BIS JOURNAL

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ БИЗНЕСА

№3 (58) 2025

Артём ЗУБКОВ
Медиа Группа «Авангард»
Технологии доверенного ИИ → 52

Дмитрий ПОНОМАРЁВ
ООО НТЦ «Фобос-НТ»
Многоликий динамический анализ → 76

Осенний марафон-2025

Дмитрий ЕВДОКИМОВ
Luntry
Всё для SOC в контейнерных средах и Kubernetes → 9

Георгий КОРАБЛЕВ
АМИКОН
От узкого специалиста до массового потребителя → 27

Юрий ШАБАЛИН
AppSec.Sting
Цифровой рубль в телефоне → 94

AgileCrypto \ 2025

Международная научно-практическая конференция

«Криптография в многополярном мире»

Место проведения:
Социалистическая республика Вьетнам,
г. Нячанг, отель «Sheraton Nha Trang Hotel & Spa»

12–15 октября 2025 года

agilecrypto.biz

Сергей ПАЗИЗИН
научный редактор
BIS Journal

Лето этого года отметилось проведением резонансных кибератак на российский бизнес. Причем серьезно пострадали в том числе и крупные компании, которые имеют возможность вкладывать значительные средства в приобретение средств защиты и привлекать квалифицированных специалистов для обеспечения ИБ. Что подтвердило старую истину: не бывает абсолютной защиты, и у всех компаний, независимо от размера бюджета на ИБ, должны быть планы по восстановлению в случае кибератак. Необходимо быть готовыми как технически — иметь резервные копии важных данных, которые останутся недоступны злоумышленникам в случае их проникновения в инфраструктуру, — так и организационно — проводить регулярные киберучения с привлечением бизнес-подразделений компании. Кроме того, важно грамотно использовать бюджет, выделяемый на ИБ: правильно выбирать средства защиты и эффективно их использовать.

Познакомиться с арсеналом современных технических средств, применяемых для выявления кибератак, а также передовым опытом обработки инцидентов и построения процессов мониторинга ИБ вы сможете на страницах этого номера и на конференции SOC Tech 7 октября 2025 года. В формировании программы этой конференции журнал принимает активное участие.

Невозможно также противостоять кибератакам, не имея средств надежной аутентификации как пользователей, так и устройств, сервисов и процессов. Она, в свою очередь, опирается на инфраструктуру открытых ключей. Анализ проблем и новейшие технические решения по данной тематике публикуются в нашем журнале и будут обсуждаться на PKI-Форуме — международной конференции по проблематике электронной подписи, которая традиционно пройдет в Санкт-Петербурге 16–18 сентября 2025 года.

Также мы продолжаем знакомить читателей с инструментами выявления уязвимостей в коде информационных систем, которые киберпреступники могут использовать для проникновения в инфраструктуру организации, и методами разработки безопасного ПО. Соответствующий раздел этого номера посвящен инструментам и методам динамического анализа кода, оценке их полезности и применимости.

BIS JOURNAL
ИЗДАЁТСЯ С 2010 ГОДА

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 (Роскомнадзором) как «BIS Journal — Информационная безопасность банков».

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

Подписан в печать 21.08.2025. Тираж 7000 экз.
Цена договорная. Отпечатан в типографии «Московский Печатный Двор», 123298, г. Москва, 3-я Хорошевская 18, корп. 1, офис 201А

 16+

ТЕМА НОМЕРА — 1: SOC

ТЕМА НОМЕРА — 2: КРИПТОГРАФИЯ В ИБ

РЕГУЛЯТОРЫ

УГРОЗЫ И РЕШЕНИЯ

ИНФРАСТРУКТУРА

ИБ В ОТРАСЛИ

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

РБПО. ДИНАМИЧЕСКИЙ АНАЛИЗ КОДА

ОБРАЗОВАНИЕ И КАРЬЕРА

ЗА РУБЕЖОМ

СУБЪЕКТЫ

ЧТО ДОЛЖНА УМЕТЬ SIEM ДЛЯ ЭФФЕКТИВНОЙ РАБОТЫ SOC

Павел ПУГАЧ
системный аналитик «СёрчИнформ»

SIEM-система — сердце любого SOC. Она собирает события безопасности из корпоративной ИТ-инфраструктуры, выявляет инциденты и предоставляет информацию специалистам. От качества и результата этих действий зависит эффективность функционирования SOC — от оперативного реагирования до разработки или модернизации ИБ-политик.

Но помимо базовых функций мониторинга, современные SIEM оборудованы самым разным функционалом. Давайте вернёмся к истокам и вспомним, какие из многочисленных возможностей SIEM действительно требуются в SOC и как удобство их реализации предопределяет эффективность всего подразделения.

ЗАДАЧИ SIEM В SOC

SIEM в SOC решает четыре основные задачи:

- Собирает и нормализует события безопасности;
- Выявляет инциденты;
- Интегрируется в процесс расследования;
- Передаёт данные в другие системы и средства защиты.

Остальной функционал, например выявление уязвимостей, тоже может быть полезен: он помогает закрыть нехватку других СЗИ. Но SOC, как правило, оборудован множеством профильных систем: SGRC, IRP, SOAR, VM и т.д. Они получают данные из SIEM и используют их для решения ИБ-задач. Получается, выбор SIEM для SOC должен основываться не на количестве функций, которые к тому же пересекаются с другими СЗИ, а на качестве и удобстве реализации основного SIEM-функционала. Пошагово пойдём по нему.

СОБРАТЬ И СТАНДАРТИЗИРОВАТЬ

SIEM в SOC отвечает за сбор и нормализацию событий безопасности из разных элементов ИТ-инфраструктуры: операционных систем, баз данных, средств защиты, сетевых устройств, «облаков», приложений и т.д.

Для этого система должна подключаться к множеству источников, «понимать» и забирать их логи. То есть поддерживать разные сетевые протоколы, стандарты хранения и передачи данных, а также механизмы выполнения команд на источниках. Например, Syslog, SSH, SNMP Trap, NetFlow и т.д.

«СёрчИнформ SIEM» собирает и нормализует события при помощи предустановленных коннекторов. Всего их три типа. Первый — персональные коннекторы для популярного оборудования, ПО и ИБ-инструментов. Например, к антивирусу Kaspersky, 1С, АПКШ «Континент» и т.д.

Второй — универсальные коннекторы к протоколам EventLog, Syslog, SSH, NetFlow и др., по которым можно получить данные от большинства других источников.

Для редких случаев, когда, например, нужно получить данные из самописного ПО, можно воспользоваться пользовательским коннектором на основе скриптов или вычитать данные напрямую из БД.

Все коннекторы, кроме пользовательского, подключаются в графическом интерфейсе. Это просто и быстро, а потому экономит силы и время.

ВЫЯВИТЬ СКРЫТОЕ

Следующая задача SIEM — выявление инцидентов: вирусных эпидемий, попыток брутфорса, компрометаций учётных записей и т.д. Для этого система должна анализировать события и позволять специалистам удобно их коррелировать.

Для выявления инцидентов, которые состоят из единичных событий, в «СёрчИнформ SIEM» есть базовый набор правил корреляции. Они покажут события, на которые стоит обратить внимание в любой инфраструктуре. Например, временное изменение параметров учётной записи, добавление нового пользователя, вход в почтовый ящик сотрудника с зарубежного IP-адреса и т.д. Базовый набор правил можно кастомизировать или быстро создать новые, если не хватило «джентльменского набора».

Для более сложных случаев существуют правила кросс-корреляции. Они позволяют выявлять инциденты, которые состоят из нескольких событий, не связанных друг с другом на первый взгляд. Например, подключение флешки и старт вирусной эпидемии.

Оба типа правил настраиваются в графическом интерфейсе. Первые — выбором событий из выпадающего списка. Вторые — выбором коннекторов, событий и параметров в графическом конструкторе. Это экономит ресурсы аналитиков SOC на сложное программирование.

НАЙТИ ПРИЧИНУ

Расследование инцидентов в SOC — это выстроенный процесс. Разные линии специалистов действуют по прописанным инструкциям и шаблонам. Задача SIEM — легко интегрироваться в этот процесс и предоставить специалистам необходимые данные в простом формате. Для этого нужна понятная визуализация. Например, дашборд с виджетами в «СёрчИнформ SIEM» даст оперативную сводку по нужным параметрам в выбранном формате.

Также нужны инструменты анализа данных, с которыми будет удобно работать. Например, журналы сработок правил корреляции и кросс-корреляции представят отчёт по всем событиям безопасности в инфраструктуре. А фильтрация по дате и времени возникновения инцидентов, их критичности, количеству и т.д. поможет сгруппировать события по опорным признакам, выявить тенденции и выстроить таймлайн развития атаки. Ещё в «СёрчИнформ SIEM» инциденты можно отобразить на специальной карте. Это упростит поиск центров аномальной активности, проблемных узлов сети и пользователей, которые связаны с большим количеством инцидентов. Так ИБ-команда расставит приоритеты и обнаружит слабые места в инфраструктуре.

Ещё в системе есть инструмент Task Management. Он работает как трекер задач и помогает организовать командную работу над ИБ-инцидентами, что актуально для координации разных линий SOC. Task Management позволяет создавать задачи и подзадачи, контролировать сроки их исполнения, определять ответственных ИБ-специалистов и фигурантов инцидентов. Прикреплять необходимую для расследования информацию: инциденты и события, документы и описания, подзадачи и т.д.

Для лёгкого взаимодействия с регулятором по API реализована прямая интеграция с ГосСОПКА. В простом интерфейсе можно подготовить отчёт по заданным регулятором критериям, к которому автоматически подтягивается «фактура» из SIEM

ПОДЕЛИТЬСЯ ДАННЫМИ

Хорошая SIEM автоматически передаёт данные в SGRC, VM, SOAR, IRP и другие компоненты SOC. Для этого в системе должны быть разные инструменты экспорта: API, утилиты и т.д.

«СёрчИнформ SIEM» поддерживает экспорт инцидентов по расписанию в формате CSV. Он хорошо подходит для обработки другими системами и позволит, например, передать данные в SGRC. Есть отправка данных в формате JSON на указанный URL-адрес при выявлении инцидента. Это позволит интегрироваться с веб-приложениями и даст гибкость в плане отправки данных.

С некоторыми системами «СёрчИнформ SIEM» готов взаимодействовать сразу «из коробки». В частности, система передаёт инциденты в R-Vision IRP для автоматизированного реагирования. А для лёгкого взаимодействия с регулятором по API реализована прямая интеграция с ГосСОПКА. В простом интерфейсе можно подготовить отчёт по заданным регулятором критериям, к которому автоматически подтягивается «фактура» из SIEM.

Наконец, доступна передача данных при помощи внешних инструментов. «СёрчИнформ SIEM» запускает указанное ПО средствами ОС и передаёт ему на вход заданные параметры инцидента.

ЗАКЛЮЧЕНИЕ

Для эффективной работы SOC SIEM-система должна работать с широким пулом источников, поддерживать разные сетевые протоколы, стандарты хранения и передачи данных. Анализировать и коррелировать разнородные события, предоставлять инструменты расследования, поддерживать автоматизированный экспорт данных в другие системы.

Если работа с SIEM устроена просто и удобно, повышается эффективность SOC. Это «разгружает» ИБ-специалистов и позволяет сосредоточиться на оперативных задачах. В результате возрастает скорость реагирования и расследования инцидентов, даже если «рук» не хватает. Опробуйте простой и эффективный инструмент в составе своей SOC — «СёрчИнформ SIEM» доступна для тестирования в полном функционале на 30 дней.

КАК РЕАГИРОВАТЬ НА КИБЕРИНЦИДЕНТЫ?

Роман ДУШКОВ
Security Vision

Когда ресурсов не хватает, кажется соблазнительным игнорировать отдельные сигналы тревоги. Но во что это может обернуться — и как сделать реагирование возможным даже в условиях кадрового дефицита? Современные кибератаки становятся всё более изощрёнными, многоступенчатыми и целенаправленными. Организациям необходимо не только уметь обнаруживать инциденты, но и активно противодействовать угрозам на всех этапах атаки — от разведки до постинцидента.

Эффективная стратегия защиты строится на трёх китах: обнаружении, реагировании и проактивной аналитике. В этой статье мы рассмотрим ключевые технологии и практики, которые формируют современную систему противодействия кибератакам, а также дадим советы по построению и усилению защищённости для компаний разного масштаба и зрелости процессов.

ПЕРЕИЗБЫТОК ДАННЫХ

Изобилие сигналов всё чаще вызывает паралич внимания в кибербезопасности: современные ИБ-команды сталкиваются не с нехваткой данных, а с их переизбытком. Угрозы, инциденты, ложные срабатывания, тревоги от различных систем — всё это сыпется на специалистов, как град.

Мы выделяем в качестве первоочередной задачи обнаружение атакующих активностей в инфраструктуре. Для этого используются как сигнатурные, так и поведенческие методы, включающие SIEM (Security Information and Event Management), EDR (Endpoint Detection and Response), NDR (Network Detection and Response) и UEBA (User and Entity Behavior Analytics) системы. В то время как одни решения агрегируют события из различных источников (серверов, сетевых устройств, приложений) и применяют прави-

ла корреляции для выявления подозрительных сценариев, другие — анализируют активность на конечных точках, выявляя вредоносные процессы, изменения в реестре, запуск скриптов и пр., или контролируют сетевой трафик на предмет аномалий и подозрительных коммуникаций.

В обнаружении большую роль играют такие модули Security Vision, как VS (Vulnerability Scanner), VM (Vulnerability Management) и SPC (Security Profile Compliance). Вместе они работают на то, чтобы не только уменьшить поверхность атак, но и найти уязвимые места до того, как ими воспользуются злоумышленники, выстроить процесс устранения уязвимостей с автопатчингом, настроить харденинг систем и привести все настройки к эталонным значениям с минимумом человеческих действий.

НАКОПЛЕНИЕ ДОЛГА

Игнорирование инцидентов, особенно тех, которые классифицируются как «низкоприоритетные» или «неподтверждённые», может показаться оправданным шагом ради сохранения ресурсов. Однако отсутствие реагирования — это путь к накоплению технического долга в области ИБ. Каждый необработанный инцидент — это потенциальное окно для злоумышленника, упущенный шанс выявить сложную целевую атаку, ослабление нормативного и аудиторского контроля, повышение риска репутационных и финансовых потерь. В условиях растущего количества источников главная задача — не отказаться от реагирования, а сделать его управляемым, масштабируемым и автоматизированным. Современные инструменты позволяют минимизировать участие человека в рутинных процессах реагирования. Вот как это реализуется:

1. AM (Asset Management) в составе решений Security Vision позволяет построить ИТ-ландшафт и определить цели для первостепенного реагирования на основе ресурсно-сервисной модели. Такая модель не только строится по принципам ITAM/CMDB (поиск ИТ-активов и инвентаризация с управлением), но и учитывает бизнес-сущности и требования компаний для помещений, поставщиков, информационных систем и процессов.

2. SOAR-платформы (Next Generation Security Orchestration, Automation and Response) позволяют автоматически анализировать контекст события (локализация, принадлежность пользователя, тип активности), выполнять действия (блокировка IP, изоляция узла, уведомление, постановка в тикет-систему).

3. Сценарии реагирования или простые регламенты с автоматизированными скриптами (на PowerShell, Bash, Python) выполняют стандартные действия по заранее утверждённому сценарию. В рамках Security Vision SOAR такие плейбуки собираются динамически в зависимости от источников, доступных СЗИ, окрестности киберинцидентов.

При этом для ИБ-команды сохраняется принцип: «Меньше не значит слабее». Небольшая команда может быть эффективной при условии централизации информации (в одном окне, по модели single pane of glass с helicopter view), автоматизации корреляции, фильтрации и приоритизации, интеграции с CMDB и ITSM (или встроенных SD) и использования облачных сервисов и MSSP (Managed Security Services), если нет ресурсов для поддержки собственной инфраструктуры. Так, например, AM, SOAR и TIP от Security Vision имеют самое большое покрытие по провайдерам услуг.

Отдельное внимание в реагировании стоит уделить решениям класса EDR (или компоненту в составе Security Vision SOAR), который позволяет расширить возможности стандартного аудита ОС за счёт перехвата системных событий (перехват осуществляется через хуки пользовательского пространства на хостах, а также на уровне драйвера ядра как Windows, так и Linux) и проактивной блокировки (которая автоматически останавливает недоверенные приложения при попытке выполнения опасных операций). Стоит подобрать систему так, чтобы она легко интегрировалась с другими СЗИ, например, для отправки подозрительных файлов в песочницу (такие интеграции через конструкторы, например, можно выполнять даже без участия вендоров).

ИИ — НЕ ТРЕНД, А ИНСТРУМЕНТ

Третий шаг в эффективной защите с уменьшением действий по реагированию — анализ больших данных. Применение ИИ — не просто тренд, а инструмент, освобождающий аналитиков от рутины и помогающий не пропустить ни единой попытки взлома. Поведенческие модели на основе машинного обучения позволяют вычленять настоящие аномалии (UEBA) и пода-

влять «шум» (это снижает объём инцидентов, требующих внимания вручную), а использование TIP поможет вовремя сверяться с базами IOC и проводить анализ киберугроз. Представьте: небольшая компания получает тревогу о возможном фишинге. SOAR-система сверяет отправителя с известными фидами, находит подтверждение и блокирует домен в почтовом шлюзе без участия специалиста.

Рассмотрим, как эти этапы на самом деле работают в компаниях разного масштаба:

◆ Компании с ограниченными ресурсами (один-два аналитика, иногда совмещающих функции ИБ и администрирования) физически не могут обрабатывать весь объём поступающей информации. Возникает вопрос: а нужно ли вообще реагировать на каждый инцидент? Security Vision предлагает использовать такие системы совместно либо за счёт внедрения единой платформы для интеграции систем от различных вендоров, либо как модули в рамках собственной экосистемы, в которой, например, модуль NG SOAR (Next Generation Security Orchestration, Automation and Response) имеет встроенные SIEM- и EDR-компоненты, а модуль UEBA отвечает за поиск аномалий в активности пользователей и устройств. Всё это работает так, чтобы обнаружение было максимально автоматизировано, а технологии ИИ использовались для снижения ложноположительных срабатываний и анализа инцидентов для быстрого подбора подходящего вердикта.

◆ Компании с большими ресурсами для обнаружения инцидентов сталкиваются с другой проблемой — недостаточной эффективностью коммуникации внутри команды или сложностью согласований и передачи ответственности. На этот случай продукты Security Vision не только выполняют роль тикетинг-системы, но и включают чаты как внутри команд, так и с ML-инструментами (LLM-модели всё чаще используются как способы обогащения данными и поиска советов «что делать»). Встроенные внутренние ИИ-помощники и интегрированные в решения GhatGPT, YangexGPT, Deepseek и другие внешние инструменты обеспечивают возможность анализа данных в рамках единого окна.

* * *

Отказ от реагирования сегодня — это высокий риск взлома завтра. Однако реагирование не обязательно означает сотни часов рутинной аналитики. Благодаря автоматизации и новым подходам даже команды из 1-2 человек могут выстроить эффективную модель реагирования и защитить компанию от большинства угроз. Вопрос не в том, реагировать или нет, а в том, как сделать реагирование доступным и устойчивым при любых ресурсах.

СОВЕТЫ ОТ ЭКСПЕРТОВ

В завершение статьи приведём ещё несколько советов от экспертов:

1. Не пытайтесь обрабатывать всё — внедрите приоритизацию, так как в реальности до 95% событий ИБ — ложные срабатывания или низкоуровневые аномалии.

2. Внедрите систему классификации инцидентов по критичности (напр., CVSS + бизнес-значимость). Необязательно реагировать на всё, нужно реагировать на важное.

3. Автоматизируйте всё, что повторяется: обогащение инцидентов (IP reputation, геолокация), уведомления и маршрутизацию тикетов, типовые действия (блокировка IP, изоляция хоста, отключение учётки) и сценарии реагирования.

4. Упростите мышление через стандарты и шаблоны, разработайте простые сценарии (или чек-листы) для 5–10 типовых инцидентов или внедрите SOAR с динамическими плейбуками.

5. Учите не только ИБ-специалистов, но и пользователей (осведомлённые сотрудники — первая линия защиты) при помощи внутренних рассылок и симуляций атак (например, фишинга).

6. Централизуйте логи (даже в Excel, если нет возможности использовать SIEM/SOAR), введите базовый журнал инцидентов (интегрированный или хотя бы в таблице), с ключевыми полями. Системность важнее идеала: лучше простая таблица, чем хаотичная переписка в Telegram.

7. Интеграция лучше, чем новая покупка, часто можно добиться результата за счёт интеграции уже имеющихся систем (почтовый шлюз + SIEM, антивирус + UEBA, AD + CMDB и т.д.).

8. Рассмотрите MSSP или облачные SOC, если невозможно выстроить внутреннюю ИБ-функцию. Не бойтесь делегировать, современные MSSP предлагают реагирование 24/7, доступ к TI и аналитикам, гибкие ценовые модели (по инциденту, по подписке), что особенно эффективно для малого бизнеса и стартапов.

9. Делайте постанализ инцидентов хотя бы 1 раз в месяц, чтобы понять не только «что произошло», но и почему и что изменить (простой формат: что произошло, почему не отреагировали раньше (если поздно), какие выводы, какие изменения внести). SV SOAR предлагает для этого встроенных ИИ-помощников, ведь регулярный постмортем даже для 1–2 инцидентов в месяц — колоссальный рост зрелости ИБ.

10. Реагирование — это не «героизм по звонку ночью», а управляемый процесс, который должен масштабироваться, быть воспроизводимым и прозрачным, а главное — жить без «звезды»-аналитика.

Реагировать нужно, но — по-умному.

ВСЁ ДЛЯ SOC В КОНТЕЙНЕРНЫХ СРЕДАХ И KUBERNETES

Дмитрий ЕВДОКИМОВ
основатель и технический директор Luntry

В эпоху стремительного развития облачных технологий и микросервисных архитектур контейнерные среды, особенно на базе Kubernetes, становятся стандартом для развёртывания и масштабирования приложений. Однако с ростом популярности этих технологий растут и вызовы в области безопасности. В данной статье мы расскажем о нашем комплексном решении, которое охватывает все аспекты безопасности контейнеров на протяжении всего их жизненного цикла, а также подробно остановимся на задачах SOC (Security Operations Center) в Kubernetes.

СПЕЦИАЛИЗАЦИЯ НА БЕЗОПАСНОСТИ КОНТЕЙНЕРОВ И KUBERNETES

Мы специализируемся именно на безопасности контейнерных сред, построенных на Kubernetes, и предлагаем уникальное решение — Luntry, которое закрывает все семь ключевых доменов безопасности контейнеров и Kubernetes — от разработки до эксплуатации и мониторинга. В рамках SOC-операций наш особый блок посвящён безопасности рантайма (Runtime) — именно те функции, которые позволяют SOC-специалистам выявлять инциденты, происходящие внутри контейнеров в реальном времени, и реагировать на них.

ВВОДНАЯ ДЛЯ SOC-СПЕЦИАЛИСТОВ, НЕ ЗНАКОМЫХ С KUBERNETES

Kubernetes — это оркестратор контейнеров, который управляет тысячами контейнеров и микросервисов, вводя новые уровни абстракции: Pods, ReplicaSet, Deployments и многие другие. Для SOC-специалиста, привыкшего к классическим Linux-системам, это может стать серьёзным вызовом. Контейнер — это, по сути, изолированный Linux-процесс с ограничениями, но в Kubernetes контейнеры объединяются в Pods, которые входят в состав более крупных сущностей, таких как Deployments.

Например, процесс Nginx может запускаться во множестве контейнеров, принадлежащих разным Deployments и находящимся в разных Namespace. Без понимания этой иерархии невозможно точно определить источник и контекст инцидента. Поэтому задача SOC — не просто видеть процессы, а восстанавливать цепочку: процесс → контейнер → Pod → Deployment и Namespace.

ПОЧЕМУ SOC НЕ ВИДИТ ИНЦИДЕНТЫ В KUBERNETES?

Частая проблема — отсутствие видимости и контроля. Возможны разные сценарии проникновения злоумышленника:

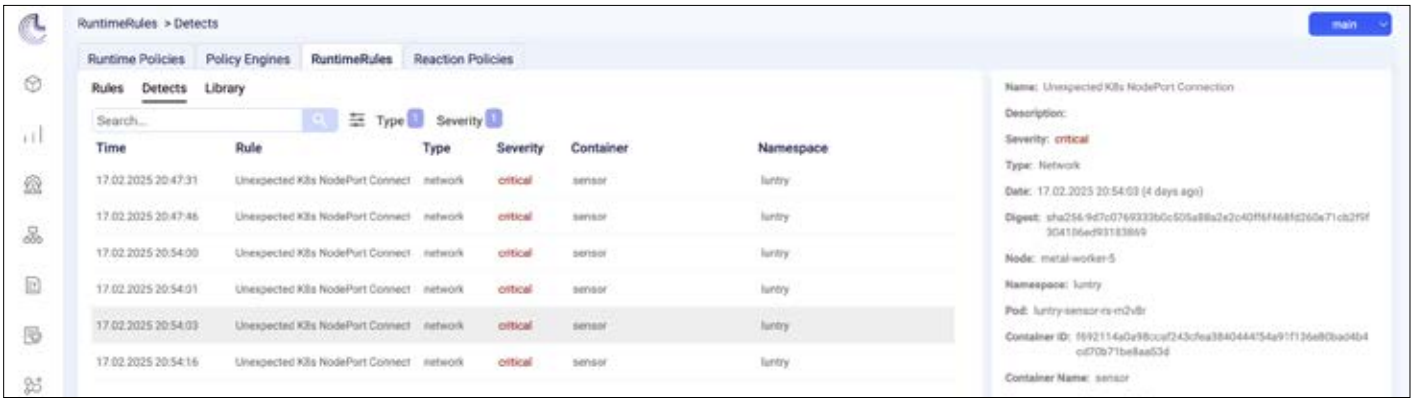
- эксплуатация неизвестных или известных уязвимостей, которые не были своевременно закрыты;
- длительный процесс патчинга, когда уязвимость остаётся открытой длительное время;
- внедрение вредоносного кода, бэкдоров или майнеров внутри контейнеров.

Наш опыт показывает, что сканирование образов на известные уязвимости и постановка задач разработчикам покрывает лишь около 15% работы по безопасности. Реальная защита наступает, когда патчи внедрены и работают в продуктиве, а до этого момента инфраструктура находится в большой опасности.

СПЕЦИФИКА БЕЗОПАСНОСТИ КОНТЕЙНЕРОВ И KUBERNETES ДЛЯ SOC

1. Уникальность каждого контейнера. Каждый контейнер — это уникальная среда с собственными настройками и конфигурациями, что усложняет применение классических методов безопасности. Традиционные EDR и агенты зачастую не понимают Kubernetes-специфику и не могут связать процессы с высокоуровневыми сущностями, что затрудняет расследование инцидентов.

2. Высокая нагрузка и объём событий. Контейнерные кластеры генерируют огромный объём событий: процессных, файловых, сетевых. Например, в одном из наших проектов на одной ноде порождается



до 100 тысяч потоков в секунду, что требует обработки миллионов событий в секунду. Это накладывает серьёзные требования к производительности и эффективности средств безопасности.

3. Динамичность и эфемерность. Контейнеры постоянно создаются, перезапускаются и удаляются. SOC-специалистам приходится сталкиваться с тем, что к моменту реакции на инцидент контейнер уже может отсутствовать, а следы инцидента — быть утеряны. Для решения этой проблемы необходимы специальные подходы к сбору и хранению данных.

4. Сетевая специфика Kubernetes. IP-адреса в Kubernetes динамичны и могут переходить после рестарта или обновления от одного микросервиса к другому. Для точного понимания сетевой активности требуется интеграция с Kubernetes Network Policy и понимание namespace и других абстракций.

ИСТОЧНИКИ ДАННЫХ ДЛЯ SOC В KUBERNETES

SOC-специалистам доступно пять уровней данных:

- **облако** — данные от облачного провайдера (если используется публичное облако);
- **кластер** — данные Kubernetes Audit Logs и Policy Engine;
- **хост** — события Linux-хоста, на котором работает Kubernetes;
- **контейнер** — процессные, файловые и сетевые операции внутри контейнера;
- **код приложения** — логи и метрики самого приложения.

Для эффективного мониторинга и реагирования необходимо собирать и анализировать данные со всех этих уровней.

МОДЕЛИ НАРУШИТЕЛЕЙ В КОНТЕЙНЕРНЫХ СРЕДАХ

В рамках контейнерной безопасности выделяют три классические модели нарушителей:

- внешний атакующий — злоумышленник, проникший в контейнер;
- внутренний атакующий — злоумышленник с доступом к Nodes кластера;
- скомпрометированный разработчик — злоумышленник с доступом к репозиториям кода, CI/CD и образам.

Естественно, атакующий может в процессе продвижений атаки переходить от одной модели к другой.

В контексте рантайма SOC-фокус направлен на обнаружение внешнего атакующего, уже находящегося внутри контейнера.

МЕТОДЫ ОБНАРУЖЕНИЯ И РЕАГИРОВАНИЯ

Для обнаружения инцидентов в контейнерах применяются три подхода:

- **сигнатурный** — поиск известных паттернов атак (blacklist), обычно по тем или иным правилам/сигнатурам, что позволяет обнаруживать только известные атаки;
- **поведенческий** — выявление аномалий на основе изучения нормального поведения контейнера и отхождений от него, позволяет обнаруживать как известные, так и неизвестные атаки;
- **гибридный** — сочетание сильных сторон сигнатурного и поведенческого подходов для максимальной эффективности.

В нашем решении Luntry предоставляется возможность использовать все перечисленные подходы, что удобно для тех или иных ситуаций для повышения гибкости и корректности работы детектирования.

При этом реагирование позволяет собрать артефакты для расследования инцидента, а механизмы предотвращения вообще не дают инциденту наступить, но это уже другая история.

ЗАКЛЮЧЕНИЕ

Безопасность контейнерных сред и Kubernetes — это комплексная задача, которая требует глубокого понимания специфики платформы и использования специализированных инструментов. Наше решение Luntry покрывает все ключевые аспекты безопасности контейнеров на протяжении всего жизненного цикла, а блок безопасности рантайма ориентирован именно на задачи SOC-мониторинга, обнаружения, реагирования и предотвращения инцидентов в реальном времени.

Для успешной работы SOC в Kubernetes необходимы знания Linux, понимание архитектуры Kubernetes и умение работать с огромным потоком событий в динамичной, распределённой среде. Только тогда можно эффективно защищать микросервисные приложения и инфраструктуру от современных угроз.

* * *

Если вы хотите узнать больше о том, как обеспечить безопасность SOC в Kubernetes и контейнерных средах, мы готовы поделиться опытом и предложить решения, проверенные на практике.

ПОДХОД SOCRATa

ЧТО МЕШАЕТ РЕГИОНАМ БЫТЬ ЗАЩИЩЁННЫМИ И КАК НАШ ЦЕНТР МОНИТОРИНГА МЕНЯЕТ ПРАВИЛА ИГРЫ В ИБ

Александр КИРИЙ
руководитель центра мониторинга «SOCRAT» ООО КСБ-СОФТ

При построении эффективной системы защиты сложно обойтись без процессов управления уязвимостями, мониторинга и реагирования на инциденты ИБ. Несмотря на всю пользу, внедрены эти процессы далеко не везде, и на это есть причины. В статье мы разобрали, что мешает организациям в регионах быть защищёнными и что может им помочь.

ТРИ КИТА

Для построения процессов нужны люди, технологии и бюджет.

- Люди. Специалисты универсальны и перегружены задачами, поэтому посвятить полный рабочий день мониторингу не получится. Из-за этого процесс затянется на долгий срок или вообще не будет организован.
- Технологии. Хорошие технологии стоят соответствующе, и нередко средств на них не хватает (также стоит учитывать, что стоимость отдельных решений выше стоимости рисков от атаки, что с точки зрения бизнеса нецелесообразно).
- Финансы. Камень преткновения при внедрении чего-либо. В разрезе органов госвласти нередки сложности с ИБ, так как в отведённый бюджет нужно и импортозаместиться, и обновить лицензии на СЗИ, и пройти контроль эффективности. В итоге на мониторинг и управление уязвимостями попросту не хватает средств.

