберзлоумышленников после успешного импортозамещения и цифровизации производственных участков.

Технические реализации концепции «Индустрия 4.0» как одного из вариантов обработки больших данных (Big Data), конечно, будут применять нейросетевые модели. Весьма многообещающе выглядят возможности современных нейронных сетей заменить обучающей выборкой классические механизмы искусственного интеллекта, требующие предварительного составления детальных исчерпывающих и логически непротиворечивых описаний возможных реальных ситуаций. При этом нейронные сети демонстрируют весьма неплохой уровень устойчивой работы даже при выходе из строя значительного количества элементов. Однако новые возможности идут рука об руку с новыми рисками ИБ. И эти риски в части производственных нейросетевых моделей, а также имитационных моделей, используемых, например, для построения цифровых двойников производств, ещё предстоит изучать и исследовать.

Таким образом, задача достижения технологического суверенитета для российской промышленности имеет вид большого комплекса взаимосвязанных задач из самых разных сфер: от фундаментальных наук, изучающих физические явления в различных промышленных процессах, до прикладных наук, предлагающих новые подходы к организации производства, и до различных направлений математики, превращающих «физику» промышленности в «цифру» информационных систем управления, контроля, безопасности.

РОССИЙСКИЕ НЕЙРОМОРФНЫЕ ТЕХНОЛОГИИ — НА ОСТРИЕ МИРОВОГО ПРОГРЕССА



Олег ВЫГОЛОВ
архитектор
решений,
«Лаборатория
Касперского»



Андрей ЛАВРЕНТЬЕВ
руководитель
отдела развития
технологий,
«Лаборатория
Касперского»



Андрей ДУХВАЛОВ
директор
департамента
перспективных
технологий,
«Лаборатория
Касперского»

Уже несколько лет назад эксперты прогнозировали грядущий бум нейроморфных вычислений. Похоже, он уже наступил, если судить по количеству тематических публикаций про импульсные (спайковые) нейросети. С чем это связано?

Хорошо известно, что в настоящее время искусственные нейронные сети (ИНС) могут решать широкий спектр задач в различных сферах жизни человека. Кроме того, идет ускоренное развитие аппаратной составляющей для обучения и инференса (прямого распространения данных в нейросети) таких сетей. Почему же внимание приковано именно к импульсным ИНС?

ЧЕМ ТАК ИНТЕРЕСНЫ ИМПУЛЬСНЫЕ НЕЙРОННЫЕ СЕТИ?

Дело в том, что импульсные сети оперируют не с числами, а с событиями, и входной поток данных для них представляется не в форме действительных чисел, а в виде событийного асинхронного набора так называемых спайков — импульсов единичной интенсивности (рис. 1). Более того, обмен информацией внутри такой сети также подразумевает использование спайков, точно так же, как это наблюдается в реальных живых организмах. Есть несколько преимуществ в передаче и обработке именно такого вида информации.

Событийный обмен позволяет реализовать так называемый локальный механизм обучения сети, который еще называют «синаптическая пластичность» (Spike-timing-dependent plasticity, STDP). Он затрагивает лишь активные в текущий момент времени части сети,

но не охватывает остальные области. Кроме того, активизация определенных нейронов сети теперь приобретает конкретный смысл и может рассматриваться как самостоятельный фактор. Например, известно, что в мозгу крыс есть устойчивые группы нейронов, активизация которых привязана к определенному месту в пространстве. Кроме того, есть мнение, что именно импульсная природа информации позволяет реализовать долгосрочную ассоциативную память, активируемую лишь по небольшому иницилируемому событию, а локальное обучение — краткосрочную память. Нельзя не отметить еще один уникальный механизм, присущий биологическим импульсным сетям, — их непрерывную адаптацию и подстройку внутренней топологии, включающую рост и отмирание межнейронных связей.

Таким образом, с точки зрения перспектив, развитие импульсных ИНС позволит решать такие сложные задачи, как имитационное и сверхбыстрое (всего на нескольких примерах) машинное обучение, создавать различные типы ассоциативной памяти, осуществлять непрерывное и адаптивное обучение сети, возможно, даже научить сети оперировать абстрактными понятиями и планировать действия без их фактического выполнения и др. Отдельно надо отметить такой интересный аспект импульсных ИНС как их устойчивость к различным атакам на системы искусственного интеллекта (этот вопрос стоит отдельного обсуждения).

НЕЙРОМОРФНЫЙ ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ

В целом, развитие импульсных ИНС идет по двум направлениям. Первое — создание

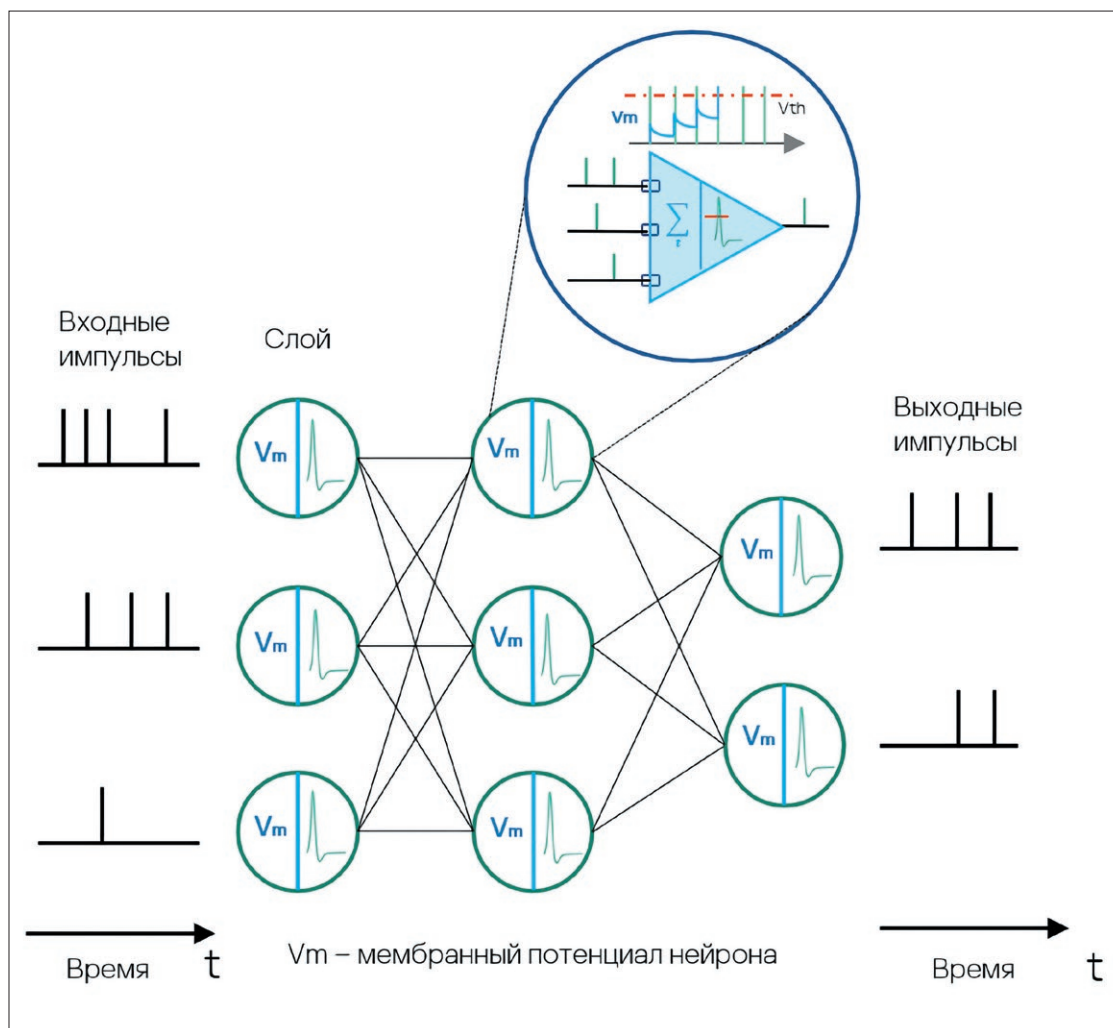


Рисунок 1. Структура импульсной нейронной сети. Источник: «Лаборатория Касперского»

алгоритмической и программной составляющей обучения и инференса таких сетей. Второе – создание специализированных нейроморфных процессоров, адаптированных именно под импульсные сети.

Отличительными чертами нейроморфных процессоров являются такие характеристики, как:

- ◆ низкое энергопотребление (милливатт-диапазон) и компактный размер;
- ◆ легкость встраивания в существующее оборудование;

◆ возможность их использования для инференса обычных «цифровых» ИНС, в том числе общедоступных. В последнем случае, можно отметить существенное увеличение быстродействия (миллисекунды) инференса таких сетей, которое во многих случаях не будет зависеть от глубины ИНС (так называемый конвейерный способ инференса).

Это означает, что нейроморфный искусственный интеллект имеет хорошие перспективы стать одной из ключевых технологий

для стремительно растущего сегмента промышленных и потребительских конечных (Edge) устройств с ИИ (Edge AI):

- ◆ сенсоры, датчики и контроллеры промышленного Интернета вещей (IIoT);
- ◆ автономные (мобильные) роботы, в том числе самообучающиеся;
- ◆ устройства умного дома;
- ◆ носимые пользовательские устройства: смартфоны, планшеты, умные часы, наушники, очки виртуальной и дополненной реальности.
- ◆ носимые медицинские устройства.

И это далеко не полный список перспективных устройств класса Edge AI.

Специфика Edge AI заключается в том, что интеллектуальные функции должны работать не в облачной инфраструктуре ЦОД с их возможностями суперкомпьютерных вычислений, а непосредственно на чипе самого устройства. Это обеспечивает преимущества в части быстродействия, снижает объем передаваемых в облако данных, а также сни-

мает многие вопросы, связанные с безопасностью данных и сохранением их конфиденциальности.

В тоже время, как правило, Edge-устройства — это оборудование в компактном форм-факторе с жесткими ограничениями по доступным вычислительным ресурсам, объему памяти и энергопотреблению. Нейроморфные системы как нельзя лучше вписываются в эти ограничения.

ПРАКТИЧЕСКИЕ ЗАДАЧИ ДЛЯ УНИКАЛЬНЫХ ВОЗМОЖНОСТЕЙ НЕЙРОМОРФНОГО EDGE AI

Среди областей применения программно-аппаратных нейроморфных систем отметим следующие:

- ◆ мобильные роботы с ИИ для распознавания обстановки на местности, привязки к картам, автономной навигации;
- ◆ системы быстрого реагирования на препятствия для беспилотных транспортных средств и систем помощи водителю;
- ◆ системы трекинга (отслеживания) быстро движущихся объектов;
- ◆ системы контроля сверхбыстрых промышленных процессов, протекающих за миллисекунды;
- ◆ системы видеоконтроля ситуационной обстановки (люди, дорожный трафик);
- ◆ видеоконтроль состояния оператора критических производств, водителей;
- ◆ автономные носимые устройства контроля здоровья человека;
- ◆ системы поддержки людей с ограниченными возможностями;
- ◆ охранные системы контроля обстановки и системы сохранения приватности;
- ◆ системы обнаружения атак на ИИ.

Преимущества нейроморфных систем еще более ярко проявляются при совместном использовании нейроморфных процессоров с видеокамерами класса DVS (Dynamic Vision Sensor, «событийное зрение») или другими устройствами с импульсной и событийной структурой данных. Особенность DVS-камеры заключается в том, что каждый пиксель DVS-матрицы работает независимо от других. Он порождает импульс (событие) при локальном (соответствующем его позиции) изменении яркости в сцене. Общее количество таких импульсов может достигать сотен миллионов в секунду, что позволяет DVS-камерам регистрировать очень быстрые процессы. Правда, в настоящее время DVS-камеры производятся только за рубежом...

Нейроморфные системы также могут применяться для поддержки работы больших (глубоких) нейросетевых моделей. Приведем конкретный пример. Нейроморфная система, благодаря низкому энергопотреблению, работает на устройстве в режиме «всегда включено» (always-on) и решает задачу обнаружения определенного события. Для умной колонки таким событием может быть, например, произнесенная пользователем команда на начало диалога (key-word spotting), для смарт-камеры видеонаблюдения — появление в поле зрения объекта заданного класса (key-image spotting) или наличие движения. При обнаружении события в работу включается большая нейросетевая модель, которая до этого находилась в режиме ожидания и не потребляла ресурсы.

РОССИЙСКИЙ ОПЫТ СОЗДАНИЯ НЕЙРОМОРФНЫХ РЕШЕНИЙ

Экосистема (технологический базис) нейроморфного ИИ состоит из нескольких основных компонентов: разработка и обучение импульсных нейронных сетей, производство и использование нейроморфных процессоров и сенсоров. Все перечисленные компоненты объединяет событийный (импульсный) характер сбора и передачи информации, а также локальный и асинхронный способ ее обработки. Это означает, что в импульсных ИНС отдельные нейроны, по сути, представляют собой вычислители, которые асинхронно обмениваются между собой дискретными импульсами-спайками. При этом генерация таких спайков происходит только в ответ на некоторое стимулирующее воздействие.

Нейроморфные процессоры фактически реализуют импульсные нейросети на специальной аппаратной архитектуре, в которой вычислительное ядро располагается как можно ближе к памяти. Такая архитектура позволяет избежать проблемы «бутылочного горлышка архитектуры фон Неймана», присущей обычным компьютерам, и связанных с этой проблемой дополнительных затрат по времени и энергии на пересылку данных между памятью и вычислительным ядром.

«Лаборатория Касперского» разрабатывает и развивает собственную программно-аппаратную платформу Kaspersky Neuromorphic Platform (KNP), предназначенную для проведения исследований в области нейроморфного машинного обучения и создания коммерческих продуктов с элементами нейроморфного ИИ. Архитектура

KNP позволяет объединить все компоненты экосистемы нейроморфного ИИ (импульсные нейросети, нейроморфные процессоры и сенсоры) в единый конвейер сквозной разработки ИИ-решений: от стадии замысла до реализации и тестирования на конечном устройстве.

Платформа KNP, анонсированная в 2022 г., сегодня применяется во внутренних проектах компании по тематике нейроморфного ИИ. Отрабатывается и расширяется функционал платформы, в том числе с учетом последних достижений в области импульсных нейросетей, совершенствуется программная архитектура. А в нынешнем году KNP станет доступна внешним пользователям как проект с открытым исходным кодом.

KNP позволяет создавать импульсные нейросети с гибкой структурной организацией на основе двух подходов:

1. Преобразование нейросетей глубокого обучения в импульсные нейросети.

2. Разработка и обучение импульсных нейросетей с использованием механизма синаптической пластичности (STDP).

Кроме того, в платформе KNP реализована глубокая интеграция с первым российским нейроморфным процессором «Алтай» (рис. 2), который является совместной разработкой компаний «Мотив-НТ» и «Лаборатория Касперского». Выпущены прототипы чипа «Алтай» с 16 нейроядрами, 512 нейронами в ядре и возможностью инференса импульсных нейросетей. Потребление одного ядра не превышает 4 милливатт.

Кроме того, изготовлены платы с 8 и 16 чипами на процессорах «Алтай». Плата с 8 чипами представляет собой ускоритель нейроморфных вычислений, подключаемый к объединительной плате (рис. 3) в десктопном форм-факторе. На одну объединительную плату может быть подключено до 16 ускорителей. Плата с 16 чипами выполнена в форм-факторе встраиваемых систем и конструктивно совместима с платой OrangePi 5.

В «Лаборатории Касперского» разработано несколько прототипов прикладных нейроморфных систем на базе KNP и чипов «Алтай»:

- ◆ Нейроморфная система машинного зрения милливатт-диапазона для мониторинга ротационного оборудования. В демонстрационном варианте система решает задачу автоматического определения скорости и направления вращения лопастей вентилятора с использованием импульсной нейронной сети. Нейронная сеть реализована на двух нейроморфных ускорителях «Алтай» и по-

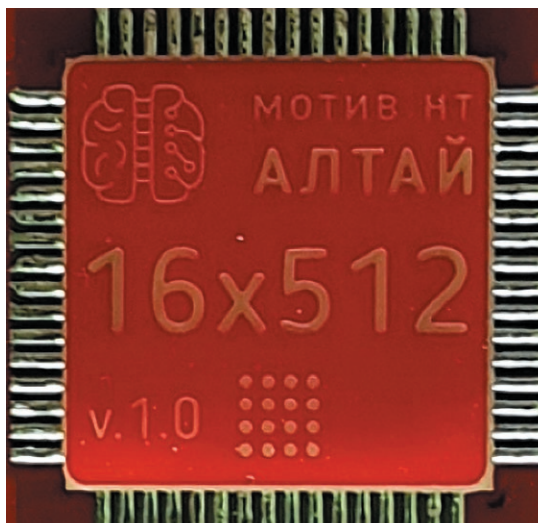


Рисунок 2. Прототип нейроморфного чипа «Алтай». Источник: «Лаборатория Касперского»

требляет в процессе работы в среднем 70 мВт электроэнергии. Для сравнения — аналогичное решение, реализованное на базе GPU, потребляет в среднем 13 Вт.

- ◆ Нейроморфная система машинного зрения для энергоэффективного измерения быстрых процессов. Демонстрационный прототип решает задачу измерения частоты мерцания светодиода (LED) в диапазоне 0,25–1,25 кГц на чипах «Алтай» с энергопотреблением почти на 3 порядка меньше энергопотребления аналогичной системы на GPU. При этом скорость инференса нейросети в 10 раз выше, чем на GPU.

- ◆ Нейроморфное Edge-устройство на двух чипах «Алтай» для защиты ML/AI-систем от состязательных атак на примере системы распознавания лиц.

В 2025 г. планируется выпуск процессора «Алтай» следующего поколения. Он будет обладать целым рядом новых важных возможностей: обучение нейросети на чипе (on-line learning), программируемая модель нейрона, программируемая синаптическая функция, динамически изменяемая структура нейросети. Это станет новым серьезным шагом вперед к созданию не только энергоэффективных и быстродействующих, но и адаптивных систем нейроморфного ИИ.

Все новые возможности процессора «Алтай» также будут поддерживаться в платформе KNP, что позволит учесть при разработке импульсных нейросетей особенности аппаратной архитектуры «Алтая» и, как следствие, создавать вычислительно-эффективные конечные решения на данной аппаратной платформе.

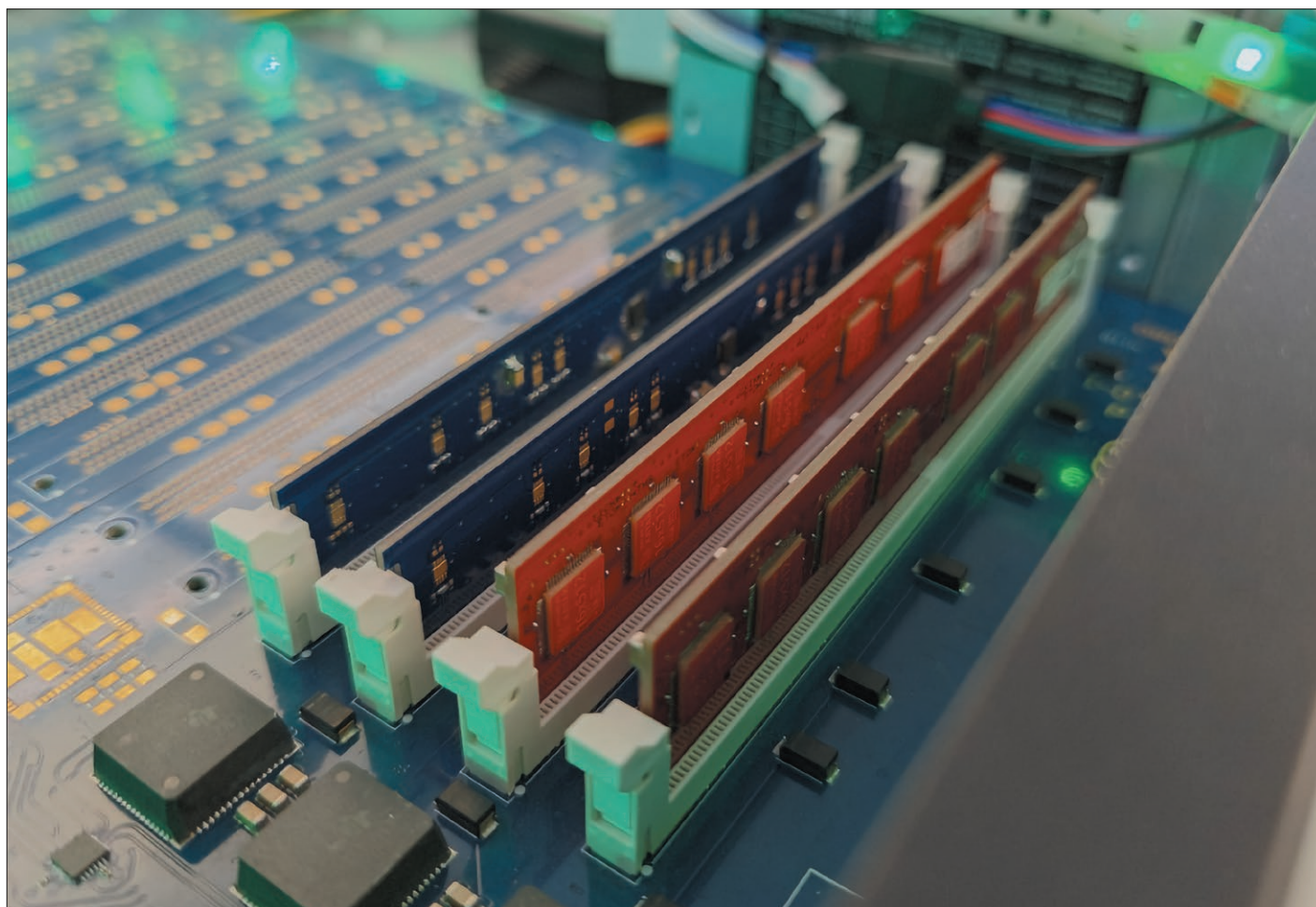


Рисунок 3. Объединительная плата с ускорителями нейроморфных вычислений «Алтай»

МЕСТО НЕЙРОМОРФНЫХ ТЕХНОЛОГИЙ В РАЗВИТОЙ СУВЕРЕННОЙ ОТРАСЛИ РОССИЙСКОГО ХАЙТЕКА

У нейроморфных научно-исследовательских разработок — огромный потенциал. В перспективе их развитие должно привести к созданию когнитивной архитектуры ИТ-систем, обладающей возможностями сенсорики и распознавания образов, понимания времени как динамики образов, адаптации к среде, планирования сложных реакций. В ближайшие несколько лет нейроморфные разработки, несомненно, лягут в основу систем ИИ, интегрированных непосредственно в конечные устройства и выполняющих интеллектуальные функции в автономном режиме без использования инфраструктуры облачных вычислений (или с минимальным ее применением). Такие системы будут обладать энергоэффективностью, высоким быстродействием, безопасностью и адаптивностью (возможностью самообучаться) за счет сочетания аппаратных и программных технологий, вдохновленных принципами работы биологического мозга.

Важно, что «Лаборатория Касперского» с партнерами активно развивает экосистему продуктов для создания российских доверенных программно-аппаратных средств нейроморфного ИИ в интересах промышленности и потребительского рынка. Нынешний уровень зрелости российских нейроморфных разработок уже сейчас позволяет создавать демонстрационные прототипы (proof-of-concept) систем обработки данных различной модальности: изображения/видео, звук, текст, сигналы от контрольно-измерительных приборов. На очереди — этап апробации нейроморфных решений в конкретных практических задачах цифровизации и интеллектуализации промышленного производства, а также в перспективных образцах потребительской электроники.

Опыт применения и анализ соответствующих эффектов — это тот этап, который поставщикам и потребителям инновационных решений нужно пройти вместе, согласованно и целенаправленно создавая суверенную отечественную инфраструктуру высокоразвитых когнитивных ИТ-систем.

«ДЛЯ РЕАЛЬНОГО ПРОРЫВА НАМ НЕ ХВАТАЕТ СИСТЕМНОГО ПОДХОДА К РАЗВИТИЮ»



Ренат ЮСУПОВ
старший
вице-президент
компании Kraftway

Технологический прорыв возможен только тогда, когда он тщательно готовится заранее, – это аксиома. Случайных технологических прорывов не бывает. Могут быть случайные открытия типа высокотемпературной сверхпроводимости, но это очень редкие события. Так что системные технологические успехи нуждаются в тщательной подготовке как со стороны государства, потому что задачи такого масштаба требуют существенных инвестиций, так и со стороны предприятий, которые не должны бояться идти в радикальную технологическую модернизацию. К тому же наши ИТ-компании, по большому счёту, сегодня работают в парадигме догоняющего. И изменить эту парадигму крайне сложно.

Простой пример – вся отечественная вычислительная техника, очевидно, базируется

на архитектуре x86. Это в чистом виде догоняющий подход: глобальные вендоры либо нам разрешают чем-то воспользоваться, либо запрещают, и тогда мы сами добываем «запретный плод», некоторым образом творчески перерабатываем и получаем примерно то же самое, но с определёнными возможностями, которые требуются, скажем, локальным законодательством по безопасности. Тот же самый подход мы видим в области СХД. Скажем, взлёт решений компании YADRO базировался на архитектуре PowerPC корпорации IBM. Технологических прорывов там нет, а есть очень аккуратная творческая переработка, подкреплённая грамотным маркетингом и удачным стечением обстоятельств в виде бегства западных вендоров с российского рынка.

Однако у такого положения вещей есть серьёзные предпосылки.

ПРОРЫВ В ТЕХНОЛОГИЧЕСКИЙ СУВЕРЕНИТЕТ — ЭТО ДОЛГО И ДОРОГО

Вообще говоря, технологические прорывы доступны только крупным компаниям. Как минимум потому, что это очень затратное занятие. Покажу на примере разработки контроллера твердотельных дисков компании Kraftway (рис. 1–2).

Мы вышли на пиковое направление – реальных производителей дисковых контрол-

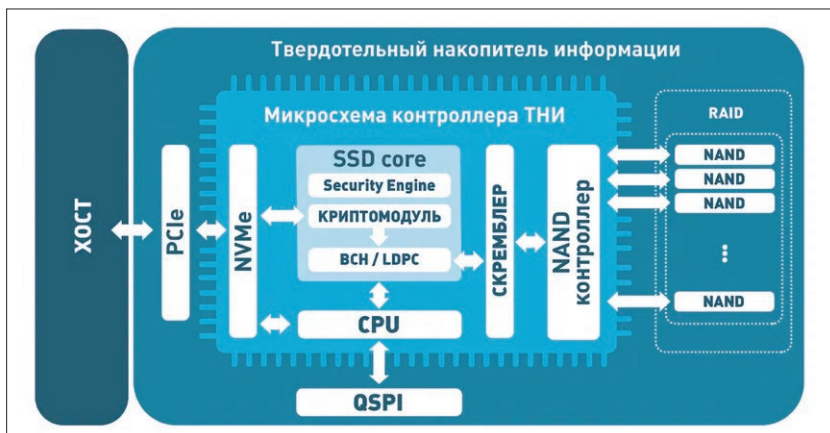


Рисунок 1–2. Источник: Kraftway

Чтобы появились «суверенные» микросхемы, вначале должны появиться всевозможные национальные архитектуры, а также крупные национальные дизайн-центры, которые поддерживают целые экосистемы разработки микросхем

леров в мире наберётся от силы полтора десятка максимум. Это производителей самих дисков много, а вот тех, кто умеет создавать современные контроллеры, — считанные единицы. Дело в том, что это очень наукоёмкое направление. Так, мы наши работы вели в тесном партнёрстве с командой математиков МГУ, которые смогли предложить нужные нам математические подходы. То есть наши дисковые контроллеры — полностью отечественные на уровне алгоритмов. На уровне электроники в них используется большое количество IP-блоков (Intellectual Property — готовый блок для проектирования микросхем), каждый из которых можно снабдить надписью «Сделано в России». И это требует колоссальных затрат времени высококлассных уникальных специалистов, а также инвестиций. Потому что один только инструментарий для создания IP-блоков стоит на уровне десятков миллионов рублей. А есть ещё такие IP-блоки, которые мы в принципе не можем заказать у российских разработчиков, поскольку их надо проектировать для конкретной фабрики. А значит, стоимость проекта вырастает кратно, поскольку IP-блоки физического уровня высокоскоростных интерфейсов стоят в разы дороже цифровых блоков. Понятно, что компания даже среднего уровня запустить такой проект не сможет, даже при наличии соответствующих умных голов.

При этом цикл разработки микросхем в самом простом случае составляет не менее трёх лет, а для более сложных изделий составляет пять и более лет. Так, мы выпустили первую модель контроллера SSD с российскими интегрированными средствами защиты в 2019 г. Это была ограниченная партия, предназначенная в первую очередь для реальных проверок работы с оборудованием различных поставщиков оборудования и ПО. В конце 2023 г. завершили создание второго поко-

ления устройства. Сейчас этот контроллер проходит стадию начального запуска, отладки и т.д. Думаю, что в ближайшее время он появится на рынке. Получается, что полный цикл от начала разработки до полноценного выхода на рынок составляет 8 лет.

Играть в такую долгую и дорогую игру очень сложно. Вот почему я считаю, что наиболее критичная трасса на пути достижения технологического суверенитета — это отечественная микроэлектроника.

О СОСТАВЛЯЮЩИХ УСПЕХА СУВЕРЕННОГО МИКРОЭЛЕКТРОННОГО БАЗИСА

Ключевая компонента электроники — это микросхемы, то есть в первую очередь фабрики под современные технологические нормы. Это ключ ко всей радиоэлектронной промышленности страны, поэтому именно с них надо начинать, если ставить задачу достижения технологического суверенитета. А для того чтобы появились «суверенные» микросхемы, вначале должны появиться всевозможные национальные архитектуры, а также крупные национальные дизайн-центры, которые поддерживают целые экосистемы разработки микросхем.

За рубежом сейчас есть 2–3 экосистемы такого рода: x86, ARM, RISC-V. Причём широкого охвата разработчиков они достигли во многом за счёт глобализации. Но нам фактор глобализации пока не очень доступен, приходится создавать собственные локальные продукты. Но ни одной экосистемы у нас пока не создано, несмотря на то что имеются сильные школы разработки микропроцессоров.

Например, «Эльбрус» — сам по себе процессор неплохой, работоспособный. Но отсутствие экосистемы существенно ухудшает его рыночные позиции. Скажем, у него нет готовой к применению программы начального старта. Если разработчик электронной аппаратуры решит сделать системную плату на базе процессора «Эльбрус», ему придётся обращаться к разработчику процессора для того, чтобы там ему написали программу начального старта. А это не что иное, как «бутылочное горлышко»: компания справляется с небольшим потоком обращений разработчиков. А если начнётся — я фантазирую — бум создания плат на процессоре «Эльбрус» и к ним пойдут десятки и сотни обращений? К сожалению, сегодня они не рассчитаны на создание экосистемы массового производства.

А как поступает в этой ситуации компания Intel? Она выпускает референсную плату и к ней — базовый набор софта, включая все необходимые инструменты, для разработки каких-либо готовых изделий на базе процессора Intel плюс подробные руководства для компаний-разработчиков. Процесс настолько отлаженный, что с этим комплектом от Intel любая компания может начать собственную разработку, даже без техподдержки со стороны вендора. Кроме того, есть сторонние производители, которые выпускают ПО BIOS: American Megatrends, Insyde и др. То есть на базе экосистемы производителя процессора складывается экосистема компаний-партнёров, которая успешно живёт своей рыночной жизнью.

У нас таких экосистем нет ни у одного отечественного производителя процессоров. Использовать их точно в отдельных проектах вполне возможно, но не в промышленных масштабах. И эту ситуацию точно нужно менять. Как именно? Простых рецептов, к сожалению, нет. Видимо, должна быть реализована какая-то форма государственно-частного партнёрства, потому что ни одна частная компания самостоятельно не вытянет создание национальной архитектуры. На это просто не хватит денег. Достаточно посмотреть на бюджеты крупных западных корпораций, которые поддерживают собственные архитектуры, — они превышают бюджеты большинства африканских государств.

«КЛАСТЕРИЗАЦИЯ» НАПРАВЛЕНИЙ РАЗВИТИЯ СУВЕРЕННОГО ХАЙ-ТЕКА

Ещё одна критически важная задача — создание технологических кластеров вокруг разных базовых технологий: процессоров, устройств хранения данных и т.д. Мы, например, делаем это сейчас собственными силами и очень рассчитываем, что со временем начнёт складываться некоторая экосистема технологий, связанных с хранением данных. Надо сказать, что эта история не сильно проще и дешевле, чем процессорная, потому что весьма наукоёмкая. Другие направления создания кластеров технологий и продуктов связаны с другими типами контроллеров, автомобильной электроникой, оборудованием АСУ ТП, где широко применяются программируемые логические контроллеры (PLC) и всевозможные промышленные компьютеры. Эти центры с соответствующим кластерным окружением ещё только предстоит создать.

Формально у нас появляются некоторые центры компетенций. Но этот формат пока не очень работает. Во многом, думаю, потому, что для активной деятельности этих центров нужна поддержка со стороны хороших научных школ, а также финансирование для создания новых наукоёмких продуктов и технологий. Иначе «жизнь» нового направления не сложится.

Аналогичные проблемы — с прорывными научными идеями: им нужна соответствующая «обвязка» в виде разработок готовой аппаратуры или ПО силами партнёров. Скажем, в России приступили к созданию установки безмасочной литографии на длине волны 13,5 нм для производства микроэлектроники с использованием рентгеновской оптики, которая способна поддерживать технологические процессы уровня 7 нм. Это пример прорывного математического подхода. Но для того чтобы на его базе появились установки, которые можно покупать и устанавливать на российских микроэлектронных фабриках, нужно ещё очень многое, помимо математических методов. В первую очередь целая школа технологов и разработчиков станков, которые хорошо понимают, с какими технологическими процессами они имеют дело. И с точки зрения затрат, это, конечно, не уровень расширения освоенного производства, а именно инвестиции в создание принципиально новой производственной инфраструктуры.

ОБ ОРГАНИЗУЮЩЕЙ РОЛИ ГОСУДАРСТВА

Хороший пример того, как китайские товарищи создавали национальную индустрию микроэлектроники, — компания YMTC (Yangtze Memory Technologies Company), ведущий производитель микросхем памяти. Я провёл немало времени, изучая их опыт непосредственно в Китае, и вот что рассказали мне ведущие сотрудники этой китайской компании, которая имела амбиции стать второй компанией в мире по производству микросхем памяти.

Начальные инвестиции составляли около 8 млрд долл., по факту дело дошло до 25 млрд долл. Планировалось запустить три очереди завода, каждая — по 100 тыс. пластин в месяц. То есть 300 тыс. пластин в месяц — это действительно производитель номер два в мире по объёмам выпускаемой NAND-памяти. Они разработали собственную архитектуру памяти. А затем приложили громадные усилия для того, чтобы насытить все сопутствующие научно-производствен-

ные направления нужными кадрами: создавали научные кластеры, привлекали сотрудников зарплатой, в несколько раз большей, чем на предыдущей работе, в том числе собирали специалистов по всему миру, буквально «скупали» целыми семьями за рубежом и возвращали на родину. Я разговаривал с менеджерами высокого звена и с удивлением обнаруживал, что они приехали в Китай, оставив успешную карьеру в США, Южной Корее и других странах в компаниях Micron Technology, Samsung, SK Hynix и др. Инвестиции в амбициозный проект предоставило государство через крупнейшую китайскую финансовую группу Tsinghua Unigroup.

В итоге они, действительно, сумели запустить это современное производство. Правда, изначально использовали импортные литографические машины и с запуском первой очереди завода сразу вошли в пятёрку крупнейших глобальных производителей. Когда стали запускать вторую и третью очереди завода, американцы забеспокоились, и тогда первыми среди китайских высокотехнологичных компаний под санкции попали именно они. Именно потому что уверенно шли к своей цели — вырасти до уровня второго в мире крупнейшего производителя NAND-памяти. На самом деле это чисто конкурентная борьба. Однако сугубо политическими методами американцам удалось притормозить развитие огромной компании. Именно притормозить, но не остановить! Сейчас они развивают суверенную литографию, и думаю, через несколько лет они полностью освободятся от какой бы то ни было зависимости от американских технологий.

Так что ключевые элементы этого большого национального проекта Китая с прицелом на глобальное лидерство — следующие: очень серьёзные бюджетные инвестиции, продуманный план создания производства — мирового лидера, первоклассная команда сотрудников: от учёных до организаторов бизнеса, которых государство помогало вернуть из разных стран мира. Вот так реализуются большие национальные проекты.

Наша страна, в принципе, идёт похожим путём. Самое большое отличие нашего пути от китайского заключается, на мой взгляд, в отсутствии системного подхода к реализации большой идеи как единого целого результата. Скажем, государство реально помогает развитию национальной радиоэлектронной промышленности. Вот только критерии помощи смещены в сторону точечной поддержки конкретных компаний. Фактически государ-

ство оказывает финансовую поддержку организации в обмен на обещание через 5–7 лет завалить рынок готовыми продуктами, которые будут хорошо продаваться. Конечно, это неплохо, что на нашем рынке появится некая отечественная «штучка», на которую будет спрос. Но что это даёт развитию радиоэлектронной промышленности страны в целом? К сожалению, здесь совсем не идёт речи про национальные архитектуры, а значит, о целых группах продуктов или секторах технологий, которые также включаются в поток общего развития. В этом нет системы — вот что плохо. Попробую предложить вариант системного подхода.

СТИМУЛИРОВАТЬ УСИЛЕНИЕ ТОЧЕК РОСТА

Другой путь движения в сторону технологического суверенитета можно выстраивать в виде группы перспективных направлений, которые опираются на существующие точки роста — научные группы, дизайн-центры и т.д. Вот эти направления и нужно поддерживать на государственном уровне, в том числе финансами. Причём инвестиции направлять на мероприятия, которые помогают унификации разработок и совместной деятельности. Речь, конечно, идёт не о консолидации бизнеса, а как минимум об обмене готовой интеллектуальной собственностью. Такой обмен у нас в стране вообще не налажен: о том, что одна компания создала тот или иной IP-блок, соседи даже не знают и по привычке покупают готовые блоки у известных зарубежных поставщиков. Это даже не смешно, ведь Минпромторг РФ субсидирует отечественные разработки, а часть этих средств уходит зарубежным компаниям вместо того, чтобы поддерживать продажи российских разработчиков. Но поскольку нет экосистемы продуктов, нет и внутренней энергии продуктов, а значит, инвестиции расходуются не так эффективно, как могли бы.

Возникают аналогии с вернееуровневым проектным подходом, который когда-то применялся в Советском Союзе для больших национальных проектов: космического, атомного и т.п. Такой крупный проект декомпозировался на подпроекты более низкого уровня без потери внутренней связности отдельных разработок. Тогда инвестиции направляются в технологические кластеры, которые охватывают целый ряд близких направлений: научных, научно-технических, производственных. И суверенное развитие начинается как раз внутри этих кластеров,

а потом выходит на уровень большого системного проекта верхнего уровня.

А что мы по факту имеем сегодня вместо системного подхода к развитию? Идея технопарков: территория, на которую приглашаются все желающие получить льготы. Такой подход может подойти малому бизнесу, который работает в конкретной понятной предметной области, — получить финансовую помощь на запуск проекта с быстрой реализацией. Но крупного долговременного экосистемного проекта на этой базе не вырастить. Технологический суверенитет станет возможным в контексте серьёзного проектного подхода. Умных мозгов у нас достаточно, но нужно направить их активность в нужное русло.

Здесь стоит вспомнить про стартапы и связанный с ним штамп, навязанный нам американским ИТ-сектором: основная движущая сила инновационного прорывного технологического развития — это амбициозные компании-стартапы, с них и начинается инновационное развитие страны. Могу согласиться разве только со словами про начало.

Стартап всегда действует в рамках некоторой собственной идеи. И вероятность того, что эта идея совпадёт с какой-то серьёзной большой задачей, которую необходимо решать и далее развивать, достаточно мала. Ведь стартапы идут по пути наименьшего сопротивления: минимум инвестиций и максимум результата при продаже. Поэтому идеи, которые их занимают, скорее прикладные, чем системные. Поэтому стартап интересен в первую очередь как кузница кадров — тех самых увлечённых людей с горящими глазами. Вот эту команду нужно проинвестировать, подключить её к серьёзным задачам в рамках глобального проекта, и они будут отлично её выполнять.

О НАУКОЁМКОСТИ ТЕХНОЛОГИЧЕСКОГО СУВЕРЕНИТЕТА

Повторю тезис про то, что технологический суверенитет — вещь наукоёмкая. Поэтому обязательный элемент движения к технологическому суверенитету — тесная связка разработчиков технологий, продуктов и систем с фундаментальной и прикладной наукой. Сегодня эта связка чаще всего формируется случайно. Так, например, было у нас: мы абсолютно случайно встретились с командой МГУ, которая работала в направлении фундаментальной математики, интересном нам. Мы посмотрели друг на друга внима-

тельнее, стали сотрудничать, и это взаимодействие вылилось в итоге в большой проект.

Это была счастливая случайность. К сожалению, события такого рода не так часто происходят. Об этом я могу судить как член экспертного совета при Минпромторге, который занимается анализом заявок на субсидирование разработок в области микроэлектроники (постановление Правительства РФ № 1252). Я вижу, какая научная подоснова имеется под каждым проектом. В целом она очень слабая. Встречаются редкие исключения, но тогда обычно заявку подают институты РАН либо крупные ведомственные НИИ, скажем, из системы «Росатома». Там серьёзная научная основа, всегда интересно узнать подробности. Но основной поток соискателей субсидий приходит с сугубо прикладными решениями, без признаков отраслевой или фундаментальной науки. Но это, как я полагаю, всего лишь результат работы нынешней системы субсидирования развития гражданской радиоэлектронной продукции.

При этом стоит подчеркнуть, что крупные российские высокотехнологичные компании работают с научной составляющей и на принципах системности. Например, мы и в прикладных работах применяем собственные фундаментальные вещи, такие как внутреннее ядро или IP-блок, которые потом тиражируются на все линейки продуктов. Тогда складывается, скажем, экосистема информационной безопасности, реализованная во всех микросхемах, и она достаточно гомогенна: один и тот же IP-блок, одни и те же инструменты разработки, одно и то же ПО, единые протоколы, спецификации — и вот уже складывается совместимая экосистема. Но это доступно только крупным компаниям, а их у нас можно по пальцам одной руки пересчитать.

Надо сказать, что очень многие элементы системного движения к технологическому суверенитету в нашей стране уже имеются. Осталось дело за тем, чтобы немного подкрутить существующее положение вещей. Скажем, подтолкнуть формирование технологических кластеров вокруг системообразующих направлений развития, расширить функционал аналитики на этом уровне, добавив к классическому конкурентному анализу профессиональные обзоры научных работ, а также внедрить модернизированные оценки локализации, которые учитывают количество и качество реализации полностью отечественных элементов в оборудовании и ПО.

«БЕЗ ПРОРЫВНЫХ ТЕХНОЛОГИЙ И ПРОДУКТОВ НЕВОЗМОЖНО ДВИЖЕНИЕ В БУДУЩЕЕ НА УРОВНЕ МИРОВЫХ ЛИДЕРОВ»



Захар КОНДРАШОВ
генеральный директор
НИИМА «Прогресс»

Технологический суверенитет страны, очевидно, связан с развитием. При всём нынешнем увлечении, в частности, государевых служащих, программированием и его популяризацией, надо отдавать себе отчёт: технологического суверенитета России без «железа» не будет! Поделюсь опытом, как мы в НИИ микроэлектронной аппаратуры «Прогресс» подходим к практической реализации задачи развития, как собственного, так и экономики страны в целом.

ПОЧЕМУ НИИ — ЭТО НЕ ДИЗАЙН-ЦЕНТР

Модель работы дизайн-центра предполагает, что сотрудникам поступает задача с конкретным техническим заданием и набором ограничивающих параметров: необходимо создать в заданный срок изделие с конкретными параметрами, которое реализует определённый функционал и способно работать в некоторых заданных условиях, например климатических и т.д. Позиции сотрудника НИИ предполагают совершенно другой уровень кругозора: в ходе научно-исследовательских работ он должен гораздо шире смотреть на область, в которой идёт работа, по сравнению с исполнителем конкретной прикладной задачи. А для того чтобы эта научно-исследовательская работа не превращалась в реализацию неких личных фантазий, сотрудник НИИ должен ещё и выступать в роли технологического предпринимателя. Нужно понимать, нужен ли кому-то вообще результат той исследователь-

ской работы, которая идёт в НИИ? Есть ли вообще шансы, что оно «взлетит»?

Научно-исследовательский поиск — это всегда выход за некие сложившиеся рамки. Поэтому работа НИИ микроэлектронной аппаратуры «Прогресс» подразумевает формирование изделия, которое реализует некоторые новые функции, возможно, даже с применением иных физических принципов либо с применением новых технологий. Собственно, здесь и проходит водораздел между обычным дизайн-центром и НИИ, подобным НИИМА «Прогресс»: работа с освоенными технологиями или режим поиска новых технологических методов решения поставленных задач.

Мы видим границы возможностей освоенных технологий, понимаем функциональные ограничения соответствующих изделий: что мы можем, например, «вытянуть» по частотам на технологии кремний — германий (SiGe), а что можно получить для похожих изделий на основе арсенида галлия (GaAs). Наши технологические заделы и соответствующие знания помогают нам найти наиболее эффективный способ реализации нужного изделия в тех или иных технологических переделах.

ТВОРЧЕСКИЕ ЗАДАЧИ НИИМА «ПРОГРЕСС»

Точка приложения наших научно-исследовательских сил — это один из самых перспективных сегментов рынка высокотехнологичных продуктов — область роботизации и систем интеллектуального управления. Почему именно роботизация? Потому что это высокочисленная индустрия, в которой решаются задачи как микроэлектроники по нашему профилю (связь, навигация, микроконтроллеры, компьютеринг, различного рода радары, сенсоры), так и интеллектуальной обработки данных (например, обработка видеоизображений, данных различной телеметрии) для того, чтобы робототехнический комплекс мог двигаться в пространстве, причём в любой стихии: на земле, в воздухе, на воде, под водой. Есть ряд работ, где мы исследуем распространение навигацион-



Рисунок 1. : Комплексированная Навигационная Система Услуг Локации (КОНСУЛ). Источник: НИИМА «Прогресс»

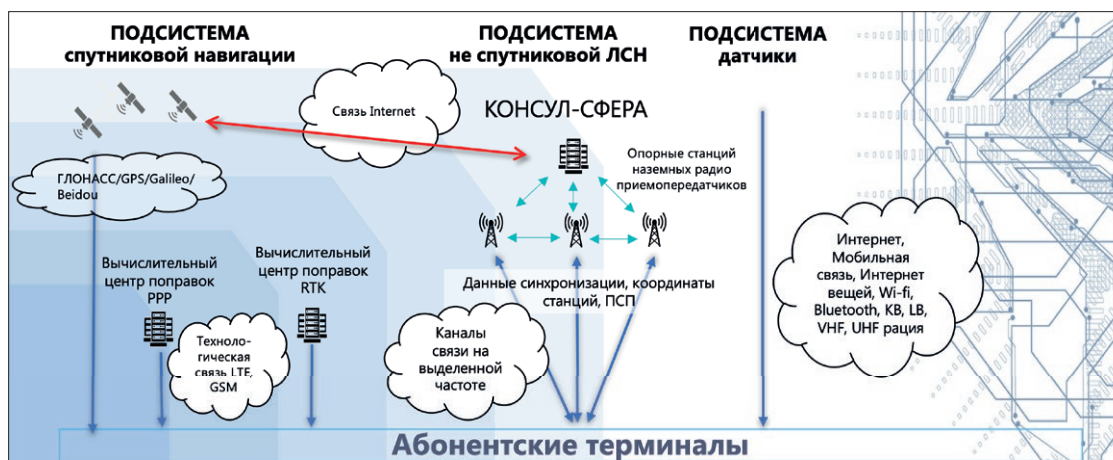


Рисунок 2. Интеграция проекта «КОНСУЛ» (НИИМА «Прогресс») с проектом «СФЕРА» («Роскосмос»). Источник: НИИМА «Прогресс»

ных и связных сигналов под землёй. В этой части возникают реальные прорывные технологии, которые могут и будут применяться для развития сопутствующих отраслей. Например, в части управления высокоавтоматизированными транспортными средствами (ВАТС) мы будем обеспечивать нашими решениями беспилотные автомобильные, морские, авиационные системы.

Например, известна проблема современных глобальных навигационных спутниковых систем (ГНСС): их сигнал можно заглушить или подделать, и такие попытки уже бывали. У нас есть свой амбициозный проект — создание комплексированной навигационной системы услуг локации «КОНСУЛ» (рис. 1).

По сути, к тем российским космическим технологиям, которые есть в России, добавляется доверенная наземная коммуникационная инфраструктура — локальная система навигации «КОНСУЛ», работающая в комплек-

се с ГНСС, как с инерциальными, так и с безинерциальными системами, а также глобальной спутниковой системой «Сфера», которую в настоящее время создаёт «Роскосмос».

По своему функционалу «Сфера» превосходит все космические системы, ранее создававшиеся в России: впервые появляется возможность объединить услуги связи, передачи данных, навигации, дистанционного зондирования Земли и сделать эти сервисы доступными всем потребителям. Особое значение имеют спутниковые группировки «Сферы» для работы в северных широтах и Арктике.

Интеграция систем «КОНСУЛ» и «Сфера», в числе прочего, даёт возможность существенно повысить точность и надёжность навигации в ряде приложений, например, за счёт того, что система «КОНСУЛ» учитывает поправки (PPP, RTK), которые передаются буквально и с земли, и с неба (рис. 2).

Эта универсальная система навигации и связи может успешно применяться на высокоавтоматизированных транспортных средствах без водителя. Ведь для этого нужна, во-первых, чётко работающая надёжная помехоустойчивая связь и, во-вторых, точная передача координат ВАС в реальном масштабе времени. Мы создаём систему такого рода, которая позволяет управлять беспилотным транспортом на автодорогах, а также на море — безэкипажное судовождение (БАС).

ПРО НАУЧНЫЙ ПРОРЫВ

Думая о направлениях стратегического научно-технического развития НИИМА «Прогресс», мы постарались понять, как выглядит в консолидированном виде вся совокупность наших технологических заделов, которая может применяться во всех отраслях деятельности, которые точно будут активно развиваться в краткосрочной и среднесрочной перспективе. И поняли, что это робототехника — универсальная сквозная индустрия, продукты которой могут применяться везде. В русле сквозных задач робототехники года три назад мы сформулировали свою концепцию управления перемещением объектов X-to-X.

В отличие от зарубежных компаний, которые сегодня мыслят в категориях V-to-X (Vehicle-to-everything, V2X) или C-to-X (Car-to-X), что подразумевает связь между транспортным средством и любым объектом, который может повлиять на транспортное средство, мы говорим о том, что два неизвестных объекта могут общаться друг с другом, определять позиционирование в пространстве друг относительно друга с тем, чтобы либо сблизиться, либо, наоборот, удалиться, избежав аварийной ситуации. Один из вариантов реализации концепции X-to-X — межмашинное взаимодействие M-to-M, которое находит всё более широкое применение, в частности, на производственных предприятиях.

На уровне практической реализации концепции X-to-X возникает целый пласт технологий, связанных с электронной компонентной базой, то есть нашей основной специализацией: навигация (навигационная аппаратура), связь между объектами (телекоммуникационное оборудование, включая специализированные СВЧ-микросхемы, которые могут выполнять роль элементов приёма-передающего тракта или самого тракта передачи данных по беспроводным технологиям Bluetooth или Wi-Fi и др.), обработка данных и управляющее воздействие (микроконтроллеры), обработка

большого объёма информации (вычислительные микропроцессоры). Подразумевается, что мы создаём и специальные технические решения, которые могут работать в открытом космосе. Специализированные задачи всегда ставились перед нашим институтом с момента его создания в 1987 г.

Разработка прорывных технологий подразумевает создание устройств, ориентированных на новые рынки. Яркий пример — устройства нового класса ЭСИМ, то есть электронные средства индивидуальной мобильности. Ими стали самокаты. Это был ответ на актуальную проблему отсутствия учёта, превышения скоростного режима и связанного с этим травматизма с участием ЭСИМ. Мы создали устройство, в котором реализован функционал контроля местонахождения и ограничения скорости самоката. Оно работает вместе с системой «ЭРА-ГЛОНАСС», которая фактически ведёт мониторинг передвижения самоката и в зависимости от конкретной геозоны, например перемещения по пешеходному тротуару, снижает скорость девайса до 5 км/ч. Вместе с новым классом устройств ЭСИМ появился соответствующий ГОСТ. Вот так мы создаём рынки, на которых применяются передовые отечественные технологии, реализованные в виде отечественных электронных устройств.

НАУЧНО-ТЕХНОЛОГИЧЕСКОЙ ЗАДЕЛ — ОСНОВА ДЛЯ ДВИЖЕНИЯ ВПЕРЁД

Развивать научно-техническое направление можно только на базе уже созданного технологического задела, ведь полёт творческой мысли любого коллектива всегда ограничен теми ресурсами и знаниями, которые накоплены к текущему моменту. Это мы чётко осознали, когда прошли путь формирования стратегии своего развития до 2030 г. Тогда мы чётко сформулировали перечень самых сильных своих компетенций: навигация, связь, специализированные микросхемы, в том числе изделия сверхвысоко-частотного диапазона. И всю последующую активность строим вокруг нашего технологического задела. Более того, мы перешли на следующую ступень развития наших продуктовых линеек, понимая, что на сегодняшнем рынке востребованы услуги высокотехнологичной отрасли. Теперь мы планируем наше бизнес-развитие по разным индустриям, исходя из того, какие услуги нужны потребителям, и из требований соответствующего регулятора.

В русле такого подхода появился, например, модем, необходимый для обеспечения связи мобильного или стационарного кассового аппарата с терминалом, который ведёт сбор платёжной информации. Второй пример — инициатива государства для помощи гражданам в экстренных ситуациях, которая получила воплощение в виде системы «ЭРА-ГЛОНАСС». Сегодня в каждом приборе «ЭРА-ГЛОНАСС» присутствует приёмник ГНСС, модем и контроллер — это всё продукция НИИМА «Прогресс».

Вот совсем свежий пример — по примеру зарубежной спутниковой сети создаётся наш аналог — низкоорбитальная передача данных в рамках спутникового проекта «Сфера». С одной стороны, наши изделия уже есть в конструкторской документации бортовых устройств. С другой стороны, мы понимаем, что абонентскому устройству, помимо собственно обмена данных, нужен достаточно широкий спектр возможностей. В частности, в какой точке находится это устройство? А оно наше или не наше? Кто этот потребитель? Можно ли ему доверять? Можно ли передавать ему тот объём данных, которые позволяют ему осуществлять те или иные функции, включая, возможно, некоторые специальные функции? Очевидно, что в этом контексте и полоса пропускания устройства должна быть несколько больше, и она должна быть закрытая, а абонентское устройство должно каким-то образом идентифицироваться. И связь должна быть доверенной, чтобы разговор нельзя было подслушать.

Задачи такого рода мы научились решать комплексно и стараемся свои компетенции передать потребителям с массового рынка. Конечно, умение решать специальные задачи, где требуется повышенный уровень безопасности, более точное позиционирование, которое работает в условиях особых требований к передаче данных, — это важно. Но только массовый рынок позволяет добиваться экономической целесообразности как по себестоимости и объёмам выпуска продукции, так и по рыночной доле присутствия.

НЕ ВЕЗДЕ НУЖНЫ ПРОРЫВНЫЕ ТЕХНОЛОГИИ

В целом в экономике наблюдается достаточно существенный дефицит рабочих рук. С ним можно бороться только через роботизацию и автоматизацию рутинных процессов. Мы уже увидели, как в результате цифровизации и применения методов искусственного интеллекта удаётся исключать рутинные дей-

ствия из бизнес-процессов, выполняемых людьми в офисах. А следующий этап развития связан с возможностью удалять рутинные операции в деятельности, связанной с физическими объектами, например, для перемещения грузов на складе по кратчайшим маршрутам или выполнения операций по сборке чего-либо (в идеале робот должен уметь собрать самого себя).

В этой части имеется неплохой методический задел, оставшийся ещё в наследство от Советского Союза, который связан с автоматизацией систем управления технологическими процессами (АСУ ТП). Для практической реализации этого направления в стране уже есть немало разработок. И вот что важно: это не требует особо высоких уровней реализации с точки зрения микроэлектроники. По большому счёту, в дополнение к тому, что сейчас происходит в этой области, достаточно создать ещё одну фабрику 40–65 нм. Там не нужны те тонкие процессы, о которых сегодня судачат в прессе! Доступных сегодня возможностей вполне хватит для того, чтобы оптимизировать, а затем автоматизировать производственные процессы. И эту активность можно закрутить достаточно быстро в масштабе всех производственных отраслей России. В результате высвободятся рабочие руки — тот трудовой потенциал, который можно направить на созидание нового, где требуется взаимодействие человека с человеком.

Так что нужно грамотно разделять две истории: развитие прорывных технологий и продуктов, без которых невозможно движение в будущее на уровне мировых лидеров, и массовая автоматизация, которая делает экономически целесообразной деятельность всех вовлечённых сторон — производителей микроэлектронных блоков и готовых систем, дистрибуторов и интеграторов, самих заказчиков.

Без прорывных вещей технологически развитое будущее недостижимо. Однако для их появления, во-первых, нужна фундаментальная и прикладная наука, которая должна специальным образом финансироваться. Во-вторых, поисковые работы очень затратны. Эти затраты тяжело нести обычной коммерческой организации, у неё просто не останется ресурсов для того, чтобы заниматься рынком. Для того чтобы реализация тех или иных прорывных разработок стала более массовым явлением, чем сейчас, наверняка, нужны дополнительные усилия в части синергии науки и бизнеса. А сама организация, занима-

ющаяся разработкой высокотехнологичной продукции, должна думать не столько о самом прорыве, сколько о том, чтобы решать важнейшие вопросы для сегодняшнего человечества: о том, как обеспечить безопасность жителей России и всей нашей планеты, как покорить космос и за счёт этого сделать жизнь на Земле более удобной и комфортной.

ДВИЖЕНИЕ — В ПАРТНЁРСТВЕ

Движение в сторону внедрения в российских компаниях и предприятиях нашей передовой продукции возможно только совместно с партнёрами. В этой части мы выбрали для себя участие в различных консорциумах, ассоциациях, других организациях, которые представляют интересы как конкретных заказчиков и общества в целом, так и вендоров в конкретных направлениях. В числе таких направлений — интеллектуализация сельского хозяйства, компоненты для автоэлектроники. НИИМА «Прогресс» является членом консорциума робототехники и систем интеллектуального управления, работает вместе с коллегами над созданием Национальной киберфизической платформы «Восток».

При этом важно, что у нас есть достаточно большой задел в виде спроектированных сложнофункциональных СФ-блоков. Ими

мы можем поделиться с коллегами по цеху на определённых условиях, чтобы они могли быстрее сделать свою разработку, ведь эти СФ-блоки уже реализованы буквально в кремнии. За счёт обмена готовыми протестированными СФ-блоками происходит, в частности, унификация проектов, что ведёт в итоге к снижению себестоимости и сроков общих работ.

Один пример эффективной совместной работы с партнёрами связан с навигационным приёмником, который мы сделали совместно с компанией НАВИА (он находится в реестре российского радиоэлектронного оборудования). В прошлом году исполнителям госпрограммы «ПЛАТОН», занимающимся оснащением устройств контроля перемещений большегрузного транспорта по федеральным трассам, было отгружено 600 тыс. единиц оборудования. Выпуск партии свыше полумиллиона штук — это значимое событие для российских поставщиков микроэлектроники.

Интересен также проект, связанный с высокоточным позиционированием. Он выполняется в настоящее время. У нас есть решение субсантиметровой точности, которое пока лучше всего подходит для задач геодезии. Оно уже было продемонстрировано специалистам Росреестра и главе Правительства РФ

«ДЛЯ РЕАЛИЗАЦИИ ТЕХНОЛОГИЧЕСКОГО СУВЕРЕНИТЕТА НЕТ ЧУДЕСНЫХ РЕШЕНИЙ. ЕСТЬ ПОСТОЯННАЯ РАБОТА НАД РАЗВИТИЕМ ТОГО, ЧТО УЖЕ СОЗДАНО»



Ольга ПЕСТЕРЕВА
заместитель генерального
директора по управлению
коммуникациями АО «Микрон»
(входит в ГК «Элемент», резидент
ОЭЗ «Технополис Москва»)

На волне популярности идеи технологического суверенитета сегодня много разговоров про технологические прорывы на разных «фронтах», в том числе в микроэлектронике прорывными направлениями называют переход на альтернативные технологии и архитектуры. Важно смотреть на этот переход в светлое будущее без розовых очков. Понимать, что для реализации в производстве прорывных достижений на базе новых физических принципов сначала нужна их

М. В. Мишустину. Речь идёт о том, что в нашей стране появится классный геодезический приёмник и можно будет полностью заменить весь парк точного геодезического оборудования в стране, которое сегодня полностью импортного производства. Мы готовимся и к этому рывку на нашем рынке, а также, думаю, сможем достойно конкурировать и на мировом уровне.

ГДЕ НУЖНА ДОПОЛНИТЕЛЬНАЯ ПОДДЕРЖКА ГОСУДАРСТВА

Государство сделало очень много полезного в части поддержки научно-исследовательских и опытно-конструкторских работ. Например, меры поддержки в рамках постановления Правительства РФ № 1252 от 30.10.2021, когда разработчику ЭКБ возмещается 90% затрат на её создание, — это реальная мера поддержки, потому что без неё очень тяжело «поднять» микросхему (ввиду высокой стоимости подготовки производства и самого пуска в «печь») и вывести на рынок.

А вот где хотелось бы увидеть более развитые меры поддержки, так это в части стимулирования спроса и компенсирования заказчику части средств на внедрение отечественных технологий в виде аппаратуры либо систем. Решение такого рода было принято в рамках постановления Правительства

РФ № 1619 от 27.09.2021 «Об утверждении Правил предоставления субсидий из федерального бюджета российским компаниям на финансовое обеспечение части затрат, связанных с внедрением российской продукции радиоэлектронной промышленности». Однако оно не заработало. По крайней мере, я не знаю ни одного проекта, который был бы таким образом реализован.

На мой взгляд, действенной мерой стала бы также компенсация затрат заказчиков на консалтинг, то есть на работу внешних консультантов по оценке реальных технологических процессов и предложений по автоматизации и роботизации с расчётом экономических параметров. Тогда при наборе «критической массы» таких проектов можно запускать крупную программу поддержки финансирования производств для приобретения средств роботизации, автоматизации, для запуска лизинговых схем или других бизнес-моделей. В любом случае сам владелец производства увидит реальные цифры, которые позволят ему оценить тот экономический эффект, который он получит от процесса автоматизации либо роботизации своего производства.

В целом здесь нужна активная позиция государства. Дело в том, что некоторое время назад в среде российских заказчиков произошла первая «революция» — она связана с ав-

проработка фундаментальной наукой, и есть путь от результатов лабораторных исследований до внедрения в реальное производство высокотехнологичных отраслей.

Производственная база отечественной микроэлектроники нуждается сейчас не столько в технологических прорывах, сколько в полноценном стабильном самообеспечении ключевых потребностей: материалы, оборудование, средства проектирования, современные разработки, специалисты, рынки. Решив эти вопросы, прорвемся.

При этом потенциал кремния еще далеко не исчерпан, даже в плане уже известных технологий. Например, идея чиплетов в сегодняшнем виде — по сути, просто одно из применений монокристаллических интегральных схем (на кремнии или других традиционных носителях группы АІІІВ), разработанных под совместное использование на одной подложке. На имеющейся технологической базе также можно реализовать много новых интересных решений с использованием интерпозера (дополнительной вставки, например, для объемной сборки нескольких чипов в единую микроэлектронную систему в процессе изготовления), 3D-сборки и т.д.

Заниматься надо всеми направлениями — и кремнием, и арсенидом/нитридом галлия, и кремний-германием и т.д. Какую из полупроводниковых технологий применить в конкретном случае, зависит от конкретной цели и стратегии, характеристик изделия и масштабов спроса — ищем материал с нужными свойствами и оцениваем целесообразность применения.

Что касается альтернативных ИТ-архитектур, то технологически наше производство позволяет поддерживать их электронной компонентной базой, и более того, использование родной компонентной базы является ключевым условием безопасности (данных, систем жизнеобеспечения, промышленной инфраструктуры) — потому что программные меры защиты не спасают в случае аппаратной уязвимости. По сути, технологический суверенитет здесь равен степени локализации критической инфраструктуры — как в старых, так и в новых архитектурах база безопасности закладывается на уровне чипа.

Общеплановый дефицит «железа» из-за коллапса глобальной логистики и старой структуры цепочек поставок компонентов уже постепенно уходит, но растет не-

томатизацией хозяйственного учёта и других базовых функций автоматизации бизнес-процессов. Те, кто сделал это первыми, в числе первых вышли на новый уровень эффективности своего бизнеса. Следующий такой вызов будет связан с автоматизацией механического труда. И там будет достигнут подобный эффект в повышении эффективности производства. Думаю, что государству пора подумать о запуске национального верхнеуровневого проекта роботизации, в котором будут разделы, призванные обучать корпоративных потребителей тому, что роботизация и автоматизация — это не роскошь, а нормальный путь развития, который приносит предприятию дополнительные блага и выгоду.

Речь идёт о массовой роботизации/автоматизации производственных предприятий, не только самых крупных, но и среднего уровня, которые даже базовой автоматизацией, может быть, особо и не занимались. А значит, предприятиям нужно предложить унифицированные решения для определённых технологических процессов: для автомобильных конвейеров, для вагоноремонтных депо и т.д. Сейчас такую просветительскую работу с отраслями, в частности, РЖД ведут консорциумы производителей техники и интеграторов. Но их силы ограничены. А для того, чтобы эти интеграторы смогли пойти во все условные

вагоноремонтные цеха страны, нужна поддерживающая государственная программа.

И ещё один важный момент: независимо от того, о какой инновационной организации мы говорим — НИИ или дизайн-центре — ощущается острый дефицит профессиональных продакт-менеджеров — тех людей, которые умеют общаться с заказчиками и понимать, как их чаяния можно заложить в создаваемое техническое решение. Таких специалистов — «переводчиков» требований заказчиков и рынка на язык заданий инженеру — нужно готовить на системном уровне, думаю, ещё со студенческой скамьи. К сожалению, сегодняшняя высшая школа не готовит конструкторов-технологов радиоэлектронной аппаратуры уровня СССР с соответствующим широким кругозором. И это остро ощущается сегодня. Не вижу ничего плохого в том, чтобы вернуть советские стандарты обучения технологов РЭА: они сегодня весьма актуальны.

И ещё стоит добавить высшей школе задачу подготовку специалистов, которые умеют управлять высокотехнологичными проектами. Российской электронной отрасли, которая «встаёт на крыло», остро нужны классические руководители проектов, имеющие наряду с познаниями в управлении также большой технологический кругозор.

стабильность и фрагментарность поставок, ужесточается внешняя сегментация и регуляторика.

Замена одного импорта на другой наши проблемы точно не решит. Поэтому нужны стимулирование и разработка нестандартных инженерных решений, а параллельно усиление имеющихся компетенций и создание базы для таких идей и решений. В софте эта база в достаточном количестве есть, и мы видим лучшую систему электронного правительства в мире. В матчасти позиции существенно слабей — предстоит восстанавливать инженерную школу, набирать опыт и силы, растить таланты. Русская инженерная школа — это высокая техническая культура, на базе которой формировался глобальный контур и технооптимизм современной экономики. Сегодня именно инженерная школа определяет скорость материализации идей по прорывным направлениям.

Вырастет новое поколение талантливых инженеров — вырулим, а без инженеров вариантов нет. Поэтому каждый, кто заинтересован, уже предпринимает усилия. И у нас тоже есть профориентационный проект «Путь Инженера», и начали в январе специальные экскурсии «Ключ к профессии», где реальные инженеры «Микрона»

показывают, в чем состоит их работа, помогают осознанно найти себя в профессии.

Все понимаем, что надеяться можно только на себя. Не будет простых решений и магических формул по стимулированию отрасли. Нужно шаг за шагом восстанавливать престиж профессии инженера, производственную базу хайтек-отрасли, восстанавливать всю экосистему микроэлектроники, как минимум, для применения в критической инфраструктуре (КИС) и чувствительных отраслях.

И это не вопрос цены: нужное изделие либо есть, либо его нет. А параллельно с этим (ни в коем случае не последовательно) нужно формировать рынки для продукции (благо, успешные примеры есть: связь, транспорт, идентификация личности и объектов, ТЭК, финтех и т.д.).

Чудес ожидать не стоит, их не будет. Есть проверенные работающие подходы к созданию и освоению новой техники. На их базе проще, быстрее и надежнее всего строятся при желании и новые системы, с применением искусственного интеллекта, нефоннеймановских архитектур и любых других технологий. И, конечно же, нужно параллельно так же упорно работать над прорывами, каждый из которых увеличивает общий шанс.

КАК «СРЕДНЕМУ КЛАССУ» ПРОМЫШЛЕННОСТИ С НИЗКИМ УРОВНЕМ ЦИФРОВОЙ ЗРЕЛОСТИ МАССОВО ПОДКЛЮЧИТЬСЯ К ЦИФРОВОЙ ТРАНСФОРМАЦИИ?



Сергей ИВАЩЕНКО
руководитель
направления маркетинга
и коммерческого
развития компании
UMNO digital

Наша компания фокусируется на сегменте предприятий промышленности с низким или вообще нулевым уровнем цифровой зрелости. Это огромный рынок потенциальных заказчиков проектов цифровой трансформации, для которого особенно остро стоят вопросы выбора подходящих решений цифровизации и процессов их внедрения. Можно сказать, что это массовый сегмент производственных предприятий среднего и небольшого масштаба, и для них критически важно преодолеть барьер больших капитальных вложений, который не позволяет запустить процессы полноценной цифровой трансформации.

Этот сегмент охватывает все отрасли российской промышленности, внутри каждой есть крупные компании — лидеры цифровизации и большой слой не менее развитых предприятий с точки зрения внедрения инновационных технологий. Например, в железнодорожной отрасли (это одно из ключевых направлений для UMNO digital) компании, которые занимаются локомотивами, демонстрируют высокий уровень цифровой зрелости, а те, что занимаются эксплуатацией грузовых вагонов, гораздо менее развиты в этом плане. В конечном итоге всё зависит от экономических параметров того объекта, для управления которым применяются меры модернизации: высокомаржинальному бизнесу легче выделить средства на цифровую трансформацию.

Кроме того, промышленность — это консервативные рынки по отношению к внедрению инновационных систем. Именно таков, например, железнодорожный рынок, что объясняется высокими требованиями транспортной безопасности. Жёсткие требования там буквально «написаны кровью», что обуславливает максимально осторожное применение инновационных подходов даже для решения понятных проблем.

Какие подходы к реализации проектов работают на практике в этом сегменте рынка? И каким образом они способны поддержать массовый охват предприятий промышленности на пути технологической модернизации и цифровой трансформации?

РЕЗУЛЬТАТИВНАЯ ПОЭТАПНАЯ ЦИФРОВИЗАЦИЯ

Надо сказать, что многие отечественные вендоры, понимая наличие экономического барьера для входа в проекты цифровой трансформации, предлагают рынку готовые недорогие решения, которыми могут воспользоваться предприятия различного масштаба. Чтобы отвечать потребности в осторожной модернизации, для предприятия можно выстроить план поэтапной цифровизации, где на каждом этапе выбираются проекты, дающие отличные эффекты в короткие сроки. Это вполне решаемая задача, поскольку старт практически с нулевого уровня даёт хороший эффект в практически любых вариантах цифровой трансформации. Например, внедрение базовой системы MES, которая сразу открывает возможность контроля цифрового следа на всех производственных этапах предприятия.

Можно сказать, что предприятию доступно множество тех самых «низко висящих плодов», то есть участков, где значительные эффекты получают с помощью достаточно простых внедрений. Яркий пример — программные роботы (RPA), которые автоматизируют некоторые постоянные действия, прежде выполняемые людьми. RPA — это

как раз ИТ-продукты для компании с низким уровнем цифровой зрелости: хороший, относительно недорогой способ первичной цифровизации и автоматизации рутинных процессов. Например, робот отлично справится с созданием транспортных накладных: эта программа сама собирает из разных источников нужные данные, формирует документ и отправляет его дальше.

Конечно, нужен системный подход к планированию этапов, и начать следует с инвентаризации текущих процессов. Это ещё не собственно цифровая трансформация, а подготовительный, но важный этап — сбор информации о том, как именно работает предприятие. Результат этой инвентаризации — реестр (карта) процессов, причём описанных в формализованном и унифицированном виде. Подготовка такой карты требует затрат времени и ресурсов, даже несмотря на то что соответствующие методики хорошо изучены и апробированы (поэтому, кстати, составление карты процессов вполне можно отдать на аутсорсинг внешней компании). Но, как говорится, овчинка стоит выделки — появляется возможность формировать цифровой след всех процессов: соответствующие данные в стандартизированном виде накапливаются в информационной системе предприятия, и их можно анализировать по различным разрезам. Например, оценить потенциальную выгоду от цифровизации тех или иных процессов, а также понять, от каких процессов вообще можно избавиться. Здесь важна именно привязка к реальным процессам, которые работают на конкретном предприятии, ведь даже один вид производства на разных заводах может быть по-разному реализован.

Есть методологический вопрос, который часто задают предприятия: какой вектор цифровизации выбрать? Двигаться ли снизу вверх по уровням предприятия, начав с базовой автоматизации? Или сверху вниз, то есть взяв за точку старта задачи повышения эффективности бизнес-процессов? Ответ зависит от того, какие производственные процессы сложно контролировать без цифры. Например, если на масштабном производстве менеджмент принимает решения, основываясь на данных, которые в устном виде докладывают начальники цехов или приносят менеджеры производственных процессов в виде отчётов, составленных вручную, значит, нужно начинать с нижнего уровня базовой автоматизации. Тогда за счёт формирования цифрового следа производ-

ства руководство получит прозрачную систему данных и управления предприятием на высшем уровне. Это ведь совершенно разные вселенные: данные, записанные вручную в некоторые журналы, и автоматически сформированные отчёты, в которых датчики зафиксировали сведения о том, сколько производственных операций было совершено, кто из мастеров выходил на смену, как именно были произведены эти операции, и никто в эти данные не вносил никаких изменений вручную. Это принципиально разный уровень доверия к отчётам и принятия решений по этим отчётам.

Но если у предприятия нет сложных производственных циклов с множеством бумажных журналов и длительного ручного процесса формирования статистики, зато есть сложный документооборот, большое количество контрагентов, с которыми тяжело налаживаются коммуникации, а коммерческий отдел долго формирует коммерческие предложения, ищет клиентов и контрагентов, то тогда точно можно начинать цифровую трансформацию с верхнего уровня.

СОЗДАНИЕ ЦИФРОВОГО ДВОЙНИКА ПРОИЗВОДСТВА

Цифровой двойник производства — это элемент цифровизации, который нередко считается принадлежностью исключительно очень крупных производственных компаний с высоким уровнем цифровой зрелости, таких как «Газпром», ОДК, «СИБУР», «КАМАЗ», «Северсталь». Скорее всего, это заблуждение бытует потому, что известные примеры внедрения технологии цифровых двойников производства, о которых сообщают СМИ, связаны именно с такими производственными предприятиями. На самом деле цифровые двойники полезны предприятию любого масштаба. Более того, я уверен, что на горизонте 15 лет все успешно работающие производственные предприятия будут использовать цифровых двойников, а остальные уйдут со сцены. Просто потому, что станут неконкурентоспособны. Один из важнейших результатов цифровизации — это возможность не только в долгосрочной, но и среднесрочной и краткосрочной перспективе вести планирование производства на основе математики в компьютере, а не субъективного опыта конкретных сотрудников предприятия.

Вопрос заключается только в том, чтобы правильно применять этот мощный подход, сообразуясь с масштабом бизнеса и задач того или иного предприятия (рис. 1). Иногда циф-

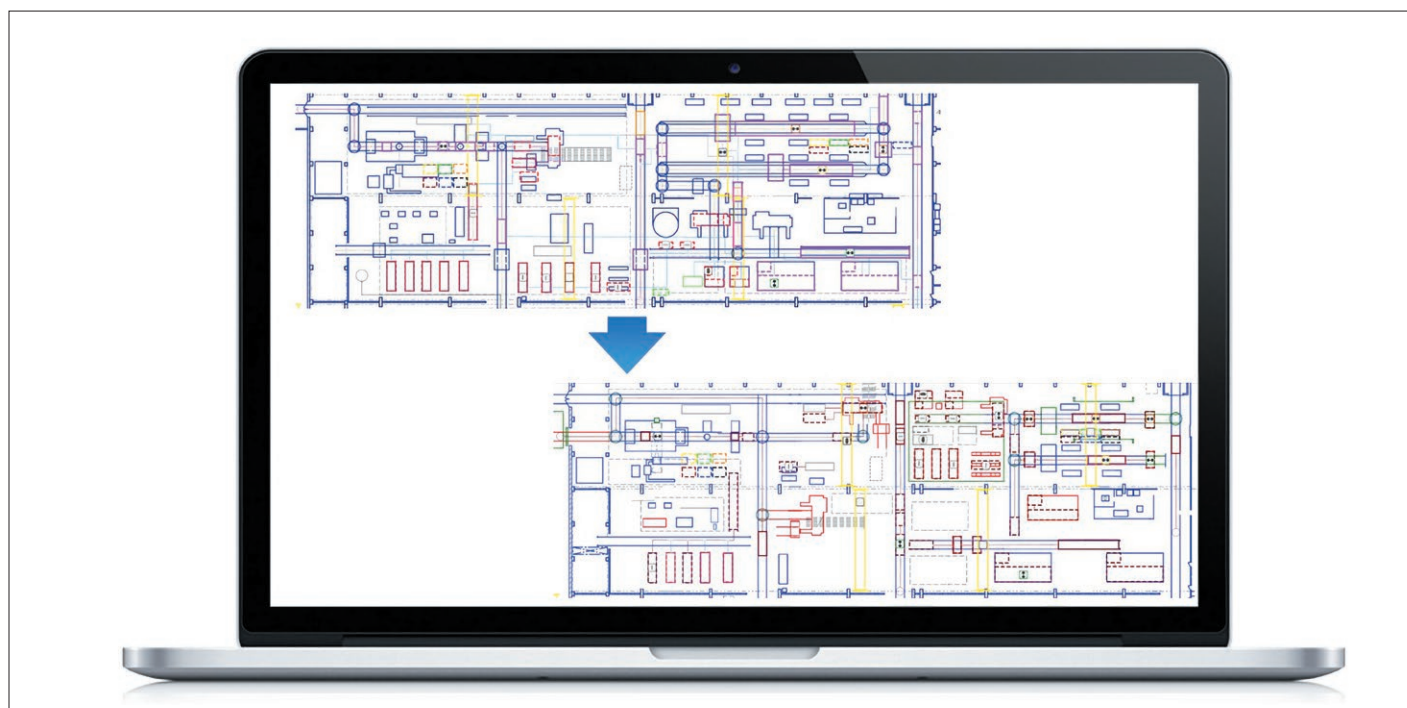


Рисунок 1. Цифровой двойник вагоноремонтного предприятия. Источник: UMNO digital

ровой двойник может даже не участвовать в самом производстве, но он нужен на стадии его запуска.

Хороший пример — цифровой двойник вертикальных элеваторов. По сути, это вертикальный конвейер, который поднимает зерно наверх и загружает его в элеватор. Вроде бы достаточно простой процесс, но в нём есть много параметров, которые помогут его настроить оптимально. Сколько нужно засыпать зерна в ковш на этом вертикальном конвейере, чтобы получить эффективные показатели на входе и выходе конвейера? То есть чтобы зерно доставлялось максимально быстро, с максимальной загрузкой и при этом с наименьшими потерями. Цифровой двойник используется в самом начале проекта для моделирования производственного процесса: анализируется несколько вариантов, выбирается оптимальный, и после этого начинается физическое строительство вертикального элеватора.

Практически любой производственный процесс можно имитировать в ПО цифрового двойника, и в каждом случае есть что оптимизировать. Например, у нас есть практически типовое решение для создания цифровых двойников вагоноремонтных депо. Оно включает имитационное моделирование процессов ремонта колёсных пар, подшипников, автосцепки, складских процессов. Данный цифровой двойник реализован в виде конструктора, который состоит из раз-

ных элементов. Есть соответствующий конструктор для предприятий железнодорожной логистики.

Важно, что по некоторым производственным процессам можно создать типизированное решение. Ведь создание цифрового двойника с нуля — это непростое занятие, которое требует глубокой сложнейшей экспертизы с множеством нюансов. В зависимости от размера предприятия это может занять от трёх месяцев до года. И это при том, что вы будете использовать развитый инструмент имитационного моделирования типа популярного ПО AnyLogic. Этот зарубежный поставщик не ушёл с нашего рынка, но вопрос его импортозамещения, конечно, актуален.

Достоинные отечественные альтернативы есть, и мы уже приступили к миграции своих решений на новую платформу. Это не быстрый процесс. Мы будем поддерживать две платформы моделирования параллельно до тех пор, пока не убедимся на 100 %, что получили качественное решение задач клиента на альтернативной платформе.

Наличие типизированных отраслевых решений цифровых двойников — это, на мой взгляд, один из ключевых элементов массовой модернизации и цифровой трансформации предприятий из реальных отраслей экономики. Масштабу этой задачи соответствует прогноз — 15 лет для полного охвата всех производств среднего и небольшого масштаба. Причём это время потребуется не для

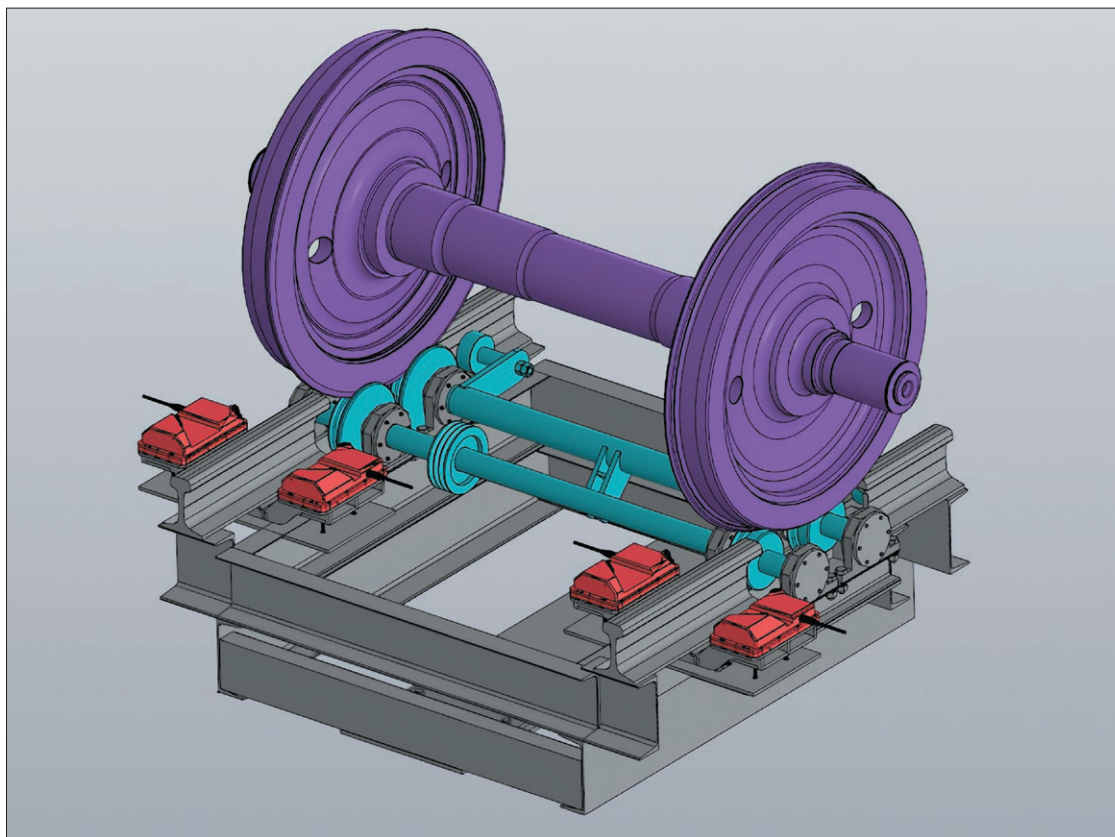


Рисунок 2. Лазерные измерения колёсной пары. Источник: UMNO digital

разработки совершенно новых программных решений, а для их массового внедрения. Нужно ведь, чтобы на каждом предприятии появилось 1–2 специалиста, которые умеют моделировать производственные процессы. Возможно, будут налажены механизмы аутстаффинга или аутсорсинга таких работ. Со временем оформятся наилучшие формы организации таких площадок и услуг моделирования производственных процессов. Это движение станет большим шагом вперёд в целом для всей промышленности России. Потому что цифровой двойник — это полные (нефрагментированные) достоверные данные о производстве. Обработка этих данных выводит предприятие на принципиально новый уровень эффективности или управляемости.

НОВЫЕ ВОЗМОЖНОСТИ УПРАВЛЕНИЯ ПРОИЗВОДСТВОМ НА ОСНОВЕ ДАННЫХ

Многочисленные вагоноремонтные депо, работающие на территории нашей страны, — это те самые предприятия с весьма низким уровнем цифровой зрелости. Им адресован продукт «Умное депо», который предназначен для эффективного старта в направлении цифровой трансформации. Это нишевое решение, сильно адаптированное под специ-

фику именно вагоноремонтных предприятий, класса MES. В системе используются магнитные RFID-метки, которые помогают формировать карту всех производственных процессов предприятия: отслеживают движение всех деталей и формируют цифровой след на уровне каждой детали, который интегрируется с учётной системой предприятия и всеми видами используемых электронных журналов. Вся система построена на базе мобильных приложений пользователей с RFID-считывателем, что позволяет сразу после внедрения ввести цифровой порядок на вагоноремонтном предприятии.

Для специальных измерений, например, итоговых размеров колёсной пары можно использовать разнообразные приборы, которые имеются на нашем рынке. Они легко встраиваются в продукт «Умное депо» (рис. 2).

Адаптация к специфике предприятий данного профиля подразумевает, в числе прочего, что в системе изначально заложены описания процессов, происходящих на всех станках, на всех постах, то есть под каждый процесс создан свой поток рабочих задач и задан порядок работы. Это помогает мастерам вагоноремонтных предприятий без специального дополнительного обучения перейти на механизмы цифрового контроля

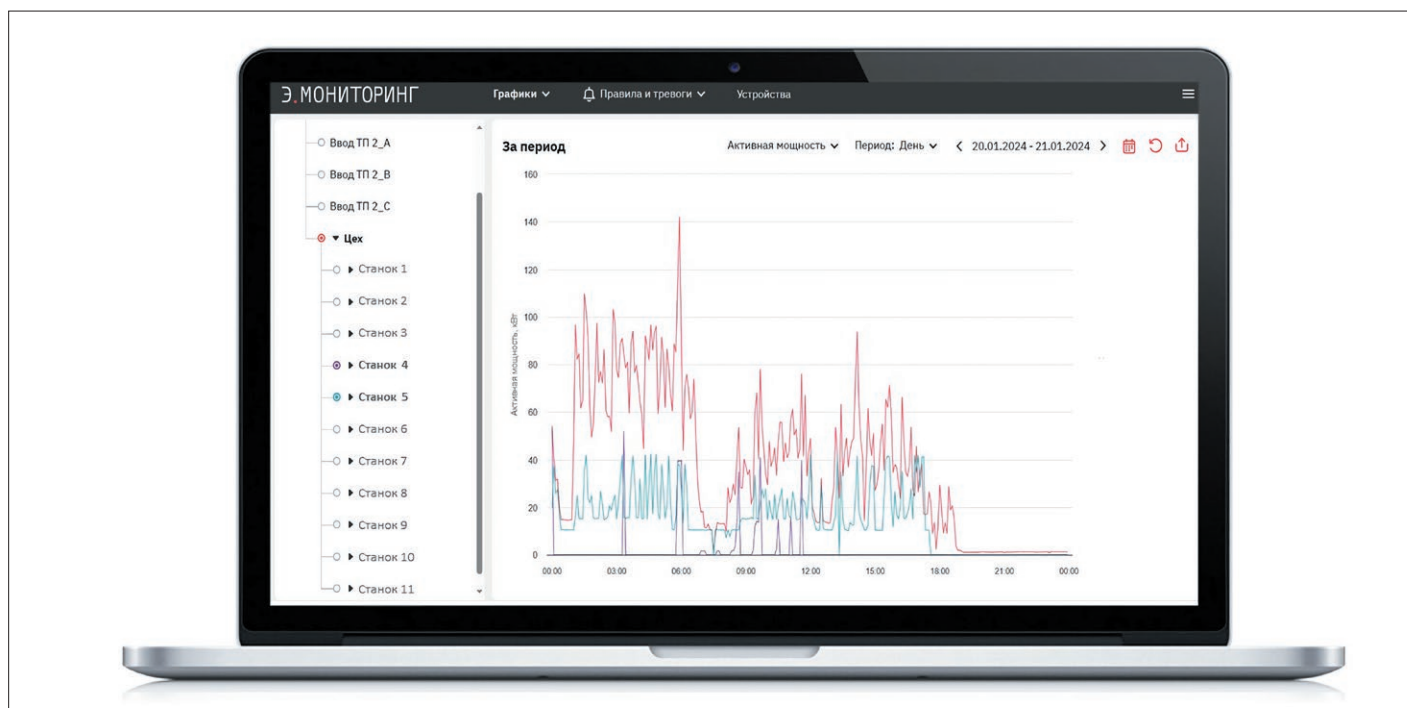


Рисунок 3. Визуализация данных по потреблению электрической мощности каждой единицей оборудования. Источник: UMNO digital

всех производственных процессов. Это именно так. Бумажные журналы полностью уходят в прошлое: нужные данные автоматически поступают в мобильный считыватель сотрудника на каждом посту, затем уходят в учётную систему и сохраняются для дальнейшей аналитической обработки или формирования отчётов.

Цифровой след процессов в данном случае очень важен: данные уходят в цифру с фамилией конкретного мастера, который держал в руках данный считыватель и ввёл данные в систему. В результате ликвидируется большое количество нарушений, связанных с ошибками человека. По статистике наших проектов, разница в сведениях по состоянию склада между учётной системой и реальностью после внедрения продукта может достигать примерно 30 %.

Для мобильных сотрудников депо предназначается продукт «Осмотр вагонов». Это тоже мобильное приложение, которое позволяет фиксировать состояние вагонов с помощью фотографирования нужных элементов и передавать данные в корпоративную информационную систему в форме детальных чек-листов. В этом приложении работают различные наукоёмкие функциональные модули типа компьютерного зрения для автоматического распознавания номеров и т.д.

Ещё одно ИТ-решение — энергомониторинг — имеет более универсальный кросс-от-

раслевой характер. Речь идёт о применении технологии промышленного интернета вещей (Industrial IoT): с помощью индукционных датчиков осуществляется сбор данных по напряжению в сети на каждой единице оборудования (с дискретностью 30 секунд) и формирование карты энергопотребления предприятия. Это приложение помогает быстро собрать цифровой след с данными о том, когда работают или не работают реальные станки и под какой нагрузкой. Эти данные важны для менеджмента предприятия. Во-первых, видно, в какое время включались станки, и это повод задуматься над трудовой дисциплиной. Во-вторых, карта показывает временные точки пиковой нагрузки. А она нередко поддаётся регулированию, а значит, можно пользоваться льготными тарифами, которые устанавливают поставщики электроэнергии. У главных энергетиков и менеджеров здесь открывается обширное поле для оптимизации бюджета предприятия (рис. 3).

РИСКИ ПРОЕКТОВ ЦИФРОВИЗАЦИИ ДЛЯ ПРЕДПРИЯТИЙ С НИЗКОЙ ЦИФРОВОЙ ЗРЕЛОСТЬЮ

Инновации для промышленности связаны с различными рисками. Часть из них, например риски промышленной безопасности, зависят от специфики внедряемых технических

решений. Но есть и общие, обуславливаемые в первую очередь тем самым низким уровнем исходной цифровизации.

- ♦ Риски управления инновационными процессами. Процессы, связанные с повышением уровня цифровой зрелости, как правило, на консервативных производствах меняют привычные технические процессы, которые складывались порой десятилетиями. Это иногда приводит к внутреннему саботажу, потому что люди не хотят обучаться новым приёмам работы. Для нивелирования этого риска важна поддержка менеджмента компании. Ведь, даже если собственник предприятия заинтересован в цифровой трансформации, прохладное отношение менеджмента может погубить проект.

- ♦ Неэффективное бесполезное внедрение. Вполне реальный риск связан с тем, что в результате цифровизации работы у сотрудников не убавится, а, наоборот, станет больше. Например, на заводе внедрили умного операционного помощника. Но для того чтобы он заработал, мастер смены должен прийти на работу на полчаса пораньше и до начала смены успеть внести в ПО помощника множество дополнительных параметров.

- ♦ Внедрение незрелого решения, которое, скорее всего, потребует постоянной поддержки и доработки на стороне вендора.

- ♦ Зависимость различных этапов производственного цикла от нового решения. Плохо, когда новое решение формирует слабо управляемую зависимость от него различных процессов, возможно, на других этапах или участках производства, но при этом становится обязательным для применения. Выйти из этой проблемной зоны можно только через ряд доработок, кастомных интеграций, приобретения дополнительного ПО и т.д. Риски такого рода снимаются с помощью создания карты производственных процессов. Обычно они имеют вид наглядных блок-схем, что позволяет самому предприятию даже без участия внешних аналитиков изучить дополнительные зависимости процессов и оценить степень их критичности.