Но выход есть всегда: передать ИБ на аутсорс компаниям, чья специализация — информационная безопасность.

ПОЧЕМУ АУТСОРС?

Специалисты таких компаний непрерывно обеспечивают информационную безопасность, приобретают насмотренность и оперативно устраняют возникающие проблемы. ИБ на аутсорсе облегчает работу ответственному лицу, но не освобождает от неё.

Центр мониторинга SOCRAT постарался облегчить жизнь ответственному лицу и внедрил в свои процессы сервисы, позволяющие оперативно взаимодействовать практически по всем вопросам ИБ. Один из таких инструментов — сервис, частично обладающий функционалом IRP-системы, но с упором на простоту взаимодействия и оперативное решение вопросов. Например, в случае выявления инцидента аналитик SOCRAT формирует карточку с описанием и рекомендациями. Ответственное лицо получает уведомление, после чего выполняет рекомендации. Если в процессе изучения возникают вопросы, ответственный может задать их в чате сервиса. В случае необходимости взаимодействия с ГосСОПКА в сервисе предусмотрены соответствующие шаблоны под формат НКЦКИ с возможностью скачать карточку для отправки в ГосСОПКА.

Так как центр мониторинга чаще всего становится точкой входа по всем вопросам ИБ: проверка регулятора, работоспособность СЗИ, оформление ОРД и прочее, то мы также предусмотрели возможность задать вопрос на любую тему, связанную с ИБ, через единое окно сервиса.

Как итог, переход на новый сервис центра мониторинга SOCRAT ускорил реакцию ответственных лиц втрое, усилив защиту организаций.

* * *

Если вас заинтересовал подход SOCRAT, подключайтесь к центру мониторинга и испытайте сервис в пилотном режиме бесплатно. Реальная проверка эффективности покажет, насколько SOCRAT способен справиться с вашими задачами.

АУТЕНТИФИКАЦИЯ

ОТ ПАРОЛЕЙ К АДАПТИВНОЙ МФА

Сергей ГРУЗДЕВ
генеральный директор «Аладдин Р.Д.»

МЕНЯЕТСЯ МИР, МЕНЯЮТСЯ ТРЕБОВАНИЯ

После начала СВО Россия столкнулась с беспрецедентным ростом атак на информационные системы (ИС) организаций – как государственных, так и бизнеса.

Что обычно происходит после успешной атаки (инцидента ИБ)? Начинается борьба с её последствиями, выделение денег на закупку и внедрение новых систем мониторинга, антивирусов, DLP, ИИ и других модных продуктов и технологий, а не устранение причин, приведших к инциденту.

Причины же большинства инцидентов банальны – слабая, неправильно реализованная система идентификации и аутентификации в ИС.

Увы, этот сегмент ИБ – самый консервативный, нормативная база здесь не менялась десятилетиями.

ПАРОЛИ

Существующая нормативная база предписывает использование для аутентификации пользователей в ИС паролей – не менее 6-ти символов при мощности алфавита 30 символов для ИС 4-го класса защищённости, не менее 8-ми символов при мощности алфавита не менее 70 символов для ИС 1-го класса защищённости, а также смену пароля через каждые 6 мес. и 1 мес. соответственно.

Насколько это надёжно сегодня? Оценки времени, затрачиваемого на прямую атаку – прямой перебор всех возможных вариантов пароля (brute force) при использовании домашнего компьютера с 12-ю графическими картами RTX 5090, приведены в таблице 1[1].

Из таблицы видно, что использование пароля менее 8-ми символов, набранного без использования цифр и/или служебных символов недопустимо. Таким образом, действующие тре-

[1] По материалам https://www.hivesystems.com/blog/are-your-passwords-in-the-green.

бования к паролю для ИС 4-го класса защищённости безнадёжно устарели в случае, если имеется возможность машинного перебора.

А если увеличить мощность вычислительного ресурса и использовать облачный ресурс, например, Amazon (AWS) или ChatGPT-4?

8-ми символьный пароль с использованием прописных, заглавных букв, цифр и спецсимволов ломается за 5 часов.

Становится очевидно — от паролей надо отказываться, либо значительно усиливать требования к ним, увеличивая их длину (не менее 11-ти символов) и мощность алфавита (количество используемых букв в разных регистрах, цифр и символов).

А теперь давайте вспомним 2020–2021 гг., когда мы сидели на удалёнке. С чем мы столкнулись? С тем, что пользователи, выучив свой сложный пароль для доступа в корпоративную ИС, не сильно задумываясь о последствиях вводили его при заказе пиццы, в различных сервисах и соцсетях. Потом эти чужие сервисы ломали, пароли массово утекали в сеть, а затем уже попадали в объединённые базы типа Collection #2–5 (25 млрд учётных записей и паролей к ним). В результате там оказывалось до 7–10% наших сотрудников со своими актуальными паролями к корпоративным ресурсам.

Тот самый пресловутый человеческий фактор...

«Честными» — правильными и действительно стойкими паролями (выбранными случайно равновероятно из слов заданной длины используемого алфавита) практически никто не пользуется, запомнить их нереально, поэтому люди пользуются парольными фразами или составными паролями на основе легко запоминаемых слов.

Но, если пароль содержит слово или большую его часть из словаря паролей, или такой пароль когда-то ранее был использован кем-то, учётная запись с этим паролем была взломана или украдена, то оценки времени взлома/подбора пароля выглядят уже совсем по-другому (Таблица 2).

Кол-во символов пароля	Только цифры	Прописные буквы (текст)	Прописные и заглавные буквы	Прописные и заглавные буквы + цифры	Прописные и заглавные буквы + цифры и спецсимволы
4	Мгновенно	Мгновенно	Мгновенно	Мгновенно	Мгновенно
5	Мгновенно	Мгновенно	57 мин.	2 часа	4 часа
6	Мгновенно	46 мин.	2 дня	6 дней	2 недели
7	Мгновенно	20 часов	4 мес.	1 год	2 года
8	Мгновенно	3 недели	15 лет	62 года	164 года
9	2 часа	2 года	791 год	3K лет	11K лет
10	1 день	40 лет	41K лет	238K лет	803K лет

Таблица 1.

K-во символов пароля	Только цифры	Прописные буквы (текст)	Прописные и заглавные буквы	Прописные и заглавные буквы + цифры	Прописные и заглавные буквы + цифры + спецсимволы
...	...	...	...	...	...
17	Мгновенно	Мгновенно	Мгновенно	Мгновенно	Мгновенно
18	Мгновенно	Мгновенно	Мгновенно	Мгновенно	Мгновенно

Таблица 2.

Резюме:

◆ Надёжность защиты ИС с помощью правильных 8-ми символьных паролей типа *t~pbE#0u* (как предписывают нам нормативные требования)– это иллюзия, такая защита ломается примерно за 5 часов при стоимости аренды ресурсов ~$20.

◆ ***Про использование паролей для аутентификации в корпоративных ИС следует забыть и использовать более надёжную аутентификацию — усиленную или строгую.***

Теперь, чтобы двигаться дальше, нужно сделать шаг назад и обновить свои знания в области аутентификации.

ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ

Основные понятия идентификации и аутентификации и требования к их реализации определены в российских национальных стандартах, основные из них:

◆ ГОСТ Р 58833–2020 (Идентификация и аутентификация. Общие положения).

◆ ГОСТ Р 70262.1–2022 (Идентификация и аутентификация. Уровни доверия идентификации).

◆ ГОСТ Р 70262.2–2025 (Идентификация и аутентификация. Уровни доверия аутентификации).

Это основа, фундамент ИБ организации. Их нужно хорошо знать и руководствоваться именно ими, а не статьями из Интернет и рекомендациями новомодных систем ИИ, частенько выдающими откровенную чушь.

Идентификация. Идентификация пользователя — это процесс и способ установления и подтверждения личности пользователя — физического лица.

Идентификация всегда производится в два этапа: первичная и вторичная.

Во время первичной идентификации пользователя производится установление (распознавание) и подтверждение его личности, присваивание ему уникального идентификатора, регистрация в ИС, а также хранение и поддержание идентификационной информации в актуальном состоянии.

Во время вторичной идентификации пользователя в ИС осуществляется опознавание пользователя путем проверки предъявленного пользователем идентификатора. При положительном результате проверки производится переход к его аутентификации.

Вторичная идентификация является многократно повторяющимся процессом, осуществляющимся каждый раз при новом запросе пользователя на доступ к ресурсам ИС.

Уровни доверия идентификации определяют степень уверенности в правильности определения личности пользователя:

◆ Низкий (некоторая уверенность).

◆ Средний (достаточно высокая уверенность).

◆ Высокий (очень высокая уверенность).

Аутентификация пользователя — это процесс подтверждения (доказательства) подлинности пользователя и принадлежности ему предъявленного идентификатора.

Идентификация и аутентификация всегда неразрывны и используются вместе. Надёжность одного процесса существенно влияет (определяет) надёжность (уровень доверия) другого.

Цели аутентификации пользователей в ИС

1) Подтверждение личности пользователя (по предъявленному им идентификатору);

2) Установление доверительных отношений между участниками (сторонами) обмена:

◆ Аутентификация одной стороны (например, источника данных) — односторонняя аутентификация,

◆ Аутентификация обеих сторон (например, элементов ИТ-инфраструктуры) — взаимная аутентификация);

3) Предоставление доступа в ИТ-инфраструктуру или в ИС только «подлинным» пользователям;

4) Подтверждение личности и правомочности владельца ключа ЭП для проверки наличия полномочий на право создания электронной подписи и фиксации неотказуемости при выполнении процедуры создания электронной подписи электронного документа.

Достоверность результатов идентификации и аутентификации и уровень доверия ИС

Достоверность (корректность, правильность) результатов идентификации и аутентификации и уровень доверия ИС зависят от ряда параметров:

1) От уровня доверия первичной идентификации — полноты, качества предоставленных документов, подтверждений корректности и подлинности представленных документов и степени их связанности с личностью пользователя.

2) От уровня доверия аутентификации, определяемого видом аутентификации, характеризуемого:

◆ количеством одновременно применяемых факторов аутентификации (одно-, двух- или трёхфакторная аутентификация),

◆ используемыми протоколами аутентификации,

◆ организацией обмена аутентификационной информацией и доказательствами (односторонняя или взаимная аутентификация),

◆ используемыми средствами аутентификации.

3) От способов реализации аутентификации в ИТ-инфраструктуре и самой ИС (всего их 8 — локальная, прямая, доменная, иерархическая, распределённая сетевая, мостовая, браузерная и браузерная с трансляцией доверия).

4) От среды функционирования и места выполнения (замкнутая доверенная или недоверенная среда, внутри или вне защищённого периметра).

Уровень доверия ИС определяется достигнутым уровнем доверия идентификации и аутентификации и не может быть выше него. При этом определяющим является используемый вид аутентификации.

Их три (см. таблицу 3).

Простая аутентификация. Простая аутентификация может применяться в ИС с низким уровнем значимости информации и несущественным размером возможного ущерба в случае возникновения инцидента ИБ.

Особенности и примеры:

- Однофакторная
  - Пароль — запоминаемый и вводимый вручную (фактор знания общего с ИС секрета);
  - Одноразовый код доступа, присылаемый из ИС на зарегистрированное в ИС устройство пользователя;
  - Электронный идентификатор, не требующий ввода PIN-кода (фактор владения).
  - ***Использование биометрии в качестве единственного фактора аутентификации не допускается (например, лицо, голос или отпечаток пальца, снятый сканером, встроенным в компьютер пользователя).***
- Односторонняя — передача аутентификационной информации осуществляется в одном направлении — от пользователя к объекту доступа (ресурс ИС), при этом пользователь не может быть уверен, что получает доступ в нужную ему ИС, что её не подменили.

Усиленная аутентификация. Усиленная аутентификация должна применяться в ИС со средним уровнем значимости информации и существенным размером возможного ущерба.

Существенными условиями и отличиями от простой аутентификации являются:

- Использование двух факторов аутентификации (2ФА) — владения аппаратным устройством и знание пароля (секрета) или
- Использование двухэтапной проверки[2] — подтверждение личности пользователя с использованием фактора знания (долговременного пароля) и одноразового пароля (кода доступа), присылаемого пользователю на его зарегистрированный в ИС мобильный телефон SMS, push-уведомление, либо
- Одноразовый пароль (OTP), сгенерированный в приложении, установленном на мобильном телефоне пользователя на основе общего с ИС секретного ключа. Секретный ключ может быть загружен в приложение при инициализации, при сканировании QR-кода или другим способом. Технически сложной является задача безопасной передачи секрета в приложение, у многих она не решена, что сводит на нет всю безопасность.

Примеры:

- Google Authenticator (его использование противоречит российскому законодательству).
- Яндекс Ключ.
- Aladdin 2FA + корпоративный высокопроизводительный сервер аутентификации JAS (решена проблема безопасной передачи секрета на устройство пользователя).
- Аппаратные OTP-токены, U2F-токены (FIDO/FIDO-2), USB-токены, в защищённую память которых загружен файл-контейнер или сертификат, содержащий пользовательский идентификатор.
- Приложение на смартфоне, генерирующее и обслуживающее OTP-токены и др.

Опасность и особенности:

- Мобильный телефон, независимо от установленной ОС, является недоверенным и небезопасным.
- Один OTP-токен позволяет подключаться только к одной ИС, для работы с OTP-токенами на стороне ИС требуется сервер аутентификации.
- ***Перехват кодов доступа, извлечение из телефона секретного ключа для генерации OTP способно дискредитировать всю ИС и дать злоумышленникам доступ в неё под видом легальных пользователей (как в своё время было со взломом RSA SecurID).***

Уровень доверия ИС	Уровень доверия идентификации	Вид аутентификации
Низкий	Низкий	Простая
Средний	Средний	Усиленная
Высокий	Высокий	Строгая

Таблица 3.

Строгая аутентификация. Строгая аутентификация пользователей обязательна для применения в ИС с доменной архитектурой с высоким уровнем значимости информации и значительным размером возможного ущерба — для всех пользователей в ГИС класса защищённости К1, для привилегированных, удалённых пользователей, мобильных пользователей переносных устройств (ноутбуков), при обработке в ИС информации ограниченного доступа, для сотрудников подрядных организаций и их ИС, подключающихся к обслуживаемой ИС[3].

При строгой аутентификации должна применяться двух- или трёхфакторная взаимная аутентификация (2ФА/3ФА) с организацией двухстороннего обмена аутентификационной информацией между пользователем и объектом доступа, либо многостороннего обмена при использовании третьей доверенной стороны (корпоративного Центра Сертификации, выполняющего функции корпоративного «нотариуса»).

В процессе строгой аутентификации должны использоваться криптографические алгоритмы и протоколы аутентификации (например, Kerberos, TLS).

Третья доверенная сторона (Центр Сертификации) выполняет функции проверяющей стороны (Центр Валидации), и может не являться прямым участником обмена между пользователями и ИС, но может обеспечивать их данными, необходимыми для аутентификации (напри-

[2] Двухэтапную проверку часто путают с двухфакторной аутентификацией. При двухэтапной проверке допускается совмещение среды функционирования в одном устройстве, т.е. со своего смартфона пользователь может работать в ИС и получать на него push, OTP или SMS для доступа в эту ИС. При двухфакторной аутентификации среда функционирования ИС и среда функционирования второго фактора аутентификации пользователя (его аппаратного средства аутентификации) должны быть разными.

[3] Из новых Требований 117-го приказа ФСТЭК России о защите информации в государственных ИС (ГИС) и иных ИС и содержащейся в них информации.

мер, Ticket Kerberos для аутентификации в домене).

Необходимые компоненты для построения корпоративной PKI, обеспечения ДОВЕРИЯ и строгой аутентификации в ИС:

1. Корпоративный Центр Сертификации (ЦС, CA – Certificate Authority)[4]

◆ Это ключевой компонент, основа системы обеспечения доверенного взаимодействия всех объектов (сетевого, компьютерного оборудования, ПО, сервисов в ИТ-инфраструктуре), субъектов (пользователей) в ИС, основа корпоративной PKI.

◆ Центр Сертификации должен быть доверенным, ему должны безусловно доверять все элементы ИС и все участники обмена для реализации концепции ZeroTrust (нулевое доверие), когда никто в ИС никому не верит, но все доверяют корпоративному «нотариусу» (CA), который всех идентифицировал, проверил и по запросу подтвердил подлинность. И это не должен быть Microsoft CA (CS) – бесплатный сыр в мышеловке и единая точка отказа в большинстве наших ИТ-инфраструктур.

◆ Центр Сертификации должен быть сертифицирован ФСТЭК России – его безопасность, корректность функционирования и уровень доверия должны быть проверены и доказаны в процессе сертификации.

2. Служба каталога с контроллером домена (для ИС с доменной архитектурой)

◆ Примеры реализации: Windows – Active Directory, Linux – ALD Pro, РЕД АДМ, Альт Домен, Samba DC, FreeIPA и др.

3. USB-токены, смарт-карты, BIO-токены/ридеры со встроенным сканером отпечатков пальцев– это пользовательские аппаратные средства 2ФА/3ФА (фактор владения). Требования к ним:

◆ Устойчивость к взлому и клонированию, уникальность (для однозначной идентификации устройства).

◆ Аппаратная реализация криптографических преобразований с неизвлекаемым закрытым ключом, обеспечивающих необходимый уровень стойкости или имеющих гарантированную стойкость[5].

◆ Энергонезависимая память, достаточная для хранения как минимум двух цифровых сертификатов формата X.509.

◆ ПИН-код устройства (фактор знания), позволяющий пользователю разблокировать доступ к закрытому ключу и операциям с ним.

◆ Для средств 3ФА/2ФА – встроенный сканер отпечатков пальцев и математика для верификации полученного со сканера отпечатка с хранящимся в памяти токена эталоном – цифровым шаблоном (биометрический фактор, подтверждающий личность пользователя и его право получить доступ к функциональности токена или смарт-карты).

4. Клиентское ПО, обеспечивающее поддержку устройств аутентификации, работу с цифровыми сертификатами и PKI.

◆ В MS Windows таким штатным клиентским ПО является Windows Smartcard Logon.

◆ В Linux (и всех российских ОС на базе Linux) штатной поддержки PKI и средств 2ФА/3ФА нет.

Это серьёзная проблема, поскольку именно PKI обеспечивает безопасное доверенное взаимодействие всех со всеми в корпоративных сетях и инфраструктурах Enterprise-класса.

5. Система централизованного управления жизненным циклом сертификатов и средств 2ФА/3ФА.

При разворачивании корпоративной PKI и внедрении строгой аутентификации возникает необходимость автоматического отслеживания срока действия цифровых сертификатов пользователей, оборудования, вовремя их обновлять, перевыпускать, учитывать выданные пользователям средства 2ФА/3ФА, вовремя блокировать их и пр., а также существенно снижать рутинную нагрузку на администраторов.

ПРОБЛЕМЫ ИМПОРТОЗАМЕЩЕНИЯ

Что нужно для внедрения строгой аутентификации и повышения живучести наших ИС?

Пока мы жили в экосистеме Windows и доверяли всему, что нам давали, мы успели привыкнуть ко всему хорошему, что там есть – удобству, встроенной безопасности, построенной на базе PKI, к уровню Enterprise.

Как только началась СВО, нам послали первое предупреждение – отозвали сертификаты для межсайтового взаимодействия, и половина Интернет-сайтов в стране «легла», точнее, не смогла обеспечить то самое доверенное взаимодействие.

Инструменты обеспечения доверия стали использоваться как инструменты давления, шантажа, как серьёзное оружие, призванное и способное парализовать ИТ-инфраструктуру гос. организаций, органов власти, организаций КИИ, экономику страны.

Давайте зададим себе вопрос, а что будет, если вдруг перестанет работать корпоративный Центр Сертификации? Перестанет выдавать новые сертификаты? Не страшно.

А если перестанет работать корневой CA (который до поры до времени находился в оффлайне, а вам надо перевыпустить сертификаты для подчинённых CA, срок действия которых заканчивается) или Центр Валидации, который и проверяет предъявляемые всеми участниками обмена сертификаты?

Вот тут и начнётся страшный сон – наши ИТ-инфраструктуры («железо», сервисы, ПО) рискуют развалиться за сутки, все компоненты перестанут доверять друг другу и взаимодействовать друг с другом. Почему сутки? Это срок жизни тикета Kerberos.

Так что же происходит при миграции на Linux? Почему там всё не так? А всё достаточно просто – в Linux нет полноценного PKI корпоративного уровня, а без него – это всё консьюмерская история, не Enterprise, к которому мы все так привыкли.

[4] Не путать с УЦ (Удостоверяющим Центром), обеспечивающим выпуск и обслуживание сертификатов открытого ключа электронной подписи (по 63-ФЗ) для юридически значимого электронного документооборота

[5] Зарубежные криптоалгоритмы RSA, ECDSA с декларируемой стойкостью, российские ГОСТы с известной/гарантированной стойкостью.

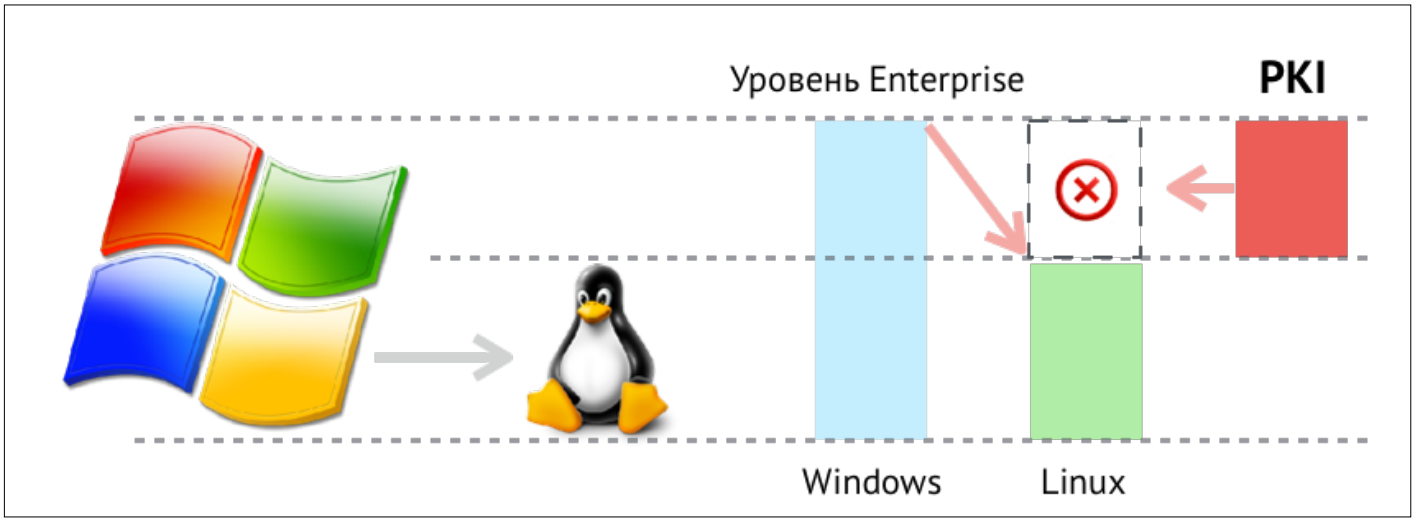


Рисунок 1.

И Open Source нам здесь, увы, не помощник — «поляна» хорошенько зачищена, поскольку это стратегическая технология, и как мне в своё время объяснили, цитирую: «Продать Enterprise PKI в Россию, это хуже, чем поставить ядерные технологии в Иран» (рис. 1).

Резюме.

Чтобы «вытянуть» Linux на уровень Enterprise, обеспечив при этом сквозную безопасность от ИТ-инфраструктуры до пользователей, реализовать доверенное взаимодействие, необходимо:

1. Внедрить корпоративную PKI — доверенный CA под Linux, который заменит MS CA — единую точку отказа, обеспечив бесшовный переход без остановки работы всех сервисов. Это обеспечит возможность «жить на два дома» — одновременно пользоваться ресурсами и из мира Windows, и новыми, из мира Linux.

2. Внедрить (поддержать с использованием нового доверенного CA) строгую аутентификацию всего используемого оборудования в ИТ-инфраструктуре.

3. Внедрить строгую аутентификацию пользователей (с использованием клиента PKI и 2ФА под Linux, обеспечивающего возможность «ходить налево» — в Windows). И не забыть про систему централизованного управления.

Ключевые различия двух экосистем (рис. 2).

Рисунок 2.

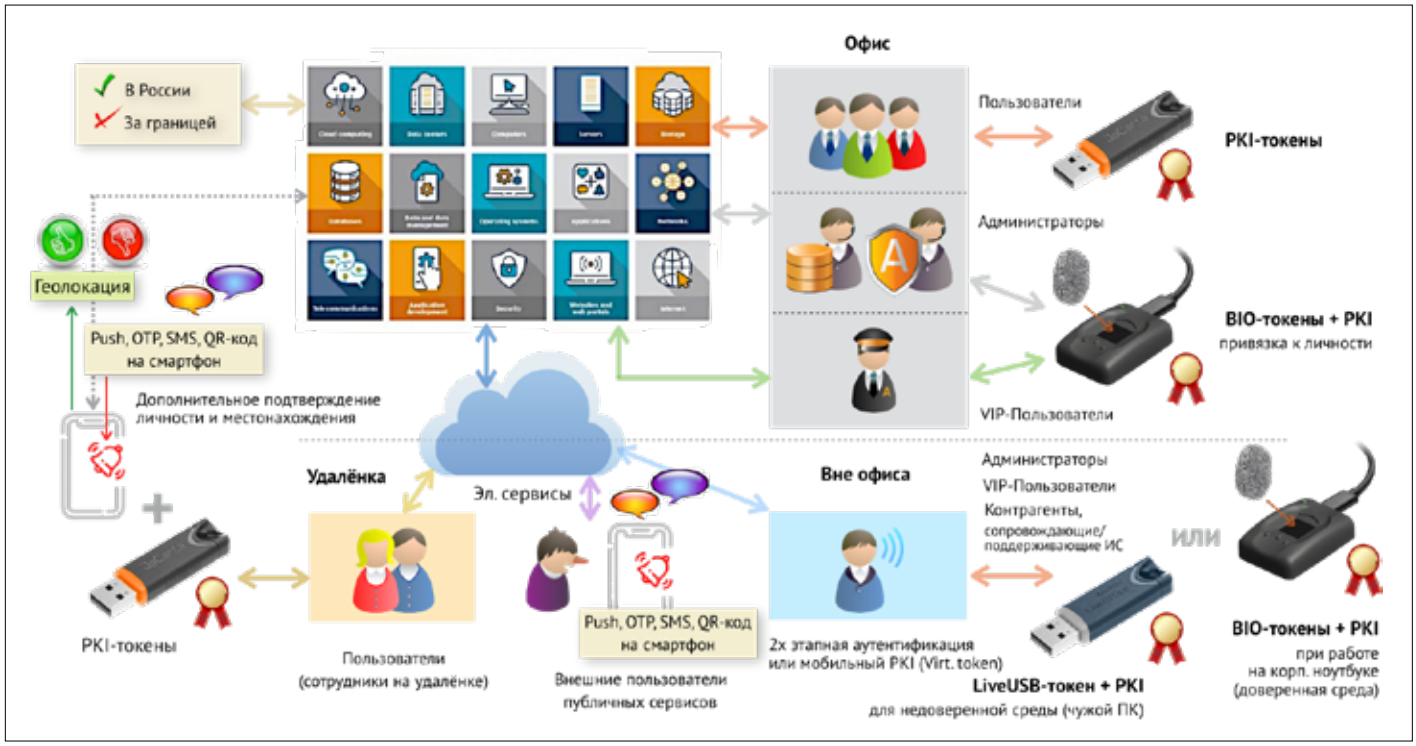


Рисунок 3.

Адаптивная многофакторная аутентификация. Самое время вспомнить про наши ИС: они не монолитны, имеют несколько сегментов, в которых хранится и обрабатывается информация разного уровня значимости. И про сотрудников, которые имеют разные уровни доступа в ИС, разные полномочия (ТОПы, ВИПы, админы), работают в разных условиях — кто-то в офисе, кто-то удалённо, из дома или с дачи, а кто-то релоцировался и работает из-за рубежа, кто-то работает на корпоративном ноутбуке, а кто-то на своём — домашнем.

А раз оно так, то разве можно подходить ко всем с одними правилами и требованиями по аутентификации? Нет, нельзя.

Для разных сегментов ИС, условий работы пользователей, для разных сред функционирования (в т.ч. средств 2ФА) должен быть определён РАЗНЫЙ набор факторов, дополнительных средств и способов подтверждения идентификационных данных и их связи с личностью пользователя.

Чем выше риск возможной атаки на систему и больше вариантов ее исполнения — тем должно быть больше дополнительных факторов, средств, способов и компенсационных мер для подтверждения личности пользователя.

Это и есть адаптивная многофакторная аутентификация (МФА), реализовать и поддерживать которую достаточно просто.

Попробуем показать и объяснить это с использованием рисунка 3.

1. Сотрудник работает в офисе

Контролируемый периметр объекта (здания, офиса), правильно настроенный корпоративный ПК, доверенная среда функционирования используемого ПО, развёрнута PKI, сотрудник работает с чувствительной информацией (CRM, ERP, персональные данные клиентов и пр.).

Для строгой аутентификации можно использовать USB-токены, смарт-карты с поддержкой PKI.

2. Привилегированные пользователи (администраторы, ВИПы, ТОПы) с корпоративными ноутбуками

Пользователи имеют расширенные полномочия и практически полный доступ ко всем ресурсам и сегментам ИС, мобильны, часто работают и в офисе, и вне его, подключаются к ИС удалённо, но со своего корпоративного ноутбука (контролируемого службой ИТ, с доверенной средой функционирования), голова забита более важными глобальными задачами и проблемами, чем непосредственно вопросы ИБ... Отсюда следствие, часто забывают ПИН-код от своего токена.

Для строгой аутентификации желательно использовать BIO-токены (отпечаток пальца вместо ПИН-кода и/или в дополнение к ПИН-коду для компенсации возникающих рисков при работе такого привилегированного пользователя вне контролируемого периметра организации).

3. Привилегированные пользователи (+ сотрудники подрядных организаций, поддерживающие ИС, внедряющие новое ПО и пр.), работающие из недоверенной среды (личный ноутбук, «чужой» ПК)

При работе из недоверенной среды для ИС возникают недопустимые риски — кража чувствительной информации, «подсаживание» специализированного трояна, организация атаки на ИС и т.п.

Для устранения этих рисков необходимо использовать специализированное средство, обеспечивающее безопасную дистанционную работу и строгую 2ФА пользова-

теля, работающего из недоверенной среды[6].

4. Сотрудники на удалёнке (с корпоративными ноутбуками — в доверенной среде функционирования).

Работают с чувствительной информацией (CRM, ERP, с персональными данными клиентов), им было дано разрешение работать удалённо, подключаясь из дома или работая на даче (где относительно безопасно).

Вопрос — а как отследить и убедиться, что сотрудник действительно работает из дома или на даче, а не уехал за границу и не работает оттуда?

Для многих организаций это недопустимый риск.

Чтобы получить геолокацию, понадобится зарегистрированный в ИС номер мобильного телефона такого сотрудника и дополнительные средства, обеспечивающие дополнительную (усиленную) аутентификацию с отправкой на него push, SMS, OTP сообщений и обработку данных геолокации по базовым станциям (увы, GPS/ГЛОНАСС теперь могут увести далеко не туда). И это в дополнение к его штатному USB-токену. Телефон нужен как «второй» фактор с возможностью получения геолокации, позволяющий осуществлять блокирование доступа из-за границы.

5. Сотрудники подрядных организаций, внешние пользователи некритичных сервисов ИС.

Сотрудники не подключаются к сегментам ИС, содержащим чувствительную информацию.

В этом случае достаточно использовать усиленную или двухэтапную аутентификацию (когда на смартфон пользователя посылается код доступа или установленное в нём приложение генерирует одноразовый пароль).

6. Внешние пользователи открытых публичных сервисов.

Являются потребителями информационных сервисов, подключаются к публичным ресурсам ИС.

Для доступа в Личный кабинет или для отправки в ИС сообщений часто требуется авторизация пользователей в ИС и их аутентификация. Если в организации уже развернут сервер для усиленной аутентификации, то имеет смысл использовать его и для аутентификации внешних пользователей с использованием push- или SMS-сообщений на его мобильный телефон.

Резюме.

Внедрение адаптивной аутентификации позволит кардинально решить проблему и устранить большое количество потенциальных проблем и инцидентов, поскольку устраняет одну из главных ПРИЧИН атак на ИС — слабую аутентификацию, обеспечит гибкость в выборе средств, методов и способов аутентификации, позволит правильно и эффективно распределить бюджет на ИБ.

Правильная система аутентификации в ИС — залог её безопасности.

[6] Требование 117-го Приказа ФСТЭК России, а также лучшие практики ИБ

ДВА ПОДХОДА

ACME V2.0 И ЕДИНАЯ СИСТЕМА АВТОМАТИЧЕСКОГО УПРАВЛЕНИЯ СЕРТИФИКАТАМИ (ЕСАУС)

Максим АРТЮХИН
Product owner, Clearway Integration

ВВЕДЕНИЕ

В условиях стремительного развития ИТ-инфраструктур управление технологическими сертификатами становится ключевым элементом безопасности серверов, устройств и корпоративных систем. Чем короче срок действия сертификата, тем меньше времени у злоумышленников для его использования в случае компрометации. Поэтому крупнейшие мировые корпорации, формирующие интернет-стандарты, к 2029 году планируют сократить максимальный срок действия TLS-сертификатов с 398 до 47 дней.

Параллельно с этим компании активно усиливают безопасность своих информационных систем: приоритетом становятся защита данных, устойчивость сервисов и контроль доступа. Это стимулирует переход к современным архитектурным решениям, таким как Zero Trust. Один из его типовых механизмов — внедрение взаимной TLS-аутентификации (mTLS), при которой сертификаты X.509 обязательны и для пользователей, и для сервисов — API, баз данных, микросервисов, прокси, инфраструктурных агентов и других компонентов.

Эти тренды кратно увеличивают нагрузку на инфраструктуру открытых ключей (PKI), требуя частого выпуска, ротации и распространения сертификатов. Без полноценной автоматизации это быстро приводит к ошибкам и простоям. Наибольшие сложности испытывают классические веб-серверы и приложения, где обновление по-прежнему выполняется вручную, а также динамические среды Kubernetes.

В динамичных контейнерных средах Kubernetes и Service Mesh (например, Istio) с использованием mTLS управление сертификатами чрезмерно усложняется: срок действия сертификата должен соответствовать среднему периоду жизни самого пода (или сервиса) — от нескольких часов до нескольких дней. Такой короткий период позволяет минимизировать риски, поскольку потенциально скомпрометированный закрытый ключ быстро становится недействительным даже без явного отзыва. В этом случае применение списков отзыва теряет смысл — они не успевают вступить в силу до истечения сертификата. Важно так же учитывать, что использование в кластере Kubernetes механизмов проверки отзыва сертификатов (CRL/OCSP) создаёт дополнительные накладные расходы и добавляет еще одну точку отказа, что негативно влияет на надежность кластера.

Kubernetes и аналогичные платформы устанавливают новый стандарт производительности для систем выпуска сертификатов. Тысячи подов и сервисных соединений, каждое из которых использует mTLS, создают нагрузку, измеряемую десятками тысяч запросов в минуту. Традиционные PKI-модели, спроектированные для значительно меньших объёмов, не выдерживают подобную нагрузку. Для соответствия новым требованиям индустрии нужна инфраструктура, способная легко масштабироваться и реализовать надежную автоматизацию выпуска десятков тысяч сертификатов за считанные минуты.

Рассмотрим два подхода для ответа на новые вызовы ИТ-отрасли: ряд решений на базе протокола ACME v2.0 и новую отечественную разработку — Единую Систему Автоматического Управления Сертификатами (ЕСАУС) на платформе ЦУГИ.

ACME: ПРОТОКОЛ С ОГРАНИЧЕНИЯМИ

ACME (Automated Certificate Management Environment, RFC8555) — открытый интернет-стандарт автоматизации выпуска, обновления и отзыва SSL/TLS-сертификатов. Он лежит в основе таких известных сервисов, как Let's Encrypt. Благодаря этому миллионы сайтов и сервисов по всему миру могут быстро внедрять HTTPS без сложных ручных процедур. В последние годы всё больше публичных, корпоративных и частных центров сертификации внедряют поддержку этого стандарта, а число совместимых продуктов и инструментов постоянно растёт.

Чтобы понимать, как работает этот протокол, важно знать: подтверждение права владения доменом — фундаментальный этап выпуска сертификата по ACME, который сохраняется с первых версий и остаётся обязательным в актуальной спецификации ACME v2. Автоматизированный клиент (например, certbot или acme.sh) инициирует запрос на сертификат в удостоверяющий центр (УЦ), указывая доменное имя. В ответ УЦ предлагает выполнить один из стандартных вызовов проверки подлинности (challenges): HTTP-01, DNS-01 или TLS-ALPN-01. Только успешно пройдя проверку, заявитель получает сертификат.

Каждый тип проверки имеет свои особенности и риски, которые необходимо учитывать при выборе метода.

HTTP-01 — простой метод, при котором на веб-сервере размещается специальный файл, доступный по порту 80. Подходит для классических сайтов, но в защищенных

инфраструктурах неудобен и менее безопасен. В Kubernetes часто возникают ошибки из-за особенностей работы Ingress Controller: несовпадение маршрутов между ресурсами, ошибки 404 при проверках и другие сбои. Кроме того, открытие порта 80 во внешнюю сеть увеличивает поверхность атаки и создаёт дополнительные риски компрометации сервисов.

DNS-01 – универсальный метод, при котором в DNS через API добавляется TXT-запись без необходимости открывать веб-сервер на порт 80. Используется для wildcard-сертификатов, а также любых доменов и сервисов, где невозможно или неудобно использовать HTTP-01. Основные недостатки: сложность разграничения прав, риск компрометации учётных данных DNS-API, уязвимость к атакам типа DNS cache poisoning (отравление DNS-кеша), что в обоих случаях может привести к подмене сертификатов. Жёсткая политика прав доступа усложняет эксплуатацию, а прокси-решения вроде acmeproxy облегчают контроль и аудит, но одновременно с этим увеличивают архитектурную сложность и не устраняют фундаментальные уязвимости DNS.

Тысячи подов и сервисных соединений, каждое из которых использует mTLS, создают нагрузку, измеряемую десятками тысяч запросов к PKI в минуту. Традиционные PKI-модели, спроектированные для значительно меньших объёмов, не выдерживают подобную нагрузку

TLS-ALPN-01 – основан на использовании расширения ALPN в процессе TLS-handshake. Для его работы сервис должен принимать входящее соединение на порт 443 и возвращать временный сертификат с ALPN-значением acme-tls/1. В Kubernetes применение этого метода затруднено, поскольку TLS-терминация обыч-

Многие ACME-решения создают иллюзию простоты и легкости внедрения, но на практике сопровождаются существенными ограничениями и скрытыми трудностями

но выполняется на уровне Ingress Controller, который занимает порт 443 и не передаёт ALPN-информацию в поды. В итоге TLS-ALPN-01 остаётся нишевым, уступая по универсальности и удобству HTTP-01 и DNS-01.

Как видно, протокол ACME изначально не ориентирован на динамичные контейнерные среды, такие как Kubernetes и Istio. Его методы проверки (HTTP-01, DNS-01, TLS-ALPN-01) не учитывают специфику распределённой маршрутизации и безопасного хранения секретов. Кроме того, в ACME отсутствует нативная поддержка сервисной идентичности SPIFFE/SPIRE — ключевого механизма безопасности и аутентификации в Istio. Поэтому для полноценного использования ACME в Kubernetes и Istio необходимы дополнительные компоненты и интеграции, обеспечивающие автоматическое выполнение вызовов проверки, безопасное управление ключами, ротацию сертификатов и поддержку сервисной идентичности.

Многие ACME-решения создают иллюзию простоты и легкости внедрения, но на практике сопровождаются существенными ограничениями и скрытыми трудностями. Чтобы разобраться в специфике построения PKI на базе ACME для Kubernetes и Istio, нужно понимать, из каких ключевых компонентов складывается процесс выпуска сертификатов с использованием внутреннего ACME-сервера и как эти элементы взаимодействуют между собой.

Для построения PKI на ACME для контейнерных сред требуются:

- **ACME-сервер** (УЦ вне Kubernetes) — принимает запросы на выпуск, обновление и отзыв сертификатов.
- **Оператор cert-manager** — нативный Kubernetes контроллер, использующий API и CRD для автоматической ротации сертификатов и их хранения в Kubernetes Secret (секретах). При этом приватные ключи доступны объектам с соответствующими правами доступа. Реальная защита этих данных напрямую зависит от уровня безопасности кластера, включая настройки RBAC, шифрование etcd, контроль доступа к API и аудит. Поэтому подход хранения ключей в секретах не соответствует принципам Zero Trust. Для повышения уровня защиты рекомендуется использовать специализированные CSI-драйверы, интегрирующиеся с внешними системами управления секретами. Кроме того, для cert-manager регулярно выявляются уязвимости (например CVE-2024–12401 и др.) и отмечены проблемы с масштабируемостью в больших кластерах (>10,000 подов).
- **CSI-драйверы для сертификатов** (csi-driver) — позволяют хранить секреты вне etcd и интегрироваться с внешними системами управления секретами, обеспечивая безопасное и контролируемое монтирование ключей и сертификатов в поды. Они поддерживают автоматическое обновление без необходимости перезапуска подов. Однако, при компрометации пода остается доступ к монтированным секретам, поэтому важно минимизировать привилегии контейнеров и контролировать обновление секретов. Требуется тщательная настройка версионности и мониторинга, особенно в масштабных средах.

Для интеграции Kubernetes с SPIFFE/SPIRE используется специализированный CSI-драйвер csi-driver-spiffe. Он автоматически выдает короткоживущие сервисные сертификаты X.509-SVID с поддержкой идентичности рабочей нагрузки (workload identity).

- **istio-csr** — интеграционный компонент Istio для работы с внешними системами управления сертификатами, включая cert-manager и корпоративные УЦ. Он автоматизирует подпись и ротацию сертификатов для рабочих нагрузок Service Mesh, используя стандарты SPIFFE для workload identity. Однако, ошибки в настройках доступа (RBAC и других механизмов разграничения прав) могут привести к серьёзным уязвимостям.

ACME-клиенты (certbot, acme.sh) применимы лишь в специализированных сценариях, например для ручной выдачи сертификатов отдельным сервисам. Они не имеют нативной интеграции с Kubernetes API и CRD, поэтому не умеют автоматически управлять объектами кластера и не синхронизируются с Ingress или внутренними сервисами вроде ClusterIP. Именно это значительно ограничивает их применение в динамичных контейнерных средах.

Пару слов про ACME-серверы. Их условно делят на публичные и внутренние корпоративные для закрытых сетей. Публичные ACME-серверы всегда сопровождаются серьезными ограничениями на взаимодействия для клиентов: лимиты на количество запросов, требование внешней доступности (порт 80 или доступ к DNS-API), фиксированный срок действия сертификатов (обычно 90 дней), отсутствие контроля над средой применения сертификата. Поэтому многие организации рассматривают вариант развёртывания корпоративного ACME-сервера для внутренней инфраструктуры, чтобы сохранить автономность, адаптировать процессы управления сертификатами под бизнес-требования и исключить внешние зависимости.

Рассмотрим популярные ACME-серверы:

- **OpenACME** — минималистичный ACME-сервер для внутренних сред, подходящий для тестовых задач и базовой автоматизации выпуска сертификатов. Основные недостатки: сла-

бая поддержка, устаревание кода, нет интеграции с HSM, отсутствие масштабируемости и защиты от современных угроз.

◆ **Pebble** — лёгкое решение, созданное для тестирования ACME-клиентов и CI/CD-автоматизации, отличается простотой установки и настройки. Однако не предназначен для промышленной эксплуатации: отсутствуют механизмы масштабирования, безопасности и отказоустойчивости, нет интеграции с HSM.

◆ **Boulder** — мощная open-source платформа, используемая в Let's Encrypt, оптимальна для публичных центров сертификации. Для корпоративных задач избыточна — очень тяжелая в сопровождении, требовательная к ресурсам и нуждается в доработках для интеграции с HSM и корпоративными системами управления доступом.

◆ **Smallstep CA:** бесплатная версия очень сильно ограничена по функционалу и содержит ряд уязвимостей (поддерживается только один промежуточный УЦ, базовые политики). Коммерческая версия недоступна для российских компаний.

◆ **EJBCA (Keyfactor):** бесплатная версия имеет существенные ограничения по функционалу (нет механизмов высокой доступности, базовые роли и политики и т.д.), не гарантирует высокий уровень безопасности и оперативной реакции на угрозы. Все обновления и исправления уязвимостей зависят от активности сообщества. Коммерческая версия недоступна в России.

◆ **Venafi Trust Protection Platform и Hashicorp Vault** — коммерческие решения с поддержкой ACME и автоматизацией жизненного цикла сертификатов, обеспечивающие высокий уровень централизованного контроля и безопасности, но также недоступны для российских компаний.

Мы рассмотрели набор компонентов для построения PKI на базе ACME. На практике такие решения редко работают как единое целое. Каждый модуль создавался под отдельные задачи и развивался в собственном темпе. При объединении их в единый стек возникает фрагментированная архитектура: разные методы управления, несинхронные обновления, отсутствие централизованной модели сопровождения.

Рассмотрим детальнее ключевые проблемы и вызовы, с которыми придется столкнуться при внедрении подобных стеков в изолированных и корпоративных инфраструктурах.

1. Импортозамещение и нормативные ограничения.

◆ Ограниченная доступность зарубежных продуктов и сервисов, отсутствие адаптации под отечественные регуляторные требования.

◆ Нет поддержки российских криптоалгоритмов (ГОСТ, Российских аппаратных СКЗИ) и отсутствие решений в Едином реестре российского ПО, что ограничивает применение в критически важных информационных инфраструктурах (КИИ) и госорганах.

2. Архитектурная сложность и отсутствие централизованной наблюдаемости.

◆ Логи компонентов разрозненные, форматы не согласованы, штатная интеграция с SIEM и централизованным аудитом, как правило, отсутствует.

◆ Нет сквозной прослеживаемости запросов между разнородными модулями.

◆ Отсутствие необходимых метрик (health-check, ошибки выпуска и продления и т.п.), что осложняет мониторинг состояния PKI.

3. Несовместимость с концепцией Zero Trust.

◆ Модель доверия ACME-решений основана на подтверждении владения доменом, а не на аттестации устройств или сервисов.

◆ Большинство реализаций протокола не предусматривают встроенных механизмов оценки контекста окружения и устройства, которому выдается сертификат — это ограничивает возможность реализации полноценного Zero Trust.

4. Эксплуатационные трудности и высокая зависимость от квалификации персонала.

◆ Поддержка ACME-стека требует глубокого понимания всех его компонентов, работы механизмов Kubernetes и методов безопасного управления ключами.

◆ Разные компоненты поддерживаются разными подразделениями, что затрудняет координацию обновлений, аудит и плановое обслуживание.

◆ Отсутствует централизованная поддержка, из-за чего выявление и устранение ошибок занимает больше времени.

5. Проблемы совместимости и жизненного цикла компонентов.

◆ Разные темпы развития компонентов и несинхронизированные обновления повышают риск несовместимостей и эксплуатации уязвимостей.

◆ Поддержка отдельных open-source проектов может быть приостановлена без предупреждения.

6. Расширение поверхности атаки и уязвимости цепочки поставок.

◆ Каждый дополнительный модуль увеличивает количество потенциальных точек атаки.

◆ Используемые библиотеки могут не проходить централизованную проверку безопасности и содержать скрытые уязвимости.

7. Недостатки в управлении доступом и разграничении ответственности.

◆ Отсутствует делегирование полномочий и чёткое разделение ролей; контроль за выпуском сертификатов фактически сосредоточен у системных администраторов или DevOps-инженеров.

◆ Размыта ответственность за выпуск, продление и отзыв сертификатов, затруднён аудит.

◆ Автоматизация на базе ACME часто обходится без участия службы информационной безопасности, что нарушает внутренние политики и снижает общий уровень контроля.

8. Сложности миграции и технологическая зависимость.

◆ Переход на УЦ другого производителя или национальные алгоритмы (ГОСТ) может потребовать переработки всей архитектуры и замены ключевых компонентов.

9. Масштабируемость и производительность.

◆ Современные Kubernetes-кластеры могут содержать до 5000 узлов и 150 000 подов, что накладывает высокие требования на производительность PKI.

◆ Частая ротация сертификатов (каждые 24–48 часов) генерирует тысячи запросов в минуту, что может вызвать тайм-ауты, сбои в cert-manager и перегрузку УЦ.

Что в итоге?

Качественные коммерческие продукты зарубежных вендоров недоступны российским компаниям, а построение PKI на базе open-source ACME-решений в корпоративных и изолированных инфраструктурах — трудная задача с огромным количеством подводных камней. При попытке объединить разные компоненты в единое и цельное решение будьте готовы к последствиям:

◆ ***фрагментированная архитектура с разнотипными механизмами управления;***

◆ ***проблемы с несовпадающими жизненными циклами компонентов ПО;***

◆ ***отсутствие единой модели сопровождения.***

ЕСАУС

На этом фоне Единая Система Автоматического Управления Сертификатами (ЕСАУС) отечественного производителя Clearway Integration — достойный ответ на современные вызовы. ЕСАУС — это комплексное централизованное решение, которое обеспечивает аудит, объединяет работу с политиками безопасности, поддерживает отечественные криптоалгоритмы, управление ролями и гибкую автоматизацию всех этапов жизненного цикла сертификатов и ключей. Предусмотрена поддержка как классических серверов, так и кластеров Kubernetes и Istio.

ЕСАУС построена на платформе ЦУГИ (№ 13033 в реестре отечественного ПО) из модульных компонентов, легко интегрируется с другими системами на платформе: отечественным УЦ MiniCA, Система Учета и Управления СКЗИ (СУУ СКЗИ 2.0) и Личным Кабинетом Пользователя Сертификатов (ЛКПС). В основе ЕСАУС — многоуровневая архитектура, разработанная специально для комфортной работы со сложными и сегментированными сетями:

◆ Принцип Zero Trust: специализированные агенты передают не только запрос на сертификат (CSR), но и сведения об окружении, в котором он был сформирован. Эта информация сверяется с утвержденными политиками выпуска сертификатов.

◆ Централизованный аудит: система ведёт полный журнал всех операций, включая сертификаты, которые УЦ обычно не регистрируют в своей базе.

◆ Архитектурные паттерны: постоянная проверка доступности компонентов друг другом; автоматический возврат к восстановившемуся компоненту после его отказа; механизмы коммуникации между компонентами для управления пропускной способностью системы и др.

◆ Гетерогенная инфраструктура: агенты для классических приложений (ОС Windows, Linux, macOS), Операторы и Цитадель для кластеров Kubernetes и Istio.

Отдельно отметим, что на волне современных трендов технологический суверенитет от зарубежных решений становится все более важным для корпоративных и государственных ИТ-инфраструктур. Особую ценность приобретает возможность гибкой миграции между разными УЦ (например, с Microsoft CA на отечественный MiniCA или другие отечественные УЦ). Благодаря поддержке широкого спектра УЦ (Microsoft CA, MiniCA, КриптоПро PKI-кластер, SafeTech CA, Aladdin eCA) ЕСАУС позволяет балансировать нагрузку и легко переключаться между УЦ разных вендоров, сохраняя непрерывность работы и надежность бизнес-процессов.

Все это дает возможность с помощью ЕСАУС решать следующие задачи:

◆ Выносить логику УЦ за пределы микросервисных платформ, возвращая контроль службе информационной безопасности, разделяя функций ИБ и администраторов Kubernetes/Istio.

◆ Выдерживать пиковые нагрузки по выпуску сертификатов в больших кластерах Kubernetes и Istio, предотвращая перегрузки на УЦ.

◆ Автоматизировать настройку информационных систем для использования обновленных сертификатов, включая координированное обновление в кластерах и в распределённых системах.

◆ Актуализировать и распространять списки доверенных корневых и промежуточных УЦ по всей организации.

◆ Изолировать УЦ от прямого доступа по сети клиентов и потребителей сертификатов.

ЗАКЛЮЧЕНИЕ

PKI в современных средах Kubernetes и Istio перестала быть просто вспомогательным инструментом и превратилась в стратегическую компетенцию. Удобные на первый взгляд ACME-решения обещают «один клик — и готово», но за этим стоит хрупкая архитектура: разрозненные компоненты, разные жизненные циклы ПО, отсутствие единого управления. Только комплексный подход, сочетающий автоматизацию, контроль, аудит и интеграцию с корпоративными системами, позволит создать по-настоящему надёжную и масштабируемую инфраструктуру доверия для современных облачных платформ.

В этом контексте ЕСАУС — это не просто инструмент, а перспективное решение, которое позволяет перейти от фрагментированного и реактивного управления сертификатами к проактивной и централизованной системе. Автоматизируя рутинные операции, минимизируя человеческий фактор и повышая уровень безопасности, ЕСАУС помогает сократить финансовые затраты за счёт экономии времени высококвалифицированных специалистов и направить освободившиеся ресурсы на решение ключевых задач бизнеса.

КРИПТОПРО КЛЮЧ

ИННОВАЦИОННОЕ РЕШЕНИЕ ДЛЯ МОБИЛЬНОЙ ПОДПИСИ

Павел ЛУЦИК
директор по развитию бизнеса и работе с партнёрами, КриптоПро

Павел СМИРНОВ
директор по развитию, КриптоПро

В условиях стремительной цифровизации общества и постоянного роста количества услуг, предоставляемых в электронном виде, электронная подпись становится все более востребованной. Крупные организации и предприятия, стремящиеся предоставлять дистанционные сервисы и оказывать цифровые услуги, нуждаются в надежной инфраструктуре электронной подписи, позволяющей обеспечить высокий уровень безопасности, удобства и юридической значимости электронного документооборота. Создание подобной инфраструктуры возможно на основе продуктов компании КриптоПро, главным компонентом которой является решение КриптоПро Ключ.

КриптоПро Ключ – это первое в России сертифицированное ФСБ решение для мобильной электронной подписи на основе инновационной технологии распределённого хранения и использования ключей электронной подписи, обеспечивающее качественно новый уровень безопасности мобильной подписи.

КриптоПро Ключ – это результат нескольких лет кропотливой работы: в основе решения лежит семейство новейших криптографических протоколов DKSSP, не имеющих аналогов в мире, которые разработаны и обоснованы специалистами КриптоПро.

КриптоПро Ключ предоставляет пользователям ряд преимуществ. Во-первых, это централизованное управление, позволяющее развертывать решение в корпоративной ИТ-инфраструктуре с поддержкой импортозамещенных технологий. Во-вторых, решение работает со всеми современными видами и форматами подписи и шифрования документов.

Решение поддерживает несколько режимов хранения и использования ключей:

- распределённо в мобильном приложении и на серверной стороне в программно-аппаратном криптографическом модуле КриптоПро HSM;
- локально, с поддержкой ключевых носителей, подключаемых к мобильному устройству бесконтактно по NFC или контактно с использованием совместимых носителей;
- локально на рабочем месте пользователя на традиционных ключевых носителях при работе через веб-ин-

терфейс (режим КриптоПро Ключ Lite).

Наиболее защищённый режим работы — распределённый, реализованный при помощи протоколов DKSSP. В данном режиме обеспечивается безопасность пользовательских ключей даже в случае компрометации клиентского устройства. Ключ подписи пользователя не появляется в открытом виде ни на одной из сторон — ни на клиентском устройстве, ни на сервере — на протяжении всего жизненного цикла. Все операции, связанные с электронной подписью, выполняются исключительно при взаимодействии между мобильным приложением пользователя и защищённым сервером, в частности — в программно-аппаратном криптографическом модуле КриптоПро HSM. Такой подход позволяет надёжно защитить ключ в самых критических ситуациях. Даже если пользователь теряет мобильное устройство или происходит компрометация сервера, ключ подписи остаётся в безопасности и не может быть скомпрометирован.

Решение предоставляет возможность интеграции с корпоративными информационными системами через REST API для реализации различных сценариев работы. Пользователи могут взаимодействовать с программным комплексом при помощи веб-интерфейса на своем рабочем месте и в мобильных приложениях на основе КриптоПро Ключ SDK и КриптоКлюч SDK. Сохраняя преемственность, КриптоПро Ключ поддерживает программные интерфейсы (API), унаследованные от КриптоПро DSS 2.0. Это обеспечивает лёгкий переход на новый продукт и современные API, как серверный, так и API для разработки мобильных приложений (КриптоПро Ключ SDK и КриптоКлюч SDK).

КриптоПро Ключ — первое и единственное на данный момент массово доступное решение для мобильной электронной подписи с сертифицированным SDK, который можно встраивать в мобильные приложения и создавать собственные решения в экосистемах крупнейших банков, удостоверяющих центров и госсектора.

КриптоПро Ключ создавался с учётом того, что пользователю, использующему электронную подпись со смартфона, важна оперативность. Он может не разбираться в особенностях криптографии и технологиях, его цель — быстро и просто подписать нужный документ. Поэтому в мобильных приложениях КриптоПро Ключ и КриптоКлюч спроектирован максимально короткий клиентский путь.

КриптоПро Ключ предоставляет следующие основные возможности:

- Управление учётными записями Пользователей с возможностью разделения на группы с различными настройками и политиками.
- Выполнение криптографических операций с применением отечественных алгоритмов:
  - аутентификация Пользователей и Операторов;
  - генерация ключей ЭП, ключей проверки ЭП, закрытых и открытых ключей шифрования;
  - формирование запросов на сертификаты;
  - создание ЭП документов;
  - зашифрование и расшифрование документов.
- Поддержка различных форматов подписи:
  - необработанная подпись по ГОСТ Р 34.10–2012;
  - подпись в формате CMS (CAdES-BES);
  - усовершенствованная ЭП (CAdES-T, CAdES-X Long Type 1);
  - подпись XML-документов (XMLDSig, XadES-BES, XadES-T);
  - подпись PDF-документов (с использованием форматов семейства CAdES, а также PAdES-B-B, PAdES-B-T, PAdES с включением доказательств проверки).
- Пакетное подписание (нескольких документов за одно подтверждение операции).
- Подписание документов в асинхронном режиме с возвращением результата (Callback) в вызывающую систему по завершении операции.
- Реализация множества способов аутентификации Пользователей, в том числе:
  - по логину и паролю с защитой канала по протоколу TLS с односторонней аутентификацией;
  - по сертификату с защитой канала по протоколу TLS с двусторонней аутентификацией (возможно использование USB-токенов и смарт-карт);
  - аутентификация и подтверждение операций пользователей по алгоритму HMAC, описанному в Рекомендациях по стандартизации ТК 26 Р 50.1.113–2016, в мобильном приложении на базе КриптоПро Ключ SDK;
  - вспомогательная аутентификация при помощи одноразовых паролей (OTP), доставляемых в SMS-сообщениях или по электронной почте.
- Интеграция со сторонними центрами идентификации по протоколу OAuth 2.0 и OpenID Connect 1.0 (в т.ч. с корпоративным доменом на базе MS AD (посредством ADFS) и OpenLDAP).
- Интеграция с удостоверяющим центром (далее — УЦ) на базе ПАК «КриптоПро УЦ» для автоматизации создания запросов на сертификаты, обработка запросов на сертификат в соответствии с требованиями выбранного УЦ.
- Визуализация (конвертация и отображение) электронных документов форматов, перечисленных в документе «ЖТЯИ.00118–01 96 01 КриптоПро Ключ. Общее описание», перед выполнением операции с ними.
- Добавление в PDF-документы видимой подписи (штампа) (отображение произвольных изображений, логотипов и текстов на штампе).
- Предоставление веб-интерфейса для Пользователей и Операторов.
- Предоставление программного интерфейса (REST API) для интеграции в бизнес-процессы.
- Предоставление SDK для встраивания в мобильные приложения.
- Реализация системы оповещений Пользователей о событиях и операциях с их ключами ЭП:
  - PUSH-уведомления;
  - SMS-сообщения;
  - E-mail-сообщения.
- Ведение аудита событий, связанных с действиями Пользователей, Операторов и эксплуатацией программного комплекса.

ОТ УЗКОГО СПЕЦИАЛИСТА ДО МАССОВОГО ПОТРЕБИТЕЛЯ

Георгий КОРАБЛЕВ
заместитель генерального директора по развитию бизнеса компании «АМИКОН»

Компания «АМИКОН» работает на рынке ИБ с 1994 года. Специализируясь на сетевой безопасности, в том числе и на средствах криптографической защиты, в настоящее время мы помогаем российским компаниям обеспечить импортозамещение и информационную независимость. Не во всех компаниях этот процесс идёт быстро, но государство планомерно ускоряет его и ужесточает контроль над ним в законодательном порядке. Принимаются меры по усилению защиты КИИ и переходу на отечественные средства защиты информации.

Это стало толчком к развитию рынка — производители российских средств защиты информации получили возможность реализовать свои планы и амбиции. И компании, имеющие потенциал и, безусловно, гибкость, этим воспользовались. Не отягощённый бюрократизированной структурой «АМИКОН» также быстро перестроился: мы создали проектную группу, которая успешно модернизирует наши продукты по требованиям клиентов, лишившихся привычных импортных средств защиты, и помогает им безболезненно вписаться в мир отечественного технологического суверенитета.

Гибкость внутренней структуры позволяет нам развивать не только новые версии наших классических, стабильно востребованных продуктов (МСЭ, NGFW, VPN, IDS), но и принципиально новые.

Если ранее наши традиционные продукты и услуги были ориентированы на технических специалистов со знанием сетевых технологий и прекрасно разбирающихся в государственном регулировании области ИБ, то сегодня мы разрабатываем продукты для массового потребителя. Речь о сотрудниках, редко задумывавшихся ранее о вопросах безопасности, очень мало знакомых с ИТ-технологиями и порой не слышавших ничего о комплаенсе.

Примером нашей продукции нового поколения для такой группы потребителей является АМИКОННЕКТ — система удобного удалённого доступа к защищённым корпоративным ресурсам. Всего одна кнопка, и от пользователя не требуется технологических знаний для работы с этим продуктом (рис. 1).