КАК «ВЫЛЕЧИТЬ» БОЯЗНЬ ИЗМЕНЕНИЙ?

«Боязнь изменений» — это «болезнь», которой подвержены, пожалуй, все промышленные предприятия, за исключением самых крупных, которых уважительно называют отечественными лидерами цифровизации. В этом вопросе «пациентам» нужна помощь. Но какая?

Государство сегодня занимается вопросами стимулирования инновационных проектов на разных рынках. Предлагает финансовую помощь. А также поддерживает деятельность различных тематических консорциумов, где разработчики технологий и продуктов совместно с заказчиками думают над внедрением инновационных решений в различных отраслях. Вот только в этих консорциумах поставщики технологий встречаются с теми самыми крупными компаниями, чьи успехи в цифровизации составляют гордость страны. Там нет «среднего класса» промышленности с низким уровнем цифровой зрелости. Как можно помочь им вступить в русло цифрового развития?

Дело здесь не в необходимости дополнительного обучения. Корень проблем — в лёгкости имплементации ИТ-решений. Для массового результата необходимо несколько модифицировать текущую структуру взаимоотношений вендоров, государства и заказчиков — промышленных предприятий среднего уровня. Конечно, отечественный вендор, как и любой поставщик, заинтересован в продажах именно своих продуктов. Но заказчикам из рассматриваемой категории нужна более тесная связка продуктов различных поставщиков, потому что им для стартового рывка требуется некоторый комплекс решений, а кастомные доработки вендора всегда стоят достаточно дорого.

И простой финансовой поддержки задуманных проектов со стороны государства недостаточно. Велика вероятность того, что предприятие выделенные деньги неправильно израсходует, совершит ошибки в силу не очень высокой цифровой зрелости. Здесь правильнее будет компенсация затрат постфактум в случае успешного выполнения проекта.

Дело в том, что в сценарии с предварительным финансированием необходимо тегоретически доказывать работоспособность предлагаемой идеи, как собственному менеджменту, так и некоторому абстрактному арбитру, воплощающему государство. Для не самого крупного завода это становится непосильной задачей. Важно сделать менеджмент союзником. А это возможно в модели, когда поощрение наступает после удачного завершения внедрения. Тогда первая удача придаст менеджменту больше уверенности в способности предприятия успешно выполнять проекты, нацеленные на повышение эффективности его деятельности, а каждая следующая подтверждённая победа будет снижать проявления болезни «боязнь перемен к лучшему».

«ГОНКА В ЛАБИРИНТЕ: МЫ НЕ ВСЕГДА ВИДИМ, КАК И КУДА БЕЖИТ НАШ СОПЕРНИК»



Иван ЧЕРНОВ
менеджер по развитию
UserGate

Глобальная цель российской отрасли информационных технологий – обеспечение технологического суверенитета страны. Основные задачи, направленные на достижение этой цели, – технологическая модернизация и цифровая трансформация – в последние два года непосредственно связаны ещё с одной – импортозамещением технологий. Сложность этой задачи определяется не только необходимостью поиска альтернативных продуктов и необходимыми для её решения затратами. Отсутствует (и едва ли возможно вообще) единство методологий при определении подходов к импортозамещению.

Это ярко видно на примере государственных и частных компаний. Так, государство особенно внимательно относится к решению двух задач, связанных с ИБ: обеспечение нормальной работы госаппарата, учреждений и компаний с государственным участием и сохранность персональных данных. По большому счёту, регулятору не так важно, как именно вы защищаете свой бизнес. Важнее, как вы защищаете имеющиеся у вас в распоряжении персональные данные. Обе эти сферы не совсем полно охватывают тот рынок, который стимулирует развитие технологий.

А частный бизнес живёт в несколько иной реальности. У некоторых компаний сохрани-

лись возможности приобретать иностранные решения, пусть даже окольными путями. И они готовы нести известные риски, с этим связанные. И если они готовы ввозить иностранные решения через третьи страны, то они могут делать это: стимулирование развития и обеспечение технологического суверенитета не вступают с этим в противоречие. Более того, та ситуация, которая сложилась сейчас, как раз конкуренцию стимулирует! А значит, способствует накоплению компетенций, развитию продуктов и повышению уровня российской ИБ-индустрии в целом.

«ДОГНАТЬ И ПЕРЕГНАТЬ»

Задача посоревноваться с западными технологиями в области информационной безопасности интересна и амбициозна. Но будем объективны: ландшафт российских ИТ отличается от мирового. Поэтому простое копирование иностранных технологий вообще не имеет практического смысла: мы не можем надеяться, что они будут работать у нас так же, как работают у них. Такое было только в 90-х – нулевых годах, когда российский ИТ-сегмент развивался как полностью открытый рынок: мы использовали иностранные сервера и программные продукты от мировых гигантов. В таких условиях метод копирования был вполне приемлемым и эффективным, так как мы защищали ИТ-ландшафт, который мало чем отличался от того, который формировался на Западе.

При этом задача «догнать и перегнать» сохраняет свою актуальность. Но не с точки зрения импортозамещения, а потому, что иностранные вендоры продолжают развивать свои продукты, и нам необходимо соответствовать мировому уровню. В первую очередь по уровню развития собственной экспертности, которая позволяет разрабатывать качественные продук-

ты. Нельзя сказать, что в этой гонке мы отстаём от западных вендоров или, наоборот, выигрываем у них. Это гонка в лабиринте, и мы не всегда видим, как и куда бежит наш соперник.

Так что российские альтернативы — это не копии, а всегда новый оригинал. И с грустью говорить о том, что у нас нет решений, являющихся полными аналогами иностранных, по меньшей мере некорректно. Практически всегда для замены одного решения другим приходится создавать новые сочетания, осуществлять перенастройку систем, то есть в той или иной мере менять архитектуру корпоративных ИТ.

При этом специфика текущего момента не требует от нас отказываться от тех технологий, которые мы использовали ранее, и от тех компетенций, которые мы приобрели ранее благодаря нашим иностранным коллегам. Но эта специфика диктует необходимость изменений в правилах поведения на рынке и концепции дальнейшего развития бизнеса. Речь идёт о необходимости обеспечения технологической независимости.

Неприемлема ситуация, в которой средства защиты можно отключить рубильником, который расположен где-то за океаном. Управлять им мы должны самостоятельно, а значит, нам нужна собственная защита. И импортозамещение в области информационной безопасности должно быть тотальным. Это в сельском хозяйстве можно отказаться от выращивания своих бананов и заменить их собственными яблоками. А вот в области ИБ такой подход уже не работает.

Технологическая независимость для ИБ-вендора означает выбор собственного, оригинального пути развития, формирование собственного стека решений. Например, наше решение Next-Generation Firewall (NGFW) — это универсальное многофункциональное решение, ядро системы безопасности, которые мы предлагаем рынку как продукт, позволяющий осуществить эффективное импортозамещение средств безопасности. Это принципиально новая разработка. Например, с помощью NGFW можно обеспечить безопасность удалённого подключения сотрудников или защитить сеть предприятия от внешних атак.

АМБИЦИИ И МИГРАЦИИ

Что касается разработки высокотехнологичных продуктов, то, по большому счёту, реализация технологической независимости

больше связана с реализацией амбиций, чем с экономической выгодой. Например, когда мы решили заняться разработкой собственного решения NGFW, это противоречило всей логике здравого смысла: разработка сложна, длительна, рынок может предложить аналогичные решения, а экономическая эффективность проекта совсем не очевидна. Тут возобладали амбиции компании — развивать собственные технологии, демонстрировать рынку свои уникальные компетенции. Но в момент глобального исхода иностранцев из России амбиции превратились в крайне востребованный продукт, который имеет хорошие перспективы, позволяет развивать технологии дальше и уже начал давать экономическую отдачу.

Как говорил классик, «безумству храбрых поём мы песню!», ведь у нас не было времени на разработку методологии импортозамещения, выстраивать эти процессы приходится буквально на ходу. В самом выгодном положении в такой ситуации оказались компании, которые успели внедрить у себя риск-ориентированное управление бизнесом. Они могли, даже используя западные технологии, выстраивать защитные контуры, работающие на импортозамещаемых технологиях.

Я уверен, что единственная методология, которая позволяет с минимумом проблем пройти через импортозамещение, — это риск-менеджмент, он гармонизирует амбиции с вызовами реального мира. Тогда удастся в спокойном режиме решить самую главную задачу — обеспечить бесперебойное функционирование существующих бизнес- и технологических процессов. А после этого приступить к планомерному созданию обновлённой системы защиты своих информационных ресурсов и выстраивать перечень приоритетных работ, исходя не из возможности реализовать ту или иную идею, а из бизнес-необходимости. Такой аудит ИТ очень полезен: чаще всего анализ показывает, что замена «один в один» и не нужна, ведь в итоге бизнесу важно эффективное решение собственных задач, включая модернизацию и цифровую трансформацию производственных активов и процессов, чем внедрение некоторого цифрового решения. И вот тут крайне полезной будет консультационная поддержка тех или иных центров компетенций — с целью выбора лучшей практики для реализации нужной бизнес-функциональности на новых импортозамещаемых продуктах или технологиях.



Kaspersky Unified Monitoring and Analysis Platform

Центральный элемент единой платформы безопасности

- Мониторинг и анализ инцидентов ИБ
- Поточковая корреляция в режиме реального времени
- Автоматическое обогащение данными об угрозах
- Масштабируемая архитектура и низкие системные требования
- Тесная интеграция с решениями «Лаборатории Касперского» и сторонних производителей
- Обеспечение соответствия законодательству в сфере безопасности объектов КИИ

kaspersky АКТИВИРУЙ
БУДУЩЕЕ

kaspersky.ru/enterprise

ДиалОгНаука

СИСТЕМНАЯ ИНТЕГРАЦИЯ В ОБЛАСТИ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

dialognauka.ru

«АКТУАЛЬНЫЕ ВОПРОСЫ ЗАЩИТЫ ИНФОРМАЦИИ»

ПО МАТЕРИАЛАМ КОНФЕРЕНЦИИ ФСТЭК РОССИИ

Анна КАТАНКИНА
корреспондент BIS Journal

В феврале в рамках международного форума «Технологии и Безопасность» прошла конференция ФСТЭК России «Актуальные вопросы защиты информации», на которой были рассмотрены вопросы технической защиты информации, создания средств защиты, безопасной разработки ПО, совершенствования сертификационных испытаний СЗИ, совершенствования требований по безопасности к информации, предъявляемой к СЗИ. С докладами выступили руководители подразделений ФСТЭК России.

ОСНОВНЫЕ НАПРАВЛЕНИЯ

Основные направления совершенствования технической защиты информации представил Виталий Лютиков, заместитель директора ФСТЭК России. Он сосредоточился на технических и технологических вопросах, находящихся в компетенции ФСТЭК, а также на нормативно-правовом регулировании.

Первое направление. Первое направление, по которому идет активная работа, — защита информационной инфраструктуры органов государственной власти (ОГВ). Основная нормативно-правовая база для этого — Приказ ФСТЭК от 11.02.2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и несколько дополнительных требований, в т.ч. по защите информации конфиденциального характера, КИИ, персональных данных и т.д. При этом требований по защите информационной инфраструктуры в целом не установлено, а есть отдельные упоминания о необходимости учета и моделирования угроз. Фактически информационно-телекоммуникационные сети, локально-вычислительные сети и рабочие места, в первую очередь, в государственных организациях, требованиями не охвачены, отметил замглавы ФСТЭК.

Последнее два года ярко показали, что большинство инцидентов, в т.ч. в ОГВ, были связаны с двумя векторами воздействия:

- ♦ на информационно-телекоммуникационную инфраструктуру через интерфейсы администратора или

привилегированных пользователей. Именно на эту инфраструктурную часть требования формально не установлены. При этом у ФСТЭК нет информации, что первоначальный доступ был произведен через интерфейсы ГИС;

- ♦ подрядчики и подрядные организации, т.е. организации, которые взаимодействуют с информационными системами для разработки и технического сопровождения услуг по защите информации. Это излюбленный вектор атак злоумышленников, отметил докладчик. Существующие требования по безопасности на подрядные организации напрямую не распространяются, тут нет механизмов проверок и контроля.

Для исправления ситуации, по поручению оперативного совещания Совета Безопасности России, ФСТЭК России подготовила законопроект, в котором предложил рассматривать как объект защиты не информационную систему, а информацию как таковую, привязав её к владельцу. Законодательная инициатива пока не получила поддержки и развития.

ФСТЭК России подготовила первую редакцию новых требований по защите информации, содержащейся в ГИС, документ проходит внутриведомственное согласование. В требованиях затронуты вопросы защиты информации, являющейся государственным ресурсом, и в иных системах ОГВ, включая подрядные организации. Но если работа над законопроектом не будет продолжена, то нормы ответственности подрядчиков и контроля за подрядными организациями останутся на бумаге.

О новых полномочиях ФСТЭК. В соответствии с Указом Президента РФ № 846 ФСТЭК получила новые полномочия, направленные на совершенствование организации и управления защиты информации и безопасности объектов КИИ. Это мониторинг текущего состояния технической защиты информации и обеспечения безопасности значимых объектов (ЗО) КИИ, организация и проведение оценки эффективности деятельности ФОИВов по технической защите информации и обеспечению безопасности ЗО КИИ.

До 1 июля 2024 г. ФСТЭК поручено разработать требования о защите информации, содержащейся в государственных и иных информационных системах, владельцами которых являются ОГВ, субъекты РФ и муниципальные образования.

Два показателя. Служба планирует переход к единой шкале оценки состояния и измерения эффективности деятельности и в ближайшее время предлагает вве-

сти два показателя для реализации полномочий ФСТЭК для всех ОГВ и организаций, находящихся в сфере регулирования:

- ♦ показатель (и методика его определения) состояния защиты информации и обеспечения безопасности объектов КИИ в ОГВ и организациях, которые базируются на достижении некоего минимального уровня защиты информации. О методике подробно рассказано ниже;
- ♦ показатель (и методика его определения) зрелости деятельности ОГВ и организаций по защите информации и обеспечению безопасности объектов КИИ.

Повышенное внимание и недостаточное внимание... Выявление и оценка угроз, борьба с уязвимостями и т.д. — следующий аспект, на который обратил внимание докладчик. Тут он затронул два момента — повышенное внимание к оценке угроз на этапе создания системы и недостаточное внимание текущим угрозам и уязвимостям.

В бумажном варианте модели угроз на этапе разработки и аттестации системы доходят по толщине до 15 см. Однако спустя непродолжительное время этот документ никто не может найти. У такого подхода есть очевидные «плюсы» и «минусы». Модели угроз позволяют определиться с нарушителями и основными векторами атак, но в процессе эксплуатации управлять этим документом и бюрократической системой вокруг него очень проблематично.

В процессе эксплуатации необходимо выявлять и оценивать текущие угрозы, считает В. Лютиков. В первую очередь, на постоянной основе реагировать на выявляемые и актуальные уязвимости. Есть продвинутое решение — киберразведка и привлечение сторонних организаций. Более простая задача — мониторинг источников, которые публикуют сведения о последних уязвимостях, эксплойтах, тактиках и техниках, применяемых нарушителями для проникновения в инфраструктуру, и управление мерами, которые реализуются в информационных системах, если иными методами обеспечить эффективную защиту невозможно. Для этого созданы методические рекомендации по выстраиванию процессов управления уязвимостями.

Инвентаризация ИТ-инфраструктуры и учёт систем информационных ресурсов, подлежащих защите, — ещё одна важная задача при обеспечении ИБ ИС. Выстраивание процессов инвентаризации — направление, которое ФСТЭК будет прорабатывать наряду с выявлением уязвимостей и угроз и реагированием на них.

Второе направление. Защита DDoS-атак — следующее направление, над которым ведётся работа. В 2023 г. количество успешных DDoS-атак стало меньше, но их мощность продолжает расти. Перед ФСТЭК стоит задача по разработке требований к организации работ по защите от DDoS-атак на трех уровнях, отметил В. Лютиков. Это национальный уровень, которым занимается Роскомнадзор; уровень провайдеров и уровень операторов информационных систем. Требования по обеспечению защищенности ГИС и ЗО КИИ РФ от несанкционированных воздействий типа «отказ в обслужи-



вании» будут изданы отдельным документом или включены в действующие нормативные документы.

Третье направление. Повышение качества работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа в соответствии с Приказами № 77 и № 110, — еще одна задача ФСТЭК. В. Лютиков отметил, что наметилась положительная динамика качества материалов аттестационных испытаний за 2022–2023 гг. по отдельным объектам информатизации. Но в части работы с ГИС и персональными данными над аттестацией необходимо работать дальше. Это обусловлено большим количеством организаций, оказывающим такие услуги, сложностью управления процессами и несоблюдением методов испытаний (анализа уязвимостей и тестирования системы на проникновение), которые должны применяться при проведении работ по аттестации ИС. Перед Службой стоит первоочередная задача по разработке комплекса методических документов (методики анализа уязвимостей, методики тестирования функций безопасности, ме-



flickr.com/photos/groteckevents

тодики испытания системы защиты информации с использованием средств тестирования), работа над ними ведется при участии экспертного сообщества.

В. Лютиков отметил, что в рамках программы «Цифровая экономика» ведется повышение системы защищенности системного программного обеспечения с открытым исходным кодом. Создан Технологический центр исследования безопасности системного ПО, идут исследования безопасности ядра ОС Linux и критичных компонентов. Большая работа проведена Институтом системного программирования РАН (ИСП РАН) и консорциумом с участием заинтересованных в исследованиях безопасности организаций. «Мы обрастаем компетенциями как со стороны специалистов, так и развиваем инструменты исследования», — отметил В. Лютиков. По результатам работы за прошлый год более 260 патчей, влияющих на безопасность, приняты международным сообществом. Это хорошие показатели с учетом того, что работы по данному направлению только начались. Такую же модель исследований предлагается применить и к другим компонентам. ФСТЭК подготовила проект методики выявления уязвимостей и недекларированных возможностей в ПО.

Четвертое направление. Отдельное направление работы — обеспечение защиты информации при внедрении технологий ИИ. Тут ФСТЭК выделяет несколько задач:

- ♦ исследование угроз безопасности при применении технологий ИИ в СЗИ;
- ♦ разработка большой языковой модели для применения в СЗИ;

- ♦ разработка и поддержка в актуальном состоянии информационных ресурсов для информирования о новых угрозах и оценки вероятности атак на СЗИ, использующие технологии ИИ;

- ♦ разработка эталонных данных для обучения и верификации моделей машинного обучения, а также эталонных базовых моделей машинного обучения для решения задач обеспечения защиты информации.

Тут важно повышение доверия к технологиям. Работа в данных направлениях будет вестись в рамках нацпроекта «Экономика данных».

Пятое направление. Еще один аспект — развитие безопасной разработки. В первую очередь он касается разработчиков средств в рамках системы сертификации ФСТЭК. Выпущены два ГОСТа по безопасной разработке, в работе еще пять: руководство по оценке безопасности разработки ПО, руководство по проведению статического анализа, руководство по разработке безопасного ПО, доверенный компилятор C/C++ и управление безопасностью ПО при использовании заимствованных и привлеченных компонентов. Также готовится новая редакция методики исследования уязвимости недекларированных возможностей, в проект уже вошли все проблемные вопросы, которые были выявлены в период действия предыдущей редакции.

И традиционный вопрос о подготовке кадров. Совместно с МГТУ им. Баумана ФСТЭК России планирует организовать курсы по внедрению технологий безопасной разработки для студентов вузов. Это масштабное мероприятие, информация о котором будет опубликована и доступна

всем желающим. Предполагается, что в работе курсов примут участие эксперты ФСТЭК и специалисты компаний, которые проведут лекции и семинары по разным аспектам безопасной разработки.

ОЦЕНКА СОСТОЯНИЯ ЗАЩИТЫ

О методическом подходе к оценке показателя состояния защиты конфиденциальной информации и обеспечения безопасности объектов КИИ в органах государственной власти и организациях рассказал Сергей Бондаренко, начальник девятого Управления ФСТЭК России.

Он отметил, что Управление находится в стадии формирования, на него в т.ч. возложены полномочия по усилению мониторинга текущего состояния защиты конфиденциальной информации, обеспечению безопасности ЗО КИИ.

При подготовке методики оценки показателя состояния защиты конфиденциальной информации и обеспечения безопасности объектов КИИ в ОГВ учитывались все документы, от требований законодательства до ведомственных НПА.

Проект методики разработан и размещен на сайте для публичного обсуждения.

В качестве критерия оценки параметров назначен показатель состояния технической защиты информации и обеспечения безопасности ЗО КИИ — показатель защищенности.

Расчет интегрального показателя защищенности ведется по формуле простой свертки с перемножением весового коэффициента группы частных показателей безопасности на сумму значений частного показателя безопасности по каждой группе. Максимальное значение показателя защищенности — единица.

Обобщенные группы частных показателей объединяют параметры по критериям — организация и управление; защита пользователей; защита информационных систем; мониторинг информационной безопасности и реагирование — и имеют разные групповые весовые коэффициенты. Частные показатели в рамках групп — индивидуальные числовые значения безопасности.

Такая оценка должна проводиться в отношении каждой информационной системы, эксплуатируемой ОГВ или организацией, и организации в целом, отметил докладчик.

Минимально необходимый уровень безопасности от актуальных угроз равен единице. Если показатель находится в диапазоне от 0,75 до 0,99, уровень безопасности не обеспечивается, имеются предпосылки к реализации угроз. При значениях ниже 0,75 возможность реализации угроз можно считать повышенной или критической.

Предложения по совершенствованию проекта методического документа принимались ФСТЭК до 15 марта 2024 г. Как отметил В. Лютиков, тестирование методики на отдельных организациях показала ее работоспособность. Предполагается, что документ будет принят в этом году.

ВОПРОСЫ СЕРТИФИКАЦИИ

Основные направления совершенствования сертификации средств защиты информации представил Дмитрий

Шевцов, начальник второго Управления ФСТЭК России. Эти направления включают сокращение сроков сертификации, совершенствование требований по безопасности информации к СЗИ, аттестацию экспертов органов по сертификации и испытательных лабораторий, повышение безопасности системного ПО и внедрение процессов безопасной разработки системного ПО СЗИ.

Работа по овершенствованию требований к СЗИ относится к уже изданным требованиям по безопасности информации к средствам контейнеризации, средствам виртуализации, многофункциональным межсетевым экранам уровня сети (NGFW) и к системам управления базами данных (СУБД). Разрабатываются требования по безопасности информации и к средствам обнаружения и реагирования уровня узла (EDR)

В рамках совершенствования требований к NGFW планируется обязательное подключение оборудования к разработанной информационной системе страновой принадлежности IP-адресов. Разработан проект методики тестирования производительности NGFW и планируется создание Центра компетенций по тестированию производительности, устойчивости функционирования и функциональных возможностей межсетевых экранов и иных сетевых устройств, реализующих функции безопасности информации. Работы проводятся в рамках национальной программы «Национальная экономика данных». Производителям необходимо привести межсетевые экраны уровня сети в соответствие требованиям в срок до 1 января 2025 г., подчеркнул спикер.

В системе сертификации ФСТЭК зарегистрировано 15 СУБД, из них четыре СУБД соответствуют требованиям к базам данных, предназначенным для хранения информации, подлежащей защите в информационной (автоматизированной) системе.

Порядок сертификации процессов безопасной разработки системного ПО СЗИ утвержден и вступает в силу с 1 июня 2024 г. Все материалы по данному вопросу размещены на портале НПА России, отметил Д. Шевцов. Он подчеркнул, что сегодня сертификация проводится по требованиям ГОСТ 2016 г. и действует три года. Готовится новый проект стандарта и в будущем сертификация будет проходить по новым требованиям.

В рамках аттестации органов по сертификации (ОС) и испытательных лабораторий (ИЛ) необходимо наличие в штате этих организаций аттестованных экспертов ОС и работников ИЛ. Требование вступает в силу с 1 марта 2025 г. Порядок аттестации таких сотрудников на соответствие требованиям при выполнении работы по оценке соответствия в отношении продукции, используемой в целях защиты сведений, составляющих гостайну или иную информацию ограниченного доступа, вступает в силу с 1 сентября 2024 г. Аттестация проводится в форме тестирования (100 вопросов по каждой области аккредитации) и решения практических задач (2 задачи по каждой области аккредитации). На выполнение заданий по каждой области выделяется 90 минут, время решения задач по каждой области — 120 минут.

ПАРАД ЗАКОНОВ

КВАРТАЛЬНЫЙ ОТЧЁТ О НОРМАТИВНОМ РЕГУЛИРОВАНИИ В СФЕРЕ ИБ



Екатерина РАЧКОВА
обозреватель BIS Journal

Пользователи портала ib-bank.ru уже заметили, что мы запустили блог «Читалка», где каждую неделю публикуем новости нормативного регулирования информационной безопасности в разных отраслях: кредитно-финансовой, транспорта, здравоохранения, образования, топливно-энергетического комплекса и др. Там же будет доступна максимально полная база действующих нормативно-методических документов различных регуляторов, а также законов и нормативных актов РФ.

В бумажной версии BIS Journal будет публиковаться регулярный обзор изменений в документах по защите информации за квартал.

НАЧАЛО ГОДА

Планы, что вступило в силу в I квартале 2024 года: Минцифры, Центральный банк, Правительство Российской Федерации

2024 год начался с публикации Плана нормативно-правовой работы Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации на 2024 год (утв. Приказом Минцифры России от 29.12.2023 № 1185).

В разрезе ИБ интерес в данном документе представляют два пункта в зоне ответственности Департамента развития отрасли информационных технологий:

- ♦ п. 1, касающийся эксперимента по предоставлению права использования программ для электронных вычислительных машин, алгоритмов, баз данных и документации к ним, в том числе исключительное право на которые принадлежит Российской Федерации, на условиях открытой лицензии и созданию условий для использования открытого программного обеспечения (март 2024);

- ♦ п. 8 о внесении изменений в некоторые акты Правительства Российской Федерации в части подтверждения и обновления биометрических персональных данных (декабрь 2024).

Кроме того, с 01.01.2024 вступили в силу:

- ♦ абзац 4 пункта 3.3 Положения Банка России от 20.04.2021 № 757-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций» (использование узлами информационной системы безопасной топологии коммуникационных сетей, программного кода и протоколов с учётом актуальных угроз безопасности и применяемых информационных технологий, в том числе реализацию системы защиты от атак, направленных на отказ в обслуживании, с возможностью фильтрации передаваемых данных, хранение узлами информационной системы доверенных сетевых адресов и реализацию механизма проверки некорректных узлов информационной системы). Проще говоря, оператор информационной системы, в которой осуществляется выпуск цифровых финансовых активов, и оператор обмена таких активов должны обеспечивать использование безопасной топологии коммуникационных сетей, программного кода и протоколов с учётом актуальных угроз информационной безопасности и применяемых технологий;

- ♦ Положение Центрального банка Российской Федерации от 07.12.2023 № 833-П «О требованиях к обеспечению защиты информации для участников платформы цифрового рубля»;

- ♦ абзацы 1 и 2 пункта 5.5. Положения Центрального банка Российской Федерации от 04.06.2020 № 719-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств»: если оператор значимой платёжной системы использует в аппаратных модулях безопасности информационной инфраструктуры платёжной системы средства криптографической защиты информации, реализующие криптографические алгоритмы, не определённые национальными стандартами Российской Федерации, то они должны иметь подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности. Однако с 01.04.2024 данное Положение утрачивает силу. Взамен вступает в силу Положение Центрального банка Российской Федерации от 17.08.2023 № 821-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств». Новое

Положение не несёт практически ничего нового для банков, ранее выполнявших 719-П, зато вводит требования к защите информации для операторов электронной платформы (операторов финансовой платформы/информационной системы, в которой осуществляется выпуск цифровых финансовых активов, операторов обмена цифровых финансовых активов при оказании указанными операторами услуг расчётов по сделкам, совершённым с использованием электронной платформы, пользователям электронной платформы).

С 23.01.2024 вступил в силу Приказ Минцифры России от 29.11.2023 № 1024 «О формах подтверждения соответствия информационных технологий и технических средств, предназначенных для обработки биометрических персональных данных, векторов единой биометрической системы, требованиям, определённым в соответствии с подпунктом «е» пункта 1 части 2 статьи 6 Федерального закона от 29 декабря 2022 г. № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации», и о внесении изменений в приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 12 мая 2023 г. № 453» (Зарегистрирован в Минюсте России 12.01.2024 № 76840). Приказом устанавливаются новые формы подтверждения соответствия информационных технологий и технических средств Закону о биометрической идентификации 572-ФЗ. Данные формы выдаются Минцифры России.

24.01.2024 вступило в силу (в день официального опубликования) Постановление Правительства РФ от 15.01.2024 № 4 «Об утверждении Правил установки, эксплуатации и модернизации в точках обмена трафиком технических средств противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети „Интернет“ и сети связи общего пользования». Данное Постановление обязывает владельцев точек обмена трафиком устанавливать технические средства защиты, определяет правила установки, эксплуатации и модернизации таких средств.

01.02.2024 вступило в силу Постановление Правительства Российской Федерации от 24.01.2024 № 58 «Об утверждении Правил оформления, переоформления и прекращения допуска граждан Российской Федерации, имеющих гражданство (подданство) ино-



стрannого государства, лиц без гражданства, иностранных граждан к государственной тайне, а также их доступа к сведениям, составляющим государственную тайну», утратило силу постановление Правительства от 22.08.1998 № 1003 «Об утверждении Положения о порядке допуска лиц, имеющих двойное гражданство, лиц без гражданства, а также лиц из числа иностранных граждан, эмигрантов и реэмигрантов к государственной тайне».

ФСТЭК РОССИИ

ФСТЭК России обновил информацию в зоне своей компетенции:

- ♦ 17.01.2024 опубликовано информационное сообщение № 240/11/142, касающееся представления сведений о кадровом обеспечении подразделений по защите информации в соответствии с утверждёнными формами представления в 2024 году указанных сведений в формате Excel. Перечень респондентов для представления сведений о кадровом обеспечении подразделений по защите информации в соответствии с данными формами был приведён в приложении к информационному сообщению;

- ♦ 19.01.2024 и затем 15.03.2024 на сайте реестров ФСТЭК России размещены обновлённый перечень органов по аттестации, реестр аккредитованных ФСТЭК России органов по сертификации и испытательных лабораторий и государственный реестр сертифицированных средств защиты информации;

- ♦ 18.03.2024 обновлено опубликованное 06.03.2024 информационное сообщение № 240/82/580 «О порядке представления субъектами критической информации



♦ ГОСТ Р «Защита информации. Идентификация и аутентификация. Типовые угрозы и уязвимости процессов идентификации и аутентификации»;

♦ ГОСТ Р «Защита информации. Идентификация и аутентификация. Рекомендации по управлению идентификацией и аутентификацией»;

♦ ГОСТ Р «Защита информации. Формальная модель управления доступом. Часть 3. Рекомендации по разработке»;

♦ ГОСТ Р «Защита информации. Формальная модель управления доступом. Часть 4. Рекомендации по верификации средства защиты информации, реализующего политики управления доступом, на основе формализованных описаний модели управления доступом».

БАНК РОССИИ

Центральный банк Российской Федерации опубликовал «Методические рекомендации по усилению

ной инфраструктуры сведений о результатах присвоения объектам критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий» (субъектам КИИ, осуществляющим деятельность в сфере транспорта, рекомендуется направлять перечни и сведения в центральный аппарат ФСТЭК России или управление ФСТЭК России по федеральному округу, на территории которого они расположены, в зависимости от ряда условий).

♦ 28.03.2024 опубликованы «Сведения о принятых национальных и международных стандартах за I квартал 2024 года».

А также опубликовал и принял участие в организации сбора замечаний и голосований по разрабатываемым проектам стандартов и методических документов:

♦ ГОСТ Р «Защита информации. Системы с конструктивной информационной безопасностью. Методология разработки»;

♦ методического документа «Методика оценки показателя состояния защиты информации и обеспечения безопасности объектов критической информационной инфраструктуры РФ»;

♦ ГОСТ Р «Защита информации. Защита информации от утечки из программной среды информационных и автоматизированных систем. Общие положения» (определяет состав участников и основное содержание процессов защиты информации от утечки из программной среды АС/ИС (за исключением ПЭМИН));

♦ ГОСТ Р «Защита информации. Идентификация и аутентификация. Уровни доверия аутентификации».

кредитными организациями информационной работы с клиентами в целях противодействия осуществлению переводов денежных средств без добровольного согласия клиента, а также заключению договоров на получение кредитных (заёмных) денежных средств под влиянием обмана или при злоупотреблении доверием и осуществлению операций с использованием указанных денежных средств, а также вовлечению граждан в деятельность по выводу и обналичиванию средств, полученных преступным путём» (утв. 28.02.2024 № 3-МР, будут применяться с 25.07.2024, с этой же даты отменяются Методические рекомендации по усилению кредитными организациями информационной работы с клиентами в целях противодействия несанкционированным операциям от 19.02.2021 № 3-МР).

Документ представляет собой новые рекомендации по предупреждению клиентов банков о рисках хищений собственных и кредитных средств злоумышленниками, а также последствиях вовлечения в деятельность по выводу и обналичиванию похищенных денег (дропперство). В числе прочего для достижения указанной цели регулятором предлагается:

♦ разработать сценарии для бесед сотрудников с клиентами при возникновении подозрений, что человек находится под влиянием мошенников и может лишиться денег;

♦ создать сервисы, позволяющие клиентам определить подозрительные звонки, а также антивирусные программы, которые помогут защитить от хищений денег различных категорий граждан, в т.ч. социально уязвимых (пожилые люди, инвалиды и другие);

♦ внедрить для банкоматов двухфакторную аутентификацию.

Также Банк России опубликовал «Методические рекомендации по управлению риском информационной безопасности и обеспечению операционной надежности» от 21.03.2024 № 7-МР (рекомендации по реализации уровней защиты стандартов ГОСТ Р 57580.3–2022 и ГОСТ Р 57580.4–2022 финансовыми организациями в зависимости от их типа).

Кроме того Центральный банк Российской Федерации опубликовал стандарт СТО БР БФБО-1.8–2024 «Безопасность финансовых (банковских) операций. Обеспечение безопасности финансовых сервисов при проведении дистанционной идентификации и аутентификации. Состав мер защиты информации» (Принят и введён в действие приказом Банка России от 28.02.2024 № ОД-326). Стандарт определяет, какие меры защиты информации следует применять финансовым организациям при проведении дистанционной идентификации и аутентификации клиентов. Состав и содержание мер целесообразно дифференцировать в зависимости от вида операции, её критичности и рисков, стандарт вступает в силу 01.07.2024 и носит рекомендательный характер.

ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Не были забыты и персональные данные (ПДн). На рассмотрение в первом квартале 2024 года поступили:

- ♦ законопроект № 502104–8 «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» (об оборотных штрафах для ИТ-компаний, допустивших утечки ПДн пользователей, в части усиления ответственности за нарушение порядка обработки персональных данных). Предлагается установить ответственность за утечку ПДн в зависимости от количества пострадавших субъектов ПДн: если утечка коснётся от 1 до 10 тыс. субъектов ПДн, то штраф для оператора ПДн составит от 3 млн до 5 млн руб. При количестве от 10 тыс. до 100 тыс. субъектов ПДн штраф составит от 5 до 10 млн руб., при более чем 100 тыс. субъектов ПДн штраф составит от 10 млн до 15 млн руб. За повторные утечки ПДн предлагается ввести оборотные штрафы от 0,1 до 3% выручки оператора ПДн за календарный год или за часть текущего года, но не менее 15 млн руб. и не более 500 млн руб.;

- ♦ законопроект № 502113–8 «О внесении изменений в Уголовный кодекс Российской Федерации» (в части установления ответственности за незаконные использование и передачу, сбор и хранение компьютерной информации, содержащей персональные данные). Предусматривает установление уголовной ответственности до 10 лет лишения свободы за незаконные использование, передачу, сбор и хранение ПДн граждан Российской Федерации.

КИИ

Также был внесён законопроект № 581689–8 «О внесении изменений в Федеральный закон «О безопасности критической информационной инфраструктуры РФ» (в части мероприятий по импортозамещению на значимых объектах критической информационной инфраструк-

туры (КИИ), категорирования с учётом типовых отраслевых перечней объектов КИИ, а также необходимости разработки отраслевых методических документов по категорированию объектов КИИ).

ОТРАСЛЕВЫЕ ДОКУМЕНТЫ

Правительство Российской Федерации опубликовало постановление от 28.02.2024 № 224 «О внесении изменений в постановление Правительства РФ от 12 февраля 2020 г. № 126» (изменения в правилах установки, эксплуатации и модернизации в сети связи оператора связи технических средств противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования).

В связи с внесением поправок в Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» утверждены новые технические условия установки технических средств противодействия угрозам устойчивости, безопасности и целостности функционирования в России сети «Интернет» и сети связи общего пользования, а также требования к сетям связи при использовании указанных средств. 26.03.2024 опубликован соответствующий приказ Роскомнадзора от 19.02.2024 № 25 «Об утверждении технических условий установки технических средств противодействия угрозам, а также требований к сетям связи при использовании технических средств противодействия угрозам».

Росстандарт 15.02.2024 приказом № 235-ст утвердил спецификацию протокола защищённого обмена для промышленных систем ГОСТ Р 71252–2024 «Информационная технология. Криптографическая защита информации. Протокол защищённого обмена для промышленных систем». Стандарт вступает в силу с 01.04.2024 взамен рекомендаций по стандартизации Р 1323565.1.029–2019.

Также с января по март был опубликован ряд отраслевых документов, из которых специалисты могут почерпнуть примеры и способы изложения тех или иных вопросов для нужд разработки собственных аналогичных документов:

- ♦ Методические рекомендации по цифровой трансформации государственных корпораций и компаний с государственным участием (опубликованы Минцифры России 12.01.2024);

- ♦ приказ Министерства экономического развития РФ от 13.11.2023 № 785 «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении Министерством экономического развития РФ функций, определённых законодательством РФ» (опубликован 22.02.2024, вступает в силу 04.03.2024. Можно брать как пример при построении собственной модели угроз и определения актуальных угроз безопасности персональных данных, в том числе в части разделения угроз на требующие и не требующие применения СКЗИ для противодействия).

«МЫ ЖИВЁМ В ДОМЕ СО СТЕКЛЯННЫМИ СТЕНАМИ...»



Виталий ТЕРЕНТЬЕВ
HeadHunter

Что такое информационная безопасность крупнейшего рекрутингового портала? В чём ее специфика и универсальность? Легко ли набрать сотрудников, имея в распоряжении такую базу соискателей? Об этом и многом другом обозреватель BIS Journal Марина Бродская беседует с CSO- и GR-директором HeadHunter Виталием Терентьевым.

ЧЕТЫРЕ «ШАПОЧКИ»

— Виталий, на конференциях вас часто представляют как директора по GR HeadHunter, хотя говорите вы, как правило, об информационной безопасности. Кто вы на самом деле: какие функции выполняете, какую должность занимаете?

— У меня четыре «шапочки» в компании. Первая — это управляющий партнёр HeadHunter по региону Центральная Азия и Закавказье. Всё, что там есть у компании, я создал и этим управляю. Вторая «шапочка» — директор по безопасности, CSO. Третья и четвёртая — это GR-директор и директор департамента специальных проектов.

— «Шапочку» по безопасности получили до 250-го Указа?

— Да, конечно. До меня службы безопасности в компании не было, создавал с нуля.

ПРО ЗАМА ПО БЕЗОПАСНОСТИ

— Сейчас компания, подпадающая под действие 250-го Указа, должна иметь зама по безопасности. Как думаете, хватит ли ему знаний, которые ему дадут на рекомендованных курсах?

— 512-часовая программа переподготовки придумана ФСТЭК и ФСБ и решает достаточно узкие задачи. Она не столько даёт знания, сколько открывает возможности. Понятно, что защищать объект КИИ вы с такими знаниями не сможете, но они дают общие, достаточно глубокие представления о предмете и, конечно, лицензию.

— Многие идут учиться для галочки...

— Процесс нужно организовывать. Каждый действует в силу своих способностей и понимания ситуации. Кто-то всё сразу делает по уму, кто-то — не сразу...

ПРО ОБРАЗОВАНИЕ, ОПЫТ И УСТАНОВКИ

— И всё же... нужна реальная подготовка: опыт, ИТ-образование...

— Айтишное образование — это замечательно и всегда плюс, но в безопасности работает довольно много людей, не имея такого образования. Главное — опыт и отношение к делу. Без этого стать безопасником, как, например, и управленцем, невозможно.

Я стал директором по безопасности одного из крупнейших банков в Центральной Азии, ещё будучи студентом, в 21 год. Диплом защищал по системе, которую сам же и создавал. С тех пор опыт только прибавлялся, причём у меня не было ни одного проваленного проекта и, надеюсь, не будет.

— Не преувеличиваете?

— Нет. Это установка: ошибиться можно, проиграть — нельзя. Если начинаете свою деятельность с такой базовой позиции, то и опыт будет соответствующий. А если начинать

BIS-СПРАВКА

hh.ru — крупнейшая платформа онлайн-рекрутинга в России, клиентами которой являются свыше 523 тыс. компаний. Обширная база компаний содержит 66 млн резюме, а среднее дневное количество вакансий в течение 2023 г. составило свыше 1,18 млн ежемесячно. По данным SimilarWeb, hh.ru занимает третье место в мире по популярности среди порталов по поиску работы и сотрудников.

с отношением «да мне всё равно, где и какой опыт получать», вас всегда будут взламывать.

— **А есть ещё распространённая установка «К нам не придут, кому мы нужны? — мы маленькие, где-то в стороне...»**

— Вот в это не верю! Если такая установка есть, значит, безопасник не умеет коммуницировать с руководством компании, не понимает сути бизнеса, который защищает, и такому безопаснику в профессии делать нечего. Это, как вы понимаете, я про уровень CISO как минимум.

ПРО ДЕПАРТАМЕНТ ИБ

— **Вы сказали, что создали службу ИБ HeadHunter с нуля. Когда это произошло?**

— Я работаю в компании 18 лет, а департамент ИБ создал семь лет назад. Начинал один, потом набрал отдел. Нашу компанию сделали талантливые и преданные делу люди, и её безопасность тоже. Они очень разные. Мы не всегда находим общий язык, но то, что мои коллеги — крутые, великолепные безопасники, — это безусловно. Счет 0:0 — благодаря им.

— **Текучка кадров у вас большая?**

— Не часто, но иногда уходят. Был кейс, когда ушла целая команда — но что приятно, не в другую компанию или к конкурентам, а в свой частный бизнес. А когда уходит родная команда, это трудно, и это очень сложносочинённый процесс.

У меня как управленца, не скрою, случались ошибки, но на компании, на её защищённости это никогда не отражалось. Иначе я занимался бы чем-то другим.

— **Как вы решаете проблему кадрового голода?**

— Как и все вокруг — с трудом. Какая разница, сидишь ты сам на большой базе соискателей или где-то её покупаешь. Мы в одинаковых условиях со своими клиентами: квалифицированных кадров не хватает всем! Более того, у меня завышенные требования к людям, поэтому срок закрытия позиции очень длинный. И это моя боль.

Сейчас у нас работают человек 15, открыто много вакансий. Нужны «зубастые волки» — джуниоров мы давно набрали...

— **Насколько то, что реализовано, отличается от первоначального замысла?**

— Не отличается. У меня хорошее стратегическое планирование. Всё, что задумывалось семь лет назад, было реализовано и продолжает реализовываться. Осталось ещё года на два.

— **А как с импортозамещением? Не стало вас врасплох?**

— Выбор технологических решений — по большей части вкусовщина. Могу сказать, что я с самого начала старался использовать продукты

и решения, которые каким-то образом имеют отношение к России. Чему сегодня очень рад, поскольку не имею головной боли на эту тему.

— **А как с бюджетом?**

— Бюджет департамента ИБ не роскошный, как у многих коллег с рынка... Получаем необходимое под конкретные задачи. Иногда хорошо, иногда с задержкой, а в целом — грех жаловаться. Скажем так: уже давно компания не страдает недостатком финансирования вопросов ИБ.

— **Были ли серьёзные инциденты?**

— Не было. Нас пытались «ломать», пытаются и будут продолжать. Но, повторюсь, счёт пока 0:0. Благодаря людям, которые здесь работают.

— **Вы вошли в Регистр организаторов распространения информации. Что-то изменилось?**

— Ничего не изменилось. Есть нормативные требования, которые любая компания, работающая с персональными данными, обязана исполнять. Система построена в соответствии с ними, нас фактически подключили с готовой инфраструктурой исполнения этой практики. Пришлось сделать минимум телодвижений, чтобы подключиться правильно.

— **HeadHunter представлен в семи странах. Насколько сложно соблюдать законодательства?**

— Сложности возникают, бывает... Но ядро защиты базового законодательства во всех странах примерно одинаковое: «не воруй, не укради, соблюдай правила по персональным данным...» Поэтому понятно, что делать. Есть, конечно, отличия, исключения, разные трактовки... Но если ты в них разбираешься, не составляет труда со всем этим управиться. А по сути различий в законодательствах наших стран в отношении ИБ практически нет.

ПРОВЕРКА КЛИЕНТОВ

— **Проверяют ли HeadHunter и другие рекрутинговые платформы работодателей на благонадёжность?**

— Обязательно, но каждая по-своему. По-разному настроены антифрод, система, контролирующая логистику... Некоторые, например, пускают к себе пользователей, которых мы не принимаем. Потому что для них это риск невысокий, а для нас — высокий.

— **То есть объявления о наборе дропперов вы отсекаете, а другие нет?**

— Дропперов набирают везде, от этого не просто избавиться. Как правило, такие вакансии маскируют под курьеров, а потом кандидата выводят на персональный разговор... Мы знаем, как с этим бороться, но это не только вопрос ИБ. Будет закон — будем решать.

О ПРОБЛЕМЕ КАДРОВ

— **Тема кадрового голода обсуждается на всех конференциях по ИБ. Но на портале HeadHunter мы видим огромное количество резюме безопасников...**

— Сейчас на одну вакансию — 0,3 резюме. Дефицит в сфере ИБ зашкаливающий, потому что настоящих специалистов действительно мало, а со временем станет ещё меньше, так как требования к уровню компетентности стремительно повышаются. Плюс мелкодисперсный рынок и неразбериха с неймингом. У одного руководителя должность называется CISO, у другого — директор по безопасности, у третьего — ещё как-то... Что уж говорить про низшие должности.

— **С учётом проблем в нейминге, как вы получаете данные по дефициту кадров в ИБ?**

— У нас есть целый исследовательский центр, который этим занимается, применяет ИИ, который анализирует в первую очередь тексты, а потом уже название вакансий. И мы точно знаем, что дефицит будет увеличиваться: проектов, которые нужно защищать, становится больше, соответственно, безопасников всё меньше. Скоро за них начнётся настоящая битва, и зарплаты в этой области должны подниматься.

— **Может, ИИ поможет?**

— К сожалению, искусственным интеллектом безопасников не заменить. Это работа творческая. Люди создают новое, каждая система защиты по-своему уникальна — под конкретные задачи.

Поэтому с людьми всё грустно. И вряд ли будет лучше: у нас не так много учебных заведений и крутых специалистов, которые готовы учить, передавать знания из рук в руки.

Айтишники могут съездить в какой-нибудь ИТ-кэмп для передачи опыта, а вот опытные безопасники не готовы делиться: зачем растить конкурентов, снижать свою стоимость на рынке и т.д. Накладываются и искажения психики, и другие специфические моменты.

— **В отличие от отрасли ИБ, где с людьми всё плохо, вузы говорят, что у них с подготовкой кадров всё хорошо, они проходят аттестации и сертификации, высоко оцениваются учебно-методическим объединением...**

— У вузов свои задачи, своя ситуация, они будут продолжать упираться и не прислушиваться к бизнесу. Это давно известно, и обсуждать это бессмысленно.

Чтобы что-то изменить, нужно делать серьёзные программные вещи. Например, направлять преподавателей ИБ из вузов в крупные ИТ-компании — на трёхмесячную

аттестацию. Не получил аттестата — не имеешь права преподавать.

Или идти по пути «Яндекса» и Сбера. Они открывают свои университеты, засылают людей преподавать в вузы. Понятно, что они таким образом «пылесосят» рынок и забирают к себе лучших. Но в процессе они обучают довольно много молодых людей, которые выходят на рынок, имея актуальные знания.

А компании по безопасности учат кого-то безопасности? Что-то не видно. Почему?

НЕ ПРОДАВАТЬ СТРАХ

— **Как эту позицию сдвинуть с места?**

— Если примут новый закон об оборотных штрафах, привлекут к ответственности две-три компании, многие забеспокоятся. Потому что в бизнесе, в безопасности, к величайшему сожалению, работает прецедентное право. И пока нет прецедентов, никто не шевелится.

Другая проблема — большинство CISO/CSO не умеют общаться с руководством, поэтому не включены в стратегию компании, в совет директоров, в информационные потоки... Живут как бы отдельно в своём периметре. Пока так будет, бизнес не зашевелится. И это проблема самих безопасников, им ситуация выгодна из-за невысокой конкуренции или нехватки компетентности. Единицы CISO могут поговорить с бизнесом на серьёзном уровне и не продавать страх. И тогда безопасность вшивается в процесс, хеджирует риски, предиктивно до момента их появления, чтобы бизнес чувствовал себя комфортно. Строить систему безопасности надо до момента постройки бизнеса, это дешевле.

— **К этому уже многие приходят...**

— Только в крупных компаниях, и то с учётом результатов, которые мы имеем. Сколько за последние три-четыре года утечек из крупных компаний произошло? Много.

— **Может, штрафы маленькие?**

— Нет, просто бизнесу всё равно. Можно жить как живётся. Хотя я не совсем согласен, что нужно обязательно вводить оборотные штрафы. Идея, может, и неплоха — внедряет ответственность. Но штрафы с учётом несовершенства закона и его разностороннего трактования не будут работать так, как хотелось бы, с ходу. Бизнес зашевелится, но только из-под палки.

ПРО ОБОРОТНЫЕ ШТРАФЫ

— **Законопроект об оборотных штрафах вызвал бурные дискуссии...**

— Законопроект неплохой. Я много спорил и с коллегами на открытых мероприятиях, и с регуляторами... Идея хорошая — реализация не самая лучшая.

Представьте, как в суде будете доказывать виновность или невиновность, когда большинство судей не знают, что такое IP-адрес? Им принесут великолепное, исчерпывающее расследование, сделанное, например, компанией Positive Technologies, а они его не примут во внимание, потому что не могут понять терминологию. И что дальше?

— **Законопроект потребует после его принятия наращивать нормативную базу...**

— Правильно, но об этом почему-то не думают. Я как GR взаимодействую с законодателями, меня слушают. Другой вопрос, как слушают? Расклад-то непростой: есть позиция государства, есть экспертная позиция. Но, кроме этого, многим сложившаяся ситуация выгодна. Например, компаниям по безопасности, получающим дополнительное финансирование. И их GR лоббирует третью точку зрения.

С точки зрения эксперта я бы этот закон доработал. Довёл до кондиции, чтобы он работал эффективно, чтобы компаниям стало наконец понятно, куда и зачем вкладывать средства.

— **В рамках подготовки ко второму чтению идёт лоббирование снижения размеров штрафов, если компания приняла меры...**

— Вас могут пощадить, только если вы тратите 0,01% от вашей выручки на безопасность. Большинство российских компаний этому показателю не соответствуют, они не в состоянии выполнить это требование. Тратится радикально меньше. Это первый момент. А второй — надо пройти аудит у регулятора на соответствие безопасности. У нас большинство компаний аудиты не проходят.

— **То есть давить только штрафами и страхом?**

— К сожалению, принято такое решение. Мне, повторюсь, идея нравится, а вот форма реализации — нет. Я не считаю, что штрафами мы добьёмся кратного увеличения безопасности. С другой стороны, понимаю, что, когда тебя не слышат, возможно, это один из способов добиться, чтобы тебя услышали. Плюс уголовная ответственность, но она не во всех разрезах возникает.

О ЧЕЛОВЕЧЕСКОМ ФАКТОРЕ

— **Эксперты «Лаборатории Касперского» заявили, что после принятия закона ждут сообщений о неизвестных нам утечках по известным им инцидентам. Вопрос, когда всплывут сами данные?**

— У любой компании есть такое состояние — «ожидания всплытия». Защитить бизнес полностью физически невозможно, даже

если вы соберёте топовую команду безопасников. Потому что всегда остаётся человеческий фактор и пресловутая социальная инженерия. Дырку в человеческой голове никаким скотчем не заклеишь, никаким файрволом не закроешь. Никакой SOC не поможет, если в голове человека «дырявый» взгляд на безопасность, которую он считает некой мелкой сервисной функцией и не понимает, что сейчас она — краеугольный камень внутри бизнес-процесса компании. Поймёт — тогда в компании и будет порядок.

ПРО ТЁМНУЮ СТОРОНУ

— **Но реальные «всплытия» утечек будут?**

— Конечно, будут. Когда появилась тема с законом, ребята с «тёмной стороны», назовём их так, свою добычу придержали и пока не афишируют — потом будет веселее шантажировать компании. С государства «плохиши» ничего не получают, а с компаний в новой ситуации можно будет получить очень много. Не забывайте, что, кроме штрафа, есть репутационные риски и многое другое, из-за чего компании могут пострадать. И с этим ничего не сделаешь.

О РЕПУТАЦИОННЫХ РИСКАХ

— **Так ли у нас важны репутационные риски? Ну, была утечка и была...**

— Это только кажется. Любой бизнес живёт во времени, и после серьёзной утечки, в которую попали ваши данные, вы эту компанию точно не забудете. Будете реже иметь с ней дело, скажете знакомым быть с ней аккуратнее. В результате организация несёт затраты на дополнительное продвижение продуктов, перестройку службы поддержки — из-за снижения доверия... Масса влияний, которые выливаются в деньги. Другой вопрос, что затраты не все считают. Но каждый выбирает свой путь.

О ОБЫВАТЕЛЯХ

— **Однако большинство обывателей не знает об утечках. Люди просто удивляются, что им позвонил очередной мошенник, который в курсе их проблем...**

— Большинство людей будут удивляться и дальше. Мы живём в доме со стеклянными стенами, и об этом нельзя забывать. Всё, что хотя бы один раз попало в интернет, рано или поздно будет использовано против личности. Это вопрос времени. Причём неважно, госсистема это или нет, всё — достояние общности. И оно не нормировано, не регламентировано и никак не контролируемо. Даже безопасники это не всегда понимают, что вы от обывателей хотите?

Беседовала
Марина Бродская

НЕ ВЫБИРАЕМ, А СОЧЕТАЕМ

ПАССИВНЫЙ И АКТИВНЫЙ МОНИТОРИНГ ПРОМЫШЛЕННОЙ СЕТИ



Андрей СТРЕЛКОВ
руководитель
направления
развития продуктов
для промышленной
безопасности,
«Лаборатория
Касперского»

Вы владелец бизнеса в области промышленного производства с большим числом АСУ ТП и SCADA-систем или ваше предприятие стоит на пороге цифровой трансформации? Тогда вам понадобится серьёзная защита промышленной сети. Если пренебречь информационной безопасностью, то последствия могут быть катастрофическими для технологических процессов. Рассказываем о базовых для защиты промышленных систем технологиях пассивного и активного мониторинга и объясняем, почему без специализированных решений вам не обойтись.

ЗАЧЕМ ОТСЛЕЖИВАТЬ ТРАФИК ПРЕДПРИЯТИЯ?

Типичное представление о кибератаке на бизнес — хакер взламывает банковскую систему и переводит миллионы на свой счёт. Но сегодня под ударом оказываются все сегменты российского бизнеса, включая производство, металлообработку, пищевую промышленность и энергетику, а киберзлоумышленники зачастую руководствуются не только финансовыми мотивами. Во втором полугодии 2023 года в России вредоносные объекты были заблокированы на 31,1% компьютеров АСУ — почти на каждом третьем устройстве!¹

В числе последствий кибератаки на систему управления технологическим процессом может быть не только финансовый ущерб. Мониторинг промышленной сети

поможет избежать нарушений в производственных процессах и техногенных катастроф. Представьте, например, к чему может привести нарушение технологических процессов в городской системе водоочистки. Подобные объекты находятся под присмотром государства, которое тщательно следит за тем, чтобы предприятия уделяли достаточно внимания вопросам кибербезопасности.

Почему так важно отслеживать трафик предприятия? Объединение систем АСУ ТП и ИТ повышает операционную эффективность бизнеса, но также увеличивает риск кибератак на производственные системы. Интеграция разных сетей создаёт новые пути для атакующих, а подключение промышленных устройств к сети расширяет поверхность атаки. Поэтому необходимо постоянно мониторить промышленную сеть, чтобы вовремя обнаруживать аномалии и потенциальные атаки — только так можно обеспечить оперативную и надёжную защиту инфраструктуры, её полную видимость. Однако из-за специфики промышленных систем делать это приходится очень осторожно. Применяемые методы мониторинга должны оказывать минимальное влияние на работу системы.

ПАССИВНЫЙ МОНИТОРИНГ: ПРОВЕРЯЕМ ТРАФИК, НЕ «ПРИКАСАЯСЬ» К НЕМУ

Определённые действия системы безопасности несут риски для промышленной сети. Например, когда сканирование трафика для поиска признаков атаки осуществляется в режиме подключения в разрыв канала. Все передаваемые данные пропускаются через защитное решение, которое может их изменить: вырезать данные из трафика или заблокировать коммуникации, если алгоритмы решат, что они несут угрозу. Но алгоритмы тоже ошибаются, и результатом манипуляций с трафиком может стать потеря данных от устройств или нарушение программы управления важным оборудованием. Кроме того, фильтрация трафика «в разрыв» может вносить задержки, негативно влияющие на работу АСУ ТП.

¹ По данным исследования Центра исследования безопасности промышленных систем и реагирования на инциденты информационной безопасности «Лаборатории Касперского» (Kaspersky ICS CERT).

Помимо активного мониторинга сети, популярно её сканирование для поиска уязвимостей и активные опросы устройств. Однако к последним может быть чувствительно промышленное оборудование, не предназначенное для взаимодействия по общепринятым протоколам.

Для бережного, неинвазивного анализа трафика используется пассивный мониторинг: специалисты ведут наблюдение, используя только его копию. Для этого настраивается зеркалирование трафика — на коммутаторе, поддерживающем такую технологию (на некоторых устройствах она называется SPAN, Switched Port Analyzer), создаётся параллельный канал, куда копируются пакеты данных, передаваемые между активами сети. Дубли пакетов отправляются на локальный сервер для анализа различными методами.

Что можно узнать, «прослушивая» трафик? Рассмотрим на примере промышленной XDR-платформы одного из российских производителей. Пассивный мониторинг, встроенный в платформу, даёт возможность выполнять следующие задачи.

Инвентаризация. Первое, с чего начинается любая реализация программы ИБ, — это составление глобального списка активов, подключённых к промышленной сети. Уже здесь возникает необходимость в применении специализированного решения: только оно сможет опознать весь спектр подключённого оборудования, включая промышленные контроллеры. Задача решения — «увидеть» в сети:

- ◆ АРМ (автоматизированные рабочие места) и серверы;
- ◆ переносные устройства (ноутбуки, смартфоны, планшеты);
- ◆ сетевое оборудование (маршрутизаторы, коммутаторы и т.д.);
- ◆ промышленное оборудование (промышленные контроллеры, интеллектуальные электронные устройства, конверторы протоколов);
- ◆ вспомогательное оборудование (принтеры, источники бесперебойного питания, системы хранения данных);
- ◆ умные IoT-устройства с подключением к интернету: различные датчики, веб-камеры, замки и т.д.

Все эти устройства могут быть использованы для кибератак на промышленную сеть, поэтому их мониторинг обязателен.

Обнаружение нелегитимных подключений и коммуникаций. Анализ трафика позволяет обнаружить новые хосты в сети, включая нежелательные (к таким могут быть отнесены и мобильные телефоны или план-

шеты), с помощью машинного обучения строить профиль разрешённых сетевых коммуникаций, а затем обнаруживать аномалии, например незапланированные сеансы удалённого подключения и отдельные сессии связи между устройствами, распространение вредоносного ПО в сети.

Обнаружение критических команд для промышленных устройств. Если в решении есть технология глубокого анализа пакетов DPI (Deep Packet Inspection), то с её помощью можно отслеживать отправку команд остановки, перезагрузки, форматирования, смены уставки, смены режима работы и параметров загрузки, передаваемых на промышленные контроллеры и другие интеллектуальные устройства.

Достаточно ли пассивного мониторинга для стопроцентной видимости в промышленной сети? Чаще всего нет. В сетевом трафике может быть недостаточно данных, чтобы точно определить атрибут актива пассивными методами. Кроме того, пассивный мониторинг не позволяет получить информацию быстро, так как приходится ждать и надеяться на появление данных об устройствах в трафике. Если нужна большая надёжность и оперативность в получении данных, можно рассмотреть применение активного опроса.

АКТИВНЫЙ МОНИТОРИНГ: НЕОБХОДИМЫ РЕШЕНИЯ С ДОКАЗАННОЙ БЕЗОПАСНОСТЬЮ ДЛЯ ПРОМЫШЛЕННОГО ОБОРУДОВАНИЯ

Пассивный мониторинг — это интроверт на публичном мероприятии, наблюдающий за окружающими и пытающийся составить представление о них из подслушанных разговоров. Чтобы получить конкретную информацию, гостю придётся принимать активное участие в беседе и задавать интересующие его вопросы — так работает активный мониторинг. Чтобы опросить конкретное устройство в промышленной сети, придётся подключаться к нему, передавать дополнительный трафик по сети, выполнять на нём инструкции.

Активный мониторинг может быть очень эффективным для сбора исчерпывающей информации о профиле и конфигурации. Как минимум с его помощью можно получить: IP и MAC-адрес, название вендора и модель устройства, версии прошивки, данные об установленном ПО и версии ОС. Существуют решения для промышленных предприятий, которые поддерживают язык OVAL (Open Vulnerability and Assessment Language, откры-

тый язык описания и оценки уязвимостей), что позволяет провести полноценную оценку сетевого оборудования и рабочей станции с ОС Windows или Linux на наличие уязвимостей и соответствие политикам безопасности — от версий конкретных программ до разрешения на автозапуск с USB-накопителя.

Как мы упоминали, активного мониторинга в промышленной среде предпочитают избегать. Это связано в том числе с особенностями оборудования, подключённого к сети. В ИТ-среде для поиска открытых портов, которые могут быть использованы злоумышленниками, используется сканирование оборудования по нескольким общепринятым протоколам. Многие промышленные устройства, особенно устаревшие, не предназначены для ответа на запросы этих протоколов или приём запросов от них. Иногда отправка активных запросов на ПЛК может даже привести к сбою в его работе или поломке. Поэтому любые предназначенные для корпоративных сетей сканеры уязвимостей и портов не должны использоваться в промышленной среде.

Тем не менее промышленное оборудование можно опрашивать активным методом, но с пониманием его специфики и ограничений. Решение с таким функционалом существует, то есть безопасное взаимодействие в рамках активного мониторинга с десятками моделей промышленных устройств от разных вендоров возможно.

СИНЕРГИЯ ПАССИВНОГО И АКТИВНОГО: ПРЕОДОЛЕВАЕМ ОГРАНИЧЕНИЯ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЯ ИХ ВМЕСТЕ

Не существует универсального подхода к обнаружению активов и анализу происходящего в промышленной сети — скорее всего, для решения ваших задач понадобятся инструменты пассивного мониторинга и дополнительные возможности для активного опроса. Один из примеров комбинированного использования — постоянный анализ трафика сети с помощью пассивного мониторинга с автоматическими плановыми проверками-опросами раз в 1–2 месяца активными методами сбора данных для подтверждения соблюдения политик безопасности.

ОБОГАЩАЕМ ДАННЫЕ: КАК ПОЛУЧИТЬ ДОПОЛНИТЕЛЬНУЮ ИНФОРМАЦИЮ ДЛЯ РАССЛЕДОВАНИЯ УГРОЗ

Комбинация пассивного и активного мониторинга помогает достаточно точно оценить происходящее в промышленной сети и состояние подключённых к ней активов. Но если

происходит сложная атака или вы хотите досконально разобраться в инциденте, потребуется ещё больше данных.

Их можно получить с помощью технологии EDR (Endpoint Detection and Response), которая позволяет проактивно обнаруживать нетиповые угрозы и целевые атаки на конечных точках. EDR записывает все события, происходящие на конечных точках, обеспечивая наиболее полные данные для расследований и исправления инцидентов безопасности. Если в решение для защиты промышленных устройств входит такая технология, то можно будет видеть не только информацию, полученную путём мониторинга сети, но и все события на хосте, связанные с инцидентом. Это помогает отследить источник угрозы или путь его проникновения в сеть, а также предупредить дальнейшее развитие атаки.

ВЫВОДЫ

Сеть промышленного предприятия с автоматизированными системами управления нуждается в специализированных средствах кибербезопасности. Обычные, предназначенные для корпоративной сети, не подходят: промышленные устройства могут быть чувствительны к их запросам и дополнительному трафику.

◆ Основным методом наблюдения за происходящим в промышленной сети является пассивный мониторинг, который позволяет анализировать трафик, не нарушая его. Однако с помощью пассивного мониторинга не всегда можно получить полную информацию об устройстве или сделать это оперативно.

◆ Активный мониторинг, в том числе с помощью запросов на языке OVAL, помогает получить исчерпывающую информацию об устройстве в сети. Однако из-за специфики промышленного оборудования его опрос должен проводиться максимально аккуратно, только по предусмотренным производителем протоколам. Корпоративные сканеры сети для этого не подойдут, так как могут вызывать сбои оборудования. Правильная реализация активного опроса позволяет свести возможность негативного воздействия на технологический процесс к нулю.

◆ Синергия между пассивным и активным мониторингом позволяет обеспечить полную прозрачность промышленной сети, отслеживать применение политик безопасности и своевременно реагировать на инциденты, минимизируя возможные ущербы и риски.

◆ Для расследования инцидентов ИБ и сложных атак необходимы дополнительные данные о событиях на пострадавшем хосте.

В ДАННЫХ ОБСТОЯТЕЛЬСТВАХ

КАК ВЫСТРОИТЬ БЕЗОПАСНЫЙ ОБМЕН ДАННЫМИ



**Александр
ТОВСТОЛИП**
руководитель
управления
информационной
безопасности
Ассоциации ФинТех

Данные становятся «топливом» для технологий, особенно это касается технологий искусственного интеллекта, и важнейшим нематериальным активом. При этом обмен данными помогает решить проблему нехватки «топлива» для технологий и может стать катализатором экономического роста. Но вопрос обмена и совместного доступа к данным сложен и многогранен, необходимо комплексное решение юридических, технических и организационных барьеров, снижение возникающих рисков и соблюдение баланса между прогрессом, безопасностью и этикой. Как этого добиться в современных условиях?

ИЗБЕЖАТЬ КОНФЛИКТА ИНТЕРЕСОВ

Сейчас, когда развитие ИИ набирает обороты и парадигма «клиентоориентированности» сменяется принципом «человекоцентричности», значение данных сложно переоценить. Обучение моделей ИИ и максимальная персонализация продуктов и предложений невозможны без огромных объемов данных из самых разных сфер. И тут мы «упираемся» в основной конфликт интересов: участникам рынка хочется получать и обогащать данные, но не хочется ими делиться. Поэтому очень важно выстроить необходимые условия для организации обмена: от нормативного регулирования до обеспечения конфиденциальности данных.

В целом все технологии обеспечения конфиденциальности можно условно разделить на 5 групп:

1. Традиционные методы: псевдонимизация, анонимизация, агрегация
2. Методы обезличивания: перемешивание, введение идентификаторов, декомпозиция, изменение состава
3. Методы криптографической защиты: шифрование, хеширование, токенизация
4. Методы безопасных вычислений: гомоморфное шифрование, доказательство с нулевым разглашением, дифференциальная конфиденциальность, вычисления в анклав, конфиденциальные многосторонние вычисления (Secure Multiparty Computation)
5. Статистические методы и машинное обучение: синтетические данные, трансферное обучение, методы дополнения моделей ИИ, федеративное обучение, имитация поведения, AutoML.

ИДЕАЛЬНАЯ ФОРМУЛА

Стоит отметить, что идеальная формула для решения дилеммы доступа и конфиденциальности представляет собой комбинацию трёх направлений: криптозащиты каналов и среды обмена, продвинутых методов обработки информации и методов снижения «чувствительности» данных.

Каждый из методов обеспечения конфиденциальности данных имеет свои особенности и ограничения. Рассмотрим на примерах.

ПРИМЕРЫ

Гомоморфное шифрование представляет собой метод, позволяющий выполнять вычислительные операции с зашифрованными данными. Он генерирует зашифрованный результат, который при расшифровке соответствует результату операций, как если бы они были выполнены с незашифрованными исходными данными. Широкое использование метода ограничено из-за отсутствия общепринятых стандартов и особенностей гомоморфных схем шифрования, которые обычно поддерживают только один тип операций, а анализ полностью зашифрованных данных значительно медленнее, чем анализ открытых данных. Использование этого метода ограничивается сценариями с узким функциона-

Участникам рынка хочется получать и обогащать данные, но не хочется ими делиться. Поэтому очень важно выстроить необходимые условия для организации обмена от нормативного регулирования до обеспечения конфиденциальности данных

лом или сценариями, где скорость вычислений не критична. Существует также схожая технология — конфиденциальные многосторонние вычисления (SMPC) — это «подраздел» гомоморфного шифрования, который позволяет пользователям вычислять значения из нескольких зашифрованных источников данных. Таким образом, модели машинного обучения могут быть применены к зашифрованным данным, поскольку SMPC используется для большего объема данных. Ограниченное применение этого метода объясняется высокими затратами на настройку и существенной стоимостью обеспечения специальных каналов связи, что делает применение этого метода экономически невыгодным.

Технология дифференциальной конфиденциальности — это криптографический алгоритм, который добавляет слой «статистического шума» к набору данных, что позволяет описывать структуры групп внутри набора данных, сохраняя конфиденциальность отдельных лиц. Добавление «шума» позволяет создать баланс между точностью и конфиденциальностью, что делает этот метод подходящим для анализа общих тенденций, но не для выявления аномалий (таких как мошенничество) или точного сравнения.

Доказательства с нулевым разглашением — это совокупность методов, которые стали применяться специалистами на практике относительно недавно. Эти технологии используют набор криптографических алгоритмов, позволяющих проверять и подтверждать информацию, не раскрывая исходных данных. Доказательства с нулевым разглашением будут играть ключевую роль в развитии технологий распределённых реестров, таких как блокчейн. Методология продолжает развиваться и уже используется в различных областях, включая платежи, инфраструктуру интернета и цифровую идентификацию.

Ещё один интересный метод, наибольшая ценность которого проявляется при большом количестве отдельных источников данных, на-

пример, на смартфонах, устройствах интернета вещей, ноутбуках, — это федеративное обучение. Это метод машинного обучения, который тренирует алгоритм на нескольких удалённых устройствах или серверах без обмена данными между ними, что позволяет минимизировать объём данных, хранящихся на централизованных серверах или в облаке, повышая тем самым конфиденциальность пользователей.

СИНТЕТИЧЕСКИЕ ДАННЫЕ

Не во всех случаях целесообразно применять реальные данные и выстраивать защиту этих наборов данных. Часто для обучения моделей ИИ применяют синтетические данные. Это искусственные данные, сгенерированные для замены реальных данных в различных целях, таких как тестирование, исследование и обучение моделей. Они сохраняют структуру и характеристики исходных данных, не содержат личной информации и могут использоваться для защиты конфиденциальности. Синтетические данные относятся к информации, созданной на основе знаний. Применимость и эффективность синтетических данных напрямую зависит от применяемых алгоритмов, качества и «широты» использованных для генерации исходных данных.

УСПЕШНЫЕ ПИЛОТЫ

Уже сейчас на российском рынке идёт активная работа по проработке подходов безопасного обмена данными и есть примеры успешной реализации таких пилотов. Например, инициатива Газпромбанка и QApp по применению конфиденциальных вычислений, «Криптоанклав» ВТБ, проект Yandex Cloud по применению подходов федеративного обучения для обеспечения конфиденциальности и эффективности при работе с медицинскими данными. Но для организации масштабного и эффективного обмена данными нужно объединить усилия всех ключевых участников рынка: государственных институтов, финансовых организаций, финтехов, технологических компаний и т.д. На площадке Ассоциации ФинТех разработаны предложения по построению экосистемы обмена данными для российского рынка, состоящей из трёх «слоёв»: государственных платформ, коммерческих платформ и однорангового взаимодействия между участниками обмена. Такая структура позволит выстроить процесс обмена данными с учётом потребностей всех заинтересованных сторон — как поставщиков, так и потребителей данных, а также рискоориентированно подойти к защите обрабатываемой информации.

ЭВОЛЮЦИЯ ПЛОХИХ БОТОВ

ИЛИ КАК МЫ БОРЕМСЯ С ФУЛСТЕКАМИ В 2024 ГОДУ



Данила ЧЕЖИН
директор
по развитию
Servicepipe

Четверть века назад был обнаружен первый ботнет, основанный на фишинге и троянах. За это время боты эволюционировали настолько, что порой их крайне сложно отличить от легитимного пользователя. И вредят они множеством способов: парсят цены, крадут уникальный контент, из-за их активности в разы возрастают траты на СМС. На популярных веб-ресурсах ботового трафика иногда даже больше, чем легитимного. К счастью, у проблемы есть решение.

Первый ботнетом принято считать **EarthLink Spammer (2000)**. Он был обнаружен и раскрыт американским интернет-провайдером EarthLink. Ботнет, созданный известным спамером Ханом К. Смитом, успел разослать 1,25 млн электронных фишинговых писем с целью получения конфиденциальной информации: логинов, паролей, номеров банковских карт. В то время на его долю приходилось около 25 % всего интернет-спама.

ЭТАПЫ ЭВОЛЮЦИИ

С 2000 по 2024 год эволюцию плохих ботов можно условно разделить на несколько ключевых этапов, отражающих изменения в технологиях и тактиках злоумышленников.

1. Ранние ботнеты (2000–2005).

В начале 2000-х годов ботнеты были

относительно простыми и основывались на вредоносных программных компонентах, таких как вирусы, трояны и черви, способных заражать компьютеры и объединять их в сети под управлением злоумышленников.

2. Развитие коммерческих ботнетов (2005–2010). У злоумышленников впервые появилась возможность арендовать готовые ботнеты для проведения атак или рассылки спама.

Cutwail (2007). Также известный как Pushdo или Pandex, один из крупнейших и долгоживущих ботнетов, активный с начала 2007 года. Компьютеры на Windows, заражённые трояном Pushdo, превращались в ботнет для фишинга, DDoS-атак и кражи переданных. На пике своей активности Cutwail рассылал 74 млрд писем в день. Ботнет был активен в течение многих лет. И впервые мог быть арендован теми, кто хотел получить доступ к добытой Cutwail конфиденциальной информации.

3. Рост сложности и масштаба (2010–2015). Для управления и координации деятельности ботов стали использоваться распределённые сети. Боты сменили тактику: вместо отправки 1000 запросов с одного IP-адреса они стали отправлять единичные запросы с 1000 разных IP. Ботнеты начали применять различные методы обхода защиты, имитируя браузеры или поведение пользователей.

Gameover Zeus (2011–2014). GOZ был одним из самых известных и разрушительных ботнетов. Он был создан на основе трояна Zeus, который изначально был предназначен для кражи финансовой информации и учётных данных банковских аккаунтов. Gameover Zeus маскировался, используя P2P-сеть для управления и координации заражёнными устройствами, что

усложняло попытки его обнаружения и нейтрализации.

4. Использование криптовалют и майнинг (2015–2020). В это время майнинг криптовалют стал одним из основных способов монетизации ботнетов. Злоумышленники использовали вычислительные ресурсы зараженных устройств для добычи криптовалюты без согласия их владельцев.

Mirai (2016). Один из первых спам-ботов, нацеленных на устройства Интернета вещей. Кроме громких инцидентов, связанных с DDoS-атаками, использовался в том числе для кликфрода (незаконной техники манипулирования стоимостью клика в рекламе). Ботнет остаётся опасным и сегодня, поскольку продолжает мутировать.

5. Развитие искусственного интеллекта и автоматизации (2020–2024). С развитием AI-технологий и машинного обучения злоумышленники стали использовать автоматизированные инструменты для создания и управления ботнетами. Это помогло адаптироваться к защитным мерам и проводить эффективные кибератаки.

Mantis (2022). Ботнет захватывал виртуальные машины и серверы, размещённые в облачных сервисах, а не полагался на устройства Интернета вещей с низкой пропускной способностью. С помощью небольшого парка из 5000 ботов смог провести рекордную DDoS-атаку в пике 26 млн HTTP-запросов в секунду (RPS).

КАК МЫ БОРЕМСЯ С БОТАМИ В 2024 ГОДУ

Мы в Servicepipe сфокусировались на интеллектуальном анализе и фильтрации трафика ещё в 2019 году. В 2021 году представили собствен-

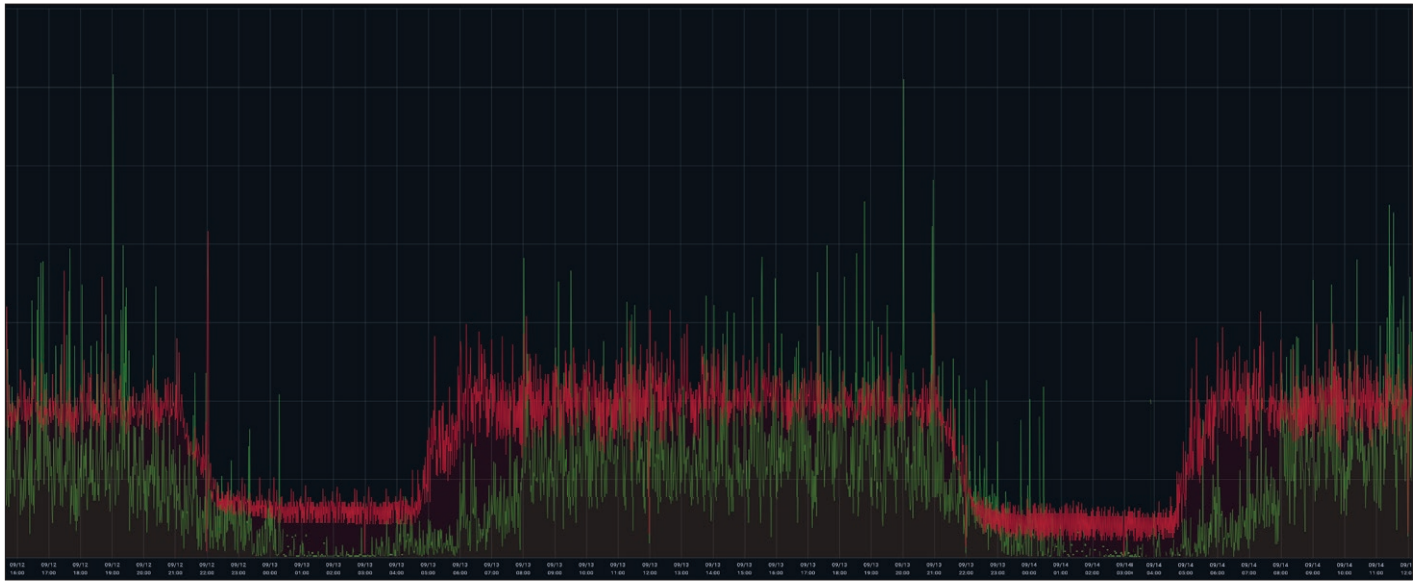


Рисунок 1. Ботнет, имитирующий под профиль пользовательской нагрузки клиента

ную антибот-технология Cybert, которая успешно защищает клиентские веб-ресурсы практически во всех отраслях российской экономики. Таким образом, для нас в Servicepipe борьба с ботами (как и с кибератаками в целом) — это ежедневное противостояние щита и меча.

Эффективная борьба с современными ботами невозможна без быстрой и тонкой фильтрации нежелательного трафика. Для тонкой фильтрации важна высокая точность при определении вредоносности запросов. А точность, в свою очередь, подразумевает предварительную классификацию, поскольку сомнительные запросы зачастую требуют дополнительных проверок перед вынесением вердикта о легитимности.

КАК МЫ КЛАССИФИЦИРУЕМ БОТОВ

При блокировке все автоматизированные угрозы Антибот Servicepipe делит на два основных класса: простую автоматизацию и продвинутых ботов.

Что такое простой бот. Простой бот (англ. Simple Automation) — так мы называем источник автоматизированных запросов, который не пытается маскироваться: «притворяться» браузером, имитировать поведение пользователя, etc.

Что такое продвинутый фулстек-бот. Продвинутый бот (англ.

Advanced Bot, Full-stack Bot) — это программный комплекс, поддерживающий стек браузера, имитирующий модель поведения реального пользователя и в случае необходимости адаптируемый ботоводом для обхода динамически меняющихся правил фильтрации веб-ресурса.

Именно из-за поддержки функционального стека браузера иногда мы называем такую автоматизированную активность фулстек-ботами, или ещё короче — фулстеками.

КАК БОТОВОДЫ МАСКИРУЮТ БОТНЕТЫ

Рассмотрим это на примере популярной ботнет-задачи — парсинга.

Допустим, ботоводу нужно посмотреть, где на ресурсе хранится информация, настроить стандартный HTTP-запрос и понять, из какого поля спарсить цену и название товара. Если веб-ресурс сопротивляется парсингу, то задача усложняется и удорожается. Зачастую в разы и даже в десятки раз.

Вопрос в том, что из обозначенных инструментов и на каком уровне ботоводы используют.

Распространённые методы маскировки ботнета:

- ♦ использование широкого пула IP-адресов из подсетей, откуда идёт легитимный трафик, переключение между IP-адресами;
- ♦ использование анонимных прокси-серверов;
- ♦ низкоинтенсивная активность;

♦ имитация суточной пользовательской активности;

♦ использование движков браузеров без графического интерфейса, так называемых headless-браузеров;

♦ эмуляция пользовательских действий: кликов и движений курсора;

♦ использование инструментов для автоматического прохождения проверок CAPTCHA;

♦ социальный инжиниринг: жалобы в техподдержку об ошибочных блокировках для отключения или снижения строгости фильтрации трафика.

После столкновения с эффективными системами защиты от ботов некоторые ботоводы адаптируют и ещё лучше маскируют свои ботнеты (рис. 1). Соответственно, алгоритмы системы фильтрации тоже должны адаптироваться к смене ботовой тактики.

КАК МЫ БОРЕМСЯ С НАСТОЙЧИВЫМИ БОТОВОДАМИ

Продолжим на примере парсинга.

При высокой ценовой конкуренции любой крупный маркетплейс парсят несколько профессиональных команд. В этих случаях стандартных методов фильтрации, дефолтных настроек Антибота и даже бот-менеджмента зачастую не хватает для блокирования вредоносной активности.

В таких ситуациях мы подключаем дополнительные модули анализа

и защиты, чтобы дообучить Антибота. Эти модули подразумевают более глубокий анализ технических параметров запросов, репутационную оценку легитимности IP-адресов и юзер-агентов, сессионный анализ, особенности прохождения проверок и ряд других мер.

Из названных инструментов собирается и конфигурируется динамически обновляемая модель (содержащая в том числе ML-модули), которая помогает устранить либо понизить ботовую нагрузку до приемлемого уровня ложноположительных срабатываний системы (False Positive). Уровень строгости фильтрации при этом определяется в плотном взаимодействии с заказчиком, чьи веб-ресурсы мы защищаем от ботов.

ХАРАКТЕРНЫЙ ПРИМЕР ДООБУЧЕНИЯ — ОБЕЛЕНИЕ ЧЕРЕЗ КАПЧУ

Обеление — это процесс признания Антиботом сомнительного запроса как легитимного после успешного

прохождения дополнительной проверки (например, CAPTCHA или JS Challenge) и пропуск его до веб-сервера.

Как было сказано выше, некоторые ботнеты активно используют специальные инструменты для автоматического прохождения капчи.

МЯГКИЕ АНТИБОТ-МЕРЫ

Некоторым заказчикам достаточно, чтобы была срезана нагрузка ботнетов, которые не умеют проходить капчу, и они готовы мириться с нагрузкой ботнетов, обелившихся через капчу. Это делается ради того, чтобы дать возможность обелиться любому потенциальному пользователю их ресурса.

СТРОГАЯ ФИЛЬТРАЦИЯ

Бывают обратные ситуации. Например, когда нагрузка ботнетов настолько высока, и риск потери информации настолько неприемлем, что капча отключается, а небольшим числом ошибочно заблокиро-

ванным пользователям предлагается воспользоваться ресурсом, используя стандартные браузеры в стандартных режимах работы.

ЗАКЛЮЧЕНИЕ

Продвинутые фулстек-боты в 2024 году — это широкий набор методов маскировки и оперативной адаптации ботнетов под антибот-системы.

Поэтому эффективное отражение настойчивых ботоводов всё чаще основывается на ситуативном дообучении алгоритмов фильтрации. В Servicepipe за это отвечает целая команда из аналитиков, специалистов по машинному обучению и эксплуатации.

Кроме того, накопленный опыт глубокой аналитики запросов ценен тем, что он помогает нам с высокой точностью отделять запросы вредоносных ботов от легитимных пользователей, действующих на веб-ресурсах хаотично и поэтому подозрительно. Например, при выборе подарка на 8 марта в интернет-магазине.

ОСНОВНЫЕ ПОНЯТИЯ, НЕОБХОДИМЫЕ ДЛЯ ЛУЧШЕГО ПОНИМАНИЯ СОДЕРЖАНИЯ СТАТЬИ

Что такое бот

Бот (англ. bot, сокращение от чеш. robot) — это программа, выполняющая автоматические повторяющиеся действия (скрипты). За счёт автоматизации боты намного быстрее пользователей выполняют заранее настроенные повторяющиеся задачи. Боты обычно заменяют или имитируют поведение пользователей.

Что такое плохой бот

Плохие боты — это программные приложения, выполняющие автоматизированные задачи для целей, противоречащих целям владельца ресурса. Они несанкционированно парсят, то есть собирают авторский контент и данные с сайтов, чтобы переиспользовать их или получить конкурентные преимущества (например, проанализировав цены, уровни запасов продукции, etc.).

Боты используются для скальпинга (получения предметов ограниченного доступа для перепродажи по более высокой цене). Применяются для DDoS-атак, нацеленных на сеть или веб-приложение. Подставляют украденные комбинации логина/пароля пользователей для захвата их учётных записей. Сканируют веб-приложения на уязвимости, злоупотребляют функционалом API и наносят другой вред, описанный в эталонных

списках OWASP Automated Threats to Web Applications и API Security Top 10.

Но одинокий плохой бот малоэффективен. Для достижения своих целей злоумышленники объединяют их в крупный программный автоматизированный комплекс, то есть в ботнет.

Что такое ботнет

Ботнет (англ. словослияние от robot + network) — это группа ботов, автоматизированные действия которых координируются из единого управляющего центра. Если один и тот же бот развёрнут на 1000 серверов — это уже ботнет. Ботнет создаётся и управляется ботоводом.

Кто такой ботовод

Ботовод — человек или группа лиц, использующие ботнет для извлечения собственной выгоды через нелегитимные запросы к сайту, мобильному приложению или API.

Разработчики и владельцы ботнета тратят на его поддержание материальные, временные и интеллектуальные ресурсы, чтобы в результате получить ещё больше ресурсов.

ЧТО НЕ ТАК С ПЕРИМЕТРОМ?

ПРАКТИЧЕСКИЕ НЕДОСТАТКИ БЕЗОПАСНОСТИ ВНЕШНЕГО ПЕРИМЕТРА В 2024 ГОДУ



Давид ОРДЯН
генеральный
директор ООО
«METASKAN»



Владимир СОЛОВЬЕВ
руководитель
направления
внедрения
средств защиты
АО «ДиалогНаука»

На сегодняшний день в России не существует публично распространённых стандартов и практик обеспечения информационной безопасности внешнего периметра. При этом проникновение через внешний периметр остаётся одним из наиболее простых и часто используемых способов проникновения в корпоративную инфраструктуру организаций. В этой статье мы рассмотрим общие подходы, а также активно используемые злоумышленниками векторы атак, которые всё ещё игнорируются большинством СЗИ.

ТИПОВОЙ СОСТАВ ВНЕШНЕГО ПЕРИМЕТРА. ВЕКТОРЫ АТАКИ

Чем больше организация, тем больше изменений в её периметре происходит каждый день. Это могут быть релизы прикладного или системного ПО, обновление прошивок оборудования, новые открытые порты или целые новые VM.

Самым простым вектором атаки являются сервисы, опубликованные в интернете по ошибке, — базы данных, самописные административные панели, сервисы IC, хранилища документов.

Многие современные веб-приложения используют технологии, которые не были популярны или не существовали ещё 5 лет назад. Один из самых типичных и при этом слабезащищённых векторов атаки — уязвимые API. Лучшей практикой тут будет загрузка API-спецификации в сканер уязвимостей. Наличие API-спецификации делает процесс поиска уязвимостей надёжнее, чем классический обход сайта пауком, ведь система поиска уязвимостей заранее знает о существовании каждого URL-адреса и каждого параметра в приложении.

Краеугольным камнем безопасности периметра является уверенность в том, что назначение каждого сервиса на внешнем периметре известно отделу ИБ и каждый опубликованный сервис прошёл процедуру приёма.

При исследовании зарубежных рынков мы общались с отделами ИБ Google и Amazon, и даже у таких гигантов есть проблема с тем, чтобы ответить на вопросы: «Что нам принадлежит?» и «Где границы нашего периметра?» (Возьмите на заметку, если планируете исследовать эти периметры.)

Наиболее простые сканеры уязвимостей попросят вас загрузить в них список проверяемых доменов или IP-адресов. Более продвинутые ре-

шения умеют проводить автоматизированную разведку всего интернета и собирать данные с помощью брутфорса dns, скрапинга поисковых систем, интеграции с Censys/Shodan, собирать данные о сертификатах из системы certificate transparency или других сторонних источников. Но все эти способы ограничены своей реализацией, и технически невозможно обнаружить доменное имя, созданное из случайного набора символов и не имеющее выписанных сертификатов или сетевых баннеров. Единственным гарантированным источником данных на вход вашей сканирующей системе может служить конфигурационный файл вашего DNS-сервера, который требуется не только выгрузить с сервера, но ещё и сопоставить его с действительностью, «как это есть» на самом деле, и только потом уже импортировать в сканирующую систему. В этом случае может помочь автоматизация процесса обновления списка реальных доменов и IP-адресов организации на стороне сканирующей системы с помощью интеграции системы по API с существующими СЗИ. Данный подход используется в решениях класса ASM (Attack Surface Management) — управление поверхностью атаки внешнего периметра. Metascan — отечественный ASM, позволяющий автоматизировать процесс поиска новых активов организации и поиска уязвимостей на них.

СКОРОСТЬ РАБОТЫ

Современные злоумышленники далеко ушли от необходимости кропотливого ручного сканирования каждого внешнего сервиса и узла. В мире киберпреступности активно применяются атакующие пайплайны,



в которых на вход подаются данные из Censys/Shodan или других глобальных сканеров, а далее происходит моментальная эксплуатация конкретного сервиса с конкретным эксплойтом. В этом случае нет возможности заблокировать злоумышленника за сканирование периметра или неудачные попытки атаки. Противостоять этому может только раннее обнаружение уязвимостей. И задача современного специалиста ИБ — обеспечить себе максимум времени на устранение обнаруженной уязвимости.

К 2024 году парадигма еженедельных/ежемесячных сканов является скорее опасной, чем полезной, так как создаёт ложное чувство защищённости: уязвимости появляются намного чаще и быстрее. При этом большинство зарубежных вендоров переходят на концепцию Continuous Vulnerability Scanning, в которой сканирование каждого домена или IP-адреса происходит несколько раз в день.

Metascan имеет обширную распределённую сеть глобальных сканеров по всей сети Интернет, что позволяет иметь полную и актуальную информацию по всем активам внешнего периметра в кратчайшие сроки.

ПОЛНОТА И КАЧЕСТВО

Многие решения по поиску уязвимостей хороши, но имеют узкую направ-

ленность. Nessus — отличный сканер для системных сервисов, но он практически беспомощен в поиске веб-уязвимостей. Acunetix — отличное решение для поиска веб-уязвимостей, но в нём отсутствуют даже механизмы сканирования портов. Помимо этого, у нас есть сетевое оборудование, сервера с интерфейсами IPMI и ILO, CMS Bitrix и 1C, IP-камеры и системы их управления, проприетарные решения от отечественных вендоров, использующих собственные протоколы, которые не определяются популярными сканерами портов, но при этом имеют учётные записи со стандартными паролями и др.

Metascan имеет более 30 модулей и движков проверок, которые могут быть запущены в любое время с необходимой частотой запуска. Модули можно кастомизировать и добавлять собственные. В качестве языка разработки модулей используется Python.

METASCAN — ОБЛАЧНЫЙ L3-L7- СКАНЕР УЯЗВИМОСТЕЙ С ЭКСПЕРТНЫМ СОПРОВОЖДЕНИЕМ

Metascan позволяет решать следующие проблемы ИБ:

- ♦ большое количество ложных срабатываний;
- ♦ низкая скорость работы сканеров уязвимостей;

♦ отдел ИБ перегружен текущей и не знает, как работать с найденными уязвимостями;

♦ узкая специализация сканеров периметра.

И если вы не можете ответить хотя бы на один следующий вопрос, мы рекомендуем вам задуматься об использовании решения Metascan:

♦ Вам известны все доменные имена и IP-адреса вашей организации?

♦ Вам известно назначение каждого сетевого порта и то, с каким бизнес-сервисом этот порт связан?

♦ Поиск уязвимостей происходит на ежедневной основе или чаще?

♦ Используются ли движки сканирования, умеющие находить уязвимости в отечественном ПО (Bitrix, 1C Предприятие, R7 Office, системы видеонаблюдения, СКУД и др.)?

Для веб-приложений используются ли движки, поддерживающие сканирование на основе API, умеющие искать уязвимости в websocket и других современных протоколах?