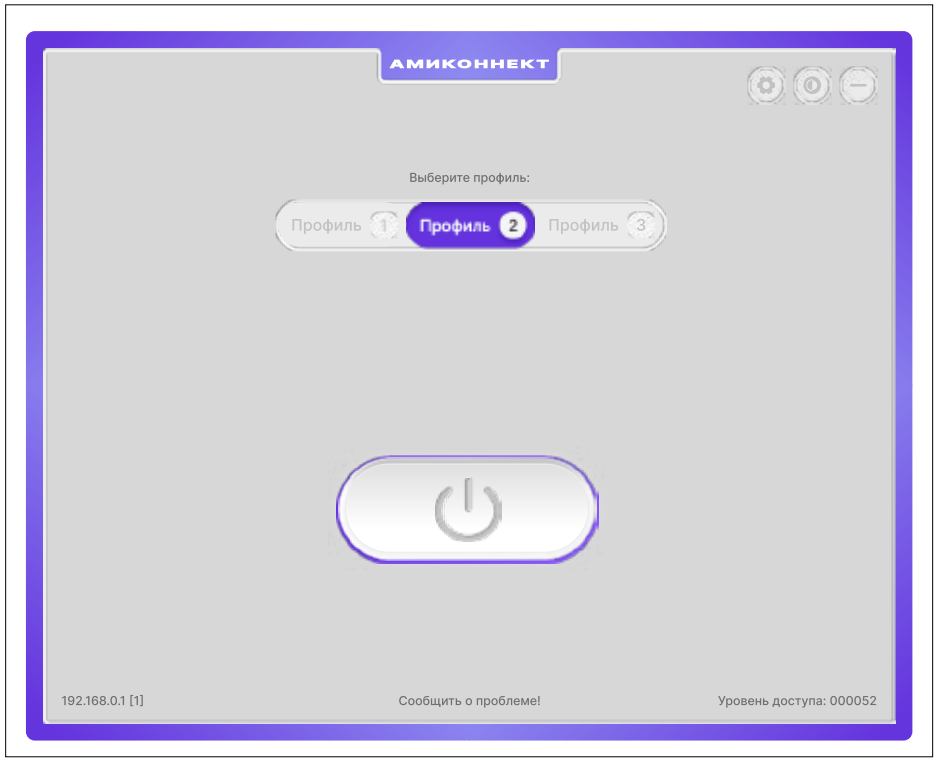


Рисунок 1. АМИКОННЕКТ

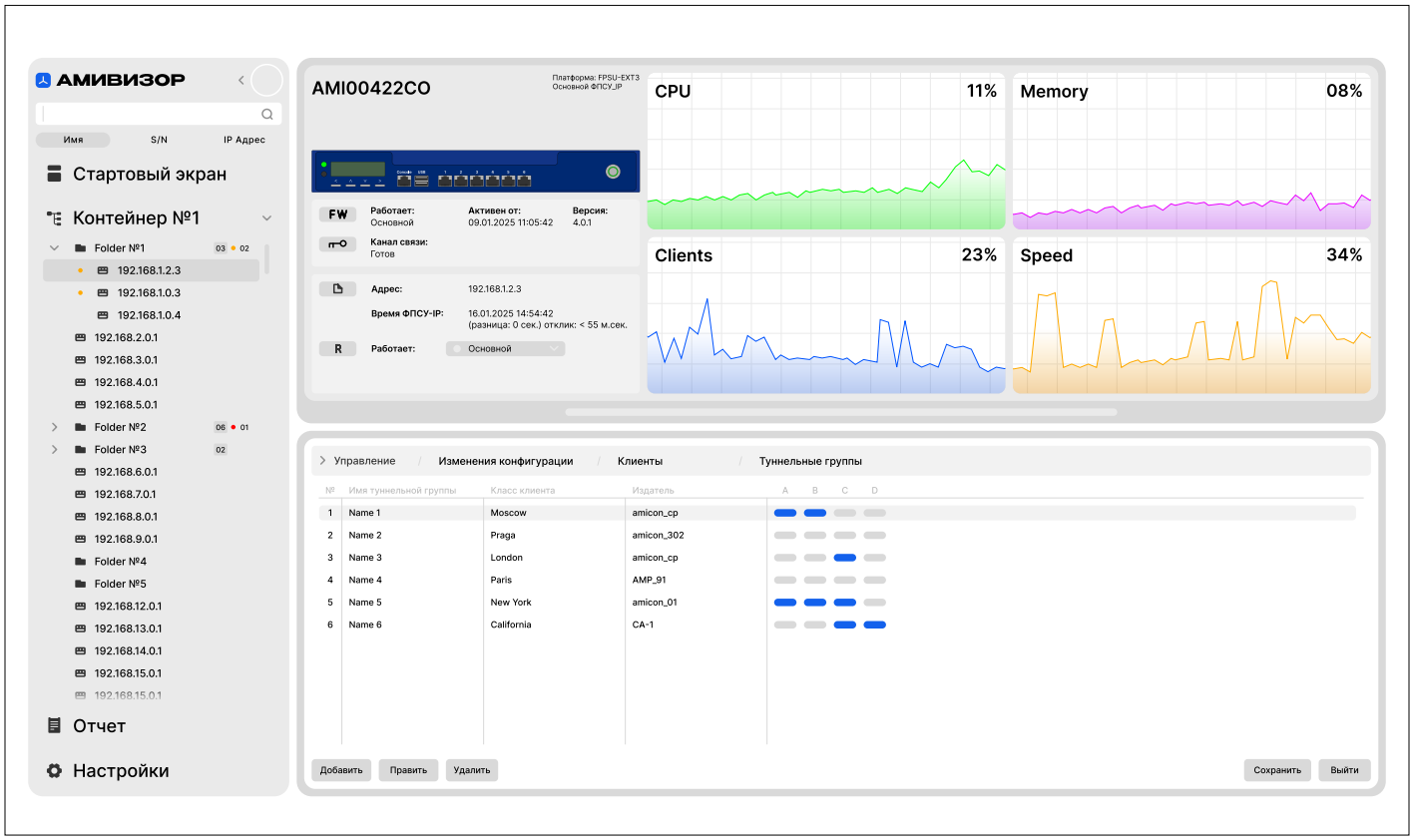


Рисунок 2. АМИВИЗОР

АМИКОННЕКТ создан для организации защищённого доступа сотрудников к корпоративным ресурсам, исключая риски перехвата и несанкционированного доступа к данным. Основой решения является PKI-инфраструктура и сертифицированные аппаратные средства ФПСУ, что гарантирует максимальный уровень защиты.

Ключевые преимущества продукта АМИКОННЕКТ:

- *импортозамещение Cisco AnyConnect — полная функциональная альтернатива с поддержкой российских криптоалгоритмов;*
- *простая интеграция — легко встраивается в существующую PKI-инфраструктуру;*
- *поддержка широкого спектра операционных систем — Windows, Linux, macOS, а также мобильных платформ (Android и iOS);*
- *двусторонняя и двухфакторная аутентификация — строгая взаимная проверка клиента и сервера через PKI-сертификаты;*
- *отказоустойчивость и масштабируемость — поддержка кластеризации и резервирования шлюзов VPN;*
- *комплаенс проверка клиентского АРМ на соответствие политикам ИБ — при интеграции с решениями технологических партнёров.*

Не только конечные пользователи ранее сталкивались с необходимостью иметь глубокие познания в сетевых технологиях и ИБ, но и ИТ-службы, занимающиеся эксплуатацией средств защиты информации. В нашем новом продукте АМИВИЗОР мы также реализовали интуитивно понятный интерфейс. Он ориентирован на ИТ-специалиста первой-второй линии техподдержки, который обладает стандартной квалификацией без глубоких знаний в области криптографии. В АМИВИЗОР используются все те стабильные и высоконадёжные технологии, которые были ранее заложены в наших продуктах семейства ФПСУ. Нам удалось обернуть надёжность и производительность наших классических продуктов в красивую и понятную упаковку. С её помощью даже непрофильный специалист может отслеживать, администрировать и обслуживать все комплексы удалённого доступа организации (рис. 2).

* * *

Наша стратегия в упрощении интерфейсов средств защиты информации и ориентации на эксплуатацию этих средств ранее не подготовленными администраторами дала свои результаты. Сейчас мы уже заканчиваем приёмо-сдаточные испытания в крупном банке. Десятки тысяч пользователей удалённого доступа уже получили удобный инструмент для комфортной работы вне офиса. Наша компания продолжает развивать продукты в сторону простоты использования и управления. Мы уверены, что интуитивно понятные и простые в использовании решения позволяют нашим клиентам сосредоточиться на их основном бизнесе, не отвлекаясь на сложные технические задачи. А это значит, что безопасность перестаёт быть проблемой и становится вашим конкурентным преимуществом.

Амикон

Российские VPN решения с ГОСТ шифрованием

180 Гбит/с
В режиме L2VPN

200 Гбит/с
В режиме МСЭ

Экосистема продуктов ФПСУ:

- NGFW 
- IDS/IPS 
- Quant 
- Амиконнект 
- VPN Site to Site 
- VPN Клиент 
- SDK/API 
- Система управления 

Операционные системы:

SberOS · Linux · РЕД ОС М · Аврора · Android · MacOS · Win · iOS

sales@amicon.ru

amicon.ru

КВАРТАЛЬНЫЙ ОТЧЁТ

НОРМАТИВНОЕ РЕГУЛИРОВАНИЕ В СФЕРЕ ИБ ВО II КВАРТАЛЕ 2025 ГОДА

Екатерина РАЧКОВА
обозреватель BIS Journal

ПЕРСОНАЛЬНЫЕ ДАННЫЕ (ПДн)

18.03.2025 опубликован приказ Минцифры России от 06.03.2025 № 150 «Об утверждении доклада о правоприменительной практике организации и осуществления федерального государственного контроля (надзора) в сфере идентификации и (или) аутентификации в 2024 году». В докладе рассматриваются вопросы идентификации и аутентификации с использованием биометрических персональных данных.

27.03.2025 опубликован проект приказа Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)»Об утверждении требований к обезличиванию персональных данных и методов обезличивания персональных данных». В числе прочего проект нормативного акта устанавливает следующие положения:

- оператор ПДн при обезличивании должен гарантировать, что после этого данные не могут быть восстановлены без дополнительной информации;
- оператор обязан использовать системы, обеспечивающие безопасность таких ПДн;
- запрещено совместное хранение исходных и обезличенных ПДн;
- все действия по обезличиванию ПДн должны фиксироваться и иметь возможность подтверждения;
- в качестве основных методов обезличивания ПДн выделяются введение идентификаторов с переменным значением, семантическое изменение состава данных, их искажение, перемешивание или удаление.

14.04.2025 опубликованы проекты постановлений Правительства Российской Федерации «О порядке формирования составов персональных данных, полученных в результате обезличивания персональных данных, сгруппированных по определённому признаку, при условии, что последующая обработка таких данных не позволит определить принадлежность таких данных конкретному субъекту персональных данных, и порядке предоставления доступа к составам таких данных» и «Об установлении требований к обезличиванию персональных данных, методов и правил обезличивания персональных данных».

28.04.2025 опубликовано постановление Правительства Российской Федерации от 24.04.2025 № 538 «Об утверждении перечня случаев формирования составов персональных данных, полученных в результате обезличивания персональных данных, сгруппированных по определённому признаку, при условии, что последующая обработка таких данных не позволит определить принадлежность таких данных конкретному субъекту персональных данных». При возникновении чрезвычайной ситуации, для противодействия терроризму, при введении чрезвычайного положения и карантина, а также при проведении исследований в сфере туризма, в экономической и социальной сферах для реализации миграционной политики и прогнозирования санитарно-эпидемиологической обстановки Минцифры России сможет формировать составы обезличенных ПДн, если последующая обработка таких данных не позволит определить их принадлежность. Постановление вступает в силу с 01.09.2025.

07.05.2025 опубликован проект приказа ФСБ России, СВР России, Министерства обороны Российской Федерации, ФСО России, МВД России «Об установлении Порядка предоставления доступа к информационным системам и (или) базам данных, содержащим сведения о лицах, указанных в частях 11 и 12 статьи 6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», обработки содержащихся в них персональных данных указанных лиц и формы предписания о предоставлении доступа к информационным системам и (или) базам данных, содержащим сведения о лицах, указанных в частях 11 и 12 статьи 6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»« (подготовлен ФСБ России). Проект устанавливает порядок предоставления доступа к информационным системам и (или) базам данных, содержащим сведения о лицах, указанных в отдельных частях статьи 6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», а также определяет форму предписания для предоставления такого доступа. Предполагается, что документ вступит в силу 01.07.2025.

12.05.2025 опубликован проект приказа «О внесении изменений в Порядок обработки, включая сбор, хранение, биометрических персональных данных, в том числе требования к параметрам биометрических персональных данных, и в Порядок размещения и обновления биометрических персональных данных в единой биометрической системе, а также случаи и сроки использования биометрических персональных данных при их размещении в единой биометрической системе в соответствии с частью 14 статьи 4 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», утверждённые приказом Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 12.05.2023 № 453». Документ вносит изменения в порядок сбора и хранения биометрических персональных данных граждан (изображение лица и запись голоса) в единой биометрической системе, а также требования к их параметрам. Необходимость изменений связана с улучшением качества техники для сбора и распознавания данных, а также с тем, что отдельные из них не соответствуют современным нормативам.

28.05.2025 опубликовано постановление Правительства Российской Федерации от 22.05.2025 № 702 «Об утверждении Правил проверки соответствия пользователей государственной информационной системы, определённой в соответствии с частью 2 статьи 13–1 Федерального закона «О персональных данных», требованиям, указанным в части 7 статьи 13–1 Федерального закона «О персональных данных»«. Постановление вступает в силу 01.09.2025.

28.05.2025 в Государственную думу Российской Федерации был внесён законопроект № 928282–8 «О внесении изменения в статью 22 Федерального закона «О персональных данных»«. В рамках данной инициативы предлагается изменить подход к раскрытию данных об операторах ПДн. В частности, если оператором ПДн выступает физическое лицо или индивидуальный предприниматель, его адрес не будет размещаться в открытой части реестра операторов ПДн. Адрес по-прежнему нужно будет указывать в уведомлении, но он будет доступен только уполномоченному органу.

11.06.2025 опубликован проект Федерального закона «О внесении изменений в статью 13 Федерального закона «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»». Законопроектом предусматривается изменение действующего порядка применения биометрических персональных данных при проходе на отдельные территории государственных органов и организаций посредством использования информационных систем, обеспечивающих функционирование контрольно-пропускных пунктов.

КРИТИЧЕСКАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА (КИИ)

04.04.2025 опубликовано информационное сообщение ФСТЭК России от 12.03.2025 № 240/82/672 «О порядке представления субъектами критической информационной инфраструктуры сведений о результатах присвоения объектам критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий». В сообщении указано, какими структурами ФСТЭК осуществляется рассмотрение подаваемых сведений в зависимости от категории субъекта КИИ.

07.04.2025 опубликован Федеральный закон от 07.04.2025 № 58-ФЗ «О внесении изменений в Федеральный закон „О безопасности критической информационной инфраструктуры Российской Федерации“». Закон уточняет порядок перевода критической информационной инфраструктуры на отечественное ПО. Правительство Российской Федерации устанавливает требования к системам, базам данных и радиоэлектронному оборудованию, а также порядок и сроки перехода КИИ на российское ПО. Субъекты КИИ из состава финансовых организаций должны согласовать этот процесс с Банком России. В каждой отрасли будут определены типы информационных систем, которые нужно будет относить к значимым объектам КИИ. Закон вступает в силу с 01.09.2025.

Также 07.04.2025 опубликован Указ Президента Российской Федерации от 07.04.2025 № 214 «О внесении изменения в Указ Президента Российской Федерации от 30 марта 2022 г. № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации»«. С 01.01.2025 из запрета органам государственной власти и заказчикам использовать иностранное ПО на принадлежащих им значимых объектах КИИ может быть сделано исключение, если оно установлено федеральным законом. Указ вступает в силу со дня подписания.

14.04.2025 опубликованы методические рекомендации № АШ-7089вн, регламентирующие с учётом установленных перечней типовых отраслевых объектов КИИ, функционирующих в сфере связи, особенности категорирования объектов КИИ и присвоения им категории значимости. Данные рекомендации разработаны Минцифры России совместно с ФСТЭК России, Ассоциацией документальной электросвязи и отдельными представителями операторов связи. В документе приводится детальное описание этапов проведения категорирования объектов КИИ.

19.05.2025 опубликован проект постановления Правительства Российской Федерации «Об утверждении отраслевых особенностей категорирования объектов критической информационной инфраструктуры в сфере связи». В документе изложены особенности категорирования объектов КИИ в сфере связи и определяется порядок установления соответствия объекта КИИ критериям значимости и показателям их значений в целях присвоения ему одной из категорий значимости.

04.06.2025 опубликован проект постановления Правительства Российской Федерации «Об утверждении Перечней типовых отраслевых объектов критической информационной инфраструктуры». Перечни сформированы для 14 отраслей, включая банковскую и иные сферы финансового рынка. Документ предполагает вступление в силу с 01.09.2025.

10.06.2025 опубликован проект постановления Правительства Российской Федерации «О внесении изменений в постановление Правительства Российской

Федерации от 08.02.2018 № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений». Согласно проекту, категорированию будут подлежать объекты критической информационной инфраструктуры, соответствующие типам информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, которые включены в перечни типовых отраслевых объектов критической информационной инфраструктуры. Также указывается, как устанавливать соответствие объекта критической информационной инфраструктуры критериям значимости и показателям их значений, рассчитывать значения показателей критериев значимости с учётом особенностей функционирования объекта и присваивать ему одну из категорий значимости либо принимать решение об отсутствии необходимости присвоения такой категории.

ПРЕЗИДЕНТ И ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

01.04.2025 опубликован Федеральный закон от 01.04.2025 № 41-ФЗ «О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации».

В рамках борьбы с телефонным мошенничеством законом устанавливается:

- самозапрет на заключение договоров об оказании услуг связи без личного присутствия;
- запрет на передачу SIM-карт третьим лицам (кроме близких родственников);
- самозапрет на спам-обзвоны и рассылки;
- обязательная маркировка всех исходящих телефонных вызовов от организаций;
- запрет сотрудникам госорганов, банков, операторов связи, цифровых экосистем общаться с гражданами и клиентами через иностранные мессенджеры.

Закон вступает в силу с 01.06.2025, за исключением отдельных положений.

21.04.2025 был опубликован Федеральный закон от 21.04.2025 № 94-ФЗ «О внесении изменений в Федеральный закон «Об электронной подписи»«. Изменения связаны с определением порядка создания и выдачи квалифицированных сертификатов ключа проверки электронной подписи для госорганов, сведения о которых не включены в ЕГРЮЛ.

16.05.2025 опубликован проект Федерального закона «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации». Законопроект предполагает, что поставщики облачных услуг по предоставлению программного обеспечения и (или) по предоставлению вычислительных ресурсов (ЦОД) на платформе «ГосТех» должны будут обеспечивать соответствие предоставляемой информационно-телекоммуникационной инфраструктуры и (или) программного обеспечения требованиям, предъявляемым к защите информации и обеспечению безопасности критической информационной инфраструктуры Российской Федерации.

22.05.2025 опубликован Федеральный закон от 23.05.2025 № 104-ФЗ «О внесении изменений в статьи 4.5 и 13.12 Кодекса Российской Федерации об административных правонарушениях и статью 1 Федерального закона «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях»«. Изменения предусматривают увеличение штрафов за нарушение требований по использованию несертифицированных СЗИ (в т.ч. сертифицированных).

МИНЦИФРЫ РОССИИ

05.06.2025 опубликован проект ведомственного акта Минцифры России «Об утверждении Требований к обеспечению информационной безопасности в рамках предоставления облачных услуг посредством государственной единой облачной платформы».

ФСБ РОССИИ

26.03.2025 Федеральная служба безопасности Российской Федерации опубликовала приказ от 18.03.2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, с использованием шифровальных (криптографических) средств». Ранее действовавший Приказ ФСБ России от 24.10.2022 № 524, соответственно, утратил силу.

09.04.2025 опубликован проект постановления Правительства Российской Федерации «О внесении изменений в постановление Правительства Российской Федерации от 10.03.2000 № 214». Проектом предлагается внести изменения в Положение о ввозе в Российскую Федерацию и вывозе из Российской Федерации специальных технических средств, предназначенных для негласного получения информации, и список видов специальных технических средств, предназначенных для негласного получения информации, ввоз и вывоз которых подлежат лицензированию.

ФСТЭК РОССИИ

25.04.2025 ФСТЭК России были опубликованы проекты следующих ведомственных актов:

- Приказ ФСТЭК России «О внесении изменений в форму направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости ему одной из таких категорий, утверждённую приказом ФСТЭК России от 22.12.2017 № 236».
- Приказ ФСТЭК России «О внесении изменений в Порядок ведения реестра значимых объектов критической информационной инфраструктуры Российской

Федерации, утверждённый приказом ФСТЭК России от 06.12.2017 № 227».

05.06.2025 опубликован проект приказа ФСТЭК России «О внесении изменений в Порядок сертификации процессов безопасной разработки программного обеспечения средств защиты информации, утверждённый приказом ФСТЭК России от 01.12.2023 № 240».

17.06.2025 опубликован приказ ФСТЭК России от 11.04.2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений». Приказ вступает в силу с 01.03.2026 взамен приказа ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах». Предусматривается, что аттестаты соответствия на государственные информационные системы и иные информационные системы, выданные до дня вступления в силу настоящего приказа, то есть до 01.03.2026, считаются действительными. В числе нововведений документа:

- Изменены и приведены в соответствие с приказом ФСБ России от 18.03.2025 № 117 правила определения масштаба информационной системы.
- Защита информационных систем, являющихся значимыми объектами КИИ, должна обеспечиваться в соответствии не только с требованиями Федерального закона № 187-ФЗ «О безопасности КИИ», но и с требованиями нового приказа.
- От оператора требуется разработать и утвердить политику ИБ, а также внутренние стандарты и регламенты по защите информации, связанные с особенностями деятельности оператора и функционирования ИС.
- Переработан базовый набор мер защиты информации.
- Изменены требования к периодической оценке показателей защищённости и уровня зрелости.
- Информационные системы, взаимодействующие с сетью «Интернет», должны проходить мероприятия по мониторингу ИБ в соответствии с ГОСТ Р 59547–2021 (раздел 5).
- Описана возможность использования искусственного интеллекта в рамках обеспечения защиты информации.
- Указана необходимость обеспечивать реализацию мер разработке ПО в соответствии с ГОСТ Р 56939–2024.
- Определён порядок проведения разработки и тестирования ПО подрядными организациями. В частности, работники подрядных организаций не смогут проводить разработку (развитие) и (или) тестирование программного обеспечения непосредственно в эксплуатируемых ИС.
- Указано, что для организации и управления деятельностью по обеспечению ИБ необходимо иметь структурное подразделение или специалистов по защите информации (30 % специалистов должны иметь профильное образование или пройти переподготовку).

ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ

18.03.2025 опубликовано Положение Банка России от 30.01.2025 № 851-П «Об установлении обязательных для кредитных организаций, иностранных банков, осуществляющих деятельность на территории Российской Федерации через свои филиалы, требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента». Положение вступило в силу через 10 дней со дня опубликования (за исключением отдельных пунктов, сроки по которым отложены), Положение Банка России № 683-П, соответственно, утрачивает силу.

15.04.2025 Банком России опубликован проект указания «О внесении изменений в Положение Банка России от 15 ноября 2021 года № 779-П». Для некредитных финансовых организаций предлагается скорректировать требования к операционной надёжности, распространить их в т.ч. на микрофинансовые организации. Для них установят перечень технологических процессов и порогового уровня допустимого времени простоя и деградации соответствующих технологических процессов. Будут введены сигнальные и контрольные значения показателей операционной надёжности, уточнены случаи информирования Банка России о выявленных событиях операционного риска, связанных с нарушением операционной надёжности.

16.05.2025 Банком России опубликован обзор отчётности об инцидентах информационной безопасности при переводе денежных средств за I квартал 2025 года.

22.05.2025 Банком России опубликован Проект указания Банка России «О внесении изменений в Положение Банка России от 20 апреля 2021 года № 757-П». Проект предполагает установление дополнительных требований по защите информации для некредитных финансовых организаций:

- изменение критериев определения уровня защиты информации по ГОСТ Р 57580.1–2017 для отдельных некредитных финансовых организаций;
- распространение минимального уровня защиты информации по ГОСТ Р 57580.1–2017 на микрофинансовые организации, операторов инвестиционной платформы;
- определение обязанности по реализации наиболее высокого из требуемых нормативными актами Банка России уровней защиты информации, в случае если в отношении объектов информационной инфраструктуры некредитной финансовой организации действуют требования, установленные на основании статьи 57.4 Федерального закона № 86-ФЗ, части 3 статьи 27 Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платёжной системе», и некредитная финансовая организация применяет единый контур безопасности в соответствии с пунктом 6.7 раздела 6 ГОСТ Р 57580.1;
- установление сроков предоставления сведений об инцидентах некредитными финансовыми организациями в Банк России;

- установление требований к расчёту значений показателей оценки выполнения требований к мерам защиты информации в отношении технологии безопасной обработки защищаемой информации и оценки выполнения требований к мерам защиты информации в отношении прикладного программного обеспечения автоматизированных систем и приложений;
- приведение термина «получатель финансовых услуг» в соответствие с изменениями в Федеральный закон от 20.07.2020 № 211-ФЗ «О совершении финансовых сделок с использованием финансовой платформы» (в ред. Федерального закона от 11.03.2024 № 45-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации»);
- установление требования об осуществлении деятельности по планированию, реализации, контролю и совершенствованию мер и мероприятий, направленных на реализацию требований, применяемых в отношении прикладного программного обеспечения автоматизированных систем и приложений и в отношении технологии обработки защищаемой информации;
- определение права некредитных финансовых организаций на реализацию процессов разработки программного обеспечения и приложений, включающих меры обеспечения безопасного жизненного цикла разработки программного обеспечения и приложений;
- уточнение требований по использованию электронной подписи и средств криптографической защиты информации;
- установление требований по регистрации информации о действиях клиентов при приёме электронных со-

общений к исполнению в автоматизированных системах и приложениях с использованием информационно-телекоммуникационной сети «Интернет».

ОТРАСЛЕВЫЕ ДОКУМЕНТЫ

11.03.2025 приняты национальные стандарты, вступающие в силу 31.03.2025:

- ГОСТ Р 59453.3–2025 «Защита информации. Формальная модель управления доступом. Часть 3. Рекомендации по разработке»;
- ГОСТ Р 59453.4–2025 «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».

24.03.2025 опубликованы национальные стандарты:

- ГОСТ Р 59453.3–2025 «Защита информации. Формальная модель управления доступом. Часть 3. Рекомендации по разработке». Стандарт устанавливает рекомендации по разработке и описанию формальных моделей управления доступом, на основе которых разрабатываются средства защиты информации, реализующие политики управления доступом;
- ГОСТ Р 59453.4–2025 «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». Стандарт устанавливает рекомендации по верификации средств защиты информации, реализующих политики управления доступом, на основе формализованного описания модели управления доступом.

Оба стандарта вступили в силу 31.03.2025.

26.03.2025 опубликован национальный стандарт ГОСТ Р 71998–2025 «Информационные технологии. Требования и оценка качества систем и программного обеспечения. Определение качества ИТ-услуг». Стандарт вступает в силу 30.06.2025.

02.06.2025 опубликован ГОСТ Р 70262.2–2025 «Защита информации. Идентификация и аутентификация. Уровни доверия аутентификации». Стандарт вступает в силу 01.10.2025.

10.06.2025 принят стандарт ГОСТ Р 72118–2025 «Защита информации. Системы с конструктивной информационной безопасностью. Методология разработки». Стандарт устанавливает требования и рекомендации для методологии разработки информационных систем (ИС), обеспечивающие реализацию конструктивных подходов к информационной безопасности. Описывает методологию разработки ИС, которая включает процессы планирования, анализа, проектирования, реализации, тестирования и сопровождения систем. Особое внимание уделяется синхронизации требований безопасности с основным функционалом системы. Вступает в силу 01.12.2025.

ШАГИ В БУДУЩЕЕ

ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ ИИ И МО ДЛЯ РЕШЕНИЯ ЗАДАЧ В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ

Александр ПУХА
директор Департамента информационной безопасности АМТ-ГРУП

Александр ГРОСУЛ
инженер ДИБ АМТ-ГРУП

Применение технологий искусственного интеллекта (ИИ) и машинного обучения (МО) в информационной безопасности (ИБ) резко возросло в последние годы, хотя их практическое использование началось значительно раньше. Так, ещё в 1980–1990-х началась разработка методов обнаружения угроз с использованием МО. Первые системы, такие как выпущенная в 1998 году Snort, применяли сигнатурный анализ по заданным правилам и статистические методы для выявления аномалий в поведении пользователей и сетевых узлов. С 2000-х алгоритмы машинного обучения, обрабатывая растущие объёмы данных, совершенствовали анализ трафика и обнаружение аномалий. К концу десятилетия методы контролируемого обучения повысили точность детектирования угроз, а неконтролируемого – позволили выявлять новые атаки через аномальные паттерны.

Развитие методов глубокого обучения и обработки естественного языка (NLP) было новым прорывом в 2010-х, позволив эффективно обрабатывать большие объёмы данных (БОД) и находя сложные взаимосвязи. Обработка естественного языка повысила возможности анализа текстовых данных, включая развитие способов выявления атак методами социальной инженерии. Последний виток развития методов привнесли алгоритмы генеративного ИИ, способного создавать новый контент на основе имеющихся данных, открывая дополнительные возможности для совершенствования моделей обнаружения угроз.

КЛЮЧЕВЫЕ НАПРАВЛЕНИЯ

Сейчас системы на основе ИИ и МО активно внедряются для борьбы с развивающимися угрозами, позволяя анализировать БОД, находить аномалии и даже прогнозировать кибератаки. Рассмотрим ключевые направления их применения.

- Обнаружение вредоносного ПО: алгоритмы МО производят анализ файлов и сетевого трафика, классификацию на основе поведения. Модели обучаются на БОД с уже известными образцами. Существуют методы статического анализа – изучение кода и структуры файлов и динамический анализ – мониторинг поведения в реальном времени (например, LSTM для системных вызовов). Применяется в EDR/XDR-решениях.
- Выявление аномалий и предотвращение атак: методы выявления аномалий и предотвращения атак анализируют сетевой трафик, логи и поведение пользователей, обнаруживая подозрительную активность. Модели обучаются на исторических данных для распознавания шаблонов атак. Технологии включают графовые нейросети (GNN) для анализа связей в сети, автоэнкодеры для выявления отклонений в поведении и алгоритмы Isolation Forest для обнаружения редких аномалий. Эти подходы активно применяются в системах UEBA и XDR.
- Борьба с фишингом и спамом: алгоритмы МО анализируют содержимое писем, URL-адреса и даже голосовые сообщения, выявляя фишинговые атаки и спам. Для распознавания поддельных логотипов и скриншотов применяются технологии компьютерного зрения, методы обработки естественного языка позволяют эффективно проводить семантический анализ текста писем. Подобные методы внедрены во многих почтовых сервисах.
- Прогностическая аналитика угроз: ИИ анализирует БОД, OSINT, телеметрию и соцсети, выявляя тренды атак. Автоматизированная обработка данных с помощью МО обеспечивает проактивную защиту. Для прогнозирования используются LSTM-сети и NLP-методы для анализа открытых источников и darknet. Реализуется в Threat Intelligence и XDR-платформах.
- Автоматизация реагирования на инциденты: алгоритмы ИИ ускоряют обработку инцидентов, позволяя автоматизировать их классификацию и первичную обработку, предлагая оптимальные меры по реагированию. Для автоматической классификации инцидентов, в частности, применяются методы обработки естественного языка, в то же время методы глубинного обучения с подкреплением позволяют автоматизировать обработку инцидентов и реагирование. Развитие этих подходов активно ведётся в SOAR-решениях.

НОВЫЕ ВОЗМОЖНОСТИ

На первый взгляд может казаться, что ИИ и МО лишь автоматизируют привычные методы – анализ аномалий или поведенческую аналитику. Однако на деле они кардиналь-

но меняют подход к защите данных, предлагая принципиально новые возможности:

◆ Эффективное обнаружение новых угроз: традиционные методы (сигнатурный анализ, правила на основе IoC) малоэффективны против сложных атак, таких как APT или новые виды ransomware. В свою очередь, модели ИИ/МО позволяют выявлять многоэтапные атаки, прогнозировать угрозы, анализируя поведение и аномалии, обучаясь на исторических данных и выявляя скрытые паттерны.

◆ Глубина и масштабируемость анализа: модели ИИ позволяют обрабатывать БОД в реальном времени, автоматически адаптироваться к новым угрозам за счёт динамического обучения, анализировать контекст, строя связи между процессами, пользователями и устройствами (например, с применением графовых нейросетей GNN). В данном случае традиционные методы, опираясь на заранее заданные правила и шаблоны, менее эффективны и дают высокий уровень ложных срабатываний.

◆ Автоматизация и скорость реагирования: большой объём ручной работы аналитиков — узкое место традиционных систем. Алгоритмы ИИ/МО позволяют снизить нагрузку на специалистов, решая рутинные задачи, позволяют реализовать эффективное реагирование, обеспечивая действия в масштабе времени, близком к реальному, тогда как человеку требуются минуты или часы.

Таким образом, решения на базе ИИ и МО — не просто «улучшенная версия» старых методов, а новый этап развития решений кибербезопасности.

КЛАССИКА ТОЖЕ В ПОЧЁТЕ

ИИ и МО расширяют возможности кибербезопасности, но классические методы защиты остаются актуальными:

◆ Против известных угроз: сигнатурный анализ и чёрные списки IP/DNS эффективны и экономичны.

◆ В регуляторных системах: требуются прозрачные методы, тогда как ИИ-решения могут быть «чёрным ящиком».

◆ В устаревших/изолированных системах: внедрение ИИ может нарушить работу из-за высокой нагрузки.

ВЫЗОВЫ И ОГРАНИЧЕНИЯ

Выбор между традиционными методами и ИИ/МО-решениями зависит от конкретных задач, ресурсов и уровня угроз. На практике наиболее эффективны комбинированные системы, где ИИ дополняет, а не заменяет традиционные методы — гибридный подход применяется в отдельных классах решений, например, EDR/XDR-платформах, TI. В то же время внедрение ИИ в системы безопасности, несмотря на все преимущества, сопряжено с рядом вызовов и ограничений.

◆ Технические ограничения: эффективность МО-моделей зависит от качества обучающих данных — узкие выборки приводят к «слепым зонам» для IoT и промышленных систем. Чрезмерная чувствительность вызывает ложные срабатывания на легитимные процессы, тогда как сложные атаки, маскирующиеся под нормальную активность, часто остаются незамеченными. Эти проблемы требуют постоянного совершенствования данных и алгоритмов анализа.

◆ Ресурсные ограничения: обучение сложных моделей (например, глубоких нейросетей) требует значительных вычислительных мощностей. Кроме того, отдельные ИИ-решения плохо совместимы с устаревшей инфраструктурой, внедрение может требовать модернизации.

◆ Уязвимости самих ИИ/МО-моделей: модели подвержены атакам, связанным со злонамеренным манипулированием входными данными (Adversarial Attacks). Это особенно опасно в системах компьютерного зрения и анализа поведения. Кроме того, при использовании облачных ИИ-сервисов возникает угроза компрометации конфиденциальной информации, передаваемой для анализа.

◆ Организационные риски: ошибки в работе ИИ-систем, например блокировка легитимных процессов или транзакций, могут приводить к нарушению производственных процессов, финансовому репутационному ущербу.

* * *

Но, несмотря на связанные риски и ограничения, ИИ и МО продолжают трансформировать подходы к обеспечению безопасности, предлагая инновационные методы борьбы с угрозами. ИИ и МО становятся неотъемлемой частью продуктов для обеспечения кибербезопасности, повышая точность и скорость обнаружения угроз, прогнозирования и автоматизации процессов. В ближайшем будущем ожидается появление автономных систем защиты, предиктивной аналитики угроз и когнитивных систем, способных анализировать контекст. Однако их успешное внедрение потребует решения проблем прозрачности моделей, устойчивости к adversarial-атакам и баланса автоматизации с человеческим контролем.

ЗАЩИТА НА МАКСИМУМ

ВЕБ-БРАУЗЕР КАК НЕВИДИМЫЙ ФРОНТ КИБЕРБЕЗОПАСНОСТИ

Валерий ЛЕДОВСКОЙ
директор по развитию ARinteg

Веб-браузер — универсальный шлюз ко всему: от внутренних систем ДБО ЭДО до портала Госуслуг, облачных CRM и корпоративной почты. И эта роль делает его главной мишенью для кибератак. Браузер превратился в невидимый фронт кибербезопасности, где угрозы часто остаются незамеченными до момента самого инцидента.

СИТУАЦИЯ

Парадокс: при почти 100% зависимости бизнеса и госсектора от браузеров централизованное управление ими — редкость. Мало где служба ИБ системно контролирует версии, расширения, плагины и настройки браузеров на всех рабочих местах через групповые политики (GPO) или системы управления мобильными устройствами (MDM). Во многих компаниях царит надежда на «встроенные механизмы защиты» и осторожность пользователей. Увы, реальность жестока: фишинг, уязвимости в расширениях, утечки через кеш и куки, атаки, связанные со скачиванием файлов без ведома пользователя, — всё это риски, против которых «надежды» бессильны.

Браузер — наиболее массово используемое клиентское ПО. Оставлять его без контроля — всё равно что строить неприступную крепость, забыв запереть главные ворота.

В этой статье поделюсь, какие инструменты позволяют вывести этот фронт из невидимой зоны в фокус стратегии ИБ.

Обеспечение безопасности браузера требует многослойной стратегии. Технические меры, такие как принудительное шифрование, регулярные обновления, блокировка опасных ресурсов, должны быть усилены интеграцией с системами защиты на разных уровнях.

Критически важны решения, обеспечивающие прозрачность содержимого запароленных архивов для DLP-контроля, инструменты автоматизации учёта персональных данных через веб-интерфейсы и ПО для корректного учёта угроз (в том числе относящихся к браузерам) в моделях ФСТЭК, а также системы мониторинга, способные выявлять сложные атаки за счёт анализа и корреляции событий не только в самом браузере, но и во всей инфраструктуре защиты.

УПРАВЛЕНИЕ ЧЕРЕЗ ГРУППОВЫЕ ПОЛИТИКИ

Управление веб-браузерами на рабочих местах — практическая необходимость, поскольку это основной шлюз для передачи данных, включая конфиденциальные. Технические средства для такого контроля:

- групповые политики в среде Windows;
- системы управления мобильными устройствами;
- готовые шаблоны конфигурации для браузеров Firefox, Яндекс Браузер и др.

В экосистеме российских операционных систем, таких как Astra Linux или РЕД ОС, аналогичные задачи решаются через централизованные конфигурационные менеджеры или встроенные инструменты администрирования.

Эти механизмы дают возможность принудительно обновлять версии программного обеспечения, блокируя эксплуатацию известных уязвимостей, запрещать установку непроверенных расширений, настраивать критически важные параметры безопасности.

Интеграция этих механизмов с системами предотвращения утечек данных и вторжений позволяет отслеживать подозрительную активность в реальном времени, например попытки перехода на фишинговые ресурсы или запуск неавторизованных плагинов.

Но реальность российского ИБ-ландшафта такова, что за пределами крупных финансовых организаций или государственных структур с мощными ИБ-подразделениями эти возможности чаще всего остаются на бумаге. Браузеры обновляются хаотично, пользователи по своему усмотрению устанавливают расширения сомнительного происхождения, а базовые настройки безопасности редко когда выходят за рамки установленных по умолчанию.

Эта бессистемность превращает браузер в эффективный канал для потенциальных утечек, особенно при активном использовании облачных сервисов.

ТИПИЧНЫЙ СЦЕНАРИЙ

Сотрудник, желая «защитить» отправляемые через веб-интерфейс облака файлы с персональными данными клиентов или финансовой отчётностью, упаковывает их в запароленный архив. Он искренне верит,

что пароль будет достаточной защитой. Но здесь возникает критическая брешь в безопасности, так как большинство систем предотвращения утечек данных физически не могут заглянуть внутрь запароленного архива, чтобы проверить его на соответствие политикам компании. И конфиденциальная информация покидает периметр организации, оставаясь необнаруженной.

Предотвратить утечку конфиденциальной информации в запароленных архивах позволяет интеграция архиватора ARZip[1] от ARinteg с DLP-системой, при которой последняя получает возможность автоматически контролировать запароленные архивы. При этом архиватор ARZip становится единственным корпоративным архиватором компании.

Ключевая ценность архиватора ARZip в данном контексте — не просто создание архивов, а организация безопасного процесса работы с конфиденциальными данными при их передаче через браузер. ARZip позволяет пользователю легко запаролить чувствительные файлы перед загрузкой в облако. Но важным является его способность интегрироваться с DLP-системой. Эта интеграция позволяет DLP выполнить анализ содержимого запароленных файлов ещё до момента их отправки во внешнюю среду.

В результате служба информационной безопасности получает действенный инструмент для контроля соответствия архивируемых данных внутренним политикам и требованиям регуляторов, предотвращая попытки скрытой упаковки и передачи конфиденциальной информации под видом «безопасного» архива, а также ведения необходимого журнала аудита всех операций шифрования и передачи.

ARZip эффективно закрывает опасную лазейку, возникающую между удобством отправки данных через привычный браузер и жёсткими требованиями к безопасности информации. Без подобного решения запароленные архивы, отправляемые через веб-интерфейс облаков, остаются непрозрачным «чёрным ящиком» для DLP, а сам браузер невольно становится легализованным каналом для скрытых утечек.

РОЛЬ В ПРОЦЕССАХ ОБРАБОТКИ ПДН

Веб-браузер — ключевой канал обработки персональных данных в финансах, госсекторе и ретейле. Каждое действие сотрудника в CRM или на госпортале через браузер — обработка ПДн, регулируемая 152-ФЗ. Браузер передаёт метаданные, хранит идентификационные куки, сохраняет кеш с конфиденциальными фрагментами, что создаёт скрытые риски, которые в случае их реализации чреваты крупными штрафами и не только.

Закон требует вести детальный реестр процессов обработки ПДн. Необходимы актуальные политики конфиденциальности, юридически корректные механизмы получения/учёта согласий (включая куки), ОРД, регламентирующие безопасную работу с ПДн через браузер (очистка кеша, сессий). Организовать эту работу в управляемый, законный процесс позволяет модуль «Учёт персональных данных» от ARinteg, с которым легко автоматизировать документооборот в рамках 152-ФЗ.

ПРОГНОЗ

Значимость браузера как рабочей среды и вектора угроз будет только возрастать. Фокус сместится на такие решения, как Яндекс.Браузер с поддержкой ГОСТ-шифрования для финансов и коммерции, Mozilla Firefox как стандарт для защищённых сред на базе отечественных ОС (Astra Linux, РЕД ОС) в госсекторе и КИИ. Ужесточение требований регуляторов (ФСТЭК, Роскомнадзор, Банк России) к защите ПДн и критической инфраструктуры сделает внедрение комплексных мер управления и мониторинга браузеров не рекомендацией, а обязательным условием выживания бизнеса.

Опыт свидетельствует: превратить браузер из слабого звена в управляемый компонент безопасности нельзя разовым действием. Это непрерывный процесс, требующий продуманного сочетания технологий, регламентов и контроля. Организации, которые уже сегодня выстраивают эту систему, инвестируя в управление, глубокий мониторинг и интеграцию защитных механизмов, создают не просто барьеры от угроз — они формируют устойчивую среду, где самый распространённый инструмент сотрудника становится надёжным элементом защищённого цифрового периметра.

[1] «Как ARZip помогает исключить утечки данных в запароленных архивах», BIS Journal №2/2025

КАК РАБОТАЕТ ПОДХОД ZERO TRUST В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Артём ТУРЕНОК
руководитель отдела технических решений АО «ДиалогНаука»

Антон ПИЛИПЕНКО
руководитель продукта Xello Datacube

Рынок кибербезопасности меняется быстрее, чем бизнес успевает адаптироваться. Компании теряют контроль над данными, сотрудники работают из дома, а в инфраструктуре — десятки, а иногда и сотни точек входа. В этих условиях традиционная модель защиты только внешнего периметра больше не работает. Это подтверждают результаты пентестов: 96% организаций оказались[1] уязвимы к внешним атакам, а в 100% случаев сотрудники получали доступ к чувствительным данным.

КОГДА СВОИ — ЭТО НОВЫЕ ЧУЖИЕ

Когда сотрудник в корпоративной сети подвергается риску — будь то удалённый сотрудник или в офисе, все меры информационной безопасности отменяются. Устройства сотрудников — новая уязвимость для специалистов информационной безопасности. 85% ИТ-специалистов считают[2], что именно действия сотрудников становятся главной причиной инцидентов — осознанных или нет. Почти треть опрошенных подтверждает, что за последние два года количество таких случаев увеличилось и продолжает расти. Причём 52% респондентов отмечают, что сотрудники не умеют распознавать[3] фишинговые письма, и в этом корень множества атак.

Корпоративные устройства (в особенности личные, BYOD) являются неконтролируемой средой, которая может хранить конфиденциальные данные, подключаемые к критически важным приложениям. Естественным решением является установка агента (применение решений класса MDM/UMM/UEM) для управления конечными точками, который решает одну проблему, но создаёт другую. Не все сотрудники готовы устанавливать подобные решения на персональные устройства, агент управляет всем устройством.

Другим подходом для контроля устройств является виртуализация рабочих мест (VDI), которая позволяет использовать личные ноутбуки и компьютеры для работы. Но эта технология имеет высокую цену, как с точки зрения стоимости лицензирования, так и с точки зрения персонала, обслуживающего её. Для удалённых пользователей, работающих в сетях с далеко не идеальными характеристиками, использование DaaS (Desktop as a Service) может быть затруднительным.

Другой вопрос, который стоит перед ИТ- и ИБ-службами — это предоставление доступа к приложениям. Для этого всё ещё используются корпоративные VPN-решения, которые основываются на модели доверия: всё, что находится внутри сети, считается надёжным и защищённым. К сожалению, злоумышленники научились использовать уязвимости, присущие VPN, что делает эту технологию серьёзной угрозой безопасности для современного бизнеса. Технология VPN расширяет внутреннюю сеть на подключённые устройства, позволяя удалённым пользователям напрямую взаимодействовать с внутренними ресурсами (обеспечивает двунаправленную связь между конечными устройствами и внутренними серверами). Таким образом, она открывает злоумышленникам возможность исследовать, сканировать и перемещаться по внутренней сети после взлома VPN.

[1] https://ptsecurity.com/ru-ru/about/news/itogi-pentestov-ot-positive-technologies-96-organizaczij-uyazvimy-pered-kibermoshennikami

[2] https://rg.ru/2024/09/17/reg-szfo/vot-tak-fokus.html

[3] https://ptsecurity.com/ru-ru/research/analytics/kakimi-budut-fishingovye-ataki-v-blizhaishem-buduschem

НА ЧЁМ СТРОИТСЯ ПОДХОД «НУЛЕВОГО ДОВЕРИЯ»

Концепция Zero Trust («нулевое доверие») предлагает кардинально другой подход, в отличие от модели, основанной на периметре, и представляет собой принципиально новую архитектуру. Эта концепция позволяет отделить безопасность и подключение к вашей сети с помощью виртуализации или контейнеризации, которая обеспечивает безопасное подключение от любого пользователя к любому сервису на границе — без предоставления доступа ко всей сети. Таким образом, модель нулевого доверия позволяет избежать чрезмерных разрешений и неявного доверия, присущих традиционным моделям подключения объектов к сети. Детальный доступ к ИТ-ресурсам с наименьшими привилегиями обеспечивается с помощью контекстно-зависимых политик, которые оценивают риски и принимают соответствующие меры.

У Zero Trust-архитектуры есть три главных принципа.

Первый — минимизация площади атаки через прямое подключение к ИТ-ресурсам и приложениям, а не сетям. Такой подход снижает риски компрометации всей сети и горизонтального перемещения для злоумышленника при взломе конечного устройства.

Второй — отсутствие доверия к пользователям и устройствам, которые проходят аутентификацию и авторизацию. Последнее предполагает допуск только тех устройств, которые зарегистрированы в системе компании, соответствуют её требованиям безопасности и находятся под контролем ИТ-службы. Авторизованные пользователи имеют доступ только к определённым приложениям, а не ко всей сети. Сегментация обеспечивает гранулярный контроль доступа.

Третий — шифрование данных как при передаче, так и в состоянии покоя. Последнее обеспечивает безопасность данных и предотвращение их использования извне (если злоумышленник получил доступ к устройству).

Подход «от пользователя к приложению», который обеспечивает концепция Zero Trust, особенно актуален для гибридной работы и распределённой инфраструктуры, позволяя цифровым экосистемам работать без прямого подключения сервисов к интернету.

РЕАЛИЗАЦИЯ ZERO TRUST ЧЕРЕЗ ИЗОЛЯЦИЮ РАБОЧЕЙ СРЕДЫ НА КОНЕЧНОМ УСТРОЙСТВЕ

Для реализации ZTNA-архитектуры обычно используются различные решения. Для проверки личности — различные решения по идентификации и аутентификации пользователей, для проверки устройств и управления доступом — системы управления корпоративными устройствами и учётными записями. Все эти решения требуют разработки политик безопасности и архитектуры, соответствующих концепции «нулевого доверия».

Но что, если совместить всё это в одном решении? Платформа Xello Datacube позволяет реализовать подход Zero Trust, создавая изолированную защищённую среду для работы с корпоративной информацией на устройствах сотрудников. Эта среда разделяет операционную систему на рабочее и личное пространство. Все данные, полученные и созданные внутри защищённого рабочего пространства, остаются в нём в зашифрованном виде без возможности несанкционированного извлечения или кражи.

В отличие от виртуализации, которая требует дополнительных серверных мощностей, изоляция на уровне операционной системы не требует дополнительных ресурсов.

Весь доступ строго регламентирован: сотрудник работает только с теми ресурсами, которые ему разрешены, а все соединения внутри зашифрованы. Работа в рабочем пространстве с данными и ресурсами возможна только через одобренные приложения, которые выдаются прямо из веб-интерфейса Xello Datacube. Это упрощает контроль со стороны ИБ-отдела и снижает нагрузку на инфраструктуру — особенно в больших распределённых командах.

В 2024 году в России утекло более 1,5 млрд записей с персональными данными — на треть больше, чем годом ранее. С 30 мая 2025 года за подобные утечки компаниям грозят штрафы до 15 млн рублей, а при повторных нарушениях — до 3% от годовой выручки.

Zero Trust в платформенном исполнении становится ответом на эти вызовы: он объединяет все ключевые компоненты защиты в единую систему, отслеживает поведение пользователей, жёстко регулирует доступ и позволяет оперативно обновлять политики при изменении уровня риска.

ЗАКЛЮЧЕНИЕ

Пентесты, проведённые компанией Positive Technologies в 2023 году, подтверждают[4]: классических средств защиты недостаточно для борьбы с современными угрозами. В 63% протестированных систем организаций злоумышленник с минимальными знаниями смог проникнуть в локальную сеть. А в 64% случаев был получен доступ к критически важной информации — от интеллектуальной собственности до персональных данных компаний.

Внутренние пентесты выявили[5] ещё более тревожную картину: во многих компаниях злоумышленнику достаточно базовых технических навыков и доступа к открытым эксплойтам, чтобы получить полный контроль над ИТ-инфраструктурой. Это означает доступ ко всем системам, учётным записям, данным и возможностям: от кражи коммерческой информации до остановки бизнес-процессов и вымогательства.

Zero Trust — это про зрелость, осознанность и понимание рисков. В мире, где работа не привязана к офису, а ИТ-среда живёт в облаках, периметра больше не существует. Оставаться в старой логике — значит осознанно выбирать уязвимость.

---

[4] https://ptsecurity.com/ru-ru/about/news/itogi-pentestov-ot-positive-technologies-96-organizaczij-uyazvimy-pered-kibermoshennikami

[5] https://ptsecurity.com/ru-ru/about/news/itogi-pentestov-ot-positive-technologies-96-organizaczij-uyazvimy-pered-kibermoshennikami

ЗАКОНОПРОЕКТ № 404786-8 НЕ ЗА ГОРАМИ

ЧТО ЭТО ЗНАЧИТ ДЛЯ БАНКОВ?

Юрий ГОРЯЧЕВ
менеджер по продукту компании NGENIX

В настоящее время на рассмотрении в Госдуме находится законопроект № 404786-8, который сформирует нормативную базу для использования облачных сервисов в финансовом секторе. Согласно проекту, банки смогут работать с облаками без риска нарушения требований регуляторов, если провайдеры облачных решений будут соответствовать строгим стандартам безопасности. Разберём, что изменит принятие закона и какие подходы к защите в облаке оптимальны для банков сегодня.

ОБЛАКА ДЛЯ БАНКОВ: МЕЖДУ НЕОБХОДИМОСТЬЮ И ОПАСЕНИЯМИ

Высокая стоимость оборудования, сложности с обновлениями и дефицит кадров заставляют банки все чаще смотреть в сторону аутсорсинга и облачных сервисов. Вместе с тем большинство финансовых организаций все еще остерегаются передавать данные в облака.

Сейчас облачные провайдеры могут пройти аттестацию по ключевым стандартам безопасности (ГОСТ Р 57580, PCI DSS, ФСТЭК № 21). Однако это не снимает всех вопросов доверия. Причина в том, что на текущий момент рынок облачных услуг для финансового сектора находится в «серой зоне» с точки зрения законодательства.

Для регулятора пока не существует понятия «облака». В рекомендациях Банка России отсутствуют чёткие правила, какие данные и бизнес-процессы можно доверять облачным сервисам, а что может привести к нарушениям.

ПОЧЕМУ ПРОВАЙДЕРУ ВСЕ РАВНО НУЖНА АТТЕСТАЦИЯ?

Наличие аттестации — важный фактор, но далеко не единственный или решающий для банков. Без чёткой правовой базы многим финансовым организациям сложно принять окончательное решение о работе с облачными сервисами.

Тем не менее, в России облачные провайдеры, желающие предоставлять услуги на рынке, где аттестация является обязательной, должны соответствовать ключевым стандартам: ГОСТ Р 57580 (система защиты информации), PCI DSS (обработка платёжных данных) и ФСТЭК № 21 (защита персональных данных). Ежегодные проверки и пересертификации обеспечивают своевременное обновление и актуальность систем защиты.

Аттестация становится базовым уровнем доверия, необходимым для выхода провайдеров на рынок финансовых учреждений. Однако без чёткой правовой базы это ещё не гарантирует массового перехода к облакам.

ЗАКОНОПРОЕКТ № 404786-8: НОВАЯ ПРАВОВАЯ БАЗА ДЛЯ РЫНКА ОБЛАКОВ В ФИНАНСОВОМ СЕКТОРЕ

С учётом текущих барьеров в Госдуме рассматривается законопроект № 404786-8, который формирует чёткие правовые рамки для облачных провайдеров. Этот законопроект вводит понятие «оператор облачных вычислений» для финансового рынка и регулирует деятельность провайдеров. Главные положения законопроекта на момент написания этой статьи:

- регистрация облачных провайдеров в реестре Минцифры, подтверждающая соответствие требованиям безопасности;
- обязанность облачных сервисов соответствовать требованиям по защите данных, включая банковскую тайну и персональные данные;
- расширение полномочий Центробанка по контролю за киберустойчивостью облачных решений.

Таким образом государство и рынок делают шаг навстречу технологиям, создавая комфортные условия для финансовых организаций и провайдеров, тем самым стимулируя широкое внедрение и развитие облачных решений в банковской сфере.

А перед банками встаёт конкретная задача — выбрать оптимальные технические решения, способные обеспечить надёжную защиту веб-ресурсов от кибератак и сохранить масштабируемость и эффективность.

КАК ВЫБРАТЬ ОПТИМАЛЬНОЕ ОБЛАЧНОЕ РЕШЕНИЕ ДЛЯ ЗАЩИТЫ ОТ КИБЕРАТАК?

Мы в NGENIX выделяем три варианта (таблица 1):

1. On-Prem (собственная инфраструктура). Банк разворачивает защиту (WAF, анти-DDoS и т.д.) на собственных мощностях, например, в своём ЦОДе. Ключи шифрования и логи находятся под контролем банка.

Преимущества:

- Максимальный контроль и прозрачность — важно для аудита и регуляторов.
- Глубокая интеграция с внутренними ИТ-системами.

Недостатки:

- Высокие капитальные и операционные расходы.
- Ограниченная гибкость при резких всплесках нагрузки.
- Сложность оперативного масштабирования и обновления инфраструктуры.

Решение подходит крупным банкам с большим бюджетом и ресурсами, готовым инвестировать в резервирование и экспертизу, однако

не всегда является оптимальным с точки зрения гибкости и экономии.

2. PaaS без раскрытия SSL-сертификата. В этом варианте провайдеру облака не передают SSL-сертификат. Анализ трафика ведётся косвенно — на основе логов и метаданных, которые PaaS-провайдер получает от серверов оригинации веб-ресурса заказчика.

Преимущества:

- Не требует аттестации.
- Уменьшается риск раскрытия банковской тайны провайдеру.
- Быстрый старт использования облака без долгого согласования.

Недостатки:

- Низкая точность обнаружения угроз из-за отсутствия расшифровки трафика.
- Высокий процент ложноположительных срабатываний, что ведёт к неудобствам для пользователей и дополнительной нагрузке на службу поддержки.
- Ограниченная масштабируемость: в случае крупных атак нагрузка ложится на инфраструктуру банка, а система фильтрации работает с задержками.
- Не подходит для защиты личных кабинетов и платёжных каналов.

3. PaaS с раскрытием SSL-сертификата (облако, расшифровывающее трафик). Провайдер получает SSL-ключи и проводит анализ и фильтрацию трафика в реальном времени.

Преимущества:

- Высокая точность фильтрации и низкий уровень ложноположительных срабатываний.
- Отсутствие перегрузок оригинации, так как весь трафик обрабатывается в облаке.
- Эластичное масштабирование при DDoS-защите — возможности облака позволяют быстро реагировать на всплески атаки.

Недостатки:

- Требуется обязательная аттестация провайдера по ГОСТ Р 57580, PCI DSS, ФСТЭК 21, а также ежегодная пересертификация.
- Детальное согласование вопросов аудита и юридической ответственности.

Модель оптимальна для критичных банковских веб-сервисов при условии доверенной аттестации и регулярной проверки.

Какие есть варианты построения эффективной защиты от кибератак? NGENIX

	On-Prem	PaaS без раскрытия SSL-сертификата	PaaS с раскрытием SSL-сертификата
Затраты на создание	На заказчике	На PaaS-провайдере	На PaaS-провайдере
Затраты на поддержку и эксплуатацию при использовании	●●●	●●	●
Гарантии доступности веб-ресурса и ответственность	На заказчике	На PaaS-провайдере	На PaaS-провайдере
Сложность масштабируемости при органическом росте нагрузки	●●●●●	●	●
Скорость масштабируемости при росте нагрузки из-за DDoS-атак	● Требует резервный запас ресурсов	●●●●● Есть заложенный запас «прочности»	●●●●● Есть заложенный запас «прочности»
Аттестация / периодическая переаттестация	На заказчике — аттестация совместно с ИС банка	Не требует аттестации (PCI DSS Ready)	На PaaS-провайдере — уровень аттестации аналогичен уровню ИС банка: PCI DSS, ГОСТ Р 57580, ФСТЭК 21 (152-ФЗ)
Производительность	Зависит от выделенных ресурсов на этапе развёртывания системы	●● Ограничена подходом к защите (по логам). При масштабной DDoS-атаке логи могут быть не доставлены из-за исчерпания ресурсов	●●●●● Нет ограничения накладываемого на систему в следствии требования по отправке логов на анализ
Эффективность	Зависит от реализации (заказчика)	●● Низкая — из-за ограничений подхода к защите (по логам)	●●●● Система защиты максимально полно анализирует каждый запрос к веб-ресурсу
Риск блокировки легитимных пользователей	Зависит от реализации (заказчика)	●●●●● Высокий процент ЛПС	● Низкий процент ЛПС
Сложность интеграции		●	●●

Таблица 1. Варианты построения эффективной защиты от кибератак

АТТЕСТОВАННОЕ ОБЛАКО — ОПТИМАЛЬНЫЙ КОМПРОМИСС?

On-Prem решение даёт полный контроль, но требует больше затрат и уступает облаку в гибкости и оперативном масштабировании. PaaS без раскрытия SSL формально защищает данные, но имеет существенные ограничения по качеству защиты. В то же время PaaS с раскрытием сертификата и при наличии обязательной аттестации предлагает наилучший компромисс: высокий уровень безопасности и управляемости рисками, а также экономическую эффективность.

Какие можно выделить ключевые критерии приемлемости провайдера?

- Наличие аттестатов по требованиям ГОСТ Р 57580, приказа ФСТЭК № 21 и PCI DSS.
- Обязательство ежегодно проходить пересертификацию после изменений инфраструктуры.
- Гарантированная локализация данных (логов и резервных копий) на территории РФ.
- Предоставление прав доступа для аудита и регулярной отчётности перед регулятором.
- Законодательно оформленные SLA, включая показатели доступности, время восстановления (RTO/RPO) и распределение ответственности в случае инцидентов.
- Разработка совместного плана реагирования на инциденты, возможности forensic-анализа и регулярных тренировок команд.

Принятие законопроекта №404786-8 должно снять ключевую проблему — правовую неопределённость использования облаков для финансового сегмента.

У банков и других финорганизаций появится возможность спокойно выбирать провайдеров по формальным критериям: присутствию в реестре Минцифры, наличию аттестации и договорных гарантий. А значит, модель аттестованного облака с раскрытием SSL-сертификата может стать прозрачным и надёжным решением наравне с традиционными on-prem.

В ЗАКЛЮЧЕНИЕ

Финансовый сектор стоит на пороге новой эры: облачные сервисы перестают быть вспомогательным инструментом и становятся ключевым элементом защиты веб-ресурсов.

Принятие закона и расширение практики аттестации сформируют надёжную законодательную базу. Аттестованное облако станет оптимальным выбором, сочетающим безопасность, прозрачность и эффективность.

Вопрос, который остаётся открытым: сколько времени понадобится банкам, чтобы перейти от осторожного интереса к реальному использованию облаков в критичных для себя процессах? Скорее всего, определённость в этом вопросе появится примерно через год после того, как законопроект № 404786-8 будет принят и вступит в силу.

ИБ В КОРПОРАЦИЯХ

КАК ПРИРУЧИТЬ МОНСТРА С ТЫСЯЧЕЙ ГЛАЗ

Полина ГОЛУБЕВА
менеджер по развитию, ИТ-Экспертиза

Егор БЫСТРОВ
технический пресейл, ИТ-Экспертиза

Лето 2025-го в России стало испытанием на выносливость и для людей, и для бизнеса. Пока столбики термометров отмечали рекордные значения, цифровое пространство не отставало: количество кибератак за полгода выросло на 27% относительно прошлого периода. Под ударом ключевые отрасли экономики и госструктуры.

Эксперты предупреждают: растёт не только количество угроз, но и качество. Ущерб наносится по финансам, репутации, инвестиционной привлекательности и юридической устойчивости. Причина в сложной структуре крупного бизнеса: множество подразделений, филиалов, подрядчиков, удалённых сотрудников с корпоративными и личными устройствами. Каждое из них может быть потенциальным нарушителем.

Департамент ИБ не является исключением, страдая разрозненностью и многозадачностью. В таких условиях видеть картину целиком и быстро реагировать вручную почти невозможно. Отсутствие единого автоматизированного центра принятия решений оставляет бреши в защите.

Типичные меры обеспечения защиты. Сначала обычно внедряют периметровые средства защиты:

- межсетевые экраны (Firewalls);
- виртуальные частные сети (VPN);
- NGFW — с глубокой проверкой пакетов и предотвращением вторжений;
- IDS/IPS, способные обнаружить и заблокировать подозрительную активность.

Их усиливают:

- EDR и NGAV на устройствах;
- регулярное внешнее сканирование известных уязвимостей;
- предотвращение утечки данных с помощью DLP.

Добиться слаженной работы этих средств сложно. В итоге конечное устройство остаётся без надёжной защиты.

Почему не иностранные аналоги. Многие компании до сих пор полагаются на зарубежные инструменты кибербезопасности. И это риск! Это как доверить взломщику установить вам замок. Такие решения часто не соответствуют требованиям российских регуляторов, не имеют сертификации СЗИ и не вписываются в политику импортозамещения. Зарубежное ПО может быть уязвимым к целевым атакам, учитывающим специфику отечественного ИТ-рынка, и само может содержать уязвимости. В текущих реалиях остаются вопросы к выпуску обновлений и поддержке.

Альтернатива от компании ИТ-Экспертиза. Рассмотрим реальный кейс. В крупной компании сложная и распределённая инфраструктура превращала каждое рабочее место в потенциальную угрозу.