Решение Metascan не привязано к человеческому фактору и может сканировать активы периметра постоянно, способно отслеживать изменения защищённости периметра 24 часа 7 дней в неделю, обнаруживать уязвимости сетевого оборудования и системных сервисов, а также проводить инвентаризацию активов компании.

«НУЛЕВОЕ ДОВЕРИЕ»: КЛЮЧЕВЫЕ ПРИНЦИПЫ...

...И ПРИМЕНЕНИЕ В СОВРЕМЕННОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



Евгения ЛАГУТИНА

руководитель группы по сопровождению проектов внедрения систем мониторинга ИБ и SOC-сервисам, «Лаборатория Касперского»

Всё в этом мире уже придумано. То, что сейчас преподносится как новинка, часто является переосмыслением давно существующих подходов, техник и решений благодаря усилиям маркетинговых кампаний. Это относится и к подходам к обеспечению информационной безопасности в компании. Например, несмотря на современную популярность рискориентированного подхода под различными названиями, его суть не изменилась с момента появления.

ПОТЕРЯ ОБЪЕКТИВНОСТИ

Основой данного подхода является определение критичности активов, что подразумевает экспертную оценку. А это, в свою очередь, приводит к потере объективности. В итоге при внедрении рискориентированного подхода в ИБ мы стремимся сконцентрироваться в первую очередь на недопущении критичных событий, но рискуем упустить из виду другие

критичные, но недооценённые в силу субъективности риски.

Поэтому, безусловно, имеет смысл постараться минимизировать влияние экспертной субъективности. Например, считая критичным всё и виноватыми всех по умолчанию. Для этого можно обратиться к существующим методологиям, которые за годы своего существования подтвердили свою актуальность и универсальность.

КОНЦЕПЦИЯ ZERO TRUST

Концепция Zero Trust, или «нулевого доверия», пересматривает рабочие процессы на основе отсутствия доверия к любому пользователю перед началом каждой операции. Как и рискориентированный подход, Zero Trust сформулирован достаточно давно, но представляется более применимым в современных условиях. Во многих исследованиях, проведённых «Лабораторией Касперского», мы обнаруживаем, что часто самые разрушительные атаки связаны с риска-

ми, которые не были учтены просто потому, что вектор атаки совершенно новый и связан, например, с развитием технологий, используемых в инфраструктуре.

ПРИНЦИПЫ ZERO TRUST

О том, что собой представляет данная концепция, как она реализуется и насколько применима в условиях современного ИТ-ландшафта, сказано довольно много, поэтому тут приведём только принципы из NIST SP 800-207 — Zero Trust Architecture, на которых основана концепция:

1. Принцип «нулевого доверия»: ни одна сущность в сети не считается автоматически доверенной. Все запросы и доступы должны быть проверены и авторизованы независимо от их источника или положения в сети.
2. Микропериметры: рекомендуется создание микропериметров для





сегментации сети на мелкие и контролируемые зоны. Это позволяет ограничить доступ и уменьшить поверхность атаки.

3. Многофакторная аутентификация: использование нескольких методов аутентификации (например, пароль и биометрические данные) для повышения безопасности.

4. Постоянный мониторинг: важность непрерывного мониторинга сети и активности пользователей для обнаружения подозрительных действий или аномалий.

5. Политики доступа: разработка и применение строгих политик доступа, определяющих условия предоставления доступа к ресурсам сети.

6. Шифрование: использование шифрования для защиты данных в пути и в покое.

7. Управление идентификацией и доступом (IAM): использование системы управления идентифика-

цией и доступом для эффективного контроля над правами доступа пользователей.

8. Сегментация сети: разделение сети на сегменты с использованием сетевых механизмов и политик безопасности.

9. Автоматизация и оркестрация: использование автоматизации для более эффективного и надёжного управления безопасностью.

10. Анализ поведения и обнаружение угроз: использование технологий и методик для обнаружения подозрительного поведения и предотвращения угроз.

11. Автоматическая реакция на угрозы: реагирование на обнаруженные угрозы автоматически или с минимальным участием человека.

12. Использование облачных сервисов: при необходимости использования облачных сервисов учитывать контекст архитектуры Zero Trust.

13. Обучение персонала: обучение сотрудников и периодическое обновление их знаний в области информационной безопасности.

14. Управление рисками: оценка и управление рисками, связанными с безопасностью сети и ресурсов.

15. Непрерывное обновление и патчинг систем: регулярное обновление и установка патчей для операционных систем и приложений.

16. Отслеживание и аудит активности пользователей: мониторинг и регистрация активности пользователей для обеспечения прозрачности и отслеживания потенциальных нарушений безопасности.

17. Защита от вредоносного программного обеспечения: применение методов и технологий для предотвращения и обнаружения вредоносного программного обеспечения.

18. Управление конфиденциальностью и целостностью данных: за-

щита данных от несанкционированного доступа и внесения изменений.

19. Резервное копирование и восстановление данных: регулярное создание резервных копий данных и возможность восстановления в случае сбоев или атак.

20. Мониторинг и защита конечных точек: обеспечение безопасности устройств и конечных точек, включая мобильные устройства и компьютеры.

ПРЕИМУЩЕСТВА МИНИМИЗАЦИИ

Перечисленные принципы можно разделить на те, которые относятся к организации процессов, и те, которые реализуются благодаря использованию соответствующих средств защиты информации (СЗИ). Если мы говорим о необходимости выбора СЗИ, то сталкиваемся с рядом сопутствующих сложностей. Одна из основных — множество вариантов решений от разных поставщиков. И тут хочется отметить, что найти единого поставщика всех средств защиты совсем непростая задача, но при этом минимизация количества производителей будет иметь значительные преимущества.

♦ **Простота администрирования.** Использование меньшего количества поставщиков средств защиты информации упрощает процесс управления и обслуживания ИБ-системы. Вместо того чтобы иметь дело со множеством различных интерфейсов и настроек, администраторы могут сосредоточиться на работе с ограниченным числом интегрированных решений, в идеале — в единственном интерфейсе. Это позволяет сэкономить время и усилия, а также уменьшить вероятность ошибок в конфигурации систем ИБ.

♦ **Нативная интеграция.** При использовании средств защиты от одного поставщика повышаются шансы на нативную интеграцию между СЗИ. Это позволяет реализовать более гармоничное взаимодействие между различными модулями и создать единое целое для более надёжной защиты информации. Благодаря интеграции данные могут легко передаваться между разными средствами защиты, обе-

спечивая быстроту реагирования на угрозы безопасности.

♦ **Упрощение обучения и поддержки.** Обучение администраторов и аналитиков и поддержка систем становятся более простыми и эффективными. Интерфейсы систем и логика их работы схожи, что способствует более быстрому освоению необходимых навыков и повышает производительность. Кроме того, становится возможным упрощение поддержки благодаря более чёткому пониманию единого процесса обслуживания и взаимодействия средств защиты.

♦ **Экономия ресурсов.** Объединение закупок и лицензий может обеспечить лучшие условия для получения скидок или объёмных лицензий. Это позволяет снизить расходы на приобретение и поддержку средств защиты информации. Кроме того, уменьшение количества используемых СЗИ от разных производителей способствует более эффективному использованию ресурсов, таких как время и усилия, необходимые для управления системами и их обслуживания.

РЕШЕНИЕ КЛАССА XDR

Один из способов, помогающих сформировать набор решений от минимального количества производителей, — выбрать решение класса XDR, которое объединяет в себе различные технологии и платформы для обеспечения комплексной и эффективной защиты организации. Решения класса XDR позволяют автоматизировать процессы обнаружения и реагирования на угрозы, а также предоставляют комплексный обзор всей сетевой инфраструктуры.

KASPERSKY SYMPHONY XDR

Мы в «Лаборатории Касперского» уже более двух лет имеем в своём портфолио решение Kaspersky Symphony XDR, в состав которого входят многие зрелые решения для обеспечения всесторонней защиты ИТ-инфраструктуры:

♦ автоматическая защита конечных точек (физических, мобильных и виртуальных) от массовых угроз;

♦ передовое обнаружение сложных угроз на уровне конечных точек и реагирование на них;

♦ детектирование с помощью передовой песочницы и реагирование на обнаружения;

♦ защита электронной почты и веб-трафика;

♦ глубокий анализ сетевого трафика и реагирование на уровне шлюзов;

♦ комплексный мониторинг и корреляция событий ИБ, встроенный модуль ГосСОПКА;

♦ унифицированный интерфейс представления информации, единый граф расследования, оркестрация и управление инцидентами;

♦ платформа повышения киберграмотности сотрудников;

♦ управление аналитическими данными о киберугрозах и встроенные потоки данных.

При этом есть и возможность подключения сторонних различных ИБ-систем.

БОЛЬШЕ ПОЛЬЗЫ — ЭТО ВАЖНО!

Если оценить степень покрытия, то получается, что перечисленных возможностей Kaspersky Symphony XDR достаточно, чтобы выполнить больше половины принципов Zero Trust, упомянутых выше. Получается, что в едином интерфейсе управления и мониторинга объединяется большая часть средств защиты информации, необходимых для обеспечения высокого уровня защищённости инфраструктуры. И при этом даёт доступ ко всем преимуществам единого производителя.

Фактически независимо от того, на какой концепции основываться при построении ИБ, рискориентированной или Zero Trust, все перечисленные плюсы от формирования набора решений от минимального количества производителей остаются актуальными. Соответственно, комплексный подход, который есть в решениях класса XDR, актуален в любом случае. Но на наш взгляд, его применение при реализации концепции Zero Trust приносит наибольшую пользу в киберзащите организаций.

ARINTEC СПЕШИТ НА ПОМОЩЬ

АУДИТ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ
НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ ЦБ РФ:
ЧТО НОВОГО?



**Олег
НЕСТЕРОВСКИЙ**
заместитель
директора
департамента
по консалтингу
и аудиту ARintec

Мы выступаем в качестве внешних ИБ-аудиторов банков и на практике нередко сталкиваемся с тем, что ответственные сотрудники, зная нормативную правовую базу регулирования направления ИБ, не знают, каким образом корректно обосновать, предоставить доказательства выполнения той или иной организационной или технической меры. Не понимают важность регламентации всех мер, в том числе технических, а также как учесть те или иные изменения законодательства.

Между тем, в условиях постоянно-го изменения геополитической обстановки требования регуляторов Банка России, ФСТЭК России, ФСБ России к защите информации ограниченного доступа ужесточаются, и это оправдано. С каждым днем совершенствуются механизмы реализации кибератак, мошеннических действий, что требует компенсационных мер в виде дополнительных требований по защите информации.

В этой статье поделюсь информацией о наиболее значимых, нововведениях в этой области, часть из которых вступит в действие уже с 1 сентября 2024 года, а также расскажу, какую пользу можно извлечь из внешнего аудита.

ЧТО ТАКОЕ АУДИТ

Напомню, что под «аудитом» понимается систематический, независимый и документируемый процесс получения свидетельств и объективного их оценивания с целью установления степени выполнения согласованных критериев аудита.

Аудит информационной безопасности позволяет проверить выполнение требований нормативных правовых актов или обоснованность и защищенность применяемых решений. В первом случае он обязателен, его игнорирование может повлечь наложение штрафов, приостановление деятельности и не только. Во втором носит добровольный характер.

Внешний аудит позволяет банкам спокойно проходить проверку в ЦБ РФ, ограждает от предписаний, штрафов и других мер ответственности. С ним вы минимизируете риски финансовых и репутационных потерь, лучше понимаете узкие места в системе защиты и знаете, какие решения надо предпринять, чтобы усовершенствовать систему защиты информации.

В настоящее время для банков крайне актуальными можно считать следующие направления в области защиты информации ограниченного доступа, а именно:

- ♦ приведение банков в соответствие требованиям ЦБ РФ;
- ♦ приведение объекта КИИ в соответствие требованиям 187-ФЗ.

ПРИВЕДЕНИЕ БАНКОВ В СООТВЕТСТВИЕ ТРЕБОВАНИЯМ ЦБ РФ

Требования доверия, уровни защиты, сроки внедрения нацстандартов. В первую очередь следует остановиться на введении в действие

28.02.2024 Центральным банком РФ стандарта СТО БР БФБО-1.8-2024 «Безопасность финансовых (банковских) операций». Обеспечение безопасности финансовых сервисов при проведении дистанционной идентификации и аутентификации. Состав мер защиты информации».

В стандарте установлены состав и содержание мер для обеспечения доверия к результатам идентификации и аутентификации клиентов — получателей услуг при дистанционном предоставлении поставщиками финансовых продуктов и услуг в целях реализации требований Банка России на технологическом участке идентификации, аутентификации и авторизации клиентов при осуществлении банковской деятельности, деятельности в сфере финансовых рынков.

Введение в действие данного стандарта является естественным продолжением, с одной стороны, принятия Федерального закона от 29.12.2022 № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации», с другой — действующего национального стандарта РФ «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности».

Если последний рассматривает требования к доверию продуктов ИТ (программного обеспечения), то вновь

введенный стандарт определяет требования доверия (состав и содержание мер защиты информации) уже к процедурам (процессам), а именно к:

- ♦ процессу идентификации;
- ♦ делегированию идентификации;
- ♦ процессу аутентификации;
- ♦ процессу аутентификации при использовании отдельных аутентификаторов;
- ♦ делегированию аутентификации.

В реальности процесс приведения процедур ИБ в соответствие предусматривает комплексный подход, включающий аудит ИБ, в результате которого в том числе приходит понимание трактовки требований Банка России, и постаудитную помощь в реализации мер защиты.

Другим знаковым нормативным документом 2024 года стали «Методические рекомендации по управлению риском информационной безопасности и обеспечению операционной надежности» (утв. Банком России 21.03.2024 № 7-МР).

Этот документ, во-первых, устанавливает в рекомендательной форме уровни защиты (управления риском информационной безопасности и обеспечения операционной надежности), которые должны реализовать кредитные и некредитные финансовые организации. В то же время, несмотря на рекомендательный характер, по результатам анализа хода проверок со стороны Банка России, рекомендуемые положения, требования контролируются на одном уровне с обязательным. Поэтому рекомендательный характер в данном случае имеет место быть только условно.

Во-вторых, определяет сроки внедрения национальных стандартов в сфере обеспечения операционной надежности ГОСТ Р 57580.3–2022 и ГОСТ Р 57580.4–2022.

Так, для банков, размер активов которых составляет 500 миллиардов рублей и более на начало текущего отчетного года установлен срок до 31 декабря 2025 года; для остальных кредитных организаций — до 31 декабря 2026 года.

Таким образом, можно отметить, что совокупность требований регулятора в полной мере затрагивает бан-

Высказывается мнение, что в законодательство будут внесены дополнения, и тогда любое предприятие, которому на правах собственности, аренды или на ином законном основании принадлежат ИС, ИТКС, АСУ ТП, станет субъектом КИИ

ковский сектор, предписывая уже сточения требований как к защите информации в целом, так и, в частности, к использованию доверенных сред/процедур идентификации и аутентификации.

ПРИВЕДЕНИЕ ОБЪЕКТА КИИ В СООТВЕТСТВИЕ ТРЕБОВАНИЯМ 187-ФЗ

Импортозамещение, доверенные ПАК на значимых объектах КИИ.

Важность защиты критической информационной инфраструктуры РФ обусловлена тем, что нарушение ее функционирования может негативно сказаться на некоторых аспектах деятельности государства, в том числе внешнеэкономической. А все банки — априори субъекты КИИ. Ужесточение требований законодательства в области защиты объектов КИИ призвано обеспечить бесперебойное функционирование системы защиты информации вне зависимости от мировой обстановки, санкций и т.п.

Сейчас, когда из России ушли некоторые западные производители, в т.ч. Cisco, Motorola и т.п., многие компании столкнулись с отсутствием альтернатив в используемых технических и программных средствах. Именно на то, чтобы исключить возникновение подобных ситуаций в будущем, и направлены текущие изменения законодательства в области защиты объектов КИИ, как наиболее важных для жизнедеятельности государства информационных систем.

Остановимся на Указе Президента РФ от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации». Его требования касаются всех субъектов КИИ

без исключения. Мало того, ведущие специалисты в области защиты информации предполагают, что объекты КИИ присутствуют практически во всех сферах жизнедеятельности. Высказывается мнение, что в законодательство будут внесены дополнения, и тогда любое предприятие, которому на правах собственности, аренды или на ином законном основании принадлежат ИС, ИТКС, АСУ ТП, станет субъектом КИИ.

Согласно п. 6 Указа, с 1 января 2025 г. запрещается использовать средства защиты информации из недружественных государств, производители которых находятся под юрисдикцией таких государств, прямо или косвенно подконтрольные им либо аффилированные с ними.

Пока непонятно, каким образом п. 6 Указа будет реализовываться, поскольку часть используемых субъектами КИИ ИС, ИТКС, АСУ ТП изначально зарубежного производства. И интеграция тех или иных отечественных средств защиты информации оказывается под огромным вопросом. Особенно если речь идет, например, об авиационной тематике. Системы самолетов в ряде случаев индивидуальны. Часть из них не поддерживается ввиду санкций. И каким образом вводить, например, отечественные системы идентификации/аутентификации в такие системы — большой вопрос.

Также с 14 ноября 2023 года вступило в действие Постановление Правительства РФ № 1912 «О порядке перехода субъектов критической информационной инфраструктуры Российской Федерации на преимущественное применение доверенных программно-аппаратных комплек-

КАЛЕНДАРНЫЙ ПЛАН

	Вид работы	Периодичность	Самооценка	Требования к внешнему подрядчику
98-ФЗ	Исполнение нормативных требований по защите коммерческой тайны	—	Да	—
152-ФЗ	Исполнения требования по защите ПДн	1 раз в 3 года	Да	Лицензия ФСТЭК России
187-ФЗ	Исполнение нормативных требований по защите КИИ	1 раз в 5 лет	Да	Лицензия ФСТЭК России
Положения Банка России (683-П, 719-П, 757-П, 802-П)	Анализ исполнения требований положений Банка России	—	Да	Лицензия ФСТЭК России
	Проведение оценки соответствия защиты информации по ГОСТ Р 57580	1 раз в 2 года*	Нет	
	Тестирование на проникновение и анализ уязвимостей	1 раз в год**	Нет	
ГОСТ Р ИСО/МЭК 27001	Оценка исполнения требований к системе менеджмента (управления) информационной безопасности	—	Да	—

* Для 757-П 1 раз в год для усиленного уровня защиты и 1 раз в 3 года для стандартного уровня защиты
** Для 802-П тестирование на проникновение не требуется

ПРЕДЛОЖЕНИЕ ПО АУДИТУ ОТ КОМПАНИИ ARINTEG

98-ФЗ	- Обследование компании на наличие информации, составляющей коммерческую тайну. - Разработка проектов документов, необходимых для ввода и поддержания режима коммерческой тайны.
152-ФЗ	- Сбор и анализ информации о процессах обработки персональных данных и их защите. - Разработка модели угроз и нарушителей. - Разработка ОРД, включая уведомление в РКН, и актуализация информации в РКН. - Разработка проектов согласий на обработку ПДн. - Предоставление рекомендаций по процессам обработки и защиты ПДн.
187-ФЗ	- Выявление критических процессов и подготовка перечня объектов КИИ, подлежащих категорированию, для предоставления в уполномоченный федеральный орган исполнительной власти (ФСТЭК России). - Категорирование объектов КИИ в соответствии с требованиями законодательства. - Формирование плана работ, включающего в себя организационные и технические меры по выполнению № 187-ФЗ и созданию системы безопасности значимых объектов КИИ. - Оценка мер защиты для значимых объектов КИИ на соответствие установленным требованиям. - Предоставление рекомендаций по построению системы безопасности значимых объектов КИИ и выполнения требований по обеспечению безопасности значимых объектов КИИ. - Разработка модели угроз и нарушителей.
Положения Банка России	Оценка выполнения требований положений Банка России в соответствии с методическими рекомендациями Банка России от 02.11.2022 г. № 12-МР «По расчету значений показателей оценки выполнения требований к технологическим мерам защиты информации и прикладному программному обеспечению автоматизированных систем и приложений в целях составления отчетности об оценке выполнения требований к обеспечению защиты информации».
ГОСТ Р 57580	- Предварительная оценка соответствия требованиям ГОСТ Р 57580.1-2017 с предоставлением организационно-технических рекомендаций по улучшению соответствия требованиям ГОСТ Р 57580.1-2017. - Итоговая оценка соответствия по методике ГОСТ 57580.2-2018.
ГОСТ Р ИСО/МЭК 27001	- Оценка соответствия системы менеджмента (управления) информационной безопасности требованиям ГОСТ Р ИСО/МЭК 27001. - Предоставление рекомендаций по приведению в соответствие СУИБ требованиям ГОСТ Р ИСО/МЭК 27001. - Подготовка проектов ОРД в области ИСО/МЭК 27001.

сов на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации».

В соответствии с рассматриваемым Постановлением переход субъектов КИИ РФ на преимущественное применение доверенных ПАК на принадлежащих им значимых объектах КИИ РФ осуществляется до 1 января 2030 года. Кроме того,

с 1 сентября 2024 года вступает запрет на использование недоверенных ПАК, если они приобретены после указанной даты.

Данное Постановление необходимо рассматривать совместно с Постановлением Правительства РФ от 22.08.2022 № 1478 «Об утверждении требований к программному обеспечению, в том числе в составе программно-аппаратных комплек-

сов, используемому органами государственной власти, заказчиками, осуществляющими закупки в соответствии с Федеральным законом «О закупках товаров, работ, услуг отдельными видами юридических лиц» (за исключением организаций с муниципальным участием), на принадлежащих им значимых объектах КИИ РФ, Правил согласования закупок иностранного программного обеспечения, в том числе в составе программно-аппаратных комплексов, в целях его использования заказчиками.

Рассмотренные документы – звенья одной цепи, направленные на обеспечение безопасности объектов КИИ вне зависимости от санкций, которым может быть подвергнута Российская Федерация.

С ARINTEG ВЫ ЛЕГКО ПРОЙДЕТЕ ПРОВЕРКИ

ARinteg – один из ведущих системных интеграторов в сфере информационной безопасности в России. Наши специалисты обладают большим опытом в области аудита и консалтинга, мы регулярно проводим оценки соответствия требованиям регуляторов в области информационной безопасности: 10–15 крупномасштабных аудитов в год.

В части аудита рассмотренных направлений ARinteg готов предложить:

- ♦ оценку выполнения требований положений Банка России;
- ♦ оценку соответствия требованиям ГОСТ Р 57580.1–2017 (включая методику ГОСТ Р 57580.2);
- ♦ пакет услуг по подготовке к категорированию объектов КИИ, включая рекомендации по защите информации, разработку моделей угроз, а также оценку соответствия требованиям регуляторов, и не только это.

Специалисты ARinteg понимают, что аудит – это не самоцель, но все-таки его необходимо проводить с требуемой периодичностью.

ARinteg выполняет весь комплекс работ по защите информации в соответствии с требованиями регуляторов: от аудита до поставки, внедрения и технической поддержки полноценной системы защиты информации ограниченного доступа.

ИБ В ОБЛАКЕ: ПОИСК КОМПРОМИССА

КАК БАНКИ МОГУТ ЗАЩИТИТЬ ВЕБ-ПРИЛОЖЕНИЯ ОТ КИБЕРАТАК В 2024 ГОДУ



Кирилл САЛОВ
директор
по развитию
в NGENIX

УДОБНЫЕ ВЕБ-ПРИЛОЖЕНИЯ — ВАЖНЫЙ ФАКТОР КОНКУРЕНТНОЙ БОРЬБЫ

Сегодня ведущие банки делают ставку на доступные, производительные и удобные веб-приложения. Публичный интерфейс для взаимодействия пользователей с банковскими услугами нужен им, чтобы конкурировать за молодую аудиторию, внедрять инновации и выпускать новые цифровые продукты.

При этом веб-приложения существуют в парадигме публичного интернета, который полон угроз. Обеспечение безопасности приложений — важнейшая задача для ИТ- и ИБ-команд, при этом им необходимо найти способ не жертвовать скоростью разработки новых продуктов или доступностью приложения для огромной и географически распределенной аудитории пользователей.

По нашей последней статистике, публичными облаками полноценно пользуются только 8% банков из российского рейтинга топ-100, тогда как для глобального списка банков топ-100 этот показатель составляет 44%

КАКИМ УГРОЗАМ ПОДВЕРЖЕНЫ БАНКОВСКИЕ ВЕБ-ПРИЛОЖЕНИЯ?

Финансовый сектор продолжает быть одной из ключевых целей для злоумышленников. В 2023 году банки и финансовые учреждения всё еще оставались в топе самых атакуемых сегментов: например, ИБ-компания Solar в 2023 году зафиксировала 6,8 тыс киберинцидентов, направленных на финансовые организации и связанных с попытками взлома. Доля нацеленных на банки DDoS-атак, составила, по различным данным, от 37% до 40% от общего количества в 2023 году, а их средняя продолжительность достигла 42 часов.

Основными угрозами для веб-приложений банков в 2024 году являются:

♦ DDoS-атаки на уровень приложений (L7).

Их мощность многократно выросла за 2 года и может достигать миллионов запросов в секунду. Причины — действия несистемных хактивистов, использующих не связанные между собой IP-адреса, появление более крупных ботнетов, а также найденная весной 2023 года уязвимость в наиболее распространенном протоколе HTTP/2, позволяющая проводить объемные атаки на прикладном уровне.

♦ Направленные бот-атаки.

В течение последних 2–3 лет борьба с ними стала насущной задачей для любого веб-сайта, который имеет сложную бизнес-логику и предоставляет в публичном интернете интерфейсы, активно обращающиеся к API. Боты используются для брутфорс-атак, направленных на взлом систем и кражу пользовательских данных, а также в различных сценариях эксплуатации логики веб-приложения. Например, так называемый «SMS-бомбинг», при котором боты инициируют отправку SMS для аутентификации на фиктивный номер, может стоить организации нескольких миллионов рублей в месяц.

ПОЧЕМУ БАНКИ НЕ ДРУЖАТ С ОБЛАКАМИ?

Преимущества облаков в части защиты публичных веб-ресурсов неоспоримы:

1. Облачные инфраструктуры обладают необходимой эластичностью и запасом емкости, чтобы выдержать любую непрогнозируемую нагрузку — легитимную и нелегитимную. Это позволяет эффективно использовать ресурсы при масштабировании и избежать затрат, связанных с закупкой и поддержкой инфраструктуры «под рост нагрузки», которая может большую часть времени простаивать.

2. Специализированные платформы бесшовно интегрируют множество функций, нужных для доступности и безопасности веб-ресурса, — это экономически выгодная и более управляемая модель, лишенная рисков интеграции и «серых зон» ответственности.

3. Облака предоставляют среду для быстрого тестирования продуктовых гипотез и реализации новых цифровых продуктов, сокращая time-to-

market и повышая позиции банков в конкурентной борьбе.

Однако ИТ-команды банковского сектора работают в строгих рамках, задаваемых регулятором, и не всегда могут воспользоваться преимуществами публичных облачных платформ для защиты от веб-атак. По нашей последней статистике, публичными облаками полноценно пользуются только 8% банков из российского рейтинга топ-100, тогда как для глобального списка банков топ-100 этот показатель составляет 44%.

С точки зрения Центрального банка РФ, веб-технологии должны соответствовать 152 ФЗ, ГОСТ Р 57580, также многие финансовые организации ориентируются на соответствие международному стандарту PCI DSS. При этом актуализация стандартов информационной безопасности, задаваемых регулятором, не может происходить так же быстро, как появление новых технологий.

В этом случае ИБ-специалисты, работающие в сфере банков и финансов, полагаются на выстраивание защищенного контура внутри собственной инфраструктуры или частного облака и использование наложенных средств безопасности. К сожалению, такая архитектура отличается высокими капитальными и эксплуатационными расходами, требует наличия в штате квалифицированных ИБ-кадров, имеющих компетенции в каждом стеке технологий или виде СЗИ, и не способна к быстрому масштабированию под колебания нагрузки.

КАК ЭФФЕКТИВНО ЗАЩИТИТЬ ВЕБ-ПРИЛОЖЕНИЯ В 2024 ГОДУ?

Российские банки ищут компромиссы, позволяющие сохранить соответствие стандартам безопасности и воспользоваться преимуществами облаков. Эти подходы имеют свои плюсы и минусы.

Некоторые банки используют публичные облака, не расшифровывая свой HTTPS-трафик внутри инфраструктуры провайдера. Это, с одной стороны, упраздняет проблему с

блюдением регуляторных стандартов, но, с другой стороны, сводит на нет преимущества публичных облаков. При таком подходе провайдер анализирует не содержимое запроса, а содержимое логов, получаемых с бэкенда банка. При массированных атаках создается высокая нагрузка на ИТ-инфраструктуру банка, повышается объем исходящего трафика — таким образом, экономическая эффективность облачной модели сходит на нет, а при особо мощной атаке бэкенд может не справиться с нагрузкой. Мировые лидеры, задающие стандарты в области защиты веба (например, Cloudflare и Akamai), не рекомендуют подобный подход и считают его неэффективным и даже опасным для доступности веб-приложений.

Второй способ воспользоваться преимуществами публичных облачных платформ — это архитектурно разделить приложение: например, вывести под отдельный поддомен нечувствительные данные, к которым не применимы требования регулятора в части защиты персональных данных, и полноценно использовать для защиты этой «публичной» части веб-приложения от DDoS и ботов все возможности публичного облака. При этом критически важные данные, к которым применимы требования по обеспечению банковской тайны, остаются внутри защищенного контура, соответствующего всем требованиям регулятора. Однако это не всегда возможно: переписать приложение — это долго, трудоемко, дорого и иногда невозможно. Иногда отказываться приходится и по другим, довольно приземленным, причинам: например, из-за строгости внутренних политик ИБ или конфликта мотиваций между ИТ-командой, отвечающей за доступность веб-ресурсов, и ИБ-

командой, отвечающих за снижение рисков.

Третий способ, который распространен за рубежом, но пока не реализован в России, — это использование публичных облаков, аттестованных по стандарту PCI DSS. При прохождении сертификации облачный провайдер получает зеленый свет от регулятора, что стандарты защиты информации позволяют банку раскрывать свой трафик на узлах провайдера и не подвергать критически важные данные риску.

В ЗАКЛЮЧЕНИЕ

Облака доказали свою эффективность в сегментах рынка, где веб-ресурс является основой бизнес-модели. При этом регуляторные ограничения остаются барьером на пути к более эффективной защите веб-ресурсов банка от актуальных киберугроз. Модель, активно используемая за рубежом и основанная на сертификации публичных облаков по стандарту PCI DSS, представляет собой наиболее оптимальный способ обеспечить защиту публичного веба в банке и доказала свою применимость: так поступают Barclay's, Bank of America, J. P. Morgan, UBS, citi и многие другие.

На что нужно обратить внимание тем, кто обеспечивает функционирование и защиту банковских веб-приложений?

- ♦ Всегда думайте о том, что нагрузка на веб-ресурсы может быть непредсказуема;

- ♦ Будьте готовы к компромиссу между командами ИТ и ИБ для обеспечения эффективной защиты веб-приложений;

- ♦ Не полагайтесь на решения оп-remise и только собственные силы — практика показывает, что с текущим фоном атак и ограничений противостоять веб-угрозам можно только играя по правилам веб-мира.

BIS-СПРАВКА

NGENIX — российский облачный провайдер комплексных услуг обеспечения производительности, отказоустойчивости и защиты веб-ресурсов от всех видов кибератак.



МАГНИТКА-2024

ГЛУБОКОЕ ПОГРУЖЕНИЕ В ПРОБЛЕМАТИКУ ИБ +
СОЛНЦЕ, СПОРТ И ХОРОШЕЕ НАСТРОЕНИЕ

Марина БРОДСКАЯ
обозреватель BIS Journal

В конце зимы в предгорьях Южного Урала состоялся традиционный форум «Цифровая устойчивость и информационная безопасность России», а по-простому, любимый форум безопасников — знаменитая «Магнитка». В этом году мероприятие объединило 300 специалистов из Москвы и Санкт-Петербурга, а также городов Поволжья, Урала и Сибири. Выступали представители федеральных и региональных органов власти, регуляторы, руководители и ведущие специалисты крупнейших промышленных и коммерческих предприятий, финансовых организаций и ри-

тейла, представители научных и учебных заведений. Обсудили вопросы импортозамещения и технологической независимости, регуляторной политики и стандартизации, проблемы развития ИИ и подготовки кадров, а также реальные кейсы защиты предприятий нефтегазового и топливно-энергетического комплекса, транспорта, металлургии и электронной промышленности.

ПАНЕЛЬНАЯ ДИСКУССИЯ

Деловая программа Форума открылась панельной дискуссией «Киберустойчивость ключевых отраслей экономики России». Наталья Касперская, InfoWatch, отметила хорошие темпы программы импортозамещения, но обратила внимание и на проблемные, с ее точки зрения, области — языки программирования и программные стеки.

Продолживший дискуссию Евгений Хасин, Минцифры России, напомнил, что с принятием западных санкций в марте 2022 г. российские компании столкнулись с многочисленными проблемами, были отозваны SSL/TSL-сертификаты, в репозиториях появились закладки, стоял вопрос об отключении от веб-сервиса GitHub. Благодаря принятым мерам по созданию отечественных центров сертификации и репозиториям, угрозы дальнейшего отключения России от центров мировой разработки были приостановлены.

Однако перед отечественными разработчиками стоит долгосрочная стратегическая задача киберустойчивости по двум направлениям:

- ♦ устойчивость и доступность ПО, средств защиты информации (СЗИ) и возможности их замещения. Здесь возникают сложности в доступности высокопроизводительных про-

граммно-аппаратных комплексов (ПАК), например NGFW. Сейчас идут активные работы по созданию отечественных решений;

♦ доверие. Насколько можно доверять свободному ПО, компиляторам и библиотекам?

Эти вопросы включены в национальную программу «Цифровая экономика», работы по ним ведутся с участием регуляторов, в первую очередь, ФСТЭК России. На базе Института системного программирования РАН ведутся работы по исследованию безопасности ядра Linux, созданию репозитория доверенного open-source ПО. В реестр отечественного ПО войдут не только операционные системы, но и СУБД, отечественные версии Java – JDK. Ведется унификация продуктов. Работы будут продолжены в рамках нацпроекта «Экономика данных». Также ведется подготовка законодательной базы, которая установит порядок использования ПО в дальнейших разработках решений.

Евгений Хасин остановился на вопросах защиты единой цифровой платформы РФ «ГосТех» и ее составляющих «ГосМаркет» и ГИС «Управление». Платформа «ГосТех» – очередной этап создания гособлака – предназначена для федеральных и региональных органов власти и позволяет быстро и эффективно создавать ГИС и цифровые сервисы на моделях PaaS и SaaS. «ГосТех» аттестован по максимальным классам защиты и категорирован как значимый объект КИИ первой категории. Создан план перевода ГИСов на платформу «ГосТех», предусматривающий перенос или создание ГИС с нуля на базе «ГосТех» с учетом будущих возможностей.

Следующий шаг развития платформы – создание общего стека ПО, который используется для создания ГИСов. «ГосМаркет» заработает в середине 2024 г. и будет содержать экземпляры доверенных СЗИ, веб-приложений, баз данных, языковых моделей и ПО.

ГИС «Управление», введение в эксплуатацию которой запланировано на конец года, с конвейером безопасной разработки, будет содержать



анализ кода и разработки отечественных производителей в зависимости от языков программирования. Конвейер будет доступен для разработчиков ГИСов для «ГосТеха». Также будет создан выходной контроль, некий аналог ОТК, который будет содержать больше средств анализа кода.

Важным элементом станет централизованное обнаружение компьютерных атак и предупреждение инцидентов на базе собственного центра ГосСОПКА «ГосТеха», оператором выступит ФГБУ НИИ «Интеграл». Работа Центра будет осуществляться в соответствии с требованиями

НКЦКИ. В будущем планируется запуск программ BugBounty для данных платформ.

О тенденциях на рынке киберугроз в связи с переходом на отечественные решения говорил представитель НКЦКИ Иван Минаев. Он отметил, что данные об угрозах поступают в ГосСОПКА и регуляторы видят тенденцию на увеличение доли отечественного ПО. Однако, оценивая качественную составляющую, регулятор не видит просадок. Чаше он сталкивается с организационными проблемами.

По данным НКЦКИ, главным трендом прошедшего года стали атаки



на цепочки поставщиков и уязвимости ПО на периметре организации. Следом идут социальная инженерия и фишинг. В 2023 г. было выявлено 200 тыс. компьютерных атак (на 28 тыс. больше, чем в 2022 г.). По статье 274.1 УК РФ «Неправомерное воздействие на критическую информационную инфраструктуру РФ» вынесено 30 судебных решений (на 2 меньше, чем в 2022 г.), к реальному сроку заключения приговорен один человек, остальные злоумышленники получили условное наказание и/или штраф.

О сложностях при импортозамещении, с которыми сталкивается одна из крупнейших в стране с точки зрения логистики и покрытия компания ОАО «РЖД», рассказал Юрий Ногинов. Он отметил, что РЖД — это 1600 систем, в прошлом году в структуре компании было выявлено 289 объектов КИИ, работают 16 ЦОД, по одному на каждое экстерриториальное объединение. Организовано децентрализованное управление.

За прошедший год структуры РЖД отметили рост числа кибератак (+36 % к 2022 г.), в т.ч. многочисленные DDoS-атаки и использование методов социальной инженерии. Проблема отрасли — более 200 случаев поджогов релейных шкафов в 2023 г. Спикер отметил, что СЗИ в РЖД имеют свои особенности, поскольку используются микропроцес-

сорные системы управления на подвижном составе, в релейных шкафах. Они должны быть устойчивы не только к кибератакам, но и к внешним факторам. Эти системы также подлежат импортозамещению.

В компании работают все виды СЗИ, что связано с использованием многочисленных устаревших систем, под которые уже не выпускаются современные средства защиты. Компания должна импортозаместить 340 тысяч АРМ, работы в этом направлении ведутся. К началу 2025 г. все СЗИ на объектах КИИ будут отечественного производства, отметил Юрий Ногинов.

С аналогичными проблемами сталкиваются в Магнитогорском металлургическом комбинате, отметил Вадим Феоктистов, ММК-Информсервис. Изначально промышленные решения были ориентированы на западные решения Oracle, СУБД, бизнес-приложения, ERP-системы. В марте 2022 г. предприятие лишилось поддержки иностранных вендоров. Была сформирована программа по переходу на отечественное ПО, которое разбито на 10 ключевых областей, включая ERP-системы, бизнес, системы управления производством. Сегодня ведется реализация программы, по многим направлениям есть импортозамещающие решения, по части — ведется их разработка.

ММК пока не рассматривает миграцию ERP-системы на 1С. На комбинате обеспечивают стабильную работу имеющихся систем и изучают рынок, в т.ч. в рамках Индустриального центра компетенции по металлургии, изучаются требования регуляторов в части защиты объектов КИИ на предприятии. До 2026 г. разработан проект, включающий 15 ключевых направлений усиления ИБ, в т.ч. методами тестирования на проникновение, повышения осведомленности работников, развития SOC и безопасной разработкой ПО.

В Челябинской области вопросы импортозамещения обсуждаются с 2014 г., рассказал Александр Козлов, заместитель губернатора региона. Однако наиболее остро вопрос встал в 2022 г. По итогам 2023 г. Челябинская область находится на седьмом месте по уровню импортозамещения, в 2022 г. она была пятой в России. «Проект импортозамещения — самый сложный, который реализовывал в жизни», — сказал Александр Козлов, поскольку он меняет поведение пользователей и культуру и невозможен без мотивации и принуждения.

ТЕМАТИЧЕСКИЕ СЕССИИ

Механизмы регулирования с точки зрения регуляторов и отрасли обсудили участники другой сессии. Обеспечение нормативно-правового регулирования в сфере ИБ разнообразно, при этом не всегда соблюдается четкое выполнение регуляторной базы, либо она выполняется формально, отметил модератор Артем Сычев, Positive Technologies. По итогам дискуссии ее участники пришли к выводам, что в существующих НПА есть все требования по ИБ, однако необходимы дополнения по ряду механизмов. Эти проблемы понимают представители органов власти, которые занимаются регулированием, и они готовы работать над ними. В числе задач — выделение из НПА технических деталей и погружение их в стандарты, разработка закона по анализу защищенности и багбаунти.

Кибербезопасность АСУ ТП — еще одна тема, рассмотренная в рамках Форума. Эксперты говорили о реаль-



ных проблемах и задачах в АСУ ТП. Подводя итоги дискуссии модератор сессии Михаил Смирнов, InfoWatch, выделил два момента:

- ♦ можно и нужно говорить о проблемах ИБ АСУ ТП через призму импортозамещения. Текущие проекты реализуются, несмотря на трудности, для этого нужны стимул и деньги;

- ♦ события последних двух лет показали, что вопросы международного разделения труда нежизнеспособны для сферы национальной и информационной безопасности, и решать их надо своими силами.

В рамках сессии «Киберустойчивость цифровых решений в электроэнергетике» представитель НКЦКИ Иван Минаев отметил, что сегодня остро стоит вопрос защиты транспортных сетей. По поручению Президента России возобновлена работа над проектом Федерального закона «Об интегрированной сети связи для нужд обороны страны, безопасности государства и обеспечения правопорядка». Работа над законопроектом по созданию специаль-

ной сети связи для нужд обороны и госбезопасности велась правительством России в 2015–2017 годах, однако документ так и не был вынесен на всеобщее обсуждение.

Обсуждая практическую пользу киберучений на киберполигоне Amprige от компании «Перспективный мониторинг», спикер подчеркнул, что в настоящее время вопрос работы таких систем не урегулирован на законодательном уровне. Эксперт отметил, что совокупные сведения об объектах КИИ 1 категории и их защищенности относятся к гостайне. При этом компании создают киберполигоны и цифровых двойников систем для использования в учебных целях и профессиональной подготовки кадров, тренировки «белых» хакеров. «Мы обучаем как защищается цифровой двойник, при этом вопрос техники, как этот образ снять», — отметил спикер. Он считает, что разработку подобных систем «надо делать правильно, с учетом мнения спецслужб». Планируется создать и Национальный киберполигон.

Представитель НКЦКИ рассказал, что в настоящее время идет подготовка требований по аккредитации киберполигонов как части экосистемы ГосСОПКА и анонсировал подготовку проекта закона «О государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак». По его словам, официально о разработке данного документа может быть объявлено позднее.

КАДРЫ. КУДА БЕЗ НИХ?

Любое мероприятия по ИБ не обходится без обсуждения кадрового вопроса. Кто и кому нужен, какими компетенциями должен обладать специалист по ИБ, чтобы здесь и сейчас уверенно защищать инфраструктуру предприятия, отрасли и страны? С такими вопросами к участникам дискуссии обратился модератор сессии Артем Сычев.

Дмитрий Правиков, завкафедрой комплексной безопасности критически важных объектов РГУ нефти и газа (НИУ) им. И. М. Губкина, встал



на защиту вузов, которые обвиняют в подготовке недостаточного количества выпускников, с низкой квалификацией, по программам, которые не соответствуют запросам рынка. Спикер отметил, что в университетах страны открыты 130 профильных кафедр «Информационная безопасность», которые ежегодно выпускают более двух тысяч молодых специалистов. Большая их часть (80–95 %) идет работать по специальности, а уровень их подготовки соответствует требованиям ФГОС. По мнению докладчика, резерв высшей школы не исчерпан, ей нужны помощь регуляторов и бизнеса.

С этим мнением поспорили представители отрасли ИБ. В частности, Лев Шумский, CSO Яндекс Банк, отметил низкое качество подготовки выпускников, их неумение рассуждать логически, незнание базовых вещей и завышенные зарплатные ожидания. Компании вынуждены проводить переподготовку и стажировку молодых специалистов, которым не хватает практических навыков.

С мнением практиков не согласился Николай Комлев, исполнительный директор АП КИТ. Он призвал представителей отрасли ИБ активнее работать в советах по формированию профстандартов и ФГОСов по новым

направлениям подготовки. «Однако с учетом бюрократических процедур при согласовании документов происходит отставание от жизни», — согласился эксперт.

Андрей Коваленко, вице-президент Академии криптографии РФ, ранее много лет возглавлявший УМО вузов в области ИБ, напомнил собравшимся о перманентной многолетней реформе высшего образования. Он отметил достоинства классического технического образования, которое ранее получали выпускники вузов, заметил, что на профильные предметы по специальностям в действующих учебных программах не отведено часов, поэтому их надо преподавать как спецкурсы или дополнительное образование. Также А. Коваленко обратил внимание на средний возраст преподавательского состава, уровень загрузки преподавателей при подготовке учебно-методических материалов и размер зарплат в вузах. По мнению эксперта, выпускникам необходимо базовое вузовское образование, которое следует дополнить специализированным.

Иван Минаев обратил внимание собравшихся на будущую аккредитацию специалистов центров ГосСОПКА. По мнению эксперта, при наличии базового образования специалисту необходимо повышение квалификации.

Участники дискуссии сошлись во мнении, что для успешного решения кадрового вопроса необходимо скорректировать программу базового высшего образования, расширить курсы ДПО на базе центров подготовки вендоров, создать центры отраслевой подготовки. Следует привлекать в отрасль людей с широким кругозором, которые понимают проблемы инфобеза, а также беречь специалистов, которые уже работают в сфере ИБ.

ДЛЯ ХОРОШЕГО НАСТРОЕНИЯ

В рамках программы активностей участники «Магнитки-2024» погрузились в неповторимую атмосферу зимы Южного Урала, неформальное общение с коллегами, участвовали в состязаниях на свежем воздухе и в специальных зонах, где все желающие могли поспорить друг с другом в спортивных и дискуссионных форматах.

Абсолютным победителем состязаний в рамках индивидуального зачета стал Иван Чернов, UserGate. Все участники соревнований получили приятные призы и незабываемые впечатления.

Организаторы «Магнитки-2024» — Минцифры России, АРПП «Отечественный софт» и неизменный и многолетний вдохновитель мероприятия — Медиа Группа «Авангард».

ТБ ФОРУМ 2024

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ: ВЫЗОВЫ И ВОЗМОЖНОСТИ



Анна КАТАНКИНА
корреспондент BIS Journal

В феврале в Москве прошел Международный форум «Технологии и Безопасность» — ТБ Форум 2024. Впервые одна из сессий на нём была посвящена вопросам развития искусственного интеллекта, опыту использования ИИ и машинного обучения в различных отраслях экономики, вопросам доверия и информационной безопасности.

МИНЦИФРЫ РОССИИ

О вопросах развития регулирования ИИ рассказал Александр Шойтов, заместитель главы Минцифры России. Он отметил повышенный интерес к вопросам ИИ со стороны Президента России, правительства и органов власти всех уровней, активное внедрение ИИ в разных отраслях. Поэтому остро встают вопросы ИБ ИИ, доверенного ИИ и больших языковых моделей (LLM), а также регулирования и стандартизации.

А. Шойтов отметил мировые тенденции в части подходов к регулированию ИИ и работы с данными: американскую, китайскую и европейскую. В странах ЕС ведется жесткая регуляторная политика, направленная на защиту прав граждан. В КНР упор сделан на защиту прав государства. В США принят свободный оборот данных, однако утверждение новых нормативных актов говорит об ужесточении требований к использованию ИИ. В целом мировое сообщество активно обсуждает технологии ИИ, безопасность их применения и необходимость регулирования.