Ключевая цель: построение модели нулевого доверия (Zero Trust), чтобы критические решения принимались без задержек и человеческих ошибок. Для этого требовалась гарантия проверки каждого устройства до подключения и объединение всех средств защиты в единый механизм.

Решением стал программный комплекс информационной безопасности САКУРА с платформой реагирования на инциденты (IRP), полностью соответствующий российским требованиям и интегрируемый с отечественными СЗИ. Теперь каждое подключение — корпоративное, личное или удалённое — проходит цепочку автоматических проверок:

1. Подключение и идентификация. Устройство попадает в открытый контур, агент САКУРА собирает уникальные аппаратные и программные атрибуты: серийные номера, GUID, сертификаты и др.

2. Проверка корпоративности и пользователя. САКУРА обращается к внешним системам, сверяя принадлежность устройства, группы пользователя и статус учётной записи.

3. Профилирование устройства (авторизация). Для разных ОС, типов устройств и зон подключения назначаются индивидуальные профили с проверками — от актуальности обновлений и антивируса до USB-контроля и шифрования диска.

4. Автоматическое реагирование. Если нет нарушений — устройству предоставляется доступ, согласно профилю. Нарушение зафиксировано — доступ ограничивается или блокируется.

5. Постоянный мониторинг. Проверки продолжаются в реальном времени, а САКУРА мгновенно ограничивает доступ при нарушениях.

Результат:

- время реакции на инциденты сокращено с часов до секунд;
- создан единый центр управления безопасностью, объединив SIEM, NAC и антивирусы в рамках одного сценария;
- одинаково эффективная обработка подключений корпоративных, личных и устройств подрядчиков.

Заключение. В ИБ выигрывает тот, кто действует на опережение. Отсканируйте QR-код и узнайте, как ПК ИБ САКУРА может стать вашим главным союзником в построении защиты.

КОНФЕРЕНЦИЯ «ЗАЩИТА ДАННЫХ»

В ДОСТИЖЕНИИ ГЛАВНЫХ ЦЕЛЕЙ НАДО СОВМЕСТИТЬ СТРАТЕГИЮ И ТАКТИКУ

Усам ОЗДЕМИРОВ
корреспондент BIS Journal

Конференция «Защита данных» прошла в апреле в Москве, в здании «Холидей Инн Сокольники». Острый интерес к заглавной теме был подогрет ужесточением ответственности за утечку и неправомерное использование персональных данных.

Открывая панельную сессию, её модератор, заместитель начальника УОИБ ДБ Банка ВТБ (ПАО) Сергей Пазизин сделал акцент на практическом характере конференции, на сессиях которой планируется рассказать об основных приемах и инструментах для снижения рисков утечки данных. В то же время, необходимо понимать, какую задачу мы решаем и какие риски связаны с накоплением передачей и обработкой персональных данных (ПДн).

«МИЛЛИАРД В ДЕНЬ!»

Спикер, выступивший первым, президент аналитической компании «Крибрум», член Совета при Президенте РФ по развитию гражданского общества и правам человека Игорь Ашманов обозначил сложившуюся вокруг утечек ПДн и мошеннических атак ситуацию как чудовищную. Если несколько лет назад у граждан похищали 50 млрд рублей, то по результатам прошлого года, судя по данным МВД,— это уже 200 млрд. По оценке Игоря Станиславовича реальность гораздо хуже и, наверное, в настоящее время воруют примерно один миллиард в день. Экономика данных реально работает, только не на нас, а на мошенников.

Игорь Ашманов привёл пример инцидента в «Яндекс.Еда», когда в сеть утекли миллионы учётных записей, а ответственные отделались штрафом в 60 тысяч рублей. Давно назрела необходимость ужесточения наказания в виде более значительных штрафов и введения «уголовки», но «этот закон два года не могли принять из-за лоббирования цифрового бизнеса»,

считает эксперт. Оборотные штрафы могут не иметь большого стимулирующего действия, так как у реальных виновников утечек есть надежда избежать наказания, поэтому риск возбуждения уголовного дела даст больший эффект. К тому же компании уже включили оборотные штрафы в бизнес-план.

БИЗНЕС ПРОТИВ ЛИЧНОСТИ

Как отметил Игорь Ашманов, такая «абсолютная безответственность при бешеном накоплении персональных данных цифровым бизнесом долго продолжаться не могла... Так что этот закон будут ещё докручивать». В условиях массового сбора данных не помогут ни технические средства, ни биометрия, ни криптография. По мнению спикера, представители крупного бизнеса стараются убедить чиновников, что данные нужны для развития индустрии. Но сферы, где они реально нужны, немногочисленны, например, в «оборонке», силовых структурах, медицине, связи, транспорте. А «безумный сбор данных» нужен бизнесу для рекламы своих товаров и увеличения продаж. Любой наш гражданин — это потенциальная цель для злоумышленников, поэтому вторжение в приватное пространство должно приводить к уголовной ответственности, а персональные данные для тех, кто их хранит и обрабатывает, должны стать токсичными, как радиоактивные материалы, резюмировал эксперт.

ТРИ ТРЕНДА

Основатель и CEO компании Privacy Advocates, соучредитель и член правления Russian Privacy Professionals Association Алексей Мунтян сосредоточил внимание аудитории на тревожных трендах в информационном поле.

Во-первых, наблюдается поляризация отношения людей к приватности в целом. У одних есть желание извлечь выгоды: условно говоря, продать персональные данные за чашку кофе. У других — протест, активизм и паранойя. Такая симптоматика свидетельствует о том, что в юридическом плане у нас не всё хорошо с защитой ПДн.

Второй тренд отражает приватность как привилегию и статус, так как некоторые люди могут позволить себе лучше защитить свои персональные данные, платя за это больше денег. Таких людей, которые понимают ценность личных данных и готовы платить, будет становиться больше.

Третий тренд проявляется в исчерпании модели охраны приватности. Алексей Мунтян провёл небольшой опрос и выяснил, что для большинства персональные данные прежде всего ассоциируются со словом «согласие». И это очень печально, так как у нас защита ПДн становится для компаний «бухгалтерией». Мы не видим с их стороны попыток минимизировать обработку ПДн, умно подходить к этому вопросу. К сожалению, согласие фактически выполняет роль своеобразного «подорожника», который можно прикладывать ко всем сомнительным местам.

УСТАРЕВШИЙ КОНЦЕПТ

Персональные данные — это взрывоопасный актив, который может взорваться у вас в руках в любой момент времени, считает эксперт. Но, безусловно, с ними необходимо работать — без этого никуда. Сложившееся в обществе напряжение говорит о кризисе правового режима обработки и защиты ПДн. По мнению Алексея Мунтяна, многие нормы имеют свои истоки в прошлой эпохе, поэтому сейчас мы наблюдаем устаревший концепт, который нуждается в модернизации. Государство также считает текущую ситуацию с утечками ПДн и практиками многих компаний по их обработке социально неприемлемой. Но желательно обсуждать законопроекты не только между государством и бизнесом, но также привлекать к этому экспертное сообщество и граждан.

НЕ ИСПОЛНЯТЬ, А ЗАЩИЩАТЬ!

Другой спикер, советник по информационной безопасности ФБК CS, доцент кафедры КБ КВО РГУ им. Губкина Андрей Курило, остановился на главных целях действующей стратегии, которые заключаются в защите жизненно важных интересов личности путём повышения защищённости КИИ. Главный приоритет — обеспечение доступности, целостности и конфиденциальности данных.

Проблема в том, констатировал Андрей Петрович, что на той, враждебной стороне базу данных использует армия людей (примерно 70 тысяч человек), технически хорошо оснащённых. Утраченные данные очень долго сохраняют свою актуальность и будут использованы на протяжении всего срока жизни человека. С этим нам придётся жить. К сожалению, абсолютная защита невозможна. Контроль не должен сводиться к выполнению требований вместо

обеспечения защищённости. В итоге приходим к тому, что нужно сокращать количество обрабатываемых данных, заключил эксперт.

О ДВУСМЫСЛЕННОСТИ ФОРМУЛИРОВОК

Директор по стратегическим проектам Ассоциации больших данных Ирина Левова уделила главное внимание юридическим аспектам. Введение новых видов ответственности — как уголовной, так и административной — ставит ряд сложных вопросов перед бизнесом из-за двусмысленности и неопределённости некоторых формулировок в законах. Если говорить о смягчающих обстоятельствах, то представителям бизнеса хотелось бы получить дополнительные разъяснения по поводу расходов оператора на мероприятия по обеспечению ИБ и подтверждения соблюдения требований к защите ПДн.

Также необходимы разъяснения регулятора в части состава преступления за незаконное использование, передачу, сбор, хранение ПДн, полученных путём неправомерного доступа (ст. 272.1 УК РФ). Естественно, двусмысленность в юридических формулировках вызывает у бизнеса беспокойство, так как в случае инцидента и наступления ответственности её тяжесть будет зависеть от трактовки статьи закона. Вот почему компании закладывают возможные штрафы в бюджет рисков.

ИНТЕНСИВНЫЙ ПРАКТИКУМ

На протяжении дня в залах конференции проходили многочисленные дискуссии и доклады на тему защиты от НСД на конечных устройствах, контроля данных, маскирования и шифрования данных, контроля каналов утечки, а также аутентификации и управления доступом. Были проведены: практический круглый стол «Как сформировать стратегию действий и защиты в ходе проверки регулирующих органов» и мастер-класс «Управление проблемами коммуникации службы ИБ и других сотрудников компании».

В ходе дискуссии «Контроль данных», где модератором выступал генеральный директор MAKVES Роман Подкопаев, участники обсудили российские DCAP-системы и сложности их внедрения и интеграции. Эксперты сошлись на том, что DCAP не заменяет другие технические средства, например, DLP — ведь каждая система выполняет свою важную функцию. Но бывают проблемы с тем, чтобы донести позицию эксперта ИБ до руководства компании. Даже прозвучало полушутливое предложение: следовало бы организовать для вендоров курсы по обучению тому, как правильно общаться с бизнесом.

НАЗАД В БУДУЩЕЕ!

Один из спикеров на панельной сессии вспомнил цитату китайского мыслителя Сунь-цзы: «Стратегия без тактики — самый медленный путь к победе. Тактика без стратегии — это просто суета перед поражением». Говоря о проблеме конфиденциальности ПДн, Сергей Пазизин заметил: стопроцентную защиту можно обеспечить, если выбивать персональные данные каменным топором на скале, как в первобытные времена. Но хотелось бы совместить безопасность и удобство использования современных информационных технологий. Некоторое время назад в справочном столе можно было узнать адрес по ФИО и дате рождения, а телефонные справочники печатались и распространялись без всяких ограничений. И мир при этом был гораздо безопаснее. Новые технологии неизбежно создают новые риски, но как минимизировать эти риски зависит от нас. Видимо, выход надо искать в гармоничном сочетании стратегии использования ПДн и тактики их защиты.

КОНФЕРЕНЦИЯ «КАДРОВОЕ ОБЕСПЕЧЕНИЕ ИБ»

РАБОТОДАТЕЛЯМ НЕ НУЖНЫ «УНИВЕРСАЛЬНЫЕ СОЛДАТЫ»

Усам ОЗДЕМИРОВ
корреспондент BIS Journal

Конференция «Кадровое обеспечение информационной безопасности РФ» и пленум Федерального учебно-методического объединения в системе высшего образования ИБ (ФУМО) состоялись в Москве в залах Конгресс-центра МТУСИ.

Выступивший с приветствием от ФСТЭК России Анатолий Марченко остановился на агрессивном характере деятельности разведывательных служб стран НАТО, направленной на подрыв безопасности нашей страны. Логика ситуации лишний раз диктует вывод о том, как важна работа по кадровому обеспечению информационной безопасности. Представитель ФУМО ИБ Владимир Богатырёв завершил эту мысль: нам противостоят серьёзные противники, и наша задача — вырастить тех, кто сможет им эффективно противодействовать.

Ведущий мероприятия, генеральный директор АНО «НТЦ ЦК» Игорь Качалин, выразил удовлетворение тем, что в конференции принимают участие представители не только учебных заведений, но и органов государственной власти и бизнес-организаций, куда устраиваются выпускники вузов и колледжей.

ОБНОВЛЕНИЕ КОНЦЕПЦИИ

Референт аппарата Совета безопасности РФ Алексей Петров был настроен оптимистично. По его словам, успешно развивается государственная система подготовки, переподготовки, повышения квалификации кадров в области ИБ, найден баланс между потребностями сегодняшнего дня и фундаментальными знаниями. Проведена работа по разработке и утверждению отраслевых планов целевой подготовки кадров для объектов КИИ. Расширена возможность трудоустройства специалистов со средним специальным образованием в области ИБ, для чего внесены изменения в соответствующие нормативно-правовые документы. Продолжается реализация проекта по созданию системы учебных научно-производственных центров по ИБ.

Если говорить о планах на ближайшее будущее, то следует уделить больше внимания мониторингу образовательных процессов и укомплектованности подразделений по защите информации, решить вопросы о мерах поддержки специалистов и стимулирования работников образовательных учреждений. Как заверил Алексей Петров, всё, что предстоит сделать в ближайшей перспективе, будет закреплено в руководящих документах. Так, уже принято решение об обновлении Концепции кадрового обеспечения в области ИБ.

ПРОЕКТЫ МИНЦИФРЫ И МИНОБРНАУКИ

Подготовка кадров в свете существующих угроз является для нас приоритетом, отметила Анастасия Казанцева, заместитель директора Департамента развития цифровых компетенций и образования Минцифры России. В целях развития ключевых навыков безопасного использования сети Интернет и формирования базовых компетенций кибербезопасности у школьников Минцифры совместно с Минпросвещением и АНО «Цифровая экономика» осуществляет просветительский проект «Цифровой ликбез». С 2020 г. в нём приняли участие более 4,7 млн. школьников и более 263 тысяч педагогов в 89 регионах.

Также Казанцева уделила внимание проекту «Цифровые кафедры», который делает упор на дополнительные профессиональные программы в области ИБ. В рамках этого проекта только по специальностям ИБ задействованы 13 вузов. В 2025 году запущен национальный проект «Экономика данных и цифровая трансформация государства», который предусматривает такие направления, как подготовка топ-специалистов в сфере ИИ и информационных технологий. Задача в том, чтобы вы-

пускники вузов обладали необходимыми компетенциями и работодателям не приходилось тратить ресурсы на их дообучение.

Заместитель директора Департамента цифрового развития Минобрнауки России Александр Матюнин порадовал аудиторию хорошей новостью: созданный в 2024 г. ведомственный центр безопасности информации в настоящее время функционирует в режиме 24/7. Развёрнуты и эксплуатируются средства мониторинга событий ИБ, системы SIEM и VM, Web Application Firewall и т.д. Департамент информирует подведомственные организации об оказываемых услугах, как подключиться к центру и взаимодействовать с ним. По словам Матюнина, в первую очередь они стараются подключать организации, у которых есть объекты КИИ.

СЛЕДУЕТ УСТРАНИТЬ...

Представитель ФСТЭК России Анатолий Марченко остановился на теме дополнительного профессионального образования и его нормативного регулирования. Действующая Концепция кадрового обеспечения в области ИБ в связи с окончанием срока её реализации нуждается в обновлении и продлении на период до 2035 года. По данным ФСТЭК, потребность в специалистах по защите информации для органов власти и предприятий ОПК в 2024 г. составляла около 11 тыс. человек.

ФСТЭК получает сведения о квалификации преподавателей из ФУМО, а также путём опроса самих образовательных организаций. Анализ показывает, что только 34% преподавателей имеют базовое образование в области ИБ, поэтому важно обеспечить их профессиональную переподготовку и повышение квалификации. Также, согласно госстандартам, как минимум один преподаватель в вузе должен иметь учёную степень в области ИБ, что не всегда наблюдается. Это упущение следует устранить. Марченко напомнил и о недостаточном материально-техническом обеспечении в вузах, за исключением передовых учреждений, имеющих хороший задел.

ФУМО: ДОКОЛЕ?!

Председатель ФУМО Евгений Белов порадовался большому представительству профессорско-преподавательского состава на конференции: в целом на все три дня зарегистрировалось около сотни вузов и около 30 организаций СПО и ДПО. Белов рассказал о работе над новой Концепцией кадрового обеспечения в области ИБ, которую провели ФУМО совместно с представителями региональных отделений, ведущими учёными и работодателями.

Среди рисков и уязвимостей были названы недостаточная укомплектованность специалистами с профильным образованием на всех уровнях, дефицит преподавательских кадров, особенно в части профессиональных компетенций, опыта практической работы, а также непрофильный характер многих организаций дополнительного образования, что связано с финансовыми трудностями. По мнению Белова, нельзя далее мириться с положением, когда результаты обучения не сходятся с потребностями экономики страны. Все образовательные программы необходимо привести в соответствие с актуальными и перспективными требованиями работодателей.

БОГА ИБ НЕТ?

Именно этой теме была посвящена пленарная дискуссия «Потребность и требования работодателей к специалистам по защите информации», которую вёл заместитель генерального директора АО «ИнфоТеКС» Дмитрий Гусев. Количество значимых объектов КИИ растёт из года в год, они подпадают под действие ФЗ-187 и приказов ФСТЭК о необходимости формирования соответствующих подразделений. Постановление правительства № 1272 детально расписывает требования к заместителю и руководителю организации по ИБ субъекта КИИ. По словам Гусева, получается портрет «универсального солдата», если не «бога информационной безопасности». Где таких специалистов найти?

В дискуссии приняли участие Алексей Кучерявенко («Ростелеком»), Артём Калашников («Газпромбанк»), Алексей Гуревич («СИБИНТЕК») и профессор ОмГТУ Павел Ложников.

Эксперты сошлись в том, что нельзя быть кладезем знаний во всём абсолютно. Не обязательно обладать всем спектром компетенций, важно собрать команду специалистов, отвечающих требованиям компании в сфере ИБ. В частности, Калашников заявил, что многое зависит от размера организации, но главное — умение руководить. Ведь по правилам он должен не менее 50% своих компетенций тратить на технологии процесса управления. Ложников «показал» ситуацию с точки зрения вуза. Когда руководитель компании приходит к ним, он ищет специалиста по защите информации, «чтобы снять свои риски», но в Омской области, где много оборонных заводов, выпускаемых местными вузами специалистов катастрофически не хватает.

«ЗАСТОЙ В ЭТИХ ДЕЛАХ ЧРЕВАТ»

Был вопрос о критериях и подходах при выборе работодателями выпускников, получивших диплом вузов или колледжей. Алексей Гуревич заверил, что его структура работает со всеми и нет каких-то шаблонных требований. Для них наиболее ценны потенциал человека, его готовность обучаться и развиваться. К счастью, у компании «СИБИНТЕК» действует внутренний корпоративный университет, который «задействуется для подтягивания знаний». Переподготовка кадров идёт не раз в три года, а на постоянной основе.

Представители работодателей, участвовавшие в дискуссии, поддержали мнение о том, что повышение квалификации должно быть непрерывным, так как сфера кибербезопасности всегда в движении. По мнению Артёма Калашникова, «застой в этих делах чреват». В его структуре предусмотрены отдельные курсы, иногда и в кооперации с вузами. Надо растить специалиста не узкого профиля, а с широким взглядом. По мере того как расширяется его компетенция, у него появляется больше возможностей и вариантов принятия решений.

Фото: ООО «Р-Конф», https://infosecurity-forum.ru

CISO FORUM 2025

ГДЕ НАЙТИ ИДЕАЛЬНОГО БЕЗОПАСНИКА

Вероника ГОРЯЧЕВА
корреспондент BIS Journal

«Кадры в ИБ: где их искать и как растить специалистов». Так называлась одна из сессий CISO FORUM 2025, который прошёл в середине апреля в Москве. Ведущие эксперты кибербезопасности обсудили все тонкости найма в условиях дефицита кадров, а также поделились лайфхаками – как построить сильную ИБ-команду в сегодняшних реалиях.

АЛЛО, МЫ ИЩЕМ ТАЛАНТЫ!

Дискуссия о кадрах в ИБ началась с вопроса ведущего: есть ли дефицит кадров на рынке? И все эксперты дружно отметили, что проблема актуальна, но оказалось, что видят они дефицит по-разному, как и пути борьбы с ним. По словам директора по продуктам Servicepipe Михаила Хлебунова, в ИТ и ИБ сейчас не просто не хватает кадров – не хватает людей, которые умеют думать и исследовать, а не просто выполнять шаблонные задания. Эксперт рассказал, что для решения проблемы найма таких людей компания идёт в вузы и там ищет талантливых думающих студентов. И. о. директора по ИБ ДЗО АО «СОГАЗ» Артём Куличкин сказал, что его компания также активно ищет таланты среди студентов, привлекая их на практики и стажировки. «Студентам ставятся специальные задачки, и среди тех, кто успешно справился с заданием, отбираются думающие ребята, многие потом остаются в компании на хардовых позициях», – рассказал он. CISO Райффайзен Банка Георгий Руденко отметил, что он, наоборот, не нанимает студентов и junior-специалистов. Его интересуют кадры уровня не ниже middle с прицелом, чтобы они вырастали в банке до middle+ или даже до senior.

Интересными цифрами поделилась директор по информационным технологиям и кибербезопасности HeadHunter Татьяна Фомина. Она отметила, что на рынке испытывается ощущение постоянно растущего дефицита кадров в сфере ИБ, но это не совсем так. Если посмотреть на hh-индекс (это соотношение числа резюме к числу вакансий), то с середины 2022 года он очень стабилен. Например, в вакансиях разработ-

чиков он составляет порядка 11, но при этом большая часть соискателей — это junior-специалисты, а вот с резюме специалистов уровня middle или senior картина обратная. За них идёт борьба, и конкуренция тут очень высокая.

СЕКРЕТЫ НАЙМА

Когда же перешли непосредственно к вопросам найма сотрудников, эксперты назвали лайфхаки, которые они используют. Артём Куличкин рассказал, как он прорабатывает с отделом кадров резюме соискателей. «Люди, занимающиеся подбором персонала, не сильно понимают в ИБ, для них SIEM, SOC и прочие аббревиатуры — незнакомые слова», — рассказывает эксперт. И потому он предложил: получая от HR пачку резюме, садиться вместе и внимательно разбирать их, отмечая, что нравится, что нет. «И в итоге HR не просто начинают разбираться, а разбираются в теме порой лучше даже junior-специалистов, которых нанимают», — резюмировал он. Татьяна Фомина считает, что также отлично работают в найме реферальные программы. Также она отметила, что принцип «нанимай медленно, увольняй быстро» крутой, но не всегда верный. Эксперт привела пример, когда из-за HR с нездоровым перфекционизмом за полгода было нанято 0 кандидатов, замена HR позволила за 4 месяца нанять шесть человек. «Если есть испытательный срок и кандидат вроде бы подходит, то лучше рискнуть, чем оставлять вакансию незакрытой», — указала она. Михаил Хлебунов отметил, что данный подход идеально подходит при сборе новой команды (например, на новое направление), если же нужен человек в уже имеющуюся команду, необходим подход «нанимай медленно...». В то же время все эксперты сошлись во мнении, что многоэтапные утомительные и сложные собеседования — зло, они могут отпугнуть нужных кандидатов.

О МАТРИЦЕ КОМПЕТЕНЦИЙ

Интересные дискуссии вызвал вопрос о матрице компетенций. Руководитель специальных проектов ГК «Солар» Нина Шипкова рассказала, что, по её мнению, «матрица компетенций» — это самый мощный инструмент для оценки навыков, глубины этих навыков, а также для понимания того, соответствует ли тот или иной человек текущей роли, какие треки у человека есть для развития — как горизонтального, так и вертикального. То есть матрица позволяет сформировать портрет роли и показать, какое необходимое обучение требуется, что нужно знать и уметь, чтобы подняться выше или перейти в другую специализацию внутри компании.

Принцип «нанимай медленно, увольняй быстро» крутой, но не всегда верный. Эксперт привела пример, когда из-за HR с нездоровым перфекционизмом за полгода было нанято ноль кандидатов, замена HR позволила за 4 месяца нанять шесть человек

Однако не все эксперты посчитали, что матрица компетенций так уж необходима. Михаил Хлебунов отметил, что в Servicepipe матрицы как таковой нет, но есть очень серьёзное инженерное ядро, и технические специалисты обучаются преимущественно внутри компании. И если в компании появляется потребность, к примеру, в новом team lead, то компания в первую очередь внутри ищет специалиста, у которого есть интерес и стремление развиваться и расти. «В компании много менеджеров среднего уровня, кто вырос из техподдержки, — отметил Михаил Хлебунов. — Если технические специалисты чувствуют, что им не хватает знаний, или есть желание выучить что-то новое, мы идём навстречу, потому что это почти всегда взаимовыгодное сотрудничество».

БЮДЖЕТ НА ОБУЧЕНИЕ

Продолжая тему повышения квалификации сотрудников, директор Управления безопасности VS Robotics Дмитрий Беляев рассказал, что в компании очень развито обучение по модулям, и модулей этих очень много. Кроме того, есть обязательные курсы для сотрудников подразделения кибербезопасности, большое количество киберучений по различным сценариям. «Помимо прочего, у нас также есть команда Blue Team (защитники) и команда Red Team (атакующие), мы проводим учения между ними, отрабатываем плейбуки, насколько корректно они созданы в рамках реагирования на SOC», — резюмировал он. Татьяна Фомина отметила, что, по её мнению, обучение в компании ни в коем случае не должно быть принудительным, а выделенные на обучение бюджеты должны быть предельно целевыми. «Я уверена на 100%, что бюджеты на обучение и решение по их расходованию нужно отдавать вниз в управление людям, которые чуть ближе к тем, кого надо учить, — указала она. — Команды и люди сами знают, чему им учиться».

ПРО СОФТ, ХАРД И ВАЙБ

В финале дискуссии эксперты обсудили, какими качествами и скилами должен обладать руководитель службы ИБ. Одни эксперты говорили о том, что важнее софт-скилы, другие — что хард-скилы. В результате все сошлись во мнении, что идеальный руководитель службы информационной безопасности должен обладать и тем, и другим. Кроме того, крайне важно, чтобы при собеседовании на должность руководителя ИБ-направления возник вайб между соискателем и нанимающим менеджером. И тогда всё получится.

«ТЕХНОЛОГИИ ДОВЕРЕННОГО ИСКУССТВЕННОГО ИНТЕЛЛЕКТА» — 2025

УЯЗВИМОСТИ НЕ ИСКЛЮЧЕНЫ, НО ДОСТОЙНЫЙ ОТВЕТ НА ВЫЗОВЫ НЕОБХОДИМ

Артём ЗУБКОВ
генеральный директор Медиа Группы «Авангард»

20 мая в Москве в пространстве кластера «Ломоносов» прошёл III Форум «Технологии доверенного искусственного интеллекта». В нём приняли участие представители профильных государственных министерств и ведомств, ведущих отечественных научно-исследовательских центров и профессиональных объединений в сфере технологий доверенного ИИ, российских технологических лидеров, реализующих успешные проекты в области ИИ, и крупнейших компаний в сфере информационной безопасности.

Ключевая сессия, которую модерировал директор ГК «Солар» Игорь Ляпунов, была посвящена изменениям и прогрессу в обсуждаемой сфере за прошедший год. Своё вступительное слово он начал с рассказа о довольно тревожных результатах исследования компании OpenAI, согласно которым уже в ближайшие годы будет создан суперинтеллект — Artificial Superintelligence (ASI), сравнимый с мощью человеческого мозга. Появление такого колоссального потенциала для экономики и связанная с ним конкуренция между передовыми державами таят в себе риски выхода ИИ из-под контроля.

Свою точку зрения на роль ИИ в развитии экономики и доверия к нему представила начальник Управления Президента РФ по развитию ИКТ и инфраструктуры связи Татьяна Матвеева. Прежде всего, согласно принятой Стратегии развития ИИ до 2030 года, для задач государственного управления в сферах, где может быть нанесён ущерб безопасности страны в целом, следует использовать технологии доверенного ИИ. В их основе должны лежать такие принципы, как объективность, недискриминация и этичность (исключено нанесение вреда человеку). Также не допускается нарушение основополагающих прав и свобод человека, нанесение ущерба интересам государства и общества. Сюда можно добавить эффективность, надёжность, отказоустойчивость и объяснимость технологий, завершила своё выступление спикер.

Как показал недавний социологический опрос трёх тысяч россиян, 96% респондентов слышали об искусственном интеллекте, но объяснить, что это такое, смогли только 42%. Опыт пользования продуктами ИИ имеют 69%, но общий уровень доверия к нему составляет лишь 38%. Если говорить по видам деятельности, то больше доверяют ИИ в сферах развлечений, услуг, промышленности и меньше — в здравоохранении, экономике и финансах, образовании, госуправлении и оказании психологической помощи. По словам Татьяны Матвеевой, доверие к ИИ формируется благодаря тому, что оптимизируется работа и улучшается качество жизни. К обратному эффекту приводят опасения, связанные с утечками персональных данных и использованием технологий в корыстных целях.

Если мы хотим стимулировать доверие к технологиям ИИ, то можно двигаться по нескольким направлениям. Роль государства здесь видится в прямом нормативно-правовом регулировании, в системе стандартизации и сертификации, единых подходах к оценке параметров технологий (например, бенчмарки). Идёт процесс саморегулирования: так, был создан Кодекс этики в сфере ИИ, к которому присоединилось более 900 организаций. Люди должны видеть эффект от внедрения технологий ИИ. Как отметила Матвеева, на региональном уровне реализуется более 500 решений, начиная от различных чат-ботов и заканчивая прогнозами чрезвычайных ситуаций, и они показывают «высокую степень повышения результативности работы, снижение нагрузки на людей, увеличение эффективности и повышение предсказуемости».

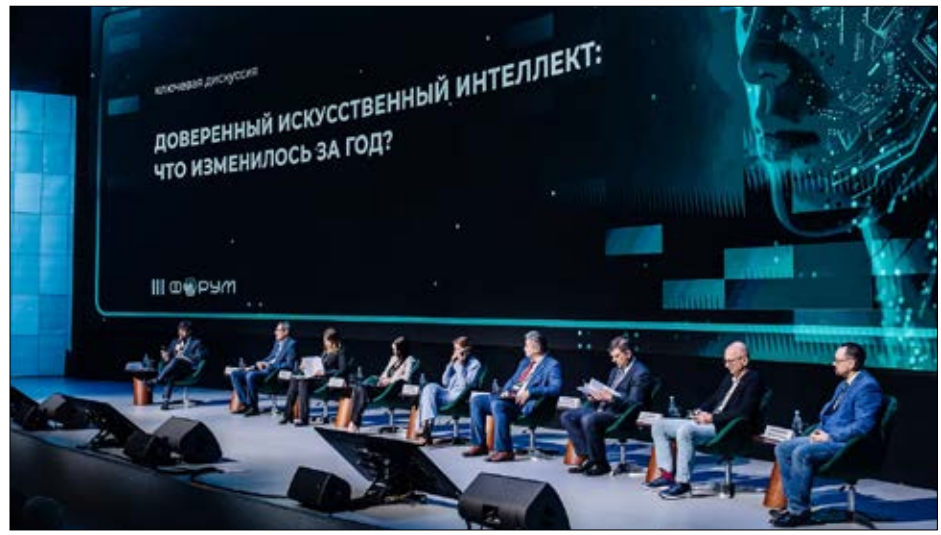
Заместитель министра цифрового развития, связи и массовых коммуникаций РФ Александр Шойтов рассказал о том, что Академией криптографии в 2024 году разработаны и направлены в ФОИВ и заинтересованные организации «Предложения в проект требований по обеспечению ИБ информационных систем, реализующих технологии ИИ». Также Академия совместно с Консорциумом исследований безопасности технологий ИИ разрабатывает профиль-

ную матрицу угроз для объектов КИИ и ГИС и приступает к её отработке с пилотными регионами России. Шойтов на слайдах представил вниманию участников модель тестирования технологий ИИ без использования в КИИ и модель для КИИ, заслуживающей высокую степень доверия.

Есть конкретные риски, связанные с использованием передовых технологий: потеря контроля над критическими инфраструктурами, финансовые потери из-за ошибок ИИ, потеря контроля над личной информацией, манипуляция сознанием и поведенческая реклама, опасность автоматизированных решений без возможности апелляции и т.д. Проблемы информационной безопасности и искусственного интеллекта имеют чисто технологический характер, считает Шойтов. Да, работа в сфере ИБ более понятна и измерима по сравнению с ИИ, но угрозы в обеих сферах взаимосвязаны, и решать эти проблемы придётся одновременно.

Модератор Игорь Ляпунов в ходе дискуссии не раз прибегал к помощи нейросети DeepSeek, которая генерировала довольно провокационные вопросы и темы. Если отдельные алгоритмы способны заменить до 40% рабочих мест, то как быть с безработицей? Насколько опасно использовать зарубежные фреймворки в российских ИИ-разработках? Не усиливает ли внедрение ИИ разрыв между Москвой и регионами? Были также «подсказки» от DeepSeek про возможную «когнитивную деградацию», экзистенциальные риски для малых культур, коллапс образования....

Не стоит «обожествлять искусственный интеллект и говорить, что он всё придумал», предложила Наталья Касперская, президент ГК InfoWatch. Ни в коем случае нельзя впускать ИИ в школьные стены, но главная проблема — это всё же «вторичность отечественного ИИ». При условии использования таких фреймворков, как PyTourch и TensorFlow, мы не получим доверенный ИИ. Эта вторичность на самом деле «даёт возможность закладок, внешнего управления и навязывания чужой повестки», считает Касперская.



Большую опасность представляет «замена коммуникации граждан на общение с искусственным интеллектом». Часть рисков мы сегодня видим, но многие нам не ясны, так как это новая технология и у человечества нет особого опыта её применения. По мнению Касперской, идёт «тихое вползание ИИ в нашу жизнь» и о рисках говорят значительно меньше, чем о преимуществах. Должна быть государственная структура, ответственная за контроль над ИИ, необходимо заниматься регулированием, «пока не стало слишком поздно», заключила Касперская.

В ходе ключевой дискуссии выступили ещё несколько спикеров. Директор Департамента стратегического развития и инноваций Минэкономразвития Оксана Сотникова рассказала о проведённом в 2024 году форсайте для определения приоритетов развития ИИ. Были выделены несколько важных направлений: обеспечение соответствия ценностям человека и общества, объяснимость, обеспечение безопасности разработки и эксплуатации, а также защита от взлома. Директор по информационным и цифровым технологиям ГК «Росатом» Евгений Абакумов сделал акцент на практической стороне вопроса: какой объём электроэнергии потребует внедрение технологий ИИ и не понадобится ли введение дополнительных мощностей?

Как отметил генеральный директор Ассоциации ФинТех Максим Григорьев, финансовый сектор одним из первых научился прагматично и практически применять искусственный интеллект: для скоринга, для управления торговыми стратегиями, противодействия мошенникам и т.д. Представители финансового рынка договорились с Альянсом в сфере ИИ о создании отраслевого клуба, который обеспечит взаимодействие, обмен информацией и формирование необходимых отраслевых практик. Дмитрий Служеникин рассказал о работе, проведённой за прошедший год в Консорциуме исследований безопасности технологий ИИ. Усилия направлены на то, чтобы «норматив не выходил пустой» и все понимали, как на деле его выполнять.

Достичь состояния, когда нет никаких уязвимостей, невозможно, но обеспечить нужный уровень доверия необходимо, полагает директор ИСП РАН Арутюн Аветисян. «Я точно не луддит. Пчёлы против мёда — это не мой стиль,— заметил спикер.— Я сам занимаюсь искусственным интеллектом и его внедрением». Регуляторика нужна, но такая, чтобы не препятствовала развитию технологий. В заключение дискуссии Игорь Ляпунов охарактеризовал ИИ как технологию, которая врывается без спроса в нашу жизнь. И следует воспринимать её как сущность, которая способна поменять мир, причём с невообразимой скоростью. Проблематика доверенного ИИ — это сложный вызов, но совместная работа профессионалов поможет ответить на него системно и прагматично.

ЧТО ВЫИГРЫВАЕТ ФИНАНСОВЫЙ СЕКТОР

ПРИ ПЕРЕХОДЕ НА ЛОКАЛЬНУЮ ИИ-ИНФРАСТРУКТУРУ

Алексей ЗОТОВ
руководитель направления ИТ-инфраструктуры K2Tex

Финансовый сектор традиционно выступает одним из лидеров по внедрению искусственного интеллекта (ИИ). Согласно данным Deloitte, около 70% финансовых организаций в мире уже используют ИИ и машинное обучение в операционной деятельности. В ближайшие пять лет влияние этих технологий на бизнес-процессы будет только усиливаться. Вместе с тем перед участниками рынка встаёт стратегическая задача: выстроить ИТ-инфраструктуру, способную не только максимально раскрыть потенциал ИИ, но и обеспечить высокий уровень безопасности данных, прозрачное управление ими и экономическую эффективность. В статье Алексей Зотов, руководитель направления ИТ-инфраструктуры K2Tex, рассказал, почему компании всё чаще используют готовые он-премис-инфраструктуры[1] и какие возможности для этого существуют сегодня на отечественном ИТ-рынке.

МИРОВОЙ ПОДХОД

Масштабы инвестиций в искусственный интеллект в финансовом секторе стремительно растут. По оценкам Juniper Research, в 2024 году глобальные затраты банковской системы на генеративный ИИ составили около $6 млрд. А к 2030 году эта сумма достигнет $85 млрд. Согласно данным Business Insider, степень внедрения ИИ напрямую зависит от размера активов банка: крупные банки внедряют технологии охотнее. В частности, ведущие финансовые институты Азии уже заявили о сокращении тысяч рабочих мест: автоматизация рутинных операций с помощью ИИ позволяет перераспределять ресурсы и снижать операционные издержки.

Кроме оптимизации затрат, ИИ обеспечивает рост доходов и создание новых бизнес-возможностей. По данным Nvidia, почти 70% компаний, внедривших ИИ-решения, увеличили доходы минимум на 5%, а более 60% — сократили расходы не менее чем на 5%.

Наибольшее применение современных технологий наблюдается в сегменте клиентских сервисов: здесь доля проникновения ИИ достигает 84%. Речевые технологии и чат-боты уже снимают нагрузку с операторов и оптимизируют работу кол-центров. А предиктивная аналитика применяется при моделировании расходов и оценке кредитоспособности клиента. В перспективе особое развитие получат интеллектуальные рекомендательные системы — для управления инвестициями, накоплениями и персонального финансового планирования. Внутренние процессы в финансовой сфере, такие как эквайринг, платёжные системы и скоринг, уже сейчас активно интегрированы с технологиями ИИ и продолжают развиваться.

РОССИЙСКИЙ ОПЫТ: ИМПОРТОЗАМЕЩЕНИЕ В ДЕЙСТВИИ

Внедрение ИИ в российском финсекторе набирает обороты, но сталкивается с системными ограничениями. По данным Ассоциации ФинТех (АФТ), на сегодняшний день только 10–15% проектов с генеративным ИИ в российских компаниях финотрасли доходят до промышленной эксплуатации, и лишь 20–25% из них показывают заметный экономический эффект. Ключевыми барьерами остаются кадровый дефицит и отсутствие единой методологической базы. При масштабировании ИИ-решений компании вынуждены пересматривать текущие ИТ-инфраструктуры, адаптируя их к требованиям ИИ. На этом этапе нередко возникает разрыв между классическими ИТ-системами и архитектурой, необходимой для машинного обучения, сбора данных и их обработки. Инфраструктурные команды не всегда способны выбрать аппа-

[1] Он-премис (от англ. on-premise) — подход, когда инфраструктура развёрнута локально, серверы и ресурсы размещаются в ИТ-контуре компании.

ратное оборудование, программный слой и прикладной софт под задачи, обозначенные дата-сайентистами, что усложняет эксплуатацию и поддержку ИИ-проектов.

Эксперты прогнозируют, что в 2026 году уровень использования ИИ в отечественных финансовых компаниях может достичь 68%. Уже сегодня ИИ помогает Альфа-Банку оптимизировать подбор персонала, Т-Банку — защищать клиентов от мошенников и автоматизировать рутинные задачи. ИИ находит всё более широкое применение в оценке рисков, в расчётах страховых премий и обработке данных в страховых компаниях.

РЕШЕНИЕ ОН-ПРЕМИС — НЕ РОСКОШЬ, А НЕОБХОДИМОСТЬ

Если на этапе пилотных проектов компании чаще всего тестируют ИИ-сервисы в публичных облаках, которые позволяют гибко и быстро развернуть необходимые вычислительные мощности и не требуют капитальных затрат, то для запуска в промышленную эксплуатацию по ряду причин предпочитают локальную инфраструктуру. Во-первых, ранее многие компании использовали решения уровня NVIDIA DGX/HGX, которые позволяли создать готовую инфраструктуру для ИИ. Сегодня покупка, поддержка и лицензирование таких решений ограничены, поэтому российские компании, на которые распространяются требования регуляторов, активно смотрят в сторону отечественных разработок. К 2027 году крупные игроки рынка планируют довести уровень импортозамещения своих ИТ-систем до 85–90%. Этому способствует и законодательная поддержка: инициатива «Искусственный интеллект» в рамках нацпроекта «Экономика данных» ставит задачу создания инфраструктуры для вычислений и хранения данных на базе отечественного оборудования, технологий и ПО до 2030 года.

Во-вторых, повышаются отраслевые требования: высокий уровень защиты данных, необходимость в мощных вычислениях и значительные энергозатраты. В условиях роста кибератак банки ужесточают контроль над информационными системами.

В ответ на спрос российский рынок предлагает готовые решения для корпоративного ИИ. В их числе как аппаратные платформы, например, от производителей Yadro, Delta Computers, FPlus или R-Style, так и готовые решения под ключ, такие как программно-аппаратные комплексы от К2 НейроТех или Скала-Р. Они разворачиваются в контуре компании, объединяя аппаратный слой, платформу управления, преднастроенное программное обеспечение и инструменты для работы с ИИ и высокопроизводительными задачами.

Локальные инфраструктуры особенно важны для банков, где утечка персональных или транзакционных данных грозит серьёзными репутационными и финансовыми потерями. Он-премис-решения позволяют чётче контролировать доступ, хранить и обрабатывать их локально с высокой производительностью, чего нельзя гарантировать при использовании облачных сервисов с распределённым хранением.

Другое немаловажное преимущество — локальная инфраструктура легко интегрируется в существующий ИТ-ландшафт организации, работает с актуальными источниками данных, учитывает бизнес-логику и минимизирует избыточные связующие слои. При обучении моделей он-премис данные получаются чище и точнее, что гарантирует безопасность и защищает от предвзятости. Это критично для задач скоринга, антифрода и анализа клиентского поведения. Размещение вычислительных ресурсов под ИИ-задачи в собственном контуре обеспечивает независимость от провайдеров и непредсказуемых факторов их инфраструктуры. Компания получает гарантированную производительность ИИ-моделей и высокую доступность системы, поскольку полностью контролирует вычислительные мощности и не зависит от технических сбоев или ограничений третьих сторон.

Для максимальной эффективности компании прибегают к гибридным моделям: ресурсы распределяются между облаком и локальной инфраструктурой, при этом чувствительные данные обрабатываются в защищённом контуре. В то же время некоторые организации разворачивают частные корпоративные облака, чтобы обучать и тестировать модели «за закрытыми дверями» на чувствительных бизнес-данных. Частные облака позволяют создавать не только больший контроль над данными, но и масштабируемость и прозрачность при распределении вычислительных ресурсов для таких задач.

Выбор вычислительной инфраструктуры — первый и важный шаг к внедрению искусственного интеллекта. Компании приходят к пониманию того, что инвестиции в собственные вычислительные мощности — это не только контроль, отказоустойчивость и безопасность сегодня, но и фундамент для стабильного внедрения ИИ-продуктов в бизнес-процессы, которые обеспечат принципиально новый уровень эффективности и конкурентоспособность на годы вперёд.

«УМНОГО ЧЕЛОВЕКА НИЧЕМ НЕ ИСПОРТИШЬ. ДАЖЕ ИСКУССТВЕННЫМ ИНТЕЛЛЕКТОМ»

Игорь ШЕРЕМЕТ
председатель Научного совета РАН «Информационная безопасность», доктор технических наук, профессор, академик РАН

Несомненно, одной из самых горячих тем в цифровизации сегодня является искусственный интеллект (ИИ). Однако для того, чтобы объективно взвесить все риски, связанные с данным направлением ИТ, нужно хорошо представлять себе особенности тех математических методов, на которых базируются современные технологии ИИ. О том, что происходит в этой области, — наша вторая беседа с академиком РАН Игорем Шереметом.

НАЧНЁМ С НАЧАЛА

— Игорь Анатольевич, давайте начнём с самого начала: какие виды информационных технологий охватывает понятие «искусственный интеллект»?

— Я стал интересоваться различными аспектами построения систем, способных выполнять те или иные функции, которые принято считать интеллектуальными, пожалуй, с 1973 года. Будучи первокурсником, я купил книгу Джеймса Слэйгла «Искусственный интеллект» — тогда она только что вышла в издательстве «Мир». А уже в 1977 г. группа выпускников, которую я возглавлял, защитила дипломные проекты, посвящённые различным компонентам спроектированной нами системы аналитических преобразований на ЭВМ. Можно сказать, что это был микровариант известных тогда систем — американской MATHLAB (не путать с широко используемой сегодня платформой MATLAB, Matrix Laboratory, для работы с матрицами) и советской «АНАЛИТИК», разработанной под руко-

водством академика Виктора Михайловича Глушкова для ЭВМ серии «МИР». Нам была доступна ЭВМ ЕС-1022 (мейнфрейм с перфокарточным вводом; алфавитно-цифровые дисплеи ЕС-7927 стали массово поставляться где-то года с 1978). И на ней удалось создать систему, которая могла дифференцировать, приводить подобные члены, подставлять значения вместо переменных с последующим упрощением выражений и даже брать интегралы по частям с использованием таблицы интегралов. При этом сами формулы хранились не в обратной польской записи, как в упомянутой системе «АНАЛИТИК», а в схеме Канторовича, что обеспечивало простую и эффективную реализацию всех необходимых преобразований. Конечно, никакого развития эта учебная работа не получила, но благодаря ей нам удалось постичь некоторые базовые принципы построения интеллектуальных систем, которые в дальнейшем неоднократно использовались при решении серьёзных и ответственных прикладных задач.

ЭВМ ЕС-1022

— Это напоминает Wolfram Alpha — известную базу знаний и набор вычислительных алгоритмов. Создатель Wolfram Alpha Стивен Вольфрам также говорит о создании «вычисляемых знаний», которые связывают между собой символические описания и соответствующие вычислительные процедуры.

— Система Wolfram Alpha появилась на свет гораздо позже — в 2009 г. И это один из множества вариантов создания систем ИИ на базе определённой теоретической модели. В моей жизни было несколько этапов, в рамках которых мне довелось разрабатывать различные универсальные теоретические модели из сферы ИИ и руководить созданием ряда прикладных систем, которые в англоязычных источниках принято называть knowledge-based (то есть основанными на знаниях). Они предназначались для комплексной интерактивной аналитической обработки гетерогенных информационных потоков в темпе их поступления от распределённых источников и с использованием больших объёмов накапливаемых гетерогенных (опять-таки!) данных. По сути, это knowledge-based OLAP (On-Line Analytic Processing).

ИСТОКИ ОВЕРХАЙПА

— С нейронными сетями в каких-либо их ипостасях приходилось встречаться?

— Конечно. Однако следует сказать, что нейронные сети в рамках всего комплекса исследований в области искусственного интеллекта были всё это время достаточно

Джеффри Хинтон

маргинальным направлением — оно приносило определённый практический эффект в ряде конкретных задач обработки зрительных образов, аудиограмм и радиосигналов, да и некоторых оптимизационных задач. И этот эффект был следствием использования нейросетей как природоподобной модели вычислений с массовым параллелизмом, то есть как компьютеров с нетрадиционной архитектурой и своеобразными технологиями конструирования. Поэтому резкий всплеск популярности нейросетей и их перемещение в центр общественного внимания как «цифрового двойника» естественного интеллекта стали для меня некоторой неожиданностью: сегодня де-факто нейросети с глубоким обучением — это мейнстрим в сфере ИИ. Более того, под влиянием оверхайпа, равного которого ни одно направление исследований и разработок в сфере ИИ никогда не имело, произошёл сдвиг в сознании всего человечества. По существу, в массовом сознании «искусственный интеллект» и «нейронные сети» — это синонимы.

— У Вас есть объяснение этого феномена?

— Насколько я могу судить, истоки этого оверхайпа уходят в 2012–2015 гг. В 2012 г. вышла в свет статья Алекса Крижевски, Ильи Суцкевера и их научного руководителя Джеффри Хинтона, в которой были описаны принципы построения 8-слойной свёрточной нейросети AlexNet. Эта сеть, будучи обученной на тестовой базе данных ImageNet из примерно 1,2 млн изображений, которые соотносились с тысячей классов, решала с ошибкой на уровне 15% задачу классификации изображений на фотографиях с высоким разрешением. При этом считалось, что человек решает эту задачу с ошибкой 5%. В 2015 г. появилась 152-слойная нейросеть ResNet, разработанная четырьмя китайскими специалистами из Microsoft, которая на этом же тесте достигла уровня 3%, то есть превзошла человека в точности распознавания. И вот это событие было воспринято не столько научной, сколько околонаучной общественностью как доказательство превосходства нейросетевой парадигмы над всеми остальными направлениями исследований и разработок в области искусственного интеллекта, которые были известны в то время.

Однако наибольший всплеск интереса к нейросетям и настоящий взлёт их планетарной популярности наблюдается с 2017 г., когда были предприняты первые попытки использования нейросетей для работы с массивами текстов и появились большие языковые модели (Large Language Models, LLM), а затем и большие мультимодальные модели (Large Multi-modal Models, LMM). По мере распространения нейроимитаторов текстового, аудио- и видеоконтента (их принято именовать генеративными предобученными трансформерами, GPT) и агрессивного, силового, я бы сказал даже оголтелого, маркетинга росла убеждённость массового пользователя в том, что это и есть искусственный интеллект, способный решать любые задачи не хуже, а то и лучше человека. А массовый пользователь — это экономическая основа успешности ключевых акторов любого сегмента ИТ-рынка.

Результат налицо: например, капитализация основного производителя графических процессоров для нейросетей NVIDIA только за 2023 г. выросла на порядок, точнее в 11 раз (!). Думаю, в аналогичной пропорции выросла прибыль производителей чипов памяти...

Видимо, в рамках журнального интервью нет необходимости углубляться в анализ очевидных базовых ограничений и смысловых нестыковок, присущих нейросетевой парадигме (именно в части нейросетей с глубоким обучением). Гораздо продуктивнее поразмышлять с общенаучных позиций о структуре исследований и разработок в сфере ИИ и его перспективах в обозримом будущем.

О КЛАССИФИКАЦИИ ИИ

— Логично. Тогда нужно дать научную классификацию различных проявлений искусственного интеллекта.

— Как мне представляется, естественный интеллект, присущий любому носителю сознания, имеет три уровня — перцептивный, вербальный и конклюзивный (от английского *conclusion* — умозаключение; не путать с термином «инклюзивный», который соотносится с доступностью, или распространённостью, различных систем и сервисов ИИ). На перцептивном уровне осуществляется онлайн-обработка потоков информации от сенсоров (органов чувств); при этом в каждый конкретный момент времени формируются первичные образы наблюдаемых объектов и реализуется их идентификация, то есть соотнесение с различными характерными признаками, классами, категориями и взаимосвязями между ними. Наблюдаемые объекты и ситуации могут некоторым образом именоваться и, в более широком смысле, отображаться в речь и текст, и это уже вербальный уровень. Однако глубокая интерпретация и в конечном итоге понимание происходящего с последующей генерацией осмысленного отклика на него выполняются на конклюзивном уровне (при этом в процессе интерпретации могут использоваться не только лексемы и фонемы с вербального уровня, но и непоименованные образы непосредственно с перцептивного уровня).

Для моделирования перцептивного уровня достаточно давно и во многих случаях успешно применяется модель нейросети, предложенная ещё в 1943 г. американскими нейрофизиологом Уорреном Маккаллоком и математиком Уолтером Питтсом и использованная в 1957 г. Фрэнком Розенблаттом в качестве базовой модели для проектирования перцептрона. Имманентным свойством этой модели является обучение (хотя правильнее было бы сказать — настройка) сети посредством обучающих выборок (training data sets) — множеств пар «вход-выход», обеспечивающих вычисление весов связей между нейронами для последующего применения нейросети к поступающим на её вход наборам сигналов в режиме реального анализа.

КУДА ВЕДЁТ GEN AI?

— Что нового добавили создатели LLM к классической модели перцептрона и механизма обучения нейросети?

— Большие языковые/мультимодальные модели — это не что иное, как попытка распространить сферу применения нейросетей с глубоким обучением на вербальный уровень, опираясь на весьма странный способ обучения нейросети — прогон всех доступных текстов на конкретном языке с целью извлечения из них информации о допустимых словосочетаниях разной длины и о допустимых разноразмерных текстовых окрестностях каждого слова. Это крайне примитивное лингво-алгоритмическое решение получило глобальное распространение и стало экономически прибыльным для дизайнеров и реселлеров его технических реализаций. Но не столько в качестве средства перевода с одного языка на другой, где оно выглядело бы достаточно естественным, сколько для целого ряда других приложений. А объединяет эти приложения одно общее свойство — отсутствие жёстких требований к качеству и достоверности информации в отклике системы.

Можно согласиться с утверждением, что LLM/LMM достаточно полно отображают синтаксис и поверхностную семантику разговорного языка. Однако претензии апологетов этого направления на решение их девайсами практически любых интеллектуальных задач представляются явно завышенными. BERT-, GPT- и DeepSeek-подобные устройства демонстрируют лишь то обстоятельство, что для прохождения теста Тьюринга, то есть для поддержания беседы на разговорном языке, тестируемому чат-боту совершенно не обязательно подниматься до конклюзивного уровня. Забавными выглядят громкие анонсы успешной сдачи чат-ботами экзаменов по дисциплинам четвёртого курса медицинского вуза, которыми ликующие промоутеры LLM/LMM пытаются доказать достижение их изделиями уровня человеческого интеллекта. На самом деле они доказывают лишь то, что, не обладая вообще никакими знаниями, а всего лишь имея доступ к текстам, смысла которых человек, сдающий экзамен, вообще не понимает, можно сдавать экзамены и получать высокие оценки. Ведь для того, чтобы понимать, нужно выходить на конклюзивный уровень, то есть владеть как минимум базовыми понятиями и набором причинно-следственных связей (ПСС) для генерации новых фактов из известных. А зачем, если можно обойтись и без них? И вот это уже настоящий провал...

— Почему?

— Именно здесь находятся истоки прогрессирующей тотальной депрофессионализации и становления имитократии — власти людей-фейков, которые имеют все формальные признаки наличия у них специальных знаний, необходимых для выполнения ими соответствующих специальных функций и принятия решений, между прочим, влияющих на судьбы и жизни других людей. Однако на самом деле упомянутые люди-фейки упо-

мянутыми специальными знаниями, мягко говоря, не обременены и уже только поэтому являются источником перманентной опасности для управляемых ими социотехнических систем (СТС).

Спрос на услуги по настройке ChatGPT в России за последний год вырос в 3,6 раза (!). Мне приходилось слышать, что 87% российских школьников используют чат-боты для выполнения домашних заданий. Трудно подтвердить или опровергнуть достоверность этой цифры, но то, что такого рода технологии довольно быстро получают массовое распространение, — непреложный факт. Причём не только в школах, но и в вузах, и в науке. Сколько рефератов, статей и, наверное, даже диссертаций в области гуманитарных наук пишется чат-ботами, оценить невозможно. Впору разрабатывать и повсеместно внедрять средства тестирования текстов не только на плагиат, но и на «ботогенность». Впрочем, генерация текстов нейроимитаторами и есть по существу алгоритмизованный плагиат!

ТАК ВОТ ТЫ КАКОЙ, НАСТОЯЩИЙ ИИ

— А как Вы оцениваете тот факт, что сегодня в сознании массового пользователя AI = ML/DL?

— Знаете, меня всегда интересовало, как и кем придумываются термины, которые потом используются специалистами в области информационных технологий по всему миру. Возьмём, например, понятие «интернет вещей». Вообще-то, вещь — это пассивный ресурс, нечто лишённое активности: шкаф, тетрадь, портфель и т.д. Но то, что обозначает аббревиатура IoT, — это на самом деле сеть сетей, объединяющая устройства, которые реализуют некоторые разумные активные функции. Поэтому называть этот объект следовало бы «интернет устройств» (Internet of Devices, IoD). Но весь мир повторяет: Internet of Things...

Или «естественный язык». Для кого и для чего он естественный? Естественный язык для строгого описания физических процессов — это язык дифференциального и интегрального исчисления в сочетании с узкопрофессиональной лексикой. Для описания химических процессов — язык формул химических веществ и уравнений химических реакций в сочетании с несколько иной, но также специфической лексикой. И так далее. А то, что стали в 60–70-е годы прошлого века называть Natural Language, — это не что иное, как разговорный (Conversational) язык.

Что же касается «AI and ML», то всем понятно, что ML — это один из процессов, присущих AI. И говорить «AI and ML» — это то же самое, что говорить «зоология и изучение жизни рыб». Но это ещё полбеды. В словосочетании «машинное обучение» о чём идёт речь, кто кого обучает? Возьмите машинное доение: там машина доит корову или корова доит машину? Очевидно, что верен первый вариант, значит, machine learning — это процесс, когда машина (компьютер) обучает человека! Но весь мир почему-то интерпретирует этот термин с точностью до наоборот: человек обучает машину! По крайней мере, так считалось до появления нейроимитаторов. Но сегодня мы видим не меньше оснований для инвертированной интерпретации термина ML/DL — машина обучает человека!

Обучает тот, кто больше знает, того, кто знает меньше; тот, кто умнее, того, кто глупее (если, разумеется, последнему хочется стать умнее). Вот мы, собственно, и пришли к «власти компьютеров над людьми»...

Я только что вернулся с международной конференции по цифровому образованию (2025 World Digital Education Conference), которая проходила в китайском городе Ухань. В ней приняло участие порядка 4 тыс. специалистов из 70 стран. Я участвовал в работе форума «Искусственный интеллект и образование», и из всего, что я там увидел и услышал, мне особенно запомнился доклад заместителя министра высшего образования, науки и технологии Индонезии под ярким названием Education in the Era of AI: Teaching Humans how to THINK, то есть «Образование в эру ИИ: обучение людей ДУМАТЬ». Презентация доклада завершалась слайдом с портретом Алана Тьюринга и вопросом из его исторической статьи от октября 1950 года: «Can machines think?». Но в данном случае вопрос звучал так: «Can YOU think?». (В скобках заметим, что Индонезия сегодня — восьмая экономика мира, четвёртая страна по численности населения в 280 млн человек, с динамично развивающейся наукой и техносферой).

НЕ О «ВОССТАНИИ МАШИН»

— Но это же не привычная страшилка о восстании машин и порабощении ими человечества?

— Это о том, что растёт поколение людей, которых в англоязычных странах именуют NEET (Non-Employed, Educated and Trained), то есть не работающие, не образованные и не обученные. И самое страшное — ровно то, о чём говорилось в упомянутом мною докла-

де — не умеющие думать! Потерявшие главный Божий дар — способность мыслить. Вся их жизнь проходит по существу виртуально и состоит в бесконечном пережёвывании информационного фаст-фуда из интернета. Это тёмная обратная сторона распространения интернет-зависимости людей, крайней формой которой стало общение с разговорным ИИ на основе LLM/LMM. Именно отсюда начинается тотальное оглупление человечества и возникают вполне оправданные опасения относительно возможности получения искусственным интеллектом управления над социумом.

Мы создали и продолжаем развивать техносферу, которая делает жизнь людей всё более комфортной. Однако эта техносфера для поддержания её в работоспособном состоянии требует от социума разнообразных специальных знаний и перманентных интеллектуальных усилий, на которые значительная его часть, отвыкшая думать, может оказаться неспособной. В итоге техносфера может перейти в режим необратимого саморазрушения, которое, в свою очередь, приведёт к деградации, а то и гибели социума...

Иными словами, ИИ на стадии «суперинтеллекта», как любят говорить околонаучные евангелисты нейросетевой парадигмы, может получить управление над социумом совсем не потому, что этот «суперинтеллект» превзошёл хотя бы средний интеллектуальный уровень людей, а потому, что последний понизился настолько, что люди вследствие собственной интеллектуальной лени стали функционировать под управлением наипримитивнейших и непредсказуемых программно-аппаратных объектов, изготовленных опять-таки далеко не самыми толковыми и грамотными инженерами. Которые, очевидно, решали одну-единственную задачу — максимизировать прибыль от массового внедрения своих незатейливых изделий.

ХИНТОН ПРОТИВ АЛЬТМАНА

Собственно, в этом, на мой взгляд, лежит корень разногласий Д. Хинтона с С. Альтманом и причина ухода Хинтона из Google в 2023 г. Джеффри Хинтон как Учёный с большой буквы и ответственный человек, безусловно, хорошо понимает, к чему ведёт массовое распространение LLM/LMM и чат-ботов на их основе. Мне его поступок вполне понятен. С некоторыми людьми из нейросетевого комьюнити действительно достаточно сложно общаться по причине их фанатичной убеж-

Сэм Альтман

дённости в том, что нет такой задачи, которую не решила бы обученная на примерах «вход — отклик» нейросеть, а все другие направления ИИ — просто никому не нужная схоластика. Ведь нейросеть — это «цифровой двойник» человеческого мозга, и этим всё сказано!..

Однако этот «двойник» не способен качественно решать даже рутинные офисные задачи. Как показало недавнее исследование, проведённое британскими специалистами, лучшая из протестированных нейросетей справилась лишь с 24% таких задач, тогда как остальные участники эксперимента показали себя ещё хуже (1,7% и ниже).

— Кстати, нейрофизиологи сегодня предлагают гораздо более сложные модели человеческого мозга, чем классический перцептрон, который положен в основу всех современных нейросетей любой глубины...

— Конечно! Модель нейрона МакКаллока — Питтса стала достоянием мирового научного сообщества в 1943 г., когда ещё не было универсальных ЭВМ с архитектурой фон Неймана, а он, напомним, анонсировал её в 1946 г. Так что авторы ограничили интеллектуальные возможности нейрона пороговой функцией от суммы уровней его входных сигналов. Однако в наши дни известно, что нейрон благодаря наличию в нём пока ещё плохо изученных микротубул реализует гораздо более сложные функции, и, перефразируя известный постулат, можно утверждать,

что нейрон ещё более неисчерпаем, чем атом. Во всяком случае, можно предположить, что это весьма нетривиальный компьютер.

А если говорить о мозге в целом, то он состоит не только из 86 миллиардов таких компьютеров и триллиона связей между ними, но и из глиальных клеток, реализующих функции памяти. Этого хранилища информации в модели МакКаллока — Питтса нет — от слова совсем, — и нейроматематикам приходится придумывать разные модификации базовой модели, типа, например, рекуррентных нейросетей, чтобы отобразить хотя бы наличие факта запоминания.

Кстати, относительно недавно кто-то из учёных заметил, что в настоящее время на Земле функционирует примерно такое же количество различных вычислительных устройств — 86 миллиардов, и в этом смысле вся наша планета является моделью человеческого мозга. Тогда что представляет собой функционирование этой мегасети устройств — «планетарного мозга» — с позиций нейросетевой парадигмы? Подаём на вход некоторых из упомянутых устройств единичные сигналы, измеряем интенсивность трафика между этими и связанными с ними устройствами, и, применяя пороговую функцию, определяем, какие из них будут «активированы», то есть сформируют единичные сигналы на своих выходах. И далее по всей планете. А что есть в этом случае «глубокое обучение»? Да просто вычисление значений интенсивностей трафика в соединениях между устройствами. Аналогия, думаю, понятна. Она со всей очевидностью показывает, что триллион синаптических связей между нейронами — это не более чем коммуникационная инфраструктура для информационного обмена между ними, и приписывать ей иное, более широкое, участие в функционировании мозга вряд ли уместно.