В России вопросами разработки доверенного ИИ занимаются Минцифры России, ИСП РАН, АНО «НТЦ ЦК», Академия криптографии РФ. Разрабатывается проект требований в сфере ИБ ИИ. Планируется, что документ будет представлен для обсуждения на втором форуме «Технологии доверенного искусственного интеллекта» в мае 2024 г., сказал А. Шойтов.

Он отметил риски общего характера при работе с ИИ: требования к коду, его происхождению и от-

крытости; требования к данным, их происхождению и качеству, верификации и обезличиванию; специфические риски ИБ, способность противостоять конкретным видам атак.

Жесткое регулирование использования ИИ потребуется в области КИИ и медицинских данных, отметил А. Шойтов. Еще одна острая тема — недостоверные данные из поисковых систем, на основе которых ИИ выдает решение. «Насколько оно достоверное — отдельное направление, тонкая тема, которая должна получить нормативное регулирование», — подчеркнул докладчик.

Замглавы Минцифры отметил, что вопросы ИБ ИИ будут включены в национальную программу «Экономика данных» на 2025–2030 годы. Он выделил три базовых направления: создание доверенных платформ разработки ИИ, тестирование на компьютерные атаки и создание моделей, методик и протоколов обезличивания данных.

Первые два направления подпадают под регулирование ИБ, третье — относительно новое, подчеркнул докладчик. Согласно подходу,

формируются три этапа предоставления доступа к обезличенным данным:

- ♦ в защищенном контуре для работников ИИ;
- ♦ между двумя субъектами, которые обмениваются такими данными;
- ♦ в случае, когда обезличенные данные выкладываются в общий доступ.

А. Шойтов отметил, что это разные подходы к обезличенным данным и они существенно различаются с т.з. разработки и рисков безопасности. В настоящее время реализуется первый этап. В Госдуме рассматриваются поправки к закону «О персональных данных», которые должны определить принципы работы бизнеса с обезличенной личной информацией в закрытом доверенном контуре.

Завершая выступление, А. Шойтов отметил слабое взаимодействие работников ИИ и разработчиков систем доверенного ИИ, машинного обучения и в целом ИБ ИИ. Он призвал стороны к более тесному сотрудничеству.

МИНПРОМТОРГ РОССИИ

Александр Сергеев, гендиректор ФГАУ «Федеральный центр прикладного развития искусственного интеллекта» Минпромторга России, рассказал о мерах поддержки разработчиков решений с ИИ со стороны государства. Так, Центр оказывает поддержку цифровой трансформации Минпромторга России и внедрению решений на базе ИИ-технологий в промышленных компаниях, сопровождает внутриведомственное внедрение технологий ИИ в бизнес-процессы министерства и его организаций.

В задачи Центра, помимо иных задач, входит комплексная экспертиза национальных стандартов в сфере ИИ в России, развитие регулирования внедрения и использования технологий ИИ в отраслях промышленности РФ. Однако в этом направлении есть проблемы с масштабируемостью решений, возникают проблемы с конфиденциальностью данных, порядком работы и обмена промышленными данными. В этой сфере требуется дополнительное регулирование, отметил докладчик. Минпромторг

и заинтересованные ведомства ведут разработку федерального закона о промышленных данных, который позволит дать определение понятию «промышленные данные» и регламентирует операции с ними.

Крупные ключевые игроки, предоставляющие меры поддержки в области ИИ по согласованию с Правительством России, работают на всех уровнях, каждое ведомство самостоятельно разрабатывает и предоставляет решения в области ИИ. Между структурами нет информационного обмена, сторонам неизвестны направления и темы разработки, подчеркнул докладчик. Также он отметил, что при разработке НПА в сфере ИИ министерствам и ведомствам важно определиться с терминологией. Сейчас в документах уже дано восемь определений искусственного интеллекта, подчеркнул А. Сергеев.

Еще одна болевая точка — связь программного и аппаратного обеспечения, которое имеет признаки ИИ. В соответствии с Постановлением правительства РФ от 23.08.2021 № 1380 Минпромторг ведет разработки программно-аппаратных комплексов с использованием ИИ. По данным Минцифры, Единый реестр российского ПО и баз данных включает 19036 программных продукта, из них 136 имеют признаки ИИ. В Единый реестр российской радиоэлектронной продукции Минпромторга включена 18531 разработка, но ни одна не использует ИИ. Задача ведомства и его структур — совместить разработки отечественных компаний, связать ПО с ИИ и аппаратные платформы, которые создают российские производители. Для этого у «Федерального центра прикладного развития искусственного интеллекта» Минпромторга России есть все возможности. Он создает все условия для эффективной работы и развития стартапов, обеспечивает доступ к передовым технологиям и ресурсам для проведения исследований и экспериментальных разработок в области ИИ, оказывает помощь во взаимодействии с функциональным заказчиком и поддерживает компании при выходе на рынки сбыта за пределами России.

СТАНДАРТИЗАЦИЯ ИИ

Председатель ТК 164 «Искусственный интеллект», директор по научным проектам НИУ «Высшая школа экономики» Сергей Гарбук рассказал о национальной системе оценки соответствия технологий ИИ требованиям в области функциональной корректности и безопасности. Основными целями стандартизации ИИ являются:

- ♦ обеспечение гарантий функциональной корректности систем искусственного интеллекта (СИИ) в условиях эксплуатации, в т.ч. при дообучении СИИ в процессе эксплуатации и при автоматизации процессов обработки информации, связанных с заменой человека-оператора;
- ♦ разработка методов и средств оценки и подтверждения безопасности СИИ, обеспечение специальных требований в области ИБ СИИ, оценка уровня социальной приемлемости СИИ, в т.ч. этических последствий разработки и применения таких систем;

♦ обеспечение терминологического единства;

♦ унификация форматов представления данных, необходимых для создания и применения СИИ;

♦ фиксация вариантов использования и лучших практик создания и применения СИИ при решении различных прикладных задач в отраслях экономики и социальной сферы.

Комплекс нацстандартов, разработанный в рамках ТК 164, включает отраслевые и межотраслевые стандарты, а также стандарты в области данных. Лидером среди отраслевых стандартов является транспортная отрасль, где приняты 24 стандарта ИИ. Разработки стандартов в области ИИ ведутся по девяти направлениям, при этом ТК 164 выделяет 14 отраслей, где могут быть применены технологии ИИ. В 2023 г. утверждены 35 стандартов ИИ, из них 12 разрабатывались на основе международных стандартов.

ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ

О ИИ-решениях и практике их применения в различных отраслях, подходах к внедрению и барьерах на пути

реализации и получении технологического превосходства участникам форума рассказали разработчики и представители госкомпаний, финансовых организаций и Ассоциации лабораторий по развитию ИИ. Еще больше решений было представлено в рамках технологической секции «Инструменты на базе AI и практика использования AI/ML в различных отраслях».

Медицина. Замруководителя проектного офиса Исследовательского центра в сфере ИИ ФГБУ «НМИЦ онкологии им. Н. Н. Блохина» Олег Зиновкин поделился опытом внедрения ИИ в сфере здравоохранения. Мощности центра позволяют вести работы над проектами в трех направлениях:

- ♦ раннее выявление онкологических заболеваний и исследования, направленные на совершенствование методов на основе машинного обучения (ML) на примере ПО с технологией ИИ по маммографическому скринингу;

- ♦ диагностика и лечение онкологических больных. Разрабатывается серия продуктов на основе ML по совершенствованию рентгенологических обследований лиц со злокачественными новообразованиями;

- ♦ разработка прикладного ПО с целью повышения качества и доступности оказания медицинской помощи пациентам со злокачественными новообразованиями.

В результате работы Центра в области ИИ планируется создание верифицированных наборов данных для решения задач разработки предиктивных интеллектуальных моделей в онкологии и разработка на их основе моделей ML для решения прикладных клинических задач в онкологии, создание программных фреймворков на основе разработанных моделей. В планах центра разработка отраслевых стандартов в сфере ИИ в здравоохранении, нормативных и методических документов, апробация разработанных решений в практической медицине и повышение квалификации специалистов, которые используют в работе системы ИИ.

Финансы. Антон Степанов, начальник отдела Управления регули-

рования цифровых сервисов и финансовых технологий Департамента Финансовых технологий Банка России, отметил активное внедрение технологии ИИ в финансовой сфере, в результате которого происходит трансформация бизнес-процессов и общерыночных практик. Главный тренд развития технологий ИИ на ближайшие годы — генеративный ИИ и LLM. Организации на финансовом рынке применяют ИИ при взаимодействии с клиентами, управлении рисками и аналитике, отметил представитель регулятора. При этом нельзя забывать о рисках ИИ, которые связаны с использованием данной технологии. Это риски разработки ИИ и искажения работы модели ИИ, риски аутсорсинга, риски в области данных и ИБ. Также возникают риски использования генеративного ИИ. Рост числа областей использования генеративного ИИ в финансовой сфере сопряжен с появлением новых специфических уязвимостей, требующих дополнительного анализа и оценки, отметил докладчик.

Банк России поддерживает создание условий, направленных на стимулирование развития ИИ на финансовом рынке с учетом риск-ориентированного принципа регулирования ИИ. Такой подход предполагает сочетание инструментов т.н. мягкого регулирования, саморегулирования и точечного нормативного регулирования пропорционально объему и вероятности реализации рисков внедрения технологий ИИ.

Аудит. Опытным эффективным использованием технологий ИИ и практике их применения в Счетной палате РФ поделился замначальника управления развития цифровых методов аудита «Центра экспертно-аналитических и информационных технологий Счетной палаты РФ» Роман Некрасов. Он отметил резкий рост производительности труда аудиторов при использовании технологий ИИ в работе. Экспериментальные системы работают в закрытом контуре без выхода во внешнюю среду. Докладчик обратил внимание на сдерживающие факторы, среди которых — дефицит размеченных

данных, недостаток компьютерных ресурсов, низкая информированность о технологии языковых моделей-трансформеров в аудиторском сообществе и плохое качество отсканированных документов, что сказывается на результатах работы.

ПОДВОДЯ ИТОГИ

«Я услышал разные доклады, ясно, что применение искусственного интеллекта — это, сомнения нет, гениально», — отметил модератор сессии Арутюн Аветисян, директор Института системного программирования РАН. Упоминание в работах популярных технологий, которые у всех на слуху, — это «хайп», считает А. Аветисян. «Но если мы говорим о зрелости технологии, то она должна возникнуть на научно-технической базе», — подчеркнул он.

Докладчик отметил, что ведущиеся сегодня разработки должны быть построены, в первую очередь, на доверии технологии, когда есть понятные процессы: от этапа дизайна и сбора данных до эксплуатации и сопровождения. Именно поэтому нужно доверять технологии, а не утверждениям маркетологов, подчеркнул А. Аветисян. Продукт должен быть сделан по ГОСТу, что можно будет проверить, иначе это просто слова. «Без научной базы невозможно построить доверенных технологий», — считает докладчик.

А. Аветисян отметил, что вопросы ИИ занимают во всем мире. Он напомнил, что технологии ИИ стали главной темой на конференции G7 весной 2023 г., был принят документ «Хиросимский процесс генеративного искусственного интеллекта». В России вопросы развития ИИ обсуждаются с 2018–2019 гг., активная работа над технологиями ведется с участием госструктур и коммерческих компаний, а также на межгосударственном уровне.

Академик подчеркнул, что как эксперт он считает, что «принципиально невозможно сделать полный автопилот». «Он должен ездить только в контролируемой среде, либо должен работать как ассистент. Не случайно, когда И. Маска спросили про автопилот, он сказал: «У меня не ав-



Арутюн Аветисян, директор Института системного программирования РАН

топилот, у меня помощник», — отметил спикер. Это указано и в документации к автомобилю.

Во времена СССР существовал ГОСТ 34, который устанавливал стадии и этапы создания автоматизированных систем, и другие стандарты по безопасности для конкретного применения, продолжил модератор.

«Без понимания технологического уровня процессный уровень вообще невозможно построить», — отметил А. Аветисян. — Только тогда у нас будет зрелая технология, которой мы можем доверять».

Продолжив приводить примеры, академик отметил, что одно дело — зайти по биометрии в метро, «даже если ты

зайдешь бесплатно, ничего страшного не произойдет», другое — если не тот человек зашел на атомный объект. «...должен быть процесс, который гарантирует отсечение и зависит от условий применения», — подчеркнул он.

Спикер отметил, что совместными усилиями необходимо разрабатывать технологически правильную гибридную модель ИИ, отрабатывать вопросы в лаборатории, чтобы не останавливать развитие новых технологий, повышающих производительность труда. Для этого требуются специалисты с хорошей математической подготовкой и технологическая база, которая позволит решать сложные задачи в области ИИ. Необходимо создать депозиторий доверенных систем ИИ, над этим вопросом работают Центр исследований безопасности системного программного обеспечения и более 50 отечественных компаний. Ведется исследование уязвимостей ядра Linux, 250 патчей принято на международном уровне.

Сообществу нужно чаще встречаться и обсуждать технологии и вопросы их развития, чтобы порознь не работать над одними и теми же задачами. В мае 2024 г. пройдет второй Форум «Цифровая экономика: технологии доверенного искусственного интеллекта», который проводит ИСП РАН совместно с Академией криптографии РФ и АНО «НКЦКИ», отметил А. Аветисян. Необходима внутренняя консолидация ресурсов и переход от конкуренции к совместной работе в ключевых технологиях.

BIS-КОММЕНТАРИЙ

Арутюн АВЕТИСЯН, директор ИСП РАН

— В прошлом году на конференции по доверенному ИИ много говорили и про **Secure by design** в основе искусственного интеллекта и про доверенные модели ИИ. На ТБ Форуме на этих вопросах остановился только А. Шойтов. Столкнутся ли разработчики продуктов, представленных на конференции, с необходимостью все переделывать?

— И да, и нет. Я думаю, что все, что делают люди, это, по сути, некий конвейер разработки с новыми свойствами, с новыми инструментами проверки. И когда они начнут внедрять свой конвейер, они проверят эти

инструменты. Если выяснят, что у них что-то не так с данными, придется перестраиваться и переобучаться.

В обычном ПО, когда начинают внедрять безопасную разработку, выясняется, что в коде очень много ошибок. Вы должны их фиксировать — у вас нет выбора. Это дополнительные финансовые расходы.

— И репутационные?

— Нет, репутационные нет, потому что не было требований. Требования должны появиться не с неба, а через **best practices**. Я думаю, что к тому моменту, когда начнет появляться научно-технологическая база и регуляторика, все, кто более-менее активен, будут это видеть и синхронизироваться. Это процесс, и в нем все постепенно устроится.



Фото: vk.com/cryptosummit

CRYPTO SUMMIT 2024

ТРЕЙДИНГ, МАЙНИНГ И ПЕРСПЕКТИВЫ РАЗВИТИЯ РЫНКА ЦФА

Алёна НИКОЛАЕВА
корреспондент BIS Journal

В Москве прошел IV ежегодный саммит по криптовалютам и блокчейн-технологиям Crypto Summit 2024, организованный группой компаний Crypto Holding при участии Российской ассоциации криптовалют и блокчейна (РАКИБ) и Бизнес-клуба российских предпринимателей из перспективных и инновационных сфер экономики t3. Основная цель мероприятия — объединить экспертов и участников отрасли, совместно выработать общий план развития индустрии на ближайшие годы.

ДИАЛОГ ИДЕТ НЕПЛОХО

На трехдневном Форуме обсуждались тенденции на рынке криптовалют, вопросы трейдинга, майнинга, перспективы развития рынка цифровых финансовых активов (ЦФА) в России. В последний день поднимались вопросы регулирования в сфере ЦФА, оборота цифровой валюты, использования криптовалют во внешнеэкономической деятельности. Представители Госдумы, Совета Федерации, Минцифры и РАКИБ обсуждали новые угрозы и риски в цифровой экономике, проблемы информационной безопасности. Завершился саммит сессией, посвященной юридическим вопросам и вопросам безопасности, где также рассмотрели проблемы контроля криптовалютных транзакций и расследова-

ния преступлений с использованием криптовалют.

Исполнительный директор РАКИБ Александр Бражников считает, что Crypto Summit 2024 прошел отлично. Подобные мероприятия дают не только эффект узнаваемости, но и единения, подчеркнул он. «Диалог с государством и бизнесом идет очень неплохо. Сообщество само по себе хорошо работает. То, что на сегодня планировали, все сделали, результат есть», — отметил он.

Оценивая вклад сообщества в конотворческую деятельность, А. Бражников подчеркнул, что отрасль нуждается в законодательном регулировании, даже если пока не все игроки рынка понимают это. «Если мы что-то не будем предлагать, не будем изменять, то нам навязжут те ус-



ловия, которые сообществу вообще не понравятся», — считает руководитель РАКИБ.

ПРО КОНЦЕПЦИЮ И ПРАКТИКОВ

В рамках Форума была представлена «Концепция развития криптовалют и майнинга в России». В ней, в частности, предлагается лицензировать разработчиков программных платформ, необходимых для коммерциализации поддержания децентрализованных блокчейн сетей (майнинговые пулы) и создать реестр майнингового оборудования с фиксацией серийных номеров ASIC и адресов, на которых осуществляется майнинг. Эти предложения нашли понимание в правительстве.

По словам А. Бражникова, сейчас идет активный диалог РАКИБ с Минцифры по широкому кругу вопросов, включая майнинг. В работе самого Форума принял участие заместитель главы ведомства Александр Шойтов. Представитель РАКИБ надеется, что в работе следующего Форума примут участие фигуры уровня вице-премьера федерального правительства.

Оценивая перспективу принятия законопроектов о регулировании об-

ращения криптовалют и регулирования майнинга, он отметил, что так или иначе они будут приняты. За весенне-летний период Ассоциация намерена подготовить свои предложения, которые должны войти в эти документы. «Теоретик пишет всегда красиво и интересно, но практик потом берётся за голову, что там написано — все написано в теории, а от практики нет ничего», — высказался спикер. РАКИБ давно работает на рынке и активно подает предложения и замечания по законопроектам, сейчас есть такая возможность.

ПРО КОМЬЮНИТИ

Участник всех саммитов, директор по развитию РАКИБ Валерий Харламов отметил качественное изменение аудитории мероприятия за прошедшее время. «Первый раз люди ходят и не понимают, что происходит. В следующий раз участники приезжают подкованными, приезжают осознанно, чтобы что-то познать и чему-то научиться», — заметил он. — Для РАКИБ это существенный плюс. Мы видим тех, кто остаётся на рынке, участвует в выставке, из года в год появляется на этих площадках. Значит, они действуют правильно, в рамках законодательства, верят в новые тех-

нологии, участвуют в жизни сообщества. Они остаются на рынке и это хорошо. РАКИБ ведет активную работу, несет свою миссию. Мы обучаем людей, рассказываем, как нужно действовать, чтобы было комфортно, и как нельзя. Мы создаем большое комьюнити, знакомим людей между собой. Они зарабатывают и помогают друг другу».

МИССИЯ ПРОСВЕЩЕНИЯ

Отдельный вопрос — безопасность, отметил В. Харламов. «Мы ведем просветительскую работу, потому что известно много случаев мошенничества, строительства финансовых пирамид, вовлечения в сферу людей, которые не образованы и не понимают новых технологий и их легко разводят «на крипте». Просвещение — удел ассоциаций, общественных организаций и государства. Государство боится, что если не введет крипторегулирование, людей будут обманывать. Людей и так будут обманывать, потому что они не образованы. Надо поднимать уровень образования и учить кибергигиене», — считает спикер.

Директор по развитию РАКИБ отметил, что Ассоциация общается со всеми государственными структурами, и готова передавать им свои знания, поскольку криптовалюты — глобальная мировая тенденция.

«ЦБ НАС НЕ ВИДИТ»

Ассоциация неоднократно проводила встречи с представителями Банка России по вопросу легализации криптовалют. «Мы предлагали много проектов как легализовать рынок криптовалют, какие большие налоги и доходы государству это принесло бы. ЦБ России против, по какой причине, мы не можем сказать», — отметил В. Харламов. Он подчеркнул, что даже в рамках Форума компании предлагают свои решения по мониторингу транзакций, платёжным системам и практическим решениям, которые дают «под ключ». «Но ЦБ нас не видит», — подчеркнул представитель РАКИБ. При этом он считает, что вопрос сдвинется с мертвой точки, как только будет получено распоряжение «сверху».

НАЙТИ НЕЛЬЗЯ СОЗДАТЬ

КАК ПРАВИЛЬНО ОБРЕСТИ МИФИЧЕСКИХ SECURITY CHAMPIONS В СВОЕЙ ОРГАНИЗАЦИИ



**Рустам
ГУСЕЙНОВ**
председатель
кооператива
«РАД КОП»
(radcop.online)

Статья продолжает развитие идей предыдущего номера и конкретизирует подходы к «выращиванию» (bildung) специалистов в области безопасной разработки (security champions), рассматривая наиболее продуктивный и реалистичный с точки зрения автора сценарий.

ВВЕДЕНИЕ

В предыдущем номере в рубрике «Актуальное мнение» мы говорили о проблематике изменений в отрасли безопасной разработки под влиянием ИИ. Но параллельно с технологическими аспектами на фоне происходящих инноваций сохраняют важность и аспекты гуманитарные. Ведь пока у «умных машин» остаются пользователи, операторы и администраторы, остаётся и необходимость их обучения, мотивации и встраивания в соответствующие технологические процессы. И судя по приводимой статистике, эта проблема пока не решена.

В том же номере другим автором¹ затрагивалась вечная тема security champions — известной концепции о том, как с помощью «передовиков» из числа разработчиков залатать дыры в ИБ в условиях дефицита

кадров и роста сложности разработки². И хотя на словах мы все понимаем, что надо делать, реальная сложность заключается в практической реализации «универсальных советов». В противном случае мы рискуем уподобиться мудрому филину из известного анекдота про мышек, которые по совету пернатого консультанта должны стать ёжиками и таким образом решить все свои проблемы.

Рассматриваемые в данной статье вопросы и предлагаемые подходы могут быть восприняты шире — как инструменты по работе с мотивацией сотрудников за рамками ниши «безопасной разработки».



Доклад «Мифические Security Champions, или Как не сойти с ума в мире безопасной разработки»,
Светлана Газизова

КЛЮЧИ К МОТИВАЦИИ

Ключом к решению любой проблемы является её формулировка в виде задачи. А для этого необходима чёткая модель мира, описывающая соответствующую проблеме систему и позволяющая спрогнозировать изменения системы, в зависимости от наших воздействий на неё. В данном случае проблема осложнена тем, что

мы говорим о системе социальной, то есть такой системе, к которой не применим инженерный подход из-за наличия внутри неё субъективного фактора. Именно тем, что внутри жизненного цикла разработки, который представляет собой совокупность персонала, процессов и технологий, находятся... ЛЮДИ, именно этим объясняется, по мнению автора, тот факт, что, несмотря на пристальное внимание к росту безопасности и качеству приложений, ситуация становится всё хуже³.

И основой здесь является не просто абстрактный и универсальный алгоритм в духе «поиска высокомотивированных сотрудников», а понимание двух ключевых аспектов мотивации и изменения поведения людей, а именно:

Поведение сотрудников сильно зависит от окружающей среды, и выбор мотивационных инструментов через «моральное удовлетворение и поддержку коллег» или, например, «денежную премию» — это не вопрос вкуса, а вопрос культуры конкретной компании и той среды, в которой она функционирует (подробнее смотри и читай в книге, приведённой на иллюстрациях ниже).

Мотивация людей может изменяться, а сотрудники могут пере-

³ В этом смысле эта история напоминает климатические проблемы — со времен 1970-х, когда экоповестка была сформулирована как наиважнейшая для долгосрочного выживания человечества, прошло более 50 лет, но до сих пор человечество не научилось «беречь планету». Аналогично с качеством и безопасностью кода: рост количества инструментов и специалистов в области безопасности приложений коррелирует с ростом угроз, уязвимостей и недостатков, что наглядно видно из отраслевых отчётов, например приводимого в прошлом материале обзора: <https://www.it-cisq.org/the-cost-of-poor-quality-software-in-the-us-a-2022-report/>.

¹ BIS Journal №1/2024. А. Жаркевич, «Security Champions. Где найти чемпионов?», стр. 90.

² Подробный контекст проблематики хорошо представлен в выступлении Светланы Газизовой на 2-й межотраслевой конференции АБИСС (QR-код представлен выше), полная ссылка: <https://www.youtube.com/watch?v=OU6irXebpro&t=680s>.

Модель управления	Культура	Лидеры		
УПРАВЛЕНИЕ ПО ЦЕННОСТЯМ	• Творчество • Глобальные инновации • Свободы	СИНТЕЗ «Чтобы сделать людей счастливыми»	БИРЮЗОВЫЕ ЛИДЕРЫ	Сетевой менеджмент
	• «Пусть цветут все цветы» • Диалог • Эксперименты	ВОЗМОЖНОСТИ «Потому что нам интересно пробовать»	ЛИДЕРЫ ФАСИЛИТАТОРЫ	
УПРАВЛЕНИЕ ПО ЦЕЛЯМ	• Быть первым • Выдающийся результат • Фокус на цели	УСПЕХ «Чтобы быть первыми»	ЛИДЕРЫ ДОСТИЖЕНИЙ	Регулярный менеджмент
УПРАВЛЕНИЕ НА ОСНОВЕ РЕГЛАМЕНТОВ	• Системность • Закон • Порядок	ПРАВИЛА «Потому что таков закон»	РЕГУЛЯРНЫЕ МЕНЕДЖЕРЫ	
УПРАВЛЕНИЕ ЧЕРЕЗ ПОРУЧЕНИЯ	• Власть • Автономия • Подвиг	СИЛА «Потому что война»	ЛИДЕРЫ КОМИССАРЫ	Персональный менеджмент
УПРАВЛЕНИЕ НА ОСНОВЕ ТРАДИЦИИ	• Общность и поддержка • Традиции • Уважение к старшим	ПРИНАДЛЕЖНОСТЬ «Потому что так принято»	ЛИДЕРЫ ОТЦЫ	

Рисунок 1. Модели управления (и мотивации) компании, в зависимости от условий среды и культуры

воспитываться, но ключевым фактором успеха или неуспеха подобных инициатив является формирование соответствующей среды, в основе чего лежит готовность руководства не на словах, а на деле изменить организацию работы и систему стимулов, в том числе самих себя (ничто не работает здесь так хорошо, как личный пример руководителей и осознание сотрудниками справедливых и универсальных правил игры).

Отсюда следует тривиальный, но часто игнорируемый вывод: не все изменения во всех организациях возможны. И если вы хотите, например, получить «вовлечённый персонал без повышения зарплатных плат», готовьтесь к необходимости выращивать культуру «бирюзовой организации», но смиритесь с тем, что более вовлечённые и творчески заряженные люди будут иначе относиться к поставленным задачам, начнут спорить, критиковать, предлагать альтерна-

тивные варианты, а цикл разработки удлинится. Либо вводите систему материального стимулирования, но не абстрактную и непонятную, зависящую от настроения начальства и не контролируемых сотрудниками факторов «невидимой руки рынка», а привязанную к их собственным достижениям и труду и распространяющуюся на всех без исключения сотрудников подразделения, вне зависимости от субъективности руководства. Желательно и на самих ру-

ководителей (например, через сбор обратной связи сотрудников о качестве руководства, как это бывает в некоторых TQM-системах).



Рисунок 2. Григорий Финкельштейн «Без шаблона» (иллюстрация ситуационного подхода к построению систем управления организациями)

НЕКОТОРОЕ ОПИСАНИЕ УЧЕБНОГО ПРИМЕРА

Чтобы не впадать в абстракции, давайте рассмотрим конкретный пример того, как это работает. Любая деятельность может быть представлена как цепочка:

Мотив → Действие → Результат → Рефлексия⁴

Последний пункт цепочки важнейший, именно здесь происходит магия сдвига мотивации и корректировки поведения сотрудников. Запускается ли эта рефлексия через обратную связь от недовольного клиента, как в ISO 9000, или в результате дружелюбной SCRUM-ретроспективы — не столь важно. Важно, что полученный человеком результат оказывается оценён в значимом для субъекта разрезе, за что он получает вознаграждение или наказание. Содержание этого вознаграждения не столь важно — оно может быть и не материальным, но по понятным причинам в большинстве

современных компаний, где люди работают всё же за деньги, именно денежный эквивалент наиболее желателен. Без него тоже можно обойтись, но на практике это означает ещё более серьёзные усилия по отбору или перевоспитанию людей, что может быть невозможно в условиях отсутствия соответствующих HR-ресурсов и желания многолетнего «выращивания» коллектива до нужного состояния.

Как это выглядит? Фактически необходимо осуществить две вещи:

1. Измерить приемлемый/ожидаемый от роли результат, идентичный «нормальной» работе;

2. Зафиксировать уровни вознаграждения за отклонения от «нормального» результата в большую сторону.

Если мы говорим о неденежной мотивации — учитывать заслуги и благодарить⁵. Если мы говорим о финансовом эквиваленте — грейдировать премии. В простейшем случае последний подход может выглядеть как премирование человека долей от сверхвыработки. Когда существует базовый бюджет подразделения, приравненный к «100 попугаям», и если подразделение вырабатывает «110 попугаев», то в ходе ревью выясняется, кто сделал «плюс 10 попугаев», и «стахановцы» получают пропорциональную прибавку к своему доходу за соответствующий период.

Думаете, это фантастика? Ничуть нет: подобная практика была реализована много лет назад в компании «Литрес»⁶. Для любителей более изощрённых схем и фундаментальных моделей можно посоветовать изучить наработки Сергея Савченко по так называемой чартаевской системе⁷. Подобные подходы хороши

тем, что решают главную проблему мотивации — отсутствие чётких и универсальных правил игры. Их единственный недостаток — сложность внедрения и полная прозрачность всех отношений (увы, чудес не бывает, и руководителям придётся перестраиваться в первую очередь, рефлексировав собственные мотивы и поведение).

ЗАКЛЮЧЕНИЕ

Таким образом, мы увидели, как проблема «поиска security champion в пустыне» превращается в решаемую задачу, и осознали, что для решения этой задачи очень важен контекст. Увы, без определённого стечения обстоятельств (в том числе субъективного фактора руководства, готового пойти на личные жертвы) реализовать благие пожелания не получится, и всё, что нам останется, — сетовать на отсутствие кадров. Подходы, предлагаемые к реализации, давно известны и хорошо апробированы, но их внедрение потребует воли и времени. Зато потом у вас, в отличие от многих, действительно будут свои security champion. Да и не только security: описанная практика позволяет корректировать мотивацию любых ролей и специализаций (см. примечание 7), и для обозначения подобного взращивания даже есть специальный термин — Bildung. Так в скандинавских странах называют подход к «взрачиванию личности» человека и формированию внутренней мотивации к той или иной деятельности. Заинтересовавшихся вопросом и желающих подробнее изучить, как могут работать подобные управленческие технологии, приглашаем в телеграм-канал нашего кооператива.



Ссылка на телеграм-канал РАД КОП, где публикуются наши материалы

⁴ Что-то подобное можно найти в творчестве различных психологов, например у знаменитого А. Маслоу: <https://gtmarket.ru/library/basis/4201/4209>.

⁵ О том, как это делать и куда эволюционировали системы внутрикорпоративного рейтинга, продолжающие дело «КОМПАСА» Водянова, можно завести отдельный разговор, но не сейчас.

⁶ Посмотреть, как это работает, можно в лекции СТО «Литрес» Дмитрия Грибова на ScrumTrek: https://youtu.be/ppbUjR_fWK-w?si=OI9JT9yI33DqwyHX

⁷ Система подразумевает внедрение внутри организации квазирыночных отношений с формированием у сотрудников «предпринимательской инициативы»: https://www.youtube.com/watch?v=p2Ww_4oJt98.

ЧТО ПОЛУЧИТ БИЗНЕС, ВНЕДРИВ БЕЗОПАСНУЮ РАЗРАБОТКУ?

КАК ПОНЯТЬ, ЧТО ТАКОЕ ВОЗВРАТ ИНВЕСТИЦИЙ, ЕСЛИ ВЫ НЕ ЭКОНОМИСТ



Светлана ГАЗИЗОВА
директор
по построению
процессов
DevSecOps,
Positive
Technologies

Компании проходят разные стадии своего жизненного цикла, которых Ицхак Адизес выделил десять. От зарождения бизнеса до его логического завершения встретятся самые разные проблемы, но вопрос «А где взять денег?» будет лейтмотивом каждого этапа развития. Потому что деньги пока что самый понятный и удобный количественный ресурс успеха той или иной активности. Хорошо, что мы научились считать эффективность инвестиций: теперь мы понимаем, зачем и куда мы движемся.

ВОЗРАСТ ИНВЕСТИЦИЙ. ТОЧКА ОТСЧЕТА

ROI (return on investment, возврат инвестиций) — коэффициент рентабельности инвестиций, который помогает рассчитать окупаемость вложений в проект. Расчёт этого коэффициента позволяет определить эффективность потраченных средств. Есть ещё понятие **ROSI (return on security investment)**¹, однако такой термин встречается реже.

Исходя из названия и описания, становится понятным, что благодаря этому расчёту вы (как отдельный человек или инвестор) можете узнать, когда все ваши затраты вернутся к вам и в каком объёме превысят вложения. Абсолютно то же самое происходит и с бизнесом: любые затраченные ресурсы компания хочет когда-то вернуть, а понимать, когда это случится, лучше уже в момент этих самых затрат.

Как правило, возврат инвестиций волнует любой бизнес — от крупного до небольших компаний с численностью до 100 человек. Всё-таки цель бизнеса — выжить. А на это может повлиять очень много факторов. Если мы говорим про безопасность, то есть много примеров, когда ошибки в подходах к обеспечению кибербезопасности были фатальными для бизнеса: например, в 2022 году компания 7-Eleven была вынуждена на несколько дней приостановить работу своих магазинов из-за киберинцидента. Помимо репутационных рисков, компания понесла ещё и денежные потери, которые они не раскрывают. Но мы знаем, что средняя стоимость утечки — около 4,45 млн долларов (согласно отчёту IBM Security).

При этом при расчёте возврата инвестиций в безопасность вообще возникает мискоммуникация с бизнесом: очень сложно обосновать затраты так, чтобы они базировались на чётко измеряемых данных — всё держалось на «страшилках» и включении затрат на информационную безопасность в операционные рас-

ходы. То есть бизнесу транслировали, что потратить деньги на безопасность необходимо, потому что:

- ◆ это примерно как страхование;
- ◆ это, наверно, должно быть;
- ◆ это вроде как управление рисками.

Звучит убедительно, да?

НЕПРОЗРАЧНАЯ ИСТОРИЯ

Это далеко не все пункты, которыми оправдывают затраты на безопасность. Именно оправдывают, потому что обоснования тут нет. История с возвратом инвестиций в отрасль безопасности приложений ещё более непрозрачна: гибкие методологии разработки диктуют свои правила, не в каждой из них найдётся место безопасности.

При этом реальная экономика денежных потоков часто не подсвечивается. Когда мы начнём декомпозировать затраты в информационную безопасность приложений, мы увидим, что они делятся на три больших блока (рис. 1). Каждый из этих блоков может как тратить деньги, так и экономить. Посмотрим на примере (рис. 2).

Допустим, для компании, которая разрабатывает приложения, критически важно быть конкурентноспособными и соответствовать пожеланиям потребителя. Для этого её приложения должны быть не только прогрессивными и функциональными, но и технологичными: рынок требует постоянных изменений и улучшений. Поэтому нам нужно снижать ручной труд в угоду автоматизации. Соответственно, для таких компаний очень важно держать фокус внимания на качестве, а не на постоянном «тушении пожаров». И уже такие аргументы приводить

¹ Впервые термин return on investment for security (ROSI) был введён в оборот экспертами в области информационной безопасности после того, как в начале 2002 года была опубликована статья в журнале CIO Magazine — Finally, a Real Return on Security Spending. Параллельно с этим появилось несколько статей, которые были посвящены количественным методам оценки инвестиций в информационную безопасность.



Рисунок 1. Декомпозицию затрат в информационную безопасность приложений можно разделить на три блока.



Рисунок 2. Распределение затрат и экономии, которую получаем по итогу

в пользу расчёта экономической эффективности.

В свою очередь, корректное использование инструментов и внедрение практик безопасной разработки позволяют улучшить показатели компании во многих аспектах, среди которых:

- ◆ увеличение скорости релизов;
- ◆ повышение эффективности разработки;
- ◆ повышение эффективности управления разработкой;
- ◆ повышение качества кода;
- ◆ обеспечение соответствия требованиям.

А уже эти пункты можно посчитать в деньгах: сколько потратим, сколько заработаем.

БЕЗОПАСНОСТЬ ПРИЛОЖЕНИЙ МОЖНО ВЫРАЗИТЬ В ДЕНЬГАХ

Благодаря отчёту 2023 Data Breach Investigation мы знаем, что 95 % всех утечек произошли в веб-приложениях, а 56 % киберинцидентов за последние пять лет связаны также с веб-приложениями. При этом, несмотря на важность веб-разработки, в компаниях 99 % сотрудников не осведомлены даже о списке

угроз OWASP. Об этом мы знаем благодаря отчёту Proof Point. При этом начать процесс работы с уязвимостями можно очень легко — используйте, например, бесплатные плагины, которые помогают разработчику прямо во время написания кода осуществлять его проверку на уязвимости и сразу исправлять их, не выходя из IDE. У нас в Positive Technologies их набор регулярно пополняет команда PT Application Inspector, статического анализатора приложений.

Логично, что из этих 99 % львиную долю занимают среди прочего и специалисты по ИТ: разработ-

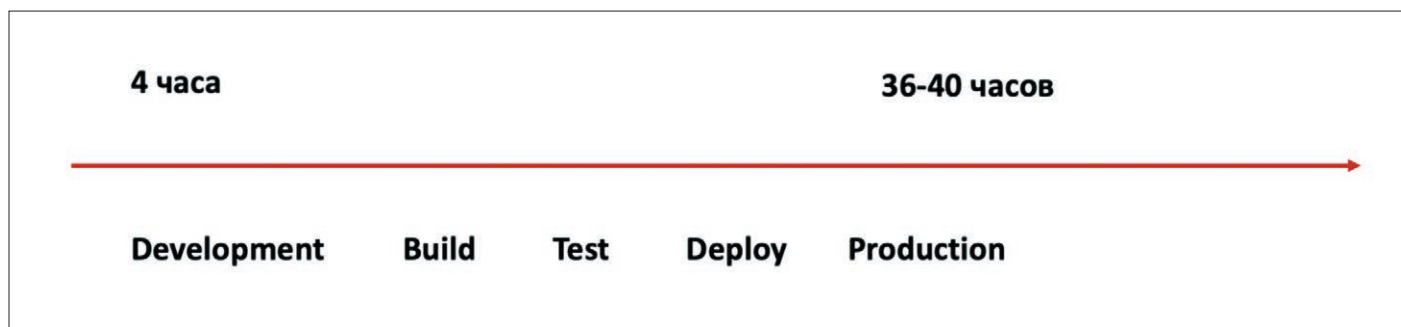


Рисунок 3. Сроки устранения подтвержденной уязвимости в зависимости от стадии разработки

чики, тестировщики и аналитики. Менее 50 % компаний вообще обучают разработчиков безопасному кодированию — большая часть предпочитает «решать проблемы по мере их поступления», то есть просто устранять уязвимости, когда они нашлись!

А найтись они могут далеко-далеко в продакшене. Например, когда будет пентест или приложение начнёт сбоить. Хуже, когда пентест будет незапланированным: тогда у вас нет времени устранять уязвимость — её уже проэксплуатировали.

При этом трудозатраты на устранение уязвимостей разнятся: например, на этапе Development (когда разработчик только пишет код) требуется около четырёх часов в среднем, чтобы устранить проблему. А уже в продуктивной среде это время возрастает до 16–40 часов. Это, кстати, хороший пример для упражнений в математике: можно взять среднюю зарплату разработчиков в час и посчитать, где вы теряете деньги (рис. 3).

КАК ПОВЫСИТЬ ЭКОНОМИЧЕСКУЮ ЭФФЕКТИВНОСТЬ С ПОМОЩЬЮ БЕЗОПАСНОЙ РАЗРАБОТКИ?

Глобально компании живут в парадигме того, что уязвимости либо экстренно устраняются в продакшене, либо до попадания в контур прода. Каждый из этих подходов имеет место, но мы считаем оптимальным превентивный подход. Всё-таки безопасность — это мера качества вашего продукта. Набор продуктов для защиты веб-приложений от киберугроз, таких как Web Application Firewall (WAF), например, PT Application Firewall, продукты SAST (Static Application Security Testing)

и DAST (Dynamic Application Security Testing) — такие как PT Application Inspector и PT BlackBox, помогают на каждом этапе жизненного цикла продукта минимизировать развитие киберинцидентов — устранить уязвимости, обнаружить и заблокировать кибератаки. Сейчас важно и защищать контейнерные среды, так как большая часть прогрессивного бизнеса перешла в Docker и Kubernetes. Есть продукты и для их защиты, например PT Container Security. В идеале нужно, чтобы ИБ-продукты, установленные в компании, работали в связке между собой. Так можно получить синергию выше, потому что платформенный подход всегда экономит время.

Когда разработчик не использовал методы безопасного кодирования и не тестировал приложение на безопасность до его попадания в продакшен, мы получим негативную картину: уязвимость всплывёт, и нам нужно будет её устранять, затратив большое количество времени. При этом обучение специалистов безопасной разработке (безопасному кодированию, внедрению и использованию нужных инструментов, ручному тестированию) занимает, как правило, меньше времени.

Так как разработчики — основная движущая сила большого пласта бизнеса, стоит сказать о том, что и ROI очень часто зависит от них. При этом практики безопасности внутри разработки приложений приносят огромную пользу — как денежную, так и репутационную. GitLab и Forrester выпустили замечательный отчёт — Total Economic Impact, где рассчитали эффективность безопасной разработки с учётом корректного использования инструментов AppSec (когда они работают как единая DevSecOps-платформа).

Цифры впечатляющие:

- ◆ ROI — 427 %.
- ◆ Срок возврата инвестиций — менее полугода.
- ◆ Чистый дисконтированный доход — более 150 млн долларов.
- Конечно, при разных вводных цифры будут отличаться, но даже при пессимистичных сценариях безопасная разработка возвращает деньги за 1,5–2 года. Мы считали.
- Посмотрим **основные** затраты на безопасную разработку:
 - ◆ обучение специалистов application security;
 - ◆ обучение сотрудников практикам безопасного кодирования и работе с инструментами безопасной разработки;
 - ◆ разбор дефектов, обнаруженных в процессе анализа приложения;
 - ◆ внедрение платных инструментов;
 - ◆ привлечение сторонних консультантов;
 - ◆ амортизация физического оборудования.

А теперь **основные** затраты, если вы не будете делать разработку безопасной:

- ◆ позднее исправление уязвимостей;
- ◆ репутационные риски;
- ◆ простой команды разработки;
- ◆ внедрение экстренных патчей;
- ◆ нецелевое расходование человеческих ресурсов.

И это только основные затраты, конкретно для вашей компании приоритеты могут меняться. Это зависит от области деятельности, численности сотрудников и стека технологий. Единственное, что не будет меняться, — это необходимость внедрения проверок безопасности в цикл вашей безопасной разработки.

СЕТИ, ЛОВУШКИ, ЗАСАДЫ, КАПКАНЫ...

КАК БОРЮТСЯ С МОШЕННИКАМИ В VK



Максим БРОНЗИНСКИЙ
руководитель команды
AntiFraud VK

Корреспондент BIS Journal Алёна Николаева беседует с руководителем команды AntiFraud VK Максимом Бронзинским.

ЗОНА ОТВЕТСТВЕННОСТИ

— Максим, давайте плясать от печки. Антифрод — это борьба с мошенничеством. Расскажите, пожалуйста, о своей команде AntiFraud. Чем она занимается, ее цели и задачи, сколько в ней человек, какое место она занимает в структуре VK и соответственно в структуре информационной безопасности VK?

— Информационная безопасность — ключевой приоритет VK. Команда Antifraud входит в департамент защиты клиентов. С одной стороны, мы сфокусированы на «охране» комфорта клиентов, чтобы они чувствовали себя уверенно в наших сервисах и не страдали от действий злоумышленников. Другая задача — быть центром компетенции для разных команд других бизнес-юнитов. Мы предоставляем им необходимый инструментарий, аналитику, «переопыление» — мониторинг отработанных мошенниками схем. В сферу нашей ответственности также входит борьба с фишингом, брутфорсом, защита на уровне непосредственной авториза-

ции и регистрации пользователя, а также предоставление нашим клиентам самых современных способов защиты — технологических и технических. Для полноты картины скажу, что мы используем в основном собственную разработку и собственную аналитику.

— Что является критерием эффективности вашей работы? Основные показатели, на которые вы ориентируетесь? Как и чем отчитываетесь перед руководством? Что является важным для вас лично?

— Соцмедиа — лакомый кусочек для злоумышленника. Тут в ход идут и прямое мошенничество, и вымогательство, и попытки взлома. И основной критерий эффективности нашей работы — оценка пользовательской безопасности, которая формируется на основании опросов и через внутреннюю аналитику. Главный показатель — число взломов пользователей и стоимость взлома. Хотя последнее является косвенным показателем, мы не можем не брать его в расчет, потому что так оценивается заинтересованность злоумышленников в наших сервисах и продуктах.

Руководство присутствует во всех наших сервисах, у них есть возможность в реальном времени видеть отзывы клиентов. Вокруг этого выстроена и система ключевых результатов, которые мы согласовываем как внутри маленьких и больших команд, так и на уровне компании.

Лично для меня важна обратная связь от клиентов, ведь эти сервисы созданы для них. И то, насколько безопасно они чувствуют себя в них, напрямую влияет на бизнес. Как говорится, больше доверия — больше клиентов.

— Каким техническим арсеналом обладаете?

— У нас нет никаких ограничений ни в технологиях, ни в экспертизе. Мы не являемся за-

BIS-СПРАВКА

VK — крупнейшая по числу пользователей российская технологическая компания. Продукты и сервисы VK помогают миллионам людей решать повседневные задачи онлайн: ими пользуются больше 95% аудитории рунета. Проекты VK позволяют общаться, играть, осваивать новые профессии, слушать музыку, смотреть и снимать видео, решать множество других задач. Компания также развивает набор продуктов и услуг для цифровизации бизнес-процессов — от интернет-продвижения и предиктивной аналитики до корпоративных соцсетей, облачных сервисов и автоматизации предприятий.

ложниками каких-то обстоятельств. Наша компания очень большая, и в ней, кажется, можно найти или заново создать все необходимое. И технологии машинного обучения, и технологии хранения или обработки данных, и аналитику, проверку гипотез, основанную на матапарате. Мы просто выбираем лучшее решение, понимаем и обосновываем, почему оно лучшее, а дальше применяем, исходя из задачи.

— **В чем специфика вашего подразделения по сравнению с антфрод-подразделениями других организаций?**

— У нас нет классической задачи антифрода — победить всех злоумышленников, мы не воюем против кого-то. Мы, скорее, боремся вместе. Повторюсь, у нас есть технологии, которые мы можем взять из соседнего подразделения. У нас есть цели, но они не в том, чтобы поймать столько-то злоумышленников. Наша миссия в том, чтобы тысячи, сотни, миллионы наших пользователей чувствовали себя спокойно и безопасно.

— **Интересно узнать статистику — общую и предметную — вашей работы?**

— К примеру, в месяц это может быть сколько-то миллиардов отбитых брутфорс-атак на пользователей. Также есть такая метрика, как количество предотвращенных взломов.

СРАВНЕНИЕ С БАНКАМИ

Много лет BIS Journal фокусировался на информационной безопасности банков, теперь наша тематика расширилась до ИБ в бизнесе и соответственно в разных отраслях. В связи с этим несколько вопросов.

— **Зампред Сбера Станислав Кузнецов недавно заявил на наших страницах, что в ноябре Сбер отразил DDoS-атаку мощностью 1 млн запросов в секунду, а также, что под давлением преступников россияне взяли кредитов на 200 млрд рублей. Происходит ли что-то подобное по масштабам в VK? Расскажите о масштабе и многообразии «ваших» угроз?**

— Происходит ли что-то подобное по масштабам в VK? Да. Я уже упоминал, что попытки брутфорс-атак на наших пользователей исчисляются миллиардами. Но суть в другом. Как мы все знаем, эмоции людей — это слабое звено любой информационной системы и ее безопасности. И тут у нас нет ничего нового по сравнению с другими масштабами или многообразием угроз. Они все одинаково направлены на то, чтобы вывести человека на какую-то эмоцию: чувство срочности, неотложности, опасности.

— **Социальная инженерия в банковской сфере хорошо изучена, хоть и не побеждена. Чем отличается мошенничество**

в социальных сетях от мошенничества в финансовой сфере?

— Опять же, принципиально ничем. Мошенник играет на чувствах, его задача — получить деньги. В случаях банковского мошенничества, вам как правило звонят «из службы безопасности банка», причем, с какого-то неизвестного номера. А в соцмедиа просто стучатся в личные сообщения или в комментарии. То есть механизмы онлайн и оффлайн не отличаются, равно как и цели.

СПЕКТР ОБМАНА

— **Расскажите об основных видах мошенничества, с которыми вы работаете. Как их можно классифицировать? Можно ли выстроить среди них рейтинг опасности для личности и общества?**

— Для общества в широком смысле мошенничество опасно массовыми фейками, информационными вбросами и так далее. Но это не наша сфера. Что касается мошенничества в соцсетях, направленного на конкретную личность, то это, как правило, три направления: доступ к аккаунту жертвы; вымогательство в прямом виде; фишинг.

Доступ к аккаунту часто получается с помощью того же фишинга, порой — с помощью прямых атак на аккаунты. Вымогательство происходит как правило в личных сообщениях, тут мошенники оперируют какой-то опасностью, неотложностью. В фишинговых атаках обычно эксплуатируют человеческую жадность. Как пример — приманка в виде выигрыша щедрых промокодов, когда пользователь переходит по сомнительной ссылке и авторизуется, вводя свои персональные данные. И далее у злоумышленника уже есть все необходимое для взлома аккаунта. Имея доступ к аккаунту, можно заняться вымогательством и т.д. То есть каждый из перечисленных выше видов преступления — это специализация на разных этапах доступа к жертвам.

— **Существуют ли среди ваших сотрудников специализация по этим видам? Какая?**

— Да, есть специализация, но скорее по типам борьбы с различными видами мошенничества. Почему важно их разделять? Потому что каждый сценарий требует достаточно глубокого погружения в продукт, понимания пользовательского поведения, применимой в сложившихся обстоятельствах схемы мошенничества. Но, опять же, повторюсь, в контексте неограниченности наших возможностей, в компании есть культура создания профессиональных сообществ и площадок. Соответственно, между всеми командами специалистов есть общая площадка, на кото-

рой мы обмениваемся новыми схемами мошенничества и технологиями для их поиска и борьбы. В различных сервисах есть ребята, которые борются конкретно с фишингом или конкретно с доступом злоумышленников к аккаунтам. Это разные люди, но так или иначе все взаимосвязано.

— **О каких новых видах и схемах обмана в интернете стало известно за последнее время?**

— Сравнительно новый тренд — дипфейки и дипвойсы, когда подделывают видео или голос. В мировой практике уже есть прецеденты, повлекшие за собой миллиардные убытки. И эти технологии стремительно совершенствуются — отличить подделку сходу часто невозможно. Соответственно меняется и отношение безопасников к этим технологиям, в частности и наши рекомендации пользователям.

— **Какие, например?**

— Главная рекомендация: не отвечайте кому попало на видеозвонок, не показывайте свое лицо, не отправляйте голосовые сообщения малознакомым людям — там ваш голос могут синтезировать. И, самое главное, если почувствуете, что на вас давят какой-то срочностью, опасностью, если понимаете, что вас пытаются вывести на эмоции — остановитесь, прекратите разговор с этим человеком. Например, попросите его перезвонить или подождать, скажите: «Я вернусь в сообщениях / я вернусь через час». После этого уточните переданную вам информацию в альтернативном источнике.

Условная ситуация: видеозвонок от мамы, которая говорит, что ей срочно нужны 5 тыс. рублей. В таком случае надо положить трубку и написать ей в мессенджере: действительно ли ей она просит у вас эту сумму? На это уйдет 5 минут, но вы сэкономите и нервы, и деньги.

ПРО КАДРЫ

— **Борьба с мошенничеством — отдельная большая, изменчивая сфера. Кто в ней работает? Можно ли назвать ее отдельной профессией? Какое у этих людей образование? Как они повышают свою квалификацию? Хватает ли вам кадров?**

— Обычно в эту сферу приходят либо с каким-то бэкграундом безопасности, либо с бэкграундом работы с контентом. Такие люди по роду своей деятельности сталкивались с мошенничеством напрямую или косвенно. Можно ли это назвать отдельной профессией? Наверное, да. В явном виде она не определена, скорее это специфическое направление в профессии безопасника. По крайней мере, я не знаю учебного заведения, где учат

бороться с мошенниками в соцсетях, но тут в любом случае требуются знания базовых принципов ИБ, логика и небезразличие — это, наверное, основные критерии, по которым набирают к нам на работу.

А повышение квалификации приходит с набиванием шишек, порой с болью наших клиентов, с совместной работой с профсообществами, форумами и чатами. Ключевым фактором в нашей специфике, по-моему, является «опубличивание» новых способов мошенничества. Ведь чем больше мы делимся опытом, тем меньше вероятность осуществления таких схем. Проще говоря, наши клиенты будут в курсе того, что не стоит отвечать на звонок от банка в мессенджере, потому что банки никогда не совершают таких звонков.

ПРО ТЕХНОЛОГИИ И ИМПОРТОЗАМЕЩЕНИЕ

— **Какими технологиями вы пользуетесь? Испытываете ли «революционную ситуацию» в связи с импортозамещением? Как оно проходит? Какие проблемы? Какова доля самообеспечения?**

— Большая доля технологий, которые мы используем, приходится на разработки внутри компании, т.е. это либо in-house разработка, либо переработанный Open source, который мы кастомизируем под себя. Кое-где применением технологии наших партнеров, но их количество не значительно.

Испытываем ли мы потребности в импорте? Нет. Да и в целом я вижу, что наши решения во многом более передовые по сравнению с зарубежными. То есть какой-то нехватки, по крайней мере, в нашей сфере, мы не ощущаем, во многом, опять-таки, благодаря обилию возможностей нашей компании.

— **Существует ли концепция импортозамещения для ИБ VK? В чем ее суть?**

— Говоря в целом, импортозамещение — это не то, что прибили гвоздями, по крайней мере, для нас это не самоцель. У нас есть возможность разрабатывать собственные решения, используя опыт коллег, есть возможность разрабатывать решения на основе Open source. Мы уже увидели немало продуктов отечественного производства, и не только в сфере ИБ. И эти продукты не только не уступают, но чаще — лучше зарубежных аналогов. Важно отметить, что мы имеем поддержку со стороны руководства и партнеров в целом, благодаря чему имеем возможность создавать уникальные вещи. Поэтому нет какой-то ярко вырабатанной концепции, скорее есть понимание нашей самостоятельности и ощущение, что мы не одиноки и всегда можем обратиться за помощью.

Беседовала
Алёна Николаева

ВЫМОГАТЕЛИ И ЧЕЛОВЕЧЕСКИЙ ФАКТОР

КАК РАСШИФРОВАТЬ ГЛАВНОЕ?



Андрей ЖАРКЕВИЧ
ведущий рубрики,
эксперт Start X

Вымогательские киберинциденты в мире стали не менее заметным явлением, чем телефонные мошенники в РФ. И если количество мошеннических звонков становится всё меньше благодаря комплексу мер со стороны государства, банков и операторов связи, успешные вымогательские атаки демонстрируют стабильный рост.

Почему же вымогатели процветают, несмотря на попытки глобального противодействия, в котором принимают участия государственные спецслужбы технологически продвинутых стран? Может быть, дело в том, что сражение с хакерами проходит не там, где нужно, а там, где получается? Давайте разбираться.

КАК ВЫГЛЯДИТ ВЫМОГАТЕЛЬСКИЙ ИНЦИДЕНТ ДЛЯ ПОСТОРОННИХ

Обычно в СМИ появляются примерно такие сообщения:

«Вымогательская группировка APTXXX проникла в сеть компании «Важное Производство», похитила персональные данные клиентов и секретные документы о продуктах, зашифровала серверы и потребовала выкуп. Работа жертвы парализована. Для расследования инцидента привлечены эксперты. Сроки восстановления работы компании пока не называются».

Иногда упоминают, что для проникновения хакеры воспользовались уязвимостью CVEXXX-YYY или другим способом, но это скорее исключение, чем правило.

ДЛЯ ПОСТРАДАВШИХ

Здесь всё намного интереснее. Руководство компании проходит все стадии по модели Элизабет Кюблер-Росс — шок, отрицание, гнев, торг, депрессия, принятие.

Шок

Всё было нормально, системы работали, люди выполняли поставленные задачи, и вдруг всё поломалось. Пропал доступ к документам, не работает сайт, компьютеры не загружаются.

ИТ- и ИБ-специалисты пытаются понять, в чём дело, обнаруживают записку от вымогателей. В ней написано, что конфиденциальные данные скопированы, а файлы зашифрованы. Вернуться к нормальной жизни можно, если заплатить выкуп. Срок такой-то. Если не заплатить, все секретные документы будут опубликованы в открытом доступе или проданы заинтересованным лицам.

Отрицание

Руководство в ярости кричит и топает ногами, требуя срочно вернуть всё как было, но единственный результат — это паника среди ИТ- и ИБ-сотрудников, которые трясущимися руками разыскивают резервные копии и судорожно пытаются понять, каким образом компанию взломали.

Гнев

Кто-то вспоминает о существовании планов обеспечения непрерывности бизнеса и аварийного восстановления, а также о том, что есть назначенные приказом ответственные по этим планам. Только оба документа хранились на сервере, который зашиф-

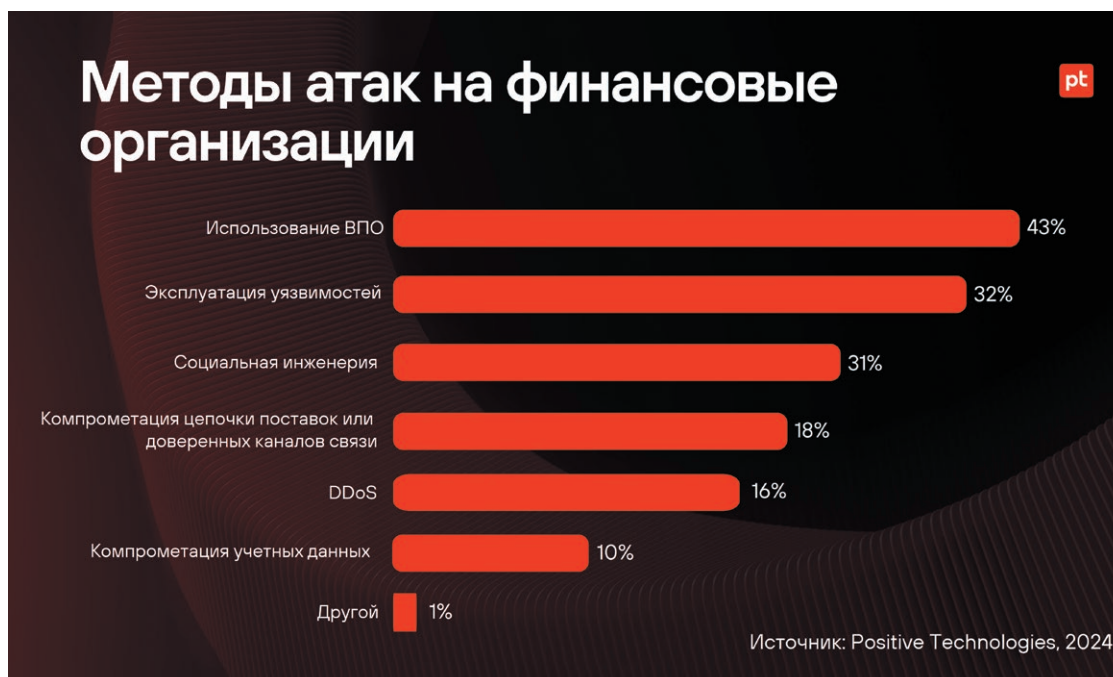


Рисунок 1. Слайд из презентации Алексея Лукацкого на Digital Kyrgyzstan в феврале 2024 года, опубликованной в телеграм-канале «Пост Лукацкого»

ровали вымогатели. Распечатанная версия неактуальна.

Руководство пытается совершить понятное и привычное действие — наказать виновных, но юристы напоминают, что об инциденте нужно сообщить регулятору, иначе накажут и руководителя, и организацию. Ищут регламент, но и он зашифрован. Интернет не работает. Наконец с телефона открывают сайт регулятора и что-то вроде отправляют.

Торг

Руководство закрывается в кабинете и пытается подсчитать стоимость простоя, чтобы понять, не выгоднее ли будет заплатить выкуп. Тем более что на горизонте маячит ненулевая вероятность штрафа за утечку персональных данных клиентов. Делать это приходится буквально на пальцах, потому что вся финансовая информация зашифрована, системы не работают.

Несмотря на трудности, решение проблемы переходит в практическую плоскость: как купить криптовалюту, как убедить регулятора, что никаких выкупов не платили, и можно ли вообще верить этим преступникам?

Депрессия

Решение принято и выполняется. Но радоваться нечему. Время восстановления работы может быть самым разным, поскольку зависит от множества факторов:

- ♦ заплатили выкуп или решили восстанавливать своими силами;

- ♦ если заплатили, то получится ли расшифровать все данные;

- ♦ если решили не платить, есть ли резервные копии всех зашифрованных данных;

- ♦ если копии не самые свежие, можно ли восстановить утраченную информацию и сколько времени это займёт.

ВАЖНОЕ НАБЛЮДЕНИЕ

В описании большинства инцидентов не говорится про IDS, IPS, DLP и прочие системы защиты. Это не потому, что их ни у кого нет. Системы защиты затрудняют действия вымогателей, но не являются определяющим фактором успешного взлома. Почему?

А потому что причина 95% всех киберинцидентов — действия людей, тот самый человеческий фактор. Об этом говорится в масштабном исследовании кибератак в 130 странах IBM Cyber Security Intelligence Index Report, проведённом в 2021 году среди тысяч клиентов компании.

В 2024 году ситуация принципиально не изменилась. Все аналогичные исследования подтверждают полученные IBM результаты.

СВЕРЯЕМ ЦИФРЫ

Чтобы не быть голословными, давайте обратимся к свежим данным, которые представил в своём выступлении на Digital Kyrgyzstan мэтр российского ИБ-сообщества Алексей Лукацкий (рис. 1).

МЕТОДЫ АТАК И ЛЮДИ

Давайте пройдемся по методам атак и выясним, насколько они зависят от действий людей.

Компрометация учётных данных

Учётные данные компрометируются не сами по себе, а потому, что люди вводят их на сторонних ресурсах, считая, что делают всё правильно. И даже кража логинов и паролей — результат небезопасных действий людей, например программиста, который сохранил пароли в базе в виде открытого текста или MD5-хеши без соли.

Компрометация цепочки поставок

Компрометация цепочки поставок может выглядеть по-разному. Например, это может быть вредоносный пакет из репозитория PyPi, имя которого очень похоже на имя настоящего. Просто программист опечатался и добавил в проект не то, что нужно.

Или это может быть взлом почтового ящика контрагента с последующим внедрением в переписку и выполнением вредоносных действий, нужных атакующим.

Но почту контрагента взломали из-за того, что он использовал пароль 123456. То есть компрометация цепочки поставок произошла из-за небезопасных действий человека.

Социальная инженерия

Здесь никаких двусмысленностей, поскольку социальная инженерия — это инструмент для воздействия на людей. Она позволяет убедить сотрудника открыть вредоносное вложение в письмо, а администратора — установить «внеочередное обновление» или отключить защиту «для проведения пентеста».

Эксплуатация уязвимостей

Уязвимости появляются не сами по себе, а в результате ошибок, допущенных разработчиками и пропущенных тестировщиками. А их эксплуатация становится возможной из-за того, что администратор не успел или забыл установить исправление безопасности, выпущенное полгода назад.

Использование ВПО

Чтобы вредоносное ПО нанесло вред, ему требуется каким-то образом попасть в инфраструктуру финансовой организации. Способов доставить ВПО не так много, и все они связаны с тем, что делают или не делают люди:

- ♦ внедрить через уязвимый сервис, например службу удалённого рабочего стола Windows;

- ♦ убедить сотрудника открыть вложение из фишингового письма и разрешить редактирование документа, чтобы при этом запустился вредонос;

- ♦ украсть логин и пароль пользователя, когда он введёт их на фишинговом сайте, а затем войти в систему от его имени и запустить ВПО;

- ♦ с помощью угроз или денег заставить сотрудника запустить файл с флешки или установить «обновление» из письма.

Получается, все перечисленные на слайде (рис. 1) методы атак, кроме DDoS, напрямую зависят от действий людей.

С атаками выяснили, теперь давайте посмотрим, как обстоят дела с защитой от шифровальщиков.

КАК СРАЖАЮТСЯ С ВЫМОГАТЕЛЬСКИМИ ГРУППИРОВКАМИ

Проблема вымогательских группировок вышла на международный уровень, поскольку преступники атакуют не только богатые компании, но и объекты критической инфраструктуры. Особо циничные требуют выкуп даже у детских больниц. Вполне закономерно, что государственные спецслужбы многих стран принимают меры противодействия, самая заметная из которых — блокировки инфраструктуры.

Блокировки инфраструктуры

В СМИ регулярно появляются сообщения об уничтожении инфраструктуры очередной вымогательской группировки. Пользуясь полномочиями, силовики разделегируют домены, которые используют вымогатели, захватывают контроль над управляющими серверами и отключают их. Затем публикуется бодрый пресс-релиз.

Спецслужбам приходится отчитываться за освоенные бюджеты, поэтому без таких вот историй успеха не обойтись. Но что на практике?

Вспомним, как в ноябре 2023 года ФБР заявила о победе над великой и ужасной группировкой BlackCat, также известной как ALPHV. Арест инфраструктуры, отключение серверов и заглушка с сообщением об аресте на главном сервере злоумышленников.

А что было потом? После нескольких недель тишины «Чёрная кошка» ожила и продолжила вымогательскую активность. Забавно, что, когда группировка действительно решила скрыться с полученным крупным выкупом в феврале 2024 года, на их сайте появилась старая заглушка о том, что сайт конфиско-

ван ФБР, Минюстом США и прочими силовыми ведомствами (рис. 2).

И это далеко не единственный случай. Многие группировки, якобы «уничтоженные» спецслужбами, проводили ребрендинг и собирали выкупы уже под новым именем. Почему?

Потому что такая борьба только выглядит серьезной. По сути же она эквивалентна тому, как если бы у офлайн-преступников отняли арендованные автомобили, на которых они возят краденое, и отпечатанную на цветном принтере вывеску с названием фиктивной компании, которая висела на двери арендованного офиса.

Попытки запретить криптовалюту

Логика борцов с вымогателями чрезвычайно прямолинейна: криптовалюта обеспечивает анонимность, её никто не контролирует, поэтому её используют для получения выкупов. Запретим криптовалюту — вымогатели не смогут получать выкуп — цель достигнута.

Криптовалюта действительно выглядит как идеальный инструмент для вымогателей, но давайте представим, что её нет. Что помешает вымогателям требовать выкуп в другой форме, например, в виде перевода на электронные кошельки или на банковские карты?

Их легче отследить и заблокировать, но вопрос в том, что, если жертва принимает решение заплатить выкуп, в её интересах хранить перевод средств в тайне до тех пор, пока вымогатели не расшифруют данные и не заверят в том, что удалили похищенное. И если говорить про отслеживание, то стоит вспомнить, что все транзакции по криптовалюте фиксируются в блокчейне, поэтому их анонимность довольно условна.

Таким образом, запрет криптовалют не окажет существенного влияния на деятельность вымогателей. Да и принципиальная возможность такого запрета с учётом децентрализованного характера криптовалют выглядит сомнительной.

Штрафы для жертв вымогателей

Утечки данных — несомненное зло. Это удар по репутации компаний, у которых данные украли, проблемы для людей, информация о которых попала в утечку. Государство не может оставлять такие инциденты без внимания, поэтому компании, допустившие утечки, получают наказание в виде штрафа.

Пока любители покарать рассуждают о справедливости такого наказания, давайте ещё раз присмотримся к ситуации, когда вымогатели похитили у компании пер-

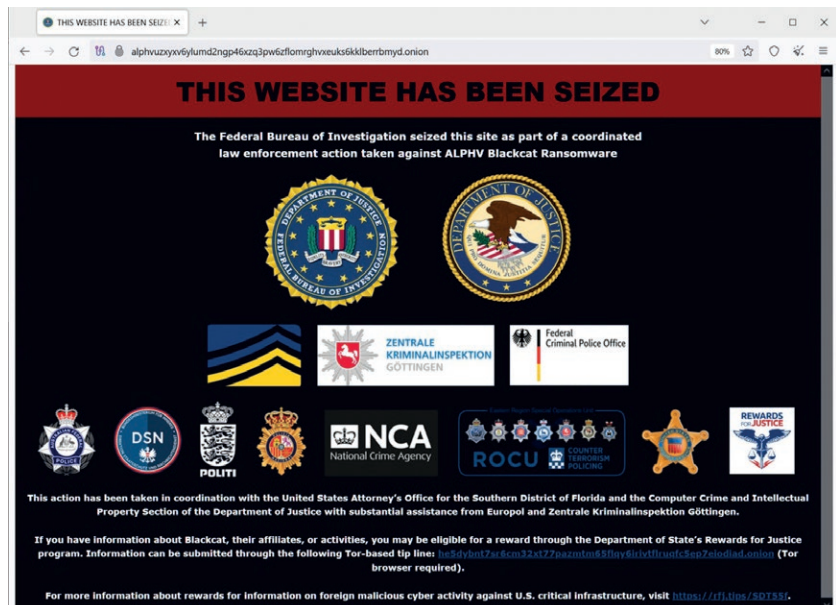


Рисунок 2. Фальшивое сообщение о «захвате» ресурса спецслужбами на Tor-сайте BlackCat

сональные данные клиентов и угрожают их публикацией.

◆ Если не заплатить выкуп, вымогатели опубликуют данные. Утечка будет обнаружена, компания получит штраф. Если нарушение повторное — штраф будет от оборота компании. А ещё придётся раскошелиться на восстановление данных и как-то компенсировать ущерб репутации.

◆ Если втихую заплатить выкуп, вымогатели не опубликуют похищенную информацию и предоставят инструмент для расшифровки. Никакой утечки, никакого штрафа, ущерб репутации минимальный, остановку работы можно объяснить техническим сбоем.

Какую таблетку должен выбрать руководитель компании, синюю или красную? А какую выбрали бы вы?

Есть и ещё одна тонкость по поводу оборотных штрафов. Они будут гигантскими для компаний с большими оборотами и нулевыми для госучреждений, у которых нет оборота. В связи с этим Ассоциация банков попросила Минцифры отказаться от введения оборотных штрафов за утечки информации, называя меру дискриминационной.

Суровые наказания для хакеров

Преступники не планируют быть пойманными, если только не стремятся к геростратовой славе. А это значит, что даже самое суровое наказание не напугает, поскольку в их представлении оно к ним не относится. Они другие, не такие, как те, кто попался. Они умнее, сильнее, хитрее и изобретательнее. И их не поймают.

Подведём итог

Подведём итог. Самые популярные методы борьбы с вымогательскими группировками на сегодняшний день выглядят довольно неубедительно. Рост числа вымогательских инцидентов и регулярное появление новых участников этого «бизнеса» наглядно подтверждают эту нерадостную тенденцию.

ЧТО ДЕЛАТЬ?

Вымогательское ПО — наглядный пример того, как достаточно простой набор инструментальных средств и умелое использование особенностей человеческой психики породили настоящее глобальное зло, многоголовую гидру, которая растёт и развивается, питаясь небезопасными действиями людей. Витязи в сияющих доспехах могут бесконечно отсекал её головы, на месте отрубленных вырастают новые. Возводить стены и менять мечи на сабли бессмысленно. Гидра вырастет и разрушит стены.

Нет смысла приобретать новые технические системы защиты, если пользователи открывают вложения из фишинговых писем, программисты пишут код с уязвимостями, а администраторы забывают установить обновления и ограничить доступ к базам данных с персональными данными. Такой подход создаёт опасную иллюзию безопасности. До очередного инцидента.

Если причина инцидентов — действия людей, значит, нужно сосредоточиться на этом и решить проблему комплексно. Для этого культура кибербезопасности должна превратиться из абстрактного словосочетания в осязаемую и всеми принимаемую часть бизнес-процессов.

Это значит, что руководители всех уровней понимают, что люди — фундамент защиты компании от кибератак. И укреплять периметр нужно не только «железками», но и тренированными и обученными сотрудниками, действия которых станут непреодолимым рубежом обороны от кибервымогателей.

Культура кибербезопасности включает в себя культуру разработки кода без уязвимостей. Это значит, что программистов нужно научить правилам написания безопасного кода, а специалистов по безопасности — формулировать требования к программистам не в стиле «всё запрещать, никуда не пускать», а так, чтобы их можно было понять и реализовать на уровне кода. И разумеется, тотальная Shift-Left Security. Думать о безопасности на стадии создания проекта, а не накануне его сдачи.

Администраторам и DevOps-инженерам тоже не стоит обманываться по поводу своей непогрешимости. Их действия тоже могут стать причиной успешной атаки. И если они откроют вложение с шифровальщиком, последствия будут хуже, чем у обычных пользователей.

Таким образом, чтобы реализовать защиту от вымогателей и других атак, использующих ошибки людей, необходим комплексный подход, объединяющий теоретические знания, практические навыки и технические факторы.

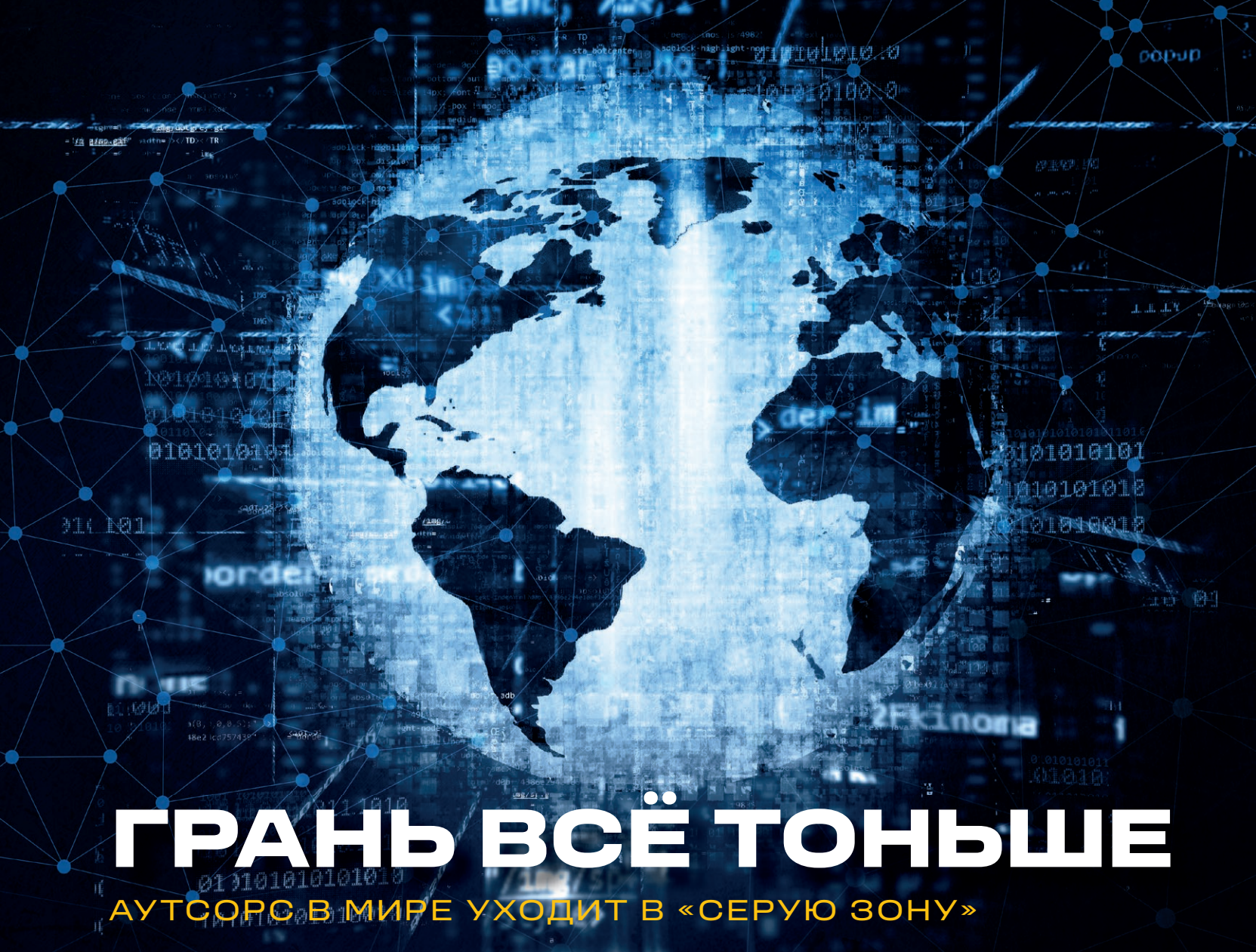
Пример практической реализации описанного подхода — экосистема Start X. Она появилась в результате развития платформы «Антифишинг», ориентированной на обучение и тренировку навыков безопасного поведения сотрудников. В ходе работы над «Антифишингом» стало понятно, что уязвимой для атак компанию могут сделать не только обычные офисные сотрудники, но и разработчики ПО, администраторы, DevOps-инженеры и сотрудники ИБ-подразделений.

В результате платформа «Антифишинг» получила новое имя — Start AWR (от awareness — осведомлённость), а кроме неё, стали развиваться новые продукты для решения проблем человеческого фактора в информационной безопасности.

Кроме Start AWR, в экосистеме имеются решения для:

- ♦ управления требованиями к безопасности создаваемых программных продуктов и организации взаимодействия безопасности и команд разработки (Start REQ);
- ♦ развития навыков практической безопасности у продуктовых команд и вовлечения их в процессы DevSecOps (Start CTF);
- ♦ прокачки навыков написания безопасного кода у разработчиков (Start EDU);
- ♦ проверки внешней поверхности атак, в том числе поиска «забытых» доменов, открытых портов и уязвимых сервисов, «тестовых» баз данных с конфиденциальной информацией и даже адресов электронной почты компании в базах утечек учётных записей (Start EASM).

Даже лучшие защитные решения не гарантируют неуязвимость. Намного важнее люди, которые используют эти инструменты. Поэтому именно на людях следует сосредоточить внимание, чтобы защитить компанию от большинства угроз.



ГРАНЬ ВСЁ ТОНЬШЕ

АУТСОРС В МИРЕ УХОДИТ В «СЕРУЮ ЗОНУ»

Марина БРОДСКАЯ
обозреватель BIS Journal

Кибернаёмники всё чаще работают в «серой зоне» между корпоративной кибербезопасностью и наступательными кибероперациями и не стремятся к публичности. На этом фоне национальные регуляторы стоят на страже интересов государства, бизнеса и инвесторов и ужесточают требования по кибербезопасности для легальных компаний.

NIST: КОНЦЕПЦИЯ КИБЕРБЕЗОПАСНОСТИ 2.0

В конце февраля 2024 г. Национальный институт стандартов и технологий США (NIST) опубликовал Концепцию кибербезопасности 2.0. Первая версия NIST Cybersecurity Framework (CSF) была издана в 2014 г. и обновлена в 2018 г.

NIST CSF «предлагает таксономию результатов кибербезопасности высокого уровня, которые могут использоваться любой организацией (независимо от её размера, сектора или зрелости), чтобы лучше понимать, оценивать, расставлять приоритеты и сообщать о своих усилиях по кибербезопасности».

Во всём мире компании, отрасли и государственные организации всё чаще полагаются на Концепцию кибербезопасности, разработанную NIST. Теперь NIST предложил потенциально важные обновления, в том числе «расширенное применение». Хотя первоначально CSF была разработана для устранения рисков кибербезопасности критической инфраструктуры, она стала широко применяться на практике, в том числе на международном уровне. CSF 2.0 принимает этот факт и признаёт, что Концепция «предназначена для использования организациями всех размеров и секторов, включая госсектор, промышленность, научные круги и некоммерческие организации, не-

зависимо от уровня зрелости их программ кибербезопасности».

Появилась и новая функция — «управление», дополнившая пять исходных функций CSF — выявление, защиту, обнаружение, реагирование и восстановление. Новая функция позволяет следить за тем, установлены ли, доводятся ли до сведения и отслеживаются ли «стратегия, ожидания и политика управления рисками кибербезопасности организации». В частности, функция управления «направлена на понимание организационного контекста; разработку стратегии кибербезопасности и управление рисками цепочки поставок в области кибербезопасности; роли, обязанности и полномочий; политику и надзор за стратегией кибербезопасности», говорится в Концепции.

По мнению NIST, «компонент управления подчёркивает, что кибербезопасность является основным источником корпоративных рисков, что должно учитываться менеджментом компаний наряду с другими показателями, такими как финансы и репутация».

Повышенное внимание к управлению рисками кибербезопасности в цепочке поставок («C-SCRM»). В рамках CSF 2.0 функция «Управление» включает категорию C-SCRM, которая расширяет аналогичную категорию, ранее описанную в функции идентификации CSF 1.1 (ID.SC). В новой интерпретации C-SCRM — систематический процесс управления рисками кибербезопасности на всём протяжении цепочки поставок с участием всех заинтересованных сторон. Например, некоторые из подкатегорий C-SCRM затрагивают вопросы интеграции C-SCRM в процессы кибербезопасности и управления рисками организации, организации комплексных проверок для снижения рисков до начала работы с поставщиками и контроля их деятельности на протяжении всей технологической цепочки или жизненного цикла услуги среди прочих аспектов.

Новые справочные инструменты. Наряду с CSF 2.0 NIST выпустил дополнительные инструменты и ресурсы, помогающие организациям внедрить Концепцию, такие как новые примеры внедрения. В частности, опубликованы новые руководства по быстрому запуску, «предназначенные для определённых типов пользователей, таких как малые предприятия, менеджеры по корпоративным рискам и организации, стремящиеся обезопасить свои цепочки поставок».

Также NIST выпустила краткое руководство по C-SCRM, в котором описывается, как использовать CSF 2.0 для создания и эксплуа-

тации возможностей C-SCRM. Аналогичным образом NIST опубликовал краткое руководство по управлению рисками предприятия, в котором содержится введение в «планирование и интеграцию общеорганизационного процесса интеграции информации по управлению рисками кибербезопасности».

Отдельный документ NIST — новый справочный инструмент по CSF 2.0, который позволяет пользователям изучать функции платформы и динамически связывает Концепцию с другими системами кибербезопасности, стандартами, руководящими принципами и ресурсами.

После публикации CSF 2.0 NIST заявил, что примеры реализации и информационные ссылки будут обновляться чаще, чем остальная часть ядра. Эти ресурсы будут публиковать и поддерживать в интернете.

ПРАВИЛА СКОРРЕКТИРУЮТ

В 2023 г. Комиссия по ценным бумагам и биржам США (SEC) разработала новые Правила раскрытия информации о кибербезопасности, чтобы повысить прозрачность инвесторов в отношении рисков кибербезопасности и фактических инцидентов кибербезопасности, влияющих на их инвестиции. Правила вступили в силу 18 декабря прошлого года, они применяются ко всем публичным компаниям, на которые распространяются требования к отчётности Закона о ценных бумагах от 1934 г. и охватывают определённые процессы корпоративного управления, а также саму информацию о существенных инцидентах кибербезопасности. У небольших компаний, предоставляющих отчётность, есть дополнительный льготный период для соблюдения Правил до 15 июня 2024 г., пишет американская версия Forbes.

Издание отмечает, что некоторые компании уже раскрыли информацию о киберинцидентах, в том числе Microsoft, Hewlett Packard, UnitedHealth Group, Prudential Financial, производитель одежды VF Corp и ипотечный брокер Loan Depot. Однако возникла новая проблема: ни одно из оповещений об инцидентах не соответствует новым Правилам раскрытия информации SEC.

Согласно требованиям Комиссии, владельцы предприятий обязаны раскрыть информацию в течение четырёх рабочих дней после того, как компания сочтёт киберинцидент существенным для разумного инвестора. Это могут быть несанкционированные действия и случайные происшествия, не связанные с целевой атакой. Если информационные системы компании выходят из строя из-за сбоя

внутренних систем и компания считает этот инцидент существенным для разумного инвестора, поскольку, например, не может обрабатывать транзакции, организация должна раскрыть информацию в соответствии с новыми правилами. Аналогичным образом происходит раскрытие информации при кибератаках и утечках данных.

Исключением из правила четырёхдневного срока может стать инцидент, который определён Министерством юстиции США как угрожающий интересам национальной или общественной безопасности. В таком случае процесс раскрытия информации проходит через ФБР.

Forbes напоминает, что Microsoft и Hewlett Packard недавно сообщили о взломе корпоративной электронной почты и ряда служб. Компания VF Corporation уведомила регуляторов об утечке данных и отключении систем перед сезоном отпусков, что сказалось на возможности обработки заказов. Ипотечный брокер Loan Depot сообщил об утечке почти 17 млн персональных данных клиентов и отключении ряда систем. Во всех случаях инвесторы не получили достоверной информации об инцидентах кибербезопасности, существенно влияющих на бизнес владельцев. Согласно правилам SEC, компании должны дать описание существенных аспектов характера, масштабов и времени инцидента и его влияния на финансовое состояние организации.

Однако компании отделались общими словами, которые недостаточны и не соответствуют новым правилам раскрытия информации SEC, поскольку вторая часть документа требует раскрытия существенных последствий. Причём не только качественных, но и количественных, выраженных в суммах штрафов, выплат, потере выручки, влиянии на прибыль, затратах на устранение последствий, потере стоимости акций.

22 февраля медицинская страховая компания UnitedHealth Group сообщила об инциденте, который привёл к отключению систем. На следующий день после взлома агентство Moody's дало компании негативный прогноз. Позднее стало известно, что хакеры украли более 6 ТБ данных поставщиков медуслуг, страховых компаний и аптек. Однако спустя 10 дней UNH не внесла поправок в первоначальное заявление о существенных аспектах инцидента. Эксперты, опрошенные изданием, отмечают, что неопределённость в отношении того, как SEC и компании определяют существенность инцидента, позволяет руководителям укло-

няться от необходимости раскрытия информации. Поэтому правила будут уточняться SEC по мере накопления практики применения, будут накладываться штрафы, которые заставят все организации разработать более структурированные процессы по всем вопросам. Институциональные инвесторы также начнут оказывать давление на советы директоров компаний, требуя подробной информации о работе и защищённости ИТ-систем.

БЕЛЬГИЯ В ТУПИКЕ

Брюссель пытается найти выход из политического тупика, связанного со схемой сертификации облачных сервисов на соответствие требованиям кибербезопасности ЕС. Бельгия предлагает отделить страновой суверенитет от функциональных требований, говорится в документе, подготовленном Национальным центром кибербезопасности страны, сообщает Euronews. Национальные правительства ЕС и Еврокомиссия ведут переговоры по этому вопросу в течение последних трёх лет.

В декабре 2019 г. Еврокомиссия обратилась к Агентству по кибербезопасности ЕС (ENISA) с просьбой подготовить добровольную схему сертификации облачных сервисов (European Cybersecurity Certification Scheme for Cloud Services, EUCS). Компании могут использовать её, чтобы продемонстрировать сертифицированные ИТ-решения, обладающие надлежащим уровнем киберзащиты, для рынка ЕС.

Схема EUCS стала предметом политических дебатов. Франция попыталась ввести в документ требования к суверенитету, направленные на исключение из сертификации по высшим параметрам безопасности компаний из стран, не входящие в ЕС. Этому предложению решительно воспротивились несколько стран ЕС и представители отрасли. Соглашение по сертификации достигнуто не было. Следующее заседание экспертной группы запланировано на март.

Бельгия, которая председательствует на встречах министров ЕС, предлагает отделить функциональные требования от требований о суверенитете. Они будут включены в схему, но с другим подходом и статусом. Предлагается сертифицировать только требования функциональной безопасности, в то время как заявления о суверенитете будут направлены в Международную организацию профильной сертификации (ICPA), и только при прохождении сертификации уровня high. Это позволило бы достичь гар-

монизации на уровне ЕС, сохранив при этом требования к национальному суверенитету для 27 государств — членов Евросоюза.

В документе утверждается, что предлагаемая схема сертификации EUCS позволит облачным провайдерам из стран, не входящих в ЕС, проходить сертификацию по высшим критериям соответствия и получить полный доступ к рынку ЕС. Этот статус позволит им участвовать в тендерах, где требования по сертификации на уровне high будут обязательными без ущерба для дополнительных требований к национальному суверенитету. Такой подход позволит одновременно обеспечить свободный рынок для услуг провайдеров и индивидуальный подход к различному уровню риска в зависимости от потенциальной геополитической угрозы.

Из двух других сертификатов, предложенных в 2019 г., был одобрен только один, для базовых ИТ-продуктов; ещё один — для 5G — всё ещё находится в разработке.

Статус ENISA по осуществлению надзора за исполнением правил кибербезопасности ЕС должен быть пересмотрен этим летом, напоминает Euronews. В настоящее время среди стран ЕС и промышленных компаний проводится исследование эффективности работы Агентства.

КТО СТОИТ ЗА УТЕЧКОЙ В КИТАЕ?

Массовая утечка данных из компании по кибербезопасности Shanghai Anxun Information Company (I-Soon) говорит о том, что даже китайские разведывательные органы полагаются на частных подрядчиков. 16 февраля в репозитории ПО с открытым исходным кодом GitHub появился 571 файл, содержащий хакерские эксплойты и внутренние материалы I-Soon, предлагающие заказчикам хакерские и разведывательные услуги, пишет портал South China Morning Post.

Утечка данных зажила собственной жизнью, несмотря на быстрые действия GitHub по блокированию доступа к материалам. Последствия утечки в обозримом будущем отразятся на разведывательных службах, СМИ, научных кругах и экспертах по безопасности, считают эксперты.

Стирание грани между услугами по ИБ и военными функциями — опасный прецедент нарушения границ, который создали частные компании по кибербезопасности. Их не волнуют вопросы репутации, несмотря на то что эти фирмы всё чаще называют частными военными структурами или кибернаёмниками. В отличие от легальных

организаций, которые подпадают под санкции, такие компании действуют вне рамок принятых международных норм.

В качестве примера можно назвать споры вокруг шпионского ПО израильской компании NSO Group Pegasus, которое используется преступными синдикатами и авторитарными режимами для подавления инакомыслия и правозащитной активности.

Западные страны уже озаботились этической составляющей вопроса, поскольку частные компании всё чаще извлекают выгоду из расширяющегося рынка шпионских программ и кибервойн, а грань между услугами по кибербезопасности и кибернаёмничеством становится всё тоньше. Впрочем, кибернаёмники работают в «серой зоне» между корпоративной кибербезопасностью и наступательными кибероперациями и не стремятся к публичности.

Тем не менее Китай сталкивается с последствиями передачи вопросов кибербезопасности на аутсорс. Он повторяет опыт США — утечку информации из АНБ при участии Эдварда Сноудена, а также зависимость России от хакеров, проводящих операции в даркнете. Наёмники действуют в «серой киберзоне» — в шпионаже появляется новое измерение.

Китай всё чаще выступает за использование частных компаний для защиты зарубежных проектов в рамках инициативы «Пояс и путь» от криминальных и террористических угроз. Как и западные страны, Пекин на собственном опыте постигает опасности и преимущества аутсорсинга услуг по безопасности.

Кроме того, в свете продолжающихся в китайском правительстве дискуссий о расширении роли частных компаний по безопасности, защищающих интересы КНР за рубежом и в киберпространстве, последствия массовой утечки данных будут зависеть от возможностей Компартии Китая контролировать «киберпушку».

Эксперты полагают, что слишком рано делать выводы из инцидента с компанией I-Soon. За утечкой данных могла стоять фигура, подобная Сноудену, действия конкурентов или операция иностранного государства. Не исключено, что причиной слива мог стать и недовольный сотрудник компании.

Так или иначе, на фоне крестового похода Министерства госбезопасности КНР против иностранного кибершпионажа и прошлогоднего пересмотра Закона о борьбе со шпионажем, охота на автора слива будет безжалостной для устрашения его последователей, считают наблюдатели.

ОДКБ. КЫРГЫЗСКАЯ РЕСПУБЛИКА

Александр
ВИНОГРАДОВ
ФГУП «ЦНИИХМ»

Сергей МЕНЬШИКОВ
основатель Belarusian
InfoSecurity Community

Андрей СИТНОВ
независимый
эксперт

Валерий СОКОЛЕНКО
заместитель начальника
службы информационной
безопасности ICBC в г. Алматы

Продолжаем серию материалов по анализу законодательства в области информационной безопасности (ИБ) стран – членов Организации Договора о коллективной безопасности (ОДКБ). На этот раз рассматриваем законодательство Кыргызской республики (далее – КР).

ТАЙНЫ

Документы КР, определяющие различные виды тайн.

Закон КР от 15 декабря 2017 года № 210 (15) «О защите государственных секретов Кыргызской Республики»

В данном Законе разграничены понятия и категории государственных и негосударственных секретов, а также определён правовой режим ограничений и допуска к данной категории информации.

Государственные секреты подразделены на следующие категории: государственная, военная и служебная тайны.

К негосударственным секретам относятся: коммерческая тайна, информация для служебного пользования, не для печати, тайна следствия, врачебная, личная и другие виды тайны. Сохранение негосударственных секретов осуществляется их собственником, а также лицами, которым они доверены по службе и роду деятельности.

В законе также определён перечень информации (сведений), которая не может быть засекречена и доступ к которой не может быть ограничен.

Отнесение информации к государственным секретам осуществляется в соответствии с «Положением о порядке определения и установления степени секретности сведе-

ний, содержащихся в работах, документах и изделиях», на основании «Перечня главнейших сведений, составляющих государственные секреты» и «Перечня сведений, подлежащих засекречиванию», утверждаемых Постановлением Правительства КР Республики, от 7 июля 1995 года № 267/9.

Закон КР от 30 марта 1998 года № 27 «О коммерческой тайне»

Под коммерческой тайной понимаются сведения, не являющиеся государственной тайной, связанные с производством, технологией, управлением, финансовой и другой деятельностью хозяйствующего субъекта, разглашение которых может нанести ущерб его интересам. Закон определяет правовые основы защиты коммерческой тайны на территории КР и порядок доступа к ней.

Закон КР от 14 апреля 2008 года № 58 «Об информации персонального характера»

Настоящий Закон направлен на правовое регулирование работы с персональными данными на основе общепринятых международных принципов и норм в соответствии с Конституцией и законами Кыргызской Республики в целях обеспечения защиты прав и свобод человека и гражданина, связанных со сбором, обработкой и использованием персональных данных.

Прописаны общие требования, касающиеся обеспечения технической безопасности данных, действующих в отношении держателей (обладателей) массива персональных данных и обработчика. Закон определяет разные категории контроля данных за доступом, допуском, пользователем, подписью и вводом, средствами передачи и транспортным контролем.



ОБЩИЕ СВЕДЕНИЯ

Кыргызская Республика — государство в Центральной Азии, расположенное в западной и центральной части горной системы Тянь-Шань и на Памиро-Алае. На севере граничит с Казахстаном, на западе — с Узбекистаном, на юго-западе — с Таджикистаном, на востоке и юго-востоке — с Китаем.

Столица — Бишкек, считается самым населённым городом республики. Государственный язык — киргизский, русский язык имеет статус официального языка.

Кыргызстан является членом ООН, СНГ, ЕАЭС, Шанхайской организации сотрудничества, Таможенного союза, Организации исламского сотрудничества, Организации тюркских государств, ТЮРКСОЙ.

Между Кыргызстаном и Россией заключено более 120 договоров, соглашений и иных документов о сотрудничестве. ВВС России располагают базой в Кыргызстане.

Органы, утверждающие законы и подзаконные акты в области ИБ в КР: Президент КР, Правительство КР, Государственное агентство по защите персональных данных при Кабинете министров КР, Национальный Банк КР.

Все документы имеют общереспубликанское значение и применяются для организации и обеспечения информационной и кибербезопасности.

**Закон КР от 28 декабря 2006 года № 213
«О доступе к информации, находящейся
в ведении государственных органов
и органов местного самоуправления
Кыргызской Республики»**

Регулирует отношения, связанные с доступом физических и юридических лиц к информации, находящейся в ведении государственных органов и органов местного самоуправления.

КОНЦЕПТУАЛЬНЫЕ ДОКУМЕНТЫ

Концептуальные документы, охватывающие вопросы информационной и кибербезопасности.

Указ Президента КР, от 31 октября 2018 года УП № 221 «Национальная стратегия развития Кыргызской Республики на 2018–2040 годы»

П. 4.5 данного документа предусматривает необходимость сосредоточения усилий на критически важных направлениях, таких как обеспечение кибербезопасности информационно-коммуникационных технологий, а также информационных систем, создание системы реагирования на киберугрозы и киберинциденты.

Постановление Правительства КР от 24 июля 2019 года № 369 «Об утверждении Стратегии кибербезопасности Кыргызской Республики на 2019–2023 годы»

Данная стратегия разработана в соответствии со статьями 10 и 17 конституционного Закона Кыргызской Республики «О Правительстве Кыргызской Республики» для формирования единой национальной политики кибербезопасности.

Целью данного документа является формирование в КР системы и политики кибербезопасности, которая защищает жизненно важные интересы государства в киберпространстве и обеспечивает как цифровую трансформацию экономики, так и устойчивое социально-экономическое развитие.

Постановление Правительства КР от 3 мая 2019 года № 209 «Концепция информационной безопасности Кыргызской Республики на 2019–2023 годы»

Концепция представляет собой совокупность официальных взглядов на обеспечение национальной безопасности КР в информационной сфере и ставит в качестве основных приоритетов информационной безопасности несколько задач по кибербезопасности, однако их перечень полностью дублирует приоритеты, указанные в Стратегии кибербезопасности.

Указ Президента КР от 20 декабря 2021 года № 570 «Концепция национальной безопасности Кыргызской Республики»

Концепция также рассматривает вопросы кибербезопасности в тесной связке с общими вопросами информационной безопасности. Однако среди задач кибербезопасности выделены обеспечение бесперебойной, устойчивой и защищённой эксплуатации сетей связи, повышение уровня защищённости государственных информационно-телекомму-

никационных систем и объектов критичной инфраструктуры, создание благоприятных условий для эффективного предупреждения и оперативного выявления (пресечения) киберпреступлений.

ЗАКОНЫ

Основные законы в области информационной и кибербезопасности КР.

Закон — нормативный правовой акт, принимаемый Жогорку Кенешем¹ в установленном порядке и регулирующий наиболее важные общественные отношения в соответствующей сфере.

Уголовный кодекс КР от 28 октября 2021 года № 127

Содержит ряд специальных норм по киберпреступлениям, в нём уточняется понятие преступлений против кибербезопасности и содержится девять статей, в рамках которых компьютерные системы или иные технические средства определяются как объект или элемент объективной стороны преступления. Четыре статьи непосредственно относятся к киберпреступлениям и выделены в отдельную главу 40 «Преступление против кибербезопасности».

Кодекс о правонарушениях КР от 28 октября 2021 года № 128

Глава 26 содержит две статьи, касающиеся правонарушений в сфере информационной безопасности, «Неправомерный доступ к компьютерной информации» и «Нарушение требований по защите информации персонального и коммерческого характера».

Закон КР от 5 декабря 1997 года № 89 «О гарантиях и свободе доступа к информации»

Настоящий Закон регулирует отношения, возникающие в процессе реализации права каждого свободно и беспрепятственно искать, получать, исследовать, производить, передавать и распространять информацию.

Закон КР от 19 июля 2017 года № 128 «Об электронной подписи»

Настоящий Закон регулирует отношения по использованию электронных подписей при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, а также при совершении юридически значимых действий.

Закон КР от 2 июля 1992 года № 938-XII «О средствах массовой информации»

¹ Жогорку Кенеш (кирг. Жогорку Кеңеш — переводится на русский как «Верховный Совет») — состоящий из 90 депутатов однопалатный парламент Кыргызстана, законодательный орган государства.

Закон определяет общие правовые, экономические и социальные основы организации сообщений через средства массовой информации и направлен на свободное функционирование средств массовой информации, регулирует их отношения с государственными органами, общественными объединениями, предприятиями, организациями и гражданами.

Закон КР от 19 июля 2017 года № 127 «Об электронном управлении»

Закон определяет порядок электронного управления в КР. В качестве одной из задач электронного управления определяется необходимость обеспечения информационной безопасности. Также отмечается, что защита прав обладателя информации осуществляется в том числе внедрением технических мер защиты информации.

Под электронным управлением в КР понимается деятельность государственных органов, органов местного самоуправления, их должностных лиц, организаций и граждан по принятию юридически значимых решений и совершению юридически значимых действий с использованием электронных документов и иной информации в электронной форме.

Закон КР от 21 января 2015 года № 21 «О платёжной системе Кыргызской Республики»

Настоящий Закон устанавливает порядок и формы осуществления платежей и расчётов, проведения денежных переводов на территории КР, определяет характеристики платёжных систем, порядок взаимоотношений между участниками платежей и расчётов, надзор (оверсайт) за платёжными системами и определяет полномочия Национального банка КР в платёжной системе КР.

Закон КР от 2 апреля 1998 года № 31 «Об электрической связи»

Закон устанавливает правовые основы для эксплуатации сетей связи и предоставления услуг электросвязи в КР, определяет компетенцию государственных исполнительных органов, уполномоченных осуществлять регулирование таких услуг, режим получения необходимых разрешений на их предоставление, а также права и обязанности юридических и физических лиц, эксплуатирующих сети электросвязи и предоставляющих услуги электросвязи (включая Кыргызтелеком), и пользователей этих услуг.

ПОСТАНОВЛЕНИЯ И ПРИКАЗЫ

Постановление Правительства КР от 21 ноября 2017 года № 762 «Об утверждении Требований к защите информа-

ции, содержащейся в базах данных государственных информационных систем».

Требования разработаны в соответствии с Законом Кыргызской Республики «Об электронном управлении» и определяют меры по защите информации, а также требования к использованию информационных технологий в государственных информационных системах и обеспечения безопасности информации, содержащейся в их базах данных.

Постановление Правительства КР от 21 мая 2020 года № 266 «О Координационном центре по обеспечению кибербезопасности Государственного комитета национальной безопасности Кыргызской Республики»

Постановление описывает основные задачи, функции и организационную деятельность координационного центра по обеспечению кибербезопасности Кыргызской Республики (CERT-KG).

Постановление Правительства КР от 6 февраля 2020 года № 66 «Об отдельных вопросах, связанных с базовыми государственными информационными ресурсами»

Описывает порядок формирования, актуализации и использования Реестра базовых государственных информационных ресурсов, разработан в соответствии с Законом КР «Об электронном управлении» и содержит «Требования к формированию, актуализации и использованию базовых государственных информационных ресурсов», данные требования разработаны в соответствии с Законом КР «Об электронном управлении» и определяют условия создания, ведения и использования базовых государственных информационных ресурсов, а также содержат перечень мер, направленных на обеспечение соблюдения прав субъектов персональных данных, и меры по защите информации, в том числе меры по ограничению доступа к конфиденциальной информации, имеющейся в базовых государственных информационных ресурсах.

Постановление Правительства КР от 31 декабря 2019 года № 744 «О некоторых вопросах, связанных с государственными информационными системами»

Настоящие Требования разработаны в соответствии с Законом КР «Об электронном управлении» и устанавливают порядок создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных или муниципальных информационных систем государственными

органами или органами местного самоуправления КР.

Постановление Правительства КР от 21 ноября 2017 года № 760 «Об утверждении Требований к обеспечению безопасности и защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищённости персональных данных»

Настоящие Требования устанавливают уровни защищённости персональных данных при их обработке в информационных системах, критерии угроз безопасности персональных данных, вошедших в перечень угроз, а также требования к обеспечению безопасности и защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищённости персональных данных, в соответствии со статьёй 21 Закона КР «Об информации персонального характера». Данные требования являются первым подзаконным актом, использующим принципы управления рисками кибербезопасности, определяя требования к защите в зависимости от уровня угроз и нанесения потенциального вреда.

КРЕДИТНО-ФИНАНСОВАЯ СФЕРА

Постановление Комитета по надзору НБ КР от 21 октября 2009 года № 21/1 «Рекомендации по обеспечению безопасности информационных систем в микрофинансовых организациях Кыргызской Республики»

Рекомендации разработаны в соответствии с Гражданским кодексом Кыргызской Республики, законами Кыргызской Республики «О Национальном банке Кыргызской Республики, банках и банковской деятельности», «О микрофинансовых организациях в Кыргызской Республике» и другими нормативными и правовыми актами Кыргызской Республики. Данный документ носит рекомендательный характер и содержит сведения и рекомендации по созданию, разработке и эксплуатации информационных систем, выбору и внедрению программного обеспечения.

Постановление Правления Национального банка КР от 2 сентября 2019 года № 2019-П-14/46-2-(ПС) «Положение о нештатных ситуациях в платёжной системе»

Положение определяет основные понятия и требования для обеспечения бесперебойного функционирования платёжной

системы, а также при возникновении нештатных ситуаций, связанных с надёжностью и бесперебойностью, доступностью, несанкционированным доступом к системе, мошенничеством и форс-мажорными обстоятельствами.

Постановление Правления Национального банка КР от 30 сентября 2019 года № 2019-П-14/50-2-(ПС) «Положение о регулировании деятельности платёжных организаций и операторов платёжных систем»

Настоящее Положение определяет требования, обязательные для исполнения платёжными организациями и операторами платёжных систем, имеющими лицензию Национального банка КР.

Постановление Правления Национального банка КР от 31 марта 2023 года № 2023-П-14/21-1-(ПС), Положение «О требованиях по обеспечению информационной безопасности операторов платёжных систем и платёжных организаций»

Положение устанавливает единые требования для операторов платёжных систем и платёжных организаций (далее – ОПС/ПО), направленных на повышение уровня информационной безопасности в ОПС/ПО, а также минимизацию возможных потерь, вызванных действиями злоумышленников, аварийными сбоями и ошибками персонала.

Постановление Комитета по надзору НБ КР от 3 декабря 2004 года № 26/1 «Методические рекомендации по проверке соблюдения безопасности информационных систем в коммерческих банках Кыргызской Республики»

Настоящие Методические рекомендации разработаны Национальным банком КР в целях оказания содействия инспекторам банковского надзора и специалистам по информационной безопасности при проведении проверки соблюдения безопасности информационных систем коммерческих банков и других финансово-кредитных организаций, лицензируемых Национальным банком, а также Государственного банка развития КР и служат для руководства при проведении проверки на месте.

ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Приказ Государственного агентства по защите персональных данных при Кабинете министров от 19 декабря 2022 года № 13-П, «Методика определения угроз безопасности в информационных системах персональных данных»

Методика устанавливает механизмы определения угроз безопасности в информационных системах персональных данных и защиты персональных данных при их обработке в информационных системах, обрабатывающих персональные данные в зависимости от требуемого уровня защищённости персональных данных.

СТАНДАРТЫ

Национальные стандарты КР:

- ♦ КМС СТБ ISO/IEC 27001:2020 «Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасностью. Требования».
- ♦ КМС ГОСТ Р ИСО 22301:2020 «Системы менеджмента непрерывности бизнеса. Общие требования».
- ♦ КМС ISO 31000:2010 «Менеджмент рисков. Принципы и руководящие указания».
- ♦ ГОСТ ISO/IEC 27014:2021 «Информационные технологии. Информационная безопасность, кибербезопасность и защита конфиденциальности. Руководство деятельностью по информационной безопасности».
- ♦ ГОСТ ISO/IEC 24760-2-2021 «Методы и средства обеспечения безопасностью. Основы управления идентичностью. Часть 2. Базовая архитектура и требования (ISO/IEC 24760-2:2015, IDT)».
- ♦ ГОСТ ISO/IEC 19896-1-2021 «Методы и средства обеспечения безопасности. Требования к компетенции специалистов по тестированию и оценке безопасности информационных технологий. Часть 1. Введение, основные понятия и общие требования».
- ♦ ГОСТ ISO/IEC 29100-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Основы защиты персональных данных».
- ♦ ГОСТ ISO/IEC 19249-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Каталог принципов построения архитектуры и проектирования безопасных продуктов, систем и приложений (ISO/IEC TS 19249:2017, IDT)».

КОММЕНТАРИЙ

Анализ правового поля КР показывает, что, несмотря на обилие нормативных правовых актов в сфере информатизации, противоречий в вопросах обеспечения информационной и кибербезопасности не существует. Однако данные нормативные документы не определяют однозначные правовые рамки, основополагающие принципы и единые подходы в вопросе обеспечения информаци-

онной и кибербезопасности КР. При их использовании не представляется возможным выстроить единый подход или системную государственную политику в данной области.

Как пример, в «Стратегии кибербезопасности» (далее — Стратегия) в целом определены общие рамки политики и законодательного обеспечения. Но данная Стратегия предусматривает значительный перекося в сторону милитаризации в вопросе кибербезопасности КР, не принимая во внимание деятельность гражданских государственных органов и частных структур. Документ не рассматривает возможность государственно-частного партнёрства в области кибербезопасности.

На уровне законов отсутствуют обозначенные в Стратегии секторы, отрасли и сфера деятельности, в которых функционируют объекты критичной инфраструктуры, в том числе и в государственном секторе. Отсутствуют критерии и параметры, определяющие принадлежность объектов к критической инфраструктуре, и не установлены обязательные требования к обеспечению безопасности как самих объектов, так и операторов критичной инфраструктуры.

Не реализованы положения, указанные в Стратегии, касательно методов и средств компьютерной криминалистики, введение в нормативные правовые акты понятия цифровых доказательств, описание и изложение его критериев, характеристик и способов фиксации.

Кроме этого, данные нормативные правовые акты в области связи, цифровизации и телекоммуникаций ведут к неоднозначному толкованию многих терминов и определений, а разрозненность субъектов информационного рынка, ответственных за обеспечение информационной безопасности, мешает проведение чёткой политики в этой направлении.

Как пример, специальный термин (киберсаботаж), используемый в Уголовном кодексе, не соответствует терминологическому глоссарию, используемому в стратегических документах в области кибербезопасности, а также в законодательстве КР, регулирующем сектор связи и телекоммуникаций.

Надеемся, что данный материал поможет ориентироваться в законодательстве КР. Мы постарались облегчить путь изучения и применения нормативных законов и подзаконных актов в области информационной и кибербезопасности одного из наших ближайших соседей — Кыргызской Республики.

«МЫ ПРИБЫЛИ СЮДА С НАДЕЖДой И РЕШИМОСТЬЮ»

КОНФЕРЕНЦИЯ ТЕГЕРАН-43



Борис СТОЛПАКОВ
историк криптографии

Тегеранская конференция 1943 г. стала венцом переломного года Второй мировой войны. Как известно, основной её темой стало открытие второго фронта союзников против Германии в 1944 г.

ВРЕМЯ ПРИШЛО

Лишь осенью 43-го сложилась благоприятная обстановка для реального обсуждения и принятия решения о месте и времени высадки союзников на севере Франции. Причиной такого положения стали успехи Красной Армии на Курской дуге, в Донбассе и на левобережной Украине. 17–24 августа президент США Ф. Рузвельт и премьер-министр Великобритании У. Черчилль на конференции в Квебеке заявили пока ещё только о намерении открыть второй фронт в Европе не ранее мая 1944 г. Накануне конференции военный министр США Стимсон сообщил президенту: «В настоящее время у нас не может быть большой надежды на то, что нам удастся пересечь Ла-Манш и вступить в схватку с противником, имея во главе командующего-англичанина». Тем не менее в решениях англо-американского штаба, участвовавшего в конференции, было записано: «Наличные силы и средства будут распределяться и использоваться в первую очередь с целью обеспечения успеха проведения операции «Оверлорд». В ответ на предложение о совместной трёхсторонней встрече между 15 ноября и 15 декабря Сталин 8 сентября написал Рузвельту: «Местом встречи было бы целесообразно назначить страну, где имеется представительство всех трёх государств, например Иран. Однако я считаю необходимым сказать, что при-

дётся ещё дополнительно уточнить момент встречи, считаясь с обстановкой на советско-германском фронте».

МНОГО СОМНЕНИЙ В ДОСТИЖЕНИИ РЕЗУЛЬТАТА

Были ещё важные сдерживающие моменты. 4 сентября начальник ГРУ И. И. Ильичёв получил донесение из Лондона от «Сони» — разведчицы Урсулы Кучински. Она тоже сообщила сведения о совещании в Квебеке. Главным в её донесении было известие о подписании американским президентом и британским премьер-министром секретного соглашения о совместных усилиях по созданию атомной бомбы. Об этом Рузвельт не проинформировал Сталина в своих письмах по поводу Квебекской встречи. 17 сентября поступило донесение из Нью-Йорка: «Рузвельт на встрече в Квебеке с Черчиллем настаивал на созыве конференции руководителей трёх стран без промедления. Черчилль предлагал подождать до стабилизации обстановки на Восточном фронте». Это сообщение подтверждало, что между Рузвельтом и Черчиллем имелись противоречия. Для принятия решения о встрече «Большой тройки» руководству СССР нужна была уверенность в достижении там значимого результата, а именно согласия США и Великобритании открыть второй фронт. В сентябре и первой половине октября Сталин не был уверен в том, что ему удастся добиться от Рузвельта и Черчилля обещания о конкретных сроках начала высадки союзников во Франции.

ВАЖНАЯ ИНФОРМАЦИЯ ПЕРЕД МОСКОВСКОЙ ВСТРЕЧЕЙ ГЛАВ МИД

На 18 октября была назначена встреча в Москве министров иностранных дел СССР, США и Великобритании с целью «рассмотреть мероприятия по сокращению сроков войны против Германии и её союзников в Европе». К этому времени необходимо было сложить ясное представление о возможностях и намерениях участников совещания. Здесь пригодилась конфиденциальная информация, полученная из Лондона, Вашингтона и Нью-Йорка.



Иллюстрация 1. Исторические фото- и киносъёмки в Тегеране, 1943 г.

Информаторы сообщали в Москву: «Второй фронт в Западной Европе не открывается по чисто политическим соображениям. В Англии уже создана 500-тысячная экспедиционная армия, которая содержится в полной готовности и которая обеспечена всем необходимым, в том числе и флотом для высадки на континенте... Американцы твёрдо решили не открывать второй фронт в Голландии, Бельгии и Франции до тех пор, пока немцы не истощат СССР или СССР не истощит немцев... Госдепартамент и военное командование не верят в возможность договориться с советским правительством по послевоенным вопросам. Отсюда тенденция не спешить со вторым фронтом, дабы обескровить Советский Союз и диктовать ему свою политику... Выражено согласие на созыв конференции с участием СССР, направленной по существу к затяжке времени. На этой конференции предполагается основным вопросом поставить послевоенные проблемы. На конференции союзники укажут, что в этом году открыть второй фронт через Францию и Голландию уже поздно и что единственная возможность для

этого — весна 1944 года. Основным стимулом созыва конференции в Квебеке был неожиданный переход Красной армии в наступление».

15 октября 1943 г. начальник ГРУ генерал-лейтенант И. И. Ильичёв направил И. В. Сталину донесение о проекте плана операции Overlord (англ. — повелитель). В донесении указывалось, что операция была разработана в середине июня 1943 г., примерный срок её начала — 1 мая 1944 года. Донесение сопровождалось подробной картой-планом операции.

В целом представленная информация свидетельствовала о том, что войска союзников готовы к вторжению, но не начнут его до тех пор, пока в войне не сложится наиболее благоприятная для них обстановка. Кроме того, союзники потребуют от СССР каких-то дополнительных обязательств.

РЕШЕНИЕ О ВСТРЕЧЕ «БОЛЬШОЙ ТРОЙКИ» ПРИНЯТО

Московская встреча министров иностранных дел союзных держав завершилась 30 октября. В Москве остались довольны её результатами, они открыли путь к встрече «Большой тройки».

Результаты московской встречи позитивно оценивались в Вашингтоне и Лондоне: «Как последователи, так и противники президента США Ф. Рузвельта не ожидали такого благоприятного исхода переговоров в Москве... Позиция Рузвельта за установление хороших отношений с СССР укрепились больше всего после срыва германского наступления под Курском и переходом Красной армии в контрнаступление... Американцы очень обеспокоены позицией англичан после войны и хотят использовать СССР как препятствие для укрепления их влияния в Европе, особенно на Балканах... В британском министерстве иностранных дел можно услышать только похвальные отзывы о конференции и увидеть приятное удивление по поводу дружественности и такта русских».

Когда Сталин понял, что сможет во время прямых переговоров добиться от Ф. Рузвельта и У. Черчилля принятия конкретных обязательств по вопросу открытия второго фронта, он принял предложение Рузвельта о проведении трёхсторонней встречи. Он согласился и с тем, что настало время обсудить с союзниками проблемы послевоенного мироустройства. В Москве, Вашингтоне и Лондоне началась подготовка к встрече «Большой тройки» в Тегеране. От руководства СССР обеспечение проведения конференции поручили наркому внутренних дел Л. П. Берии.

ПОЛОЖЕНИЕ В ИРАНЕ

Территория Ирана тогда контролировалась советскими, английскими и американскими войсками. Части Красной Армии и британский военный контингент вошли в Иран в конце августа 1941 г. В ноте правительства СССР иранскому руководству от 25 августа говорилось: «Германские агенты <...> превратили территорию Ирана в арену подготовки военного нападения на Советский Союз <...>. Это требует от Советского правительства немедленного проведения в жизнь тех мероприятий, которые оно не только вправе, но и обязано принять в целях самозащиты». Действительно, ввод частей Красной Армии в северные районы страны произошёл в точном соответствии с советско-иранским Договором 1921 г. Юго-западные провинции Ирана заняли английские войска. Американские войска вошли в Иран в конце 1942 г. под предлогом обеспечения безопасности доставки военных грузов для СССР. Они заняли южные иранские порты. 9 сентября 1943 г. Иран объявил войну Германии.

Тегеран, расположенный в 90 км к югу от Каспийского моря, входил в советскую зону ответственности. Благодаря усилиям советской разведки деятельность немецкой агентуры там находилась под контролем и в любое время могла быть пресечена. Важной заботой при организации конференции стало также обеспечение надёжной связи членов советской делегации с Москвой.

«ДОКЛАДЫВАЮ ПЛАН...»

Рассекреченный в 1992 г. документ (илл. 2) позволяет узнать пути, по которым была организована проводная связь.

«Народному Комиссару Внутренних Дел товарищу БЕРИЯ Л. П.

Во исполнение Вашего личного указания от 10.11.43 г. — докладываю план организации проводной телеграфной связи «Бодо» Москва — Тегеран:

1. Проводная телеграфная связь Москва — Тегеран организуется по двум самостоятельным каналам:

а) по направлению через Сталинград — Ставрополь — Тбилиси — Ереван;

б) по направлению через Куйбышев — Ташкент — Ашхабад — Сари.

Кроме того, как резерв, по мере надобности, будет задействована средняя точка медной цепи ВЧ связи на участке Минеральные Воды — Баку — Шахсевар — Сари. Схема организации связи прилагается.

2. Для обеспечения организации указанной в п. 1 связи, необходимы следующие мероприятия:

а) Указание Командующему войсками Зак. Фронта — о немедленном выделении и переброске в Тегеран к исходу 13.11.43 г. (самолётами или поездом) двух совершенно исправных комплектов Бодо-дуплекс с соответствующим личным составом и электропитанием, могущим обеспечить автономную работу каждого комплекта отдельно;

б) Указание Командующему войсками САВО об усилении охраны и ремонта линии ВЧ связи на участке Сари — Тегеран, для чего выделить одну роту связистов и немедленно перебросить таковую на указанный участок;

в) Возложить ответственность за исправное состояние связи Москва — Тегеран на участке Тбилиси — Тегеран на Командующего войсками Зак. Фронта и на участке Ташкент — Тегеран на Командующего войсками САВО;

г) Возложить на Народного Комиссара Связи товарища ПЕРЕСЫПКИНА оборудование организуемой телеграфной связи трансляционными установками и обслуживание их по трассе Москва — Сталинград — Ставрополь — Минеральные Воды — Тбилиси — Ереван — Тегеран и Москва — Куйбышев — Ташкент — Ашхабад — Тегеран, согласно прилагаемой схемы.

3. Ответственным за состояние связи Москва — Тегеран, с местопребыванием непосредственно в Тегеране, от Главного Управления Связи Красной Армии выделяется начальник отдела ГУСКА — подполковник тов. БУХОНОВ М. Н.

4. Срок установления связи по настоящему плану — к исходу 16.11.43 г.

Прошу Ваших указаний. Зам. начальника ГУСКА генерал-лейтенант войск связи А. Стрелков. 11 ноября 1943 г.»

Добавим здесь, что аппаратура «Бодо» использовалась вместе с шифровальными приставками, доставленными из Москвы.

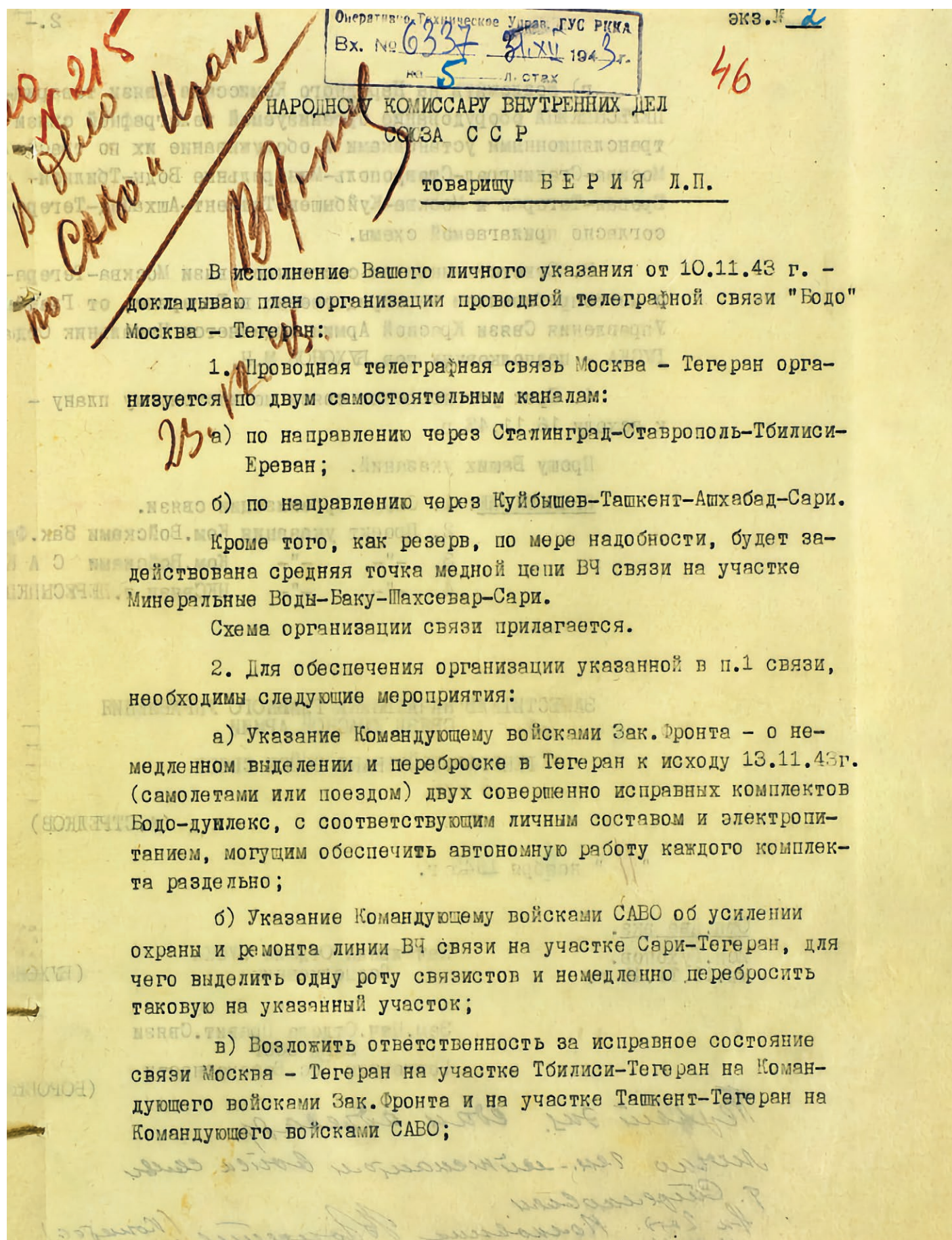


Иллюстрация 2. Лицевая сторона документа



Иллюстрация 3. За круглым столом в Тегеране

СОВЕТСКО-БРИТАНСКИЙ ДИПЛОМАТИЧЕСКИЙ КОМПЛЕКС В ТЕГЕРАНЕ

В конце ноября И. В. Сталин покинул Москву. Литерный поезд прошёл по маршруту Москва — Сталинград — Баку. В состав официальной делегации входили Сталин, Молотов и Ворошилов. От Баку до Тегерана делегация летела на самолёте. Рузвельт и Черчилль встретились в Каире, а 28 ноября делегации трёх держав были уже в Тегеране. Известно, что после прибытия Рузвельта в Тегеран Молотов сообщил союзникам об опасности террористического акта. Американский президент принял приглашение поселиться в здании советской дипломатической миссии, которое было временно освобождено от дипломатического и технического персонала. Советский Союз владел в Тегеране большим хорошо оборудованным посольством. Здесь располагались здание дипломатической миссии, резиденция посла, где разместились советская делегация, и другие служебные здания. В палаточном городке на обширной посольской территории (9 га) устроились несколько сотен опытных бойцов, способных не только обеспечить надёжную охрану, но и принять бой в случае необходимости.

Британское и советское посольства располагались напротив друг друга на двух сторонах одной улицы шириной не более 50 м. Это позволило организовать на время конференции единый

советско-британский дипломатический комплекс, объединённый крытым переходом. Вокруг него создали три кольца усиленной охраны. В целях безопасности на время конференции Тегеран был отрезан от внешнего мира. Не работала связь, не выходили газеты, передвижение по городу также было ограничено.

ПЕРВЫЕ ОБСУЖДЕНИЯ ПОСЛЕВОЕННОГО МИРОУСТРОЙСТВА

Переговоры шли с 28 ноября по 1 декабря. Хотя до разгрома фашистской Германии было ещё далеко, Рузвельт надеялся сокрушить её к концу 1944 г., к президентским выборам в США. В беседе со Сталиным 29 ноября он предложил обсудить послевоенное мироустройство. Рузвельт говорил о необходимости обеспечения длительного мира после войны. Сталин поддержал идею создания международной организации, основанной на принципах объединённых наций, эту идею поддержал и Черчилль.

Как известно, в Тегеране советская делегация добилась многого. Главное, был определён срок открытия второго фронта в Западной Европе — май 1944 г. — и решён вопрос о главнокомандующем этим фронтом. Окончательную дату начала высадки союзных войск в Нормандии планировали определить в первой половине 1944 г.

В итоговом документе, зафиксировавшем военные решения, говорилось: «Конференция приняла

Декларация трёх Держав

Мы, Президент Соединённых Штатов, Премьер-Министр Великобритании и Премьер Советского Союза, встречались в течение последних четырёх дней в столице нашего союзника — Ирана и сформулировали и подтвердили нашу общую политику.

Мы выражаем нашу решимость в том, что наши страны будут работать совместно как во время войны, так и в последующее мирное время.

Что касается войны, представители наших военных штабов участвовали в наших переговорах за круглым столом, и мы согласовали наши планы уничтожения германских вооружённых сил. Мы пришли к полному соглашению относительно масштаба и сроков операций, которые будут предприняты с востока, запада и юга.

Взаимопонимание, достигнутое нами здесь, гарантирует нам победу.

Что касается мирного времени, то мы уверены, что существующее между нами согласие обеспечит прочный мир. Мы полностью признаём высокую ответственность, лежащую на нас и на всех Объединённых нациях, за осуществление такого мира, который получит одобрение подавляющей массы народов земного шара и который устранил бедствия и ужасы войны на многие поколения.

Совместно с нашими дипломатическими советни-

ками мы рассмотрели проблемы будущего. Мы будем стремиться к сотрудничеству и активному участию всех стран, больших и малых, народы которых сердцем и разумом посвятили себя, подобно нашим народам, задаче устранения тирании, рабства, угнетения и нетерпимости. Мы будем приветствовать их вступление в мировую семью демократических стран, когда они пожелают это сделать.

Никакая сила в мире не сможет помешать нам уничтожать германские армии на суше, их подводные лодки на море и разрушать их военные заводы с воздуха.

Наше наступление будет беспощадным и нарастающим.

Закончив наши дружественные совещания, мы уверенно ждём того дня, когда все народы мира будут жить свободно, не подвергаясь действию тирании, и в соответствии со своими различными стремлениями и своей совестью.

Мы прибыли сюда с надеждой и решимостью. Мы уезжаем отсюда действительными друзьями по духу и цели.

Подписано в Тегеране 1 декабря 1943 года.

РУЗВЕЛЬТ
СТАЛИН
ЧЕРЧИЛЛЬ

Иллюстрация 4. Публикация Декларации в газете «Правда»

к сведению, что операция «Оверлорд» будет принята в течение мая 1944 г., вместе с операцией против Южной Франции. Эта последняя операция будет предпринята в масштабе, в каком это позволяет наличие десантных средств. Конференция далее приняла к сведению заявление маршала Сталина, что советские войска предпримут наступление примерно в то же время с целью предотвратить переброску германских войск с восточного на западный фронт. <...> Конференция согласилась, что военные штабы трёх держав должны отныне держать тесный контакт друг с другом в отношении предстоящих операций в Европе. В частности, было принято решение, что между соответствующими штабами должен быть согласован план мистификации и обмана противника в отношении этих операций». Надо сказать, что согласование планов штабов, безусловно, имело место весь 1944 г.

«РУССКИЕ НЕ ИМЕЮТ НЕЗАМЕРЗАЮЩИХ ПОРТОВ НА БАЛТИЙСКОМ МОРЕ»

О ходе обсуждений ныне можно судить по опубликованной стенограмме заседаний. Вот её фрагмент.

Заседание за круглым столом 1 декабря.

«Черчилль. Моё предложение гласит: «В принципе было принято, что очаг польского государства

и народа должен быть расположен между так называемой линией Керзона и линией реки Одер, с включением в состав Польши Восточной Пруссии и Опельнской провинции. Но окончательное проведение границы требует тщательного изучения и возможного расселения населения в некоторых пунктах».

Сталин. Русские не имеют незамерзающих портов на Балтийском море. Поэтому русским нужны были бы незамерзающие порты Кёнигсберг и Мемель (ныне Клайпеда — Б.С.) и соответствующая часть территории Восточной Пруссии. Тем более что исторически это исконные славянские земли. Если англичане согласны на передачу нам указанной территории, то мы будем согласны с формулой, предложенной Черчиллем».

МЫ ПРИБЫЛИ СЮДА С НАДЕЖДОЙ И РЕШИМОСТЬЮ»

7 декабря 1943 г. в советской печати было опубликовано сообщение о встрече руководителей СССР, США и Великобритании в Тегеране и текст Декларации трёх Держав, где говорилось: «...Все народы мира будут жить свободно, не подвергаясь действию тирании, и в соответствии со своими различными стремлениями и своей совестью».

Мы прибыли сюда с надеждой и решимостью. Мы уезжаем отсюда действительными друзьями по духу и цели» (илл. 4).

«ДОКЛАДЫВАЮ О ВЫПОЛНЕНИИ»

Ещё долго военные руководители, в том числе и связисты, рапортовали об обеспечении конференции. Вот что отметил в своём ныне рассекреченном сообщении начальник связи Закавказского фронта.

«Начальнику Главного Управления связи Красной Армии

Маршалу войск связи тов. ПЕРЕСЫПКИНУ

Докладываю о выполнении Вашего приказа по организации связи Москва — Тегеран, на период переговоров Маршала Советского Союза товарища Сталина с президентом Северо-Американских Соединённых Штатов Рузвельтом и премьер-министром Англии Черчиллем, на Тегеранской конференции, с 20 ноября по 4 декабря 1943 года.

1. Согласно расчёту, указанному в шифрограмме заместителя начальника генерального штаба — генерала армии т. Антонова, в распоряжение представителя ГУСКА подполковника т. Бухонова, из состава 121 полка связи было выделено и передано в гор. Баку:

а) Личный состав — начальник группы зам. командира телеграфно-телефонного батальона 121 полка связи майор Конев <...>.

Для технического обслуживания двух раздельно действующих аппаратов были выделены два техника <...>.

Для работы на двух раздельно действующих аппаратах Бодо и обслуживания их был выделен личный состав, согласно указанному расчёту полностью, в том числе 18 телеграфистов бодистов <...>.

б) Аппаратура. Были выделены два комплекта аппаратов Бодо дуплекс с соответствующим количеством источников питания, экспломатериалов, принадлежностей и инструмента. Аппараты Бодо были выделены из групп аппаратуры ВТУ штаба фронта, действующие, вполне исправные <...>.

2. После того когда мне стало известно назначение выделенной группы связистов и аппаратуры, мною был заменен майор Конев, вместо него на самолёте был выслан командир т/т батальона 121 полка связи майор Гренадеров, с ним также был послан лучший, опытный техник бодист 121 полка ст. техник-лейтенант Рзаев. Дополнительно сверх расчёта были посланы запасная головка приёмника Бодо и другие запчасти, которые дополнительно были выделены за счёт разукomплектования действующей аппаратуры Бодо, так как в наличии их не имелось в течение 2-х лет.

3. В пути следования на автомашинах, от Астара до Тегерана и от Тбилиси до Тегерана, вследствие тряски произошли незначительные повреждения в комплектах Бодо. Все неисправности в аппара-

тах были устранены силами личного обслуживающего состава <...>.

4. Для обеспечения бесперебойности прохождения работы были подготовлены и проверены провода:

а) Индо-линии № 157 и 268 на участке — Тегеран, Тавриз, Ереван, Тбилиси — основное направление;

б) Средняя точка бронзовой цепи ВЧ связи и физический провод на участке — Баку, Астара, Сари, Тегеран — дополнительное направление.

Провода индо-линии на территории Ирана от Джульфы (Иранская) до Тегерана, под руководством моего заместителя полковника Модова, были прикрыты эксплостами 110, 167, 697 Отд. кабельно-шестовых и 285 Отд. телеграфно-строительных рот. 110 и 167 Отд. кабельно-шестовые роты были переброшены из района Тбилиси.

На проводах индо-линии № 157 и 268 на территории Ирана, эксплостами было заменено 827 битых изоляторов, произведена чистка изоляторов от осевшей на них пыли. На отдельных, прилегающих к дороге участках линии, общим протяжением до 348 км, произведена очистка проводов от ветвей деревьев, вросших в провода, в населённых пунктах и городах, в том числе на территории дворца губернатора г. Казвин и на улицах г. Тегеран, общим протяжением до 30 км. Вопросы обрезки ветвей в каждом случае надо было согласовывать с соответствующими иранскими властями, а в отдельных дворах и садах с владельцами их. Провода № 157 и 268 были изолированы — отсоединены от вводов и спрямлены во всех иранских пунктах связи. В городе Тегеран от индо-линии к советскому посольству был наведён запасной кабельный шлейф. Всего на трассе Тегеран — Минеральные Воды было поставлено на эксплуатацию 8 рот.

Благодаря перечисленным выше мероприятиям, добросовестному и старательному отношению всего личного состава, обслуживавшего связь Москва — Тегеран, вся выделенная нами аппаратура и провода нашего основного направления работали безотказно, за исключением двух случаев повреждений на проводах: первый — в районе Джульфы (Иранская) одна автомашина колонны автомашин, перегоняемых в Советский Союз, ведомая водителем-иранцем, наскочила на столб индо-линии, выбила его и порвала все 4 провода. Второй случай — в 7 км от Тегерана команда военнослужащих англичан, подвешивая свой кабель, при переходе через индо-линию порвала все 4 провода. Указанные повреждения были устранены эксплостами в первом случае через 2 ч. 17 м., во втором случае через 1 ч. 47 м. <...>.

Начальник Упр. связи Закавказья генерал-майор войск связи Шуватов»

Главный результат тегеранской конференции — высадка союзников в Нормандии осуществилась спустя полгода, 6 июня 1944 г.

ТЁМНАЯ СТОРОНА СИЛЫ... ЗНАНИЙ

ЗАМЕТКИ БЕЗОПАСНИКА

Александр ИГОНИН
эксперт BIS Journal

Как мы уже обсуждали, люди и процессы — неотъемлемая часть системы защиты информации. Где-то внутри этих компонентов находятся знания, которыми обладает команда и которые используются в повседневной работе. Именно им хотелось бы посвятить эту заметку. Уточню, что акцент будет не на профессиональных навыках, кои имеются у множества кандидатов на рынке труда, а на специфическом знании инфраструктуры, процессов, культуры и «болевых точек» конкретной организации.

В современном бизнесе люди покидают компании довольно часто: уходят к конкурентам, переезжают в другие города и страны, увольняются вследствие высокой нагрузки или выгорания. Из моей практики скажу: даже при наличии организованной базы знаний очень непросто подробно и в то же время доступно систематизировать эти знания так, чтобы новые сотрудники максимально быстро и полно их усваивали и могли применять на практике. Основным каналом передачи таких специфических знаний остаётся коммуникация между «бывалыми» и «новичками» — достойную замену этому пока не придумали.

Часто бывает, что большие пласты ключевых знаний распределены между буквально двумя-тремя ключевыми сотрудниками. Вспомним известный «фактор автобуса»: что случится с проектом (или операционной деятельностью), если такой сотрудник попадёт под автобус и больше не сможет работать? К сожалению, об этом задумываются далеко не все, и мы всё ещё много где видим сквозящий в кадровой политике догмат об «очереди за забором».

Очередь-то, конечно, имеется, причём немаленькая. И у многих в этой очереди даже найдётся требуемый набор профессиональных навыков. Но вот есть ли у них знания именно о вашей организации и используемых в ней технологиях? Сколько времени новые люди будут во всём разбираться, особенно если предыдущие специалисты окажутся недоступны? Какие риски (или даже убытки) грозят организации в этом случае?

Бизнес должен понимать и уважать ценность команды, которая состоит не только в конечном результате, но и в накопленном багаже знаний. Увы, до сих пор удержанию ключевых работников часто уделяется недостаточно внимания, а иногда в пылу конфликтов и оптимизаций их и вовсе увольняют целыми пачками. Правда, потом, после лихорадочного поиска новых кадров на рынке, обычно приходит понимание, что в очереди за забором людей хоть и много, да все какие-то не такие. И в итоге компания пытается за астрономические деньги найти тех, кто сумеет выполнить хотя бы часть накопившихся задач — и быстро, потому что за медлительность современный рынок карает беспощадно.

Значит ли это, что автор призывает никого и никогда не увольнять и не сокращать? Отнюдь — я лишь предлагаю помнить, что при расставании с ключевыми специалистами (и тем паче с командами) нужно всегда планировать этот процесс заблаговременно и стараться обеспечить максимально плавный транзит знаний от их «хранителей» к новым сотрудникам. А для этого нужно обеспечить достаточно продолжительный переходный период и поддерживать хорошие отношения с коллективом. Ну, и учитывать, что после даже качественно проведённого транзита продуктивность обязательно снизится на какое-то время, пока будет идти адаптация.

Такие вот вроде бы банальные истины, понятные любому, кто имеет минимальный опыт работы «на земле»... Но почему-то до сих пор встречаются случаи, когда весь отдел узнаёт о своём увольнении день в день — а потом через месяц-два на пепелище приходят новые сотрудники, которые вынуждены чуть ли не археологические раскопки проводить, пытаясь понять, как же всё тут устроено (потому что даже если документация есть, то где она лежит, никому не ведомо). Автор статьи никогда не был топ-менеджером, но ему всегда было интересно, а что же на уме у руководителей, которые допускают подобные кадровые решения. Хочется верить, что со временем таких странных историй будет становиться меньше.



ФОРУМ

РОССИЯ 20²⁴

17 19

сентября



XXII

**международная
конференция**
по проблематике
инфраструктуры
открытых ключей
и электронной
подписи

г. Санкт-Петербург
Отель «Коринтия»



pki-forum.ru

Kaspersky Symphony XDR

Кибербезопасность
в виртуозном исполнении



kaspersky активируй
будущее