К тому же несостоятельность эксплуатируемых сегодня подходов к моделированию интеллектуальных функций на основе искусственных нейросетей МакКаллока — Питтса становится более чем очевидной, если сопоставить энергопотребление человеческого мозга (20–21 Вт) и нейросетевых компьютеров, реализующих LLM/LMM (мегаватты), не говоря уже об их габаритах, растущих по мере возрастания числа элементов нейросети, то есть её «интеллектуальных» возможностей.

Уместно заметить, что в наши дни 25% электроэнергии, вырабатываемой энергосистемой США, потребляется центрами обработки данных. Конечно, ЦОДы реализуют массу других функций, и применение больших языковых/мультимодальных моделей пока не главная из них, но совершенно бессмысленный вклад переработки огромных массивов текстов для обучения чат-ботов в эту непостижимую цифру, несомненно, растёт... Как и вклад майнинга криптовалют, коих в мире уже более 8 тысяч... Вот и Илон Маск высказался в том смысле, что распространение ИИ уже в 2025 году может быть ограничено в связи с нехваткой электроэнергии...

Но Сэм Альтман и его паства не оставляют усилий, направленных на развитие своего коммерческого успеха...

ЧТО ВМЕСТО НЕЙРОСЕТИ?

— Если настоящий интеллект появляется только на конклюзивном уровне, то в чём заключается его принципиальное отличие от вербального уровня, на котором функционируют нейросети и LLM/LMM?

— Приведу очень простой пример. Задаём чат-боту вопрос: сколько лет Овечкину? В базе чат-бота есть уйма текстов с упоминанием знаменитого хоккеиста, относящихся к различным датам. В одном тексте он значится двадцатилетним, в другом — ему 35 лет и т.д. Что ответит бот? А что угодно... Что извлечёт его совершенно непрозрачный недетерминированный алгоритм генерации ответов из накопленной базы («корпуса») текстов и какие слова в него подставит. В лучшем случае выберет биографическую статью из «Википедии». Вот это и есть вербальный уровень, на котором работает бот. Я уж не говорю о нередких случаях так называемых галлюцинаций, когда бот начинает говорить вообще не пойми о чём — во всяком случае, не о том, что интересует его собеседника...

— А как эта задача решалась бы на конклюзивном уровне?

— Если бы эта задача решалась на конклюзивном уровне, то отбирались бы тексты, в которых содержится дата рождения Александра, фиксировался текущий момент времени, и из этих двух значений определялась искомая величина. Но для того чтобы это произошло, бот должен обладать соответствующей причинно-следственной связью (ПСС), то есть умозаключением (conclusion), применив которое он мог бы выдать нам правильный ответ. Таким образом, бот, работающий на конклюзивном уровне, должен иметь базу знаний как совокупность ПСС и уметь её применять для получения таких фактов, которые в явном виде в базе

текстов отсутствуют. В математической логике подобные процессы именуются дедуктивным выводом.

ОБ ИНЖЕНЕРИИ ЗНАНИЙ

— Откуда эта база знаний возьмётся у бота?

— Для начала от людей, ответственных за обучение ботов. Издавна (с 80-х годов прошлого столетия, когда появились экспертные системы) они именуются инженерами знаний (knowledge engineers). Однако как раз необходимость их участия в обучении всегда считалась специалистами по нейросетям слабым местом систем с базами знаний (БЗ): сначала нужно знания получить от экспертов (этот этап принято назвать knowledge acquisition, то есть приобретение, или извлечение, знаний), да ещё с поправкой на субъективность полученных знаний, их неполноту, недостоверность, противоречивость и так далее. В то же время для обучения нейросети вообще никаких людей не требуется: достаточно направить на входы и выходы сети обучающую выборку и через какое-то время получить готового оракула, способного решить любую задачу из рассматриваемого класса.

Правда, здесь сразу возникает ключевой вопрос: до какой степени использованная выборка репрезентативна с точки зрения применения обученной нейросети в будущем? Иными словами, выборки от сегодняшнего и от завтрашнего дня одинаковы (или хотя бы похожи, что бы под этим ни понималось)? А если нет, то для чего нужно такое обучение и такая нейросеть?!

Похоже, в нейросетевом сообществе не принято оперировать такими ключевыми понятиями инженерии знаний, как интенсионал и экстенсионал базы знаний. Интенсионал — это совокупность ПСС, то есть собственно БЗ. А экстенсионал — это совокупность фактов, которые можно получить из некоторого исходного множества фактов (базы данных), применяя ПСС к ним и новым фактам, полученным на предыдущих шагах применения упомянутых ПСС (неважно, делается это человеком или системой логического вывода, СЛВ). Иными словами, экстенсионал — это множество фактов, каждый из которых можно в явном виде или в результате некоторых цепочек рассуждений получить от системы с конклюзивным ИИ. Сформулировав и передав системе запрос с указанием, какого рода факты нас интересуют, мы получим ровно те элементы экстенсионала, которые соответствуют запросу (в общем случае таковых может быть несколько). При этом за каждым таким фактом будет находиться обосновывающая его цепочка рассуждений (то есть применённых ПСС), которая может быть предоставлена автору запроса для объяснения, почему этот факт имеет место. Нейросеть же не рассуждает, а просто выдаёт вам отклик на обращение, и понять, почему он именно такой, а не другой — это ваша проблема...

Как ребёнка учат перемножению целых чисел? Дают базу фактов, называемую таблицей умножения (1 × 1 = 1, 1 × 2 = 2, ..., 9 × 9 = 81), и совокупность правил (то есть ПСС), позволяющих перемножать числа любой длины на основе этих фактов. Таким образом, в рассматриваемом случае экстенсионал — это множество фактов вида $x \times y = z$, где x, y и z — целые числа. А как будут учить умножению в рамках нейросетевой парадигмы? Построят нейросеть с $m + n$ двоичными входами и k двоичными выходами (здесь m, n и k — число двоичных разрядов максимальных допустимых значений x, y и z). И начнут подавать на вход и выход обучающие триплеты $\langle x, y, z \rangle$, выбранные некоторым случайным образом. Что будет способна выдать нам по запросам сеть, обученная на миллиарде таких триплетов? Как бы странно это ни прозвучало, но я не убеждён, что результатом подачи на вход обученной таким образом сети чисел 80 и 12 будет появление на её выходе числа 960...

При этом в инженерии знаний вопросы самообучения интеллектуальных систем, естественно, также рассматриваются, но это делается на корректном фундаменте индуктивного вывода, целью которого является формирование новых причинно-следственных связей, исходя из фактов и ПСС, уже имеющихся в базе знаний. (Это направление ассоциируется в массовом сознании с Data Mining.)

Естественно, по мере развития теории и практики нейросетей от множества иллюзий, возникших на волне оверхайпа, пришлось избавляться. Сначала появилось «обучение с учителем», затем «обучение с подкреплением», и наконец — промпт-инженеры (prompt engineers), которые, как сказано в «Википедии», «используют знания в области лингвистики, логики и машинного обучения для структурирования входных данных таким образом, чтобы добиться от модели высокой точности, когерентности и предсказуемости». В общем, от чего ушли, к тому и вернулись...

БИБЛИОТЕКАРИ И КОУЧИ

Вот только эффективность и ценность инженера знаний на порядки выше, ибо он выполняет гораздо более нужную работу, чем компенсация примитивизма и «косоватости» базовой лингво-алгоритмической платформы, которая, что ни делай, в силу заложенных в неё сомнительных базовых принципов умнее и полезнее не станет. Инженер знаний, загружая и корректируя ПСС, реально используемые для интеллектуальной обработки входных информационных потоков и обслуживания потребителей результатами этой обработки, перманентно поддерживает интеллект системы в состоянии, адекватном текущим запросам потребителей и особенностям первичных сведений, поступающих от их источников.

Иными словами, промпт-инженер — это библиотекарь, тогда как инженер знаний — это коуч, время от времени корректирующий логику функционирования опекаемой им системы посредством локальной коррекции её базы знаний. При этом фронтенд-библиотекарь — по определению «узкое горло» системы, которая в силу этого принципиально не способна вести обработку достаточно интенсивного потока запросов. Сколько таких специалистов нужно, чтобы подобную обработку реализовать? Сколько им нужно платить? И какова будет полная стоимость владения такой системой? Это все вопросы, не предполагающие практически приемлемых ответов. С другой стороны, бэкенд-коуч никоим образом не лимитирует возможности системы по обработке входного потока просто потому, что он в ней не участвует, ограничиваясь далеко не столь частыми операциями коррекции базы знаний в офлайне.

Как говорится, почувствуйте разницу: люди, обучая друг друга (родители — ребёнка, учитель — ученика, преподаватель — студента и т.д.), передают знания в виде фактов и более или менее общих причинно-следственных связей. При этом человек всю свою жизнь старается вывести из имеющихся у него ПСС новые, более общие, универсальные, инвариантные к особенностям непредсказуемых ситуаций будущего. И в этом, собственно, заключается суть мозговой активности человека. А обучение посредством обучающих выборок — это уровень формирования условных рефлексов наподобие опытов с собакой Павлова. То есть простейших ПСС типа «стимул — реакция».

Кстати, в связи с промпт-инженерами вспомнился забавный случай. Стартап под названием BuilderAI анонсировал создание нейросети Natasha, способной разрабатывать любые программы по заказу пользователей. За восемь лет своего существования эта компания привлекла 500 млн долл., причём среди её инвесторов оказался даже Microsoft. Всё бы ничего, только при ближайшем рассмотрении Natasha оказалась софтверхаусом из более чем 700 программистов, которые и разрабатывали требуемые программы. То есть естественный интеллект выдавал себя за искусственный. Сколько ещё таких «нейросетей» на нашей планете? Это история про человеческую наивность, манипулируемость и некритичность мышления. То есть снова о том, как люди теряют навыки мышления...

О МАТЕМАТИКЕ НАСТОЯЩЕГО ИИ

— Наверное, для организации функционирования реально интеллектуальной системы важно учитывать, что упомянутые Вами запросы потребителей к базе знаний и первичные сведения зачастую подвержены изменениям?

— Я уже упоминал в начале нашего разговора, что на одном из этапов моей профессиональной деятельности мне пришлось заниматься созданием систем класса knowledge-based OLAP. Именно в силу крайне изменчивых условий функционирования объектов, для которых разрабатывались эти системы, и, как следствие, вариативности логики обработки поступающей информации реализация упомянутой логики в виде «жёстких», то есть не модифицируемых на местах эксплуатации, программ была практически невозможна. С другой стороны, те модели представления знаний (фреймы, семантические сети, продукции, клаузулы Хорна и т.п.) и принципы построения интеллектуальных («экспертных») систем на их основе, которые в то время (80-е годы прошлого века) были известны, находились заведомо далеко по своим возможностям от требуемого уровня. (Апологеты GenAI называют этот ИИ «слабым», и здесь с ними можно согласиться.) К тому же повсеместно использовавшиеся тогда реляционная модель данных и реляционные СУБД не обеспечивали работу с неформализованными данными: текстовыми, битовыми, мультимедийными.

В этой ситуации я взял на себя смелость разработать и реализовать совершенно «перпендикулярный» подход к моделированию данных и знаний, взяв за основу логические формализмы, оперирующие строками символов — системы Поста и формальные грамматики Хомского. При этом база данных представляла собой множество фактов — строк (текстов), структура которых задавалась базой

метаданных — множеством контекстно-свободных порождающих правил. А база знаний, представлявшая собой совокупность расширенных продукций Поста, обеспечивала формирование новых фактов из имеющихся в базе данных и полученных на предыдущих шагах логического вывода. При этом разработанные методы сокращения избыточного перебора в процессе вывода (включая ассоциативный доступ к фактам) исключали комбинаторный взрыв по мере роста объёма баз данных и знаний и обеспечивали обработку входного потока сообщений в темпе их поступления.

SIEM КАК ПРИМЕР

— Каких результатов в моделировании ИИ удалось в результате достичь?

— Оценивая то, что было тогда сделано, можно сказать, что была предпринята вполне успешная попытка разработать интеллектуальную технологию, охватывающую единой универсальной моделью представления знаний конклюзивный и вербальный уровни ИИ[1].

В пользу практичности и универсальности предложенного тогда математического аппарата и основ его реализации свидетельствует его успешное применение в такой, казалось бы, далёкой от исходных областей применения сфере, как системы SIEM (Security Information and Event Management).

SIEM — это системообразующее средство обеспечения кибербезопасности, обеспечивающее выявление на ранней стадии признаков подготовки и проведения сложных кибератак на основе комплексной интеллектуальной обработки потоков сообщений от локальных средств защитного периметра (межсетевых экранов, антивирусов, IDS/IPS, DLP и т.п.). При этом база знаний системы SIEM, во-первых, отображает логику анализа alarm-сигналов и фрагментов сетевого трафика (битовых и/или текстовых строк) от упомянутых средств в жёстком реальном времени. А во-вторых, оперативно корректируется инженером знаний по мере поступления от инженеров по анализу угроз и белых хакеров выявленных ими причинно-следственных связей, которые позволяют вскрыть вторичные глубокие признаки и состояние ведущейся атаки.

Скажу откровенно: более сложного и при этом практически ценного приложения ИИ я не знаю. Это как раз тот случай, когда искусственный интеллект должен превосходить и реально превосходит естественный.

[1] Детальное описание подхода содержится в монографии «Интеллектуальные программные среды для АСОИ», выпущенной издательством «Наука» в 1994 г. Краткое введение в математические и реализационные основы подхода и описание его State-of-the-Art по состоянию на 2019 г. — в главах «Augmented Post Systems: Syntax, Semantics, and Application» и «Set-of-Strings» Framework for Big Data Modelling» сборника «Introduction to Data Science and Machine Learning», доступного онлайн.

Причём интеллект не среднего человека и тем более не NEET-а, а самый что ни на есть изощрённый, носителем которого являются киберпреступники, обладающие просто эзотерическими знаниями в области хакинга и фантастической изобретательностью. И это превосходство ИИ есть величайшее благо для социума! Именно так и должно строиться взаимодействие искусственного и естественного интеллекта.

РОЛЬ ИИ В РЕАЛЬНОЙ ЭКОНОМИКЕ

— Каким образом эти представления о функционировании ИИ находят отражение в реальных процессах создания интеллектуальных систем в нашей стране?

— Важно, что в последние годы в нашей стране много и громко говорится о технологической независимости. Однако до сих пор эти дискуссии, да и практические действия также сосредоточиваются на замещении импортной элементной базы и программного обеспечения аналогами отечественного производства, вкупе с призывами выйти на лидирующие позиции по ключевым направлениям научных исследований.

Мне представляется, что основой технологической независимости России должна быть её интеллектуальная независимость. А это подразумевает в первую очередь рациональное целеполагание, то есть выбор реально значимых для нашего общества на данном этапе его существования направлений исследований и точек приложения драгоценного и, скажем прямо, не очень многочисленного интеллектуального ресурса.

У нас, к сожалению, нередко решающую роль в упомянутом выборе играет своеобразный научный снобизм, то есть, по сути, некритичное копирование структуры исследований и разработок, реализуемых в США. Этот снобизм подпитывается оценкой эффективности работы российских учёных на основе индексов Хирша и иных наукометрических показателей, отражающих их вклад в развитие научных направлений, реализуемых в западных странах. Помимо того, что эти направления могут быть для нашей страны, мягко говоря, не особенно актуальны, они ещё и могут быть откровенно бессмысленными и тупиковыми даже для самих упомянутых западных стран.

— А западная модель бизнес-ориентированности передовых разработок эффективна для сферы ИИ и всей области ИТ?

— Бизнес-ориентированная модель спонсирования разработок в ИТ-секторе, которая применяется сегодня, — это, по существу, краудфандинг, что предполагает наличие массового покупателя этих разработок. Поэтому на ИТ-рынке процветают те компании, которые могут путём активного силового воздействия на массовое сознание приобрести указанного массового покупателя. Пример LLM/LMM и, как его иллюстрация, «нейросети» Natasha в этой части особенно показателен.

Другой не менее показательный пример — блокчейн. Промоутеры этой технологии некоторым образом сумели внедрить в массовое сознание восприятие её как чего-то сверхбезопасного и сверхэффективного, сыграв на желании части населения иметь неконтролируемые правоохранительной системой доходы в криптовалюте. А в результате получилось с точностью до наоборот!

БЛОКЧЕЙН КАК ЕЩЁ ОДИН ВИД ОВЕРХАЙПА

— Поясните, пожалуйста!

— Смотрите. Взломать систему обеспечения кибербезопасности банка — дело практически нереальное даже для киберпреступников экстра-класса. В то же время получить доступ к терминальному устройству клиента этого банка (установить на этом устройстве свой «троян») — задача хотя и не простая, но вполне решаемая. (Как правильно говорят банковские киберсекьюрити, деньги крадут не у банка, а у его клиентов.) Однако, даже решив эту задачу, злоумышленник получит доступ к банковским счетам только одного клиента, чьё устройство он поставил под контроль. Но если злоумышленник поставил под контроль устройство одного из участников блокчейна, то он получил доступ ко всему блокчейну, то есть ко всем переводам криптовалюты между его участниками (как к истории, так и к текущим операциям в реальном времени)!

А с другой стороны, правоохранительным органам для получения полного контроля над операциями в криптовалюте всех членов подозрительного социума, использующих блокчейн, достаточно внедрить в него одного-единственного инсайдера. «Большой секрет для маленькой такой компании», каковым он замышлялся изобретателями биткойна, при попытке его некритичного распространения на более-менее многочисленные и по определению незамкнутые социумы на деле оказался совсем не секретом, а наоборот. Я уже не говорю про совершенно бессмысленную репликацию одной и той же базы данных на устройствах всех участников блокчейна.

— Почему это действие Вы считаете бессмысленным?

— Очевидно, что никто из этих участников не будет наращивать память своего терминала до бесконечности. А значит, он будет сливать всю цепочку операций блокчейна в облако, то есть в некоторое централизованное хранилище с непрозрачной системой администрирования и управления, где эта цепочка с весьма ненулевой вероятностью может стать достоянием лиц, внешних по отношению к участникам блокчейна. То есть опять, как и в случае появления профессии промпт-инженера LLM/LMM, — от чего ушли, к тому и пришли, только ещё хуже... В абсолютном выигрыше снова только производители памяти для систем хранения данных... Но ведь реально на это ведутся миллионы людей. И всё это под названием «системы распределённых реестров» на базе всё того же некритичного восприятия популярных за рубежом направлений технологического развития массово проникло в российскую информационную инфраструктуру.

Я уже не говорю о вопросах кибербезопасности с точки зрения установки на упомянутых миллионах интернет-терминалов бесплатного freeware-софта, реализующего доступ ко всем расхайпованным сервисам. Что этот софт в реальности делает, к каким ресурсам получает доступ, никто никогда не проверяет и проверять не будет. А потом изумляемся терабайтным DDoS-штурмам сервисных порталов и изощрённой скрытой инфраструктуре APT-атак с прокси-цепочками из десятков скачков, скрывающих источники этих атак...

КТО И КАК ЛОВИТ РЫБКУ В ВОДАХ ИИ

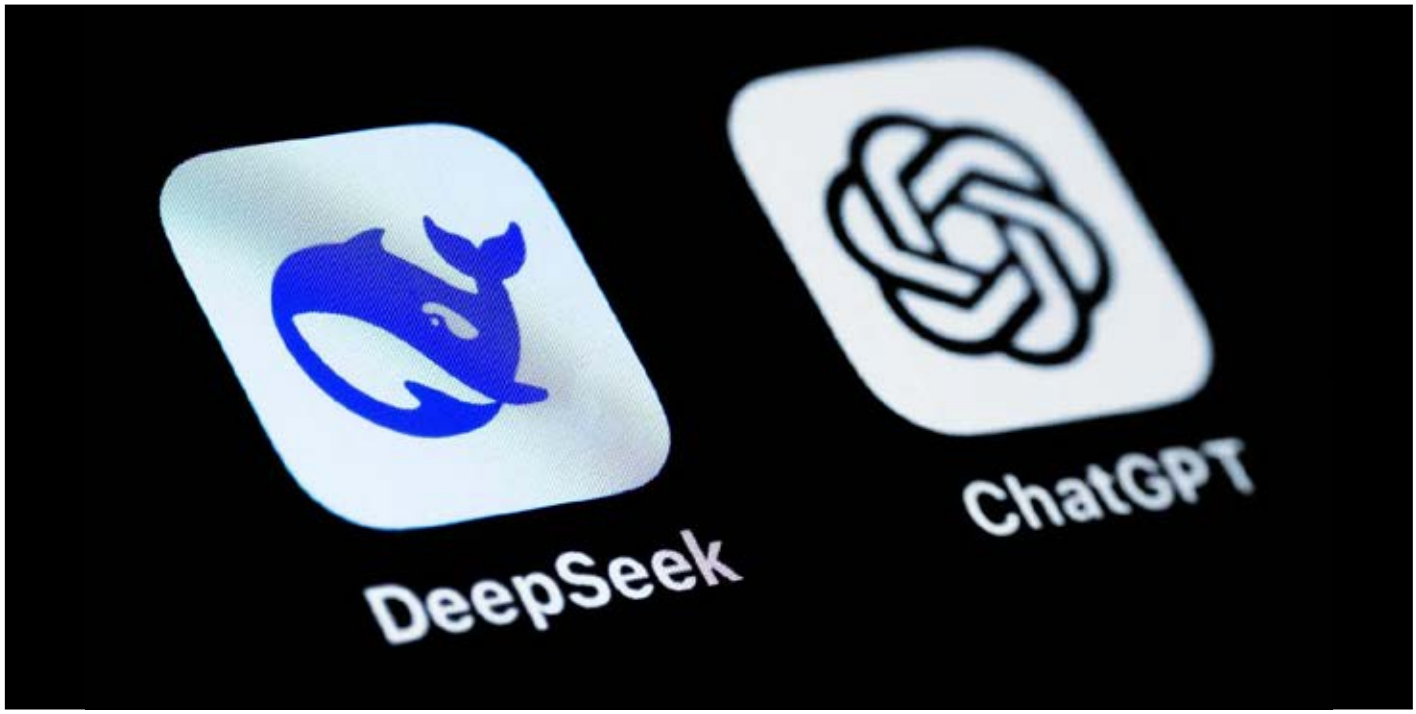
— Это приносит большие дивиденды родине этих технологий?

— Я бы не сказал... Сами американцы, в первую очередь законодательная власть, бьют тревогу относительно состояния своего научно-технологического сектора — того, что они именуют STEM (Science-Technology-Engineering-Mathematics). По их оценкам, США уже давно не в лидерах мирового рейтинга STEM, и способов вернуть их на лидирующие позиции пока не видно. В индексе готовности к внедрению передовых технологий (Frontier Technologies Readiness Index), опубликованном в 2025 году Конференцией ООН по торговле и развитию (UNCTAD), США на 2-м месте после Китая по уровню исследований и разработок (R&D), на 4-м месте по уровню развития информационных и коммуникационных технологий (ICT) и, что уж совсем плохо, на 17-м месте в мире по уровню обученности персонала (Skills Rank) и уровню готовности промышленности (Industry Rank).

Деньги и комфортные условия для работы талантливых учёных и инженеров теперь могут предложить многие страны, а население США всё больше и больше состоит из NEET-ов. Всем известно, чем закончилась попытка перенести производство широкой номенклатуры чипов из Китая на территорию США: оказалось, что специалистов, способных решить эту задачу, в Штатах попросту нет (более чем убедительное подтверждение семнадцатых мест в упомянутых Skills Rank и Industry Rank). И введя заградительные пошлины на китайские товары, американский президент их очень быстро отменил в части комплектующих для производимых в США компьютеров, смартфонов и телекома, ибо в ином случае их стоимость выросла бы до величин, исключающих их приобретение массовым покупателем. (Это, кстати, к вопросу об американской системе целеполагания, предсказательного моделирования и оценки последствий принятия политических решений на высшем уровне.)

Сложившаяся благодаря распространению социальных сетей и мессенджеров американская «экономика внимания», которую правильнее называть «экономикой созерцания», предполагает переток финансовых средств от массового потребителя интернет-контента к наиболее ловким и удачливым его изготовителям (не хочется называть их производителями, ибо никакого производства там нет) и массовое перемещение населения из реального в виртуальный мир, в котором те же NEET-ы и существуют. Известный лозунг Make America great again! — это, с одной стороны, признание того, что Америка сейчас вообще-то не great, а с другой — не очень понятно, как они смогут это сделать с неуклонно тупеющим населением.

Буквально сегодня по новостным лентам разлетелось сообщение о том, что «нейросеть GPT-4 способна в 64% случаев более убедительно отвечать на вопросы оппонентов в социально-политических дебатах и аргументировать свою позицию с учётом воззрений оппонента, чем реальные пользователи глобальной сети». В общем, в США дело явно идёт к тому, что нейроимитатор (AI Being) в обозримом будущем примет участие в президентских выборах, в ходе предвыборных дебатов победит своих оппонентов из числа людей (Human Beings) и будет избран президентом Соединённых Штатов... Это крайняя



форма имитократии и есть ровно то самое «восстание машин», о котором Вы упомянули в одном из своих предшествующих вопросов. Однако истоком этого «восстания» является совсем не нейросетевой «суперинтеллект», а человеческая, мягко говоря, инфантильность.

О НЕЗАВИСИМОСТИ

К сожалению, мы со своим сформированным за последние тридцать с лишним лет нашей истории провинциальным отношением ко всему американскому продолжаем следовать за США в кильватере, хотя без устали говорим о своём стремлении к научно-технологической независимости. Однако понимаемая таким образом независимость — это в ряде случаев не более чем копирование российскими специалистами далеко не самых нужных нашей стране и не самых качественных зарубежных технологий и образцов техники.

О КИТАЕ

— Китай можно рассматривать как пример правильного понимания интеллектуальной независимости на уровне целой страны?

— Да. Именно китайские учёные и инженеры на практике показывают, что такое интеллектуальная независимость страны. Мне вспоминается российско-китайский форум по цифровой экономике 2023 года, где мне довелось быть спикером на пленарном заседании наряду с профессором Гун Ке, исполнительным директором Китайского института стратегии развития искусственного интеллекта нового поколения. Его доклад имел ошеломляющий подзаголовок: From Chat — to AI, from AI — to Real Economy. И здесь все понятия правильно расставлены по своим местам. Сегодняшним чат-ботам очень далеко до «настоящего» ИИ, а ему, в свою очередь, — до задач реальной экономики. И хотя в номинации Chat непонятно откуда взявшийся китайский продукт DeepSeek мгновенно посрамил Сэма Альтмана и его распиаренные изделия, попутно заметно уронив капитализацию NVIDIA, понятно, что это далеко не мейнстрим для практического приложения многочисленного и рафинированного интеллектуального ресурса китайской науки. Хотя, заметим, по количеству публикаций и патентов в области нейросетей учёные из КНР традиционно в лидерах мировых рейтингов. А упомянутый DeepSeek — это как бы побочный продукт эволюции: «Хотите чат-бот? Можем и такое. Нет проблем. И заодно замкнём на себя немалые финансовые потоки краудфандинга разработок чат-ботов».

В таком же русле развития несколько раньше TikTok — китайская альтернатива Instagram и Facebook — продемонстрировал лавинообразное распространение по территории США и совершенно не случайно был признан американским конгрессом угрозой их национальной безопасности.

Китайский сегмент мировой ИТ-индустрии мне знаком не понаслышке. С 2024 г. я являюсь почётным членом (Fellow) Китайской компьютерной федерации (China

Computer Federation, CCF) и приглашённым профессором-руководителем (Chair Professor) Харбинского политехнического университета — фактически китайской Бауманки. В русле этой деятельности делюсь с китайскими коллегами знаниями в области интеллектуальных технологий поддержки значимого для развития китайской экономики программно-целевого планирования с обратной связью. В первую очередь речь идёт о разрабатываемой мною с 2005 года теории рекурсивных мультимножеств и её приложениях к задачам системного анализа, исследования операций, цифровой экономики, а в последнее время и к естественным наукам (в частности, инжинирингу химических реакций[2]). Данная теория — это не что иное, как математическая основа указанных технологий.

...И О РОССИЙСКОЙ НАУКЕ

— Почему это так заинтересовало Ваших учёных коллег из Китая?

— Насколько я могу судить, мой подход заинтересовал коллег обратной методологией разработки ассистивного ИИ, предназначенного для оптимизации управления большими социотехническими системами, то есть, по существу, для реализации обратного перехода «from Real Economy — to AI». Иными словами, не испытывать методом проб и ошибок, какая из вновь появляющихся моделей и технологий ИИ окажется наиболее пригодной для применения в процессах управления экономикой, а разработать технологию, изначально ориентированную на решение задач планирования и управления в больших системах. Причём разработать, начиная с математического аппарата и модели представления знаний и до уровня решения на их основе задач предсказательного моделирования, то есть прогноза последствий от принятия тех или иных управленческих решений.

Так вот. Взяв мультимножества в качестве базовой модели данных и распространив на неё логику разработки расширенных систем Поста, оперирующих строками символов, удалось сконструировать простой в освоении и применении, гибкий и универсальный математический аппарат — мультимножественные грамматики и метаграмматики. Мультимножество отличается от множества наличием в нём повторяющихся элементов. Например, рубль и юань — это множество из двух различимых объектов, тогда как 3 рубля и 5 юаней — это мультимножество из двух мультиобъектов, каждый из которых состоит из своего количества неразличимых объектов. Мультимножества — это естественный язык для представления наборов (комплектов, коллекций) разнородных ресурсов и в конечном итоге ресурсных баз социотехнических и технических систем. Мультимножественные грамматики — столь же естественный язык для представления технологических баз таких систем, то есть множеств входящих в их состав устройств, перерабатывающих входные наборы ресурсов в выходные. Экстенсионал мультиграмматической базы знаний — это множество наборов ресурсов, которые может произвести технологическая база системы, имея её исходную ресурсную базу. Заказ — это набор ресурсов, который нам необходим. Система логического вывода, приняв заказ, формирует множество возможных способов получения выходного мультимножества, то есть возможных производственных цепочек, каждая из которых обеспечивает получение требуемого набора ресурсов. Указав, какими ресурсами мы располагаем, мы получим от СЛВ, по существу, план (целевую программу) работы социотехнической системы по выполнению заказа, которое в данном конкретном случае и есть цель её функционирования. Эта базовая технология может применяться в огромном количестве постановок, модификаций и содержательных интерпретаций для решения широкого круга интеллектуально сложных практических задач большой размерности. При этом все они решаются посредством дедуктивного вывода, то есть применением неизменной базы знаний, соответствующей неизменной технологической базе СТС.

Мультимножественные метаграмматики — инструмент индуктивного вывода, то есть, с практической точки зрения, решения задач

[2] Введению в эту теорию посвящена монография «Рекурсивные мультимножества и их приложения», вышедшая в издательстве «Наука» в 2010 г.

Наиболее полное изложение текущего состояния в этой области – в монографии «Multigrammatical Framework for Knowledge-Based Digital Economy», выпущенной в издательстве Springer Nature в 2022 г.

Вопросы применения мультимножественных грамматик в химии рассмотрены в статье «Мультимножественные грамматики как базовая модель представления знаний для интеллектуальных систем инжиниринга химических реакций», опубликованной в Докладах Российской академии наук. Серия «Химия, науки о материалах» в 2024 г.

Взаимосвязи мультиграмматического фреймворка и нейросетевой парадигмы исследуются в статье «Multigrammatical modelling of neural networks», вышедшей в 4-м номере журнала «Computer Optics» за 2024 г.

синтеза социотехнических систем (например, киберфизических производств), способных выполнять требуемые функции в заданных условиях. При этом в процессе вывода база знаний изменяется, что обеспечивает планирование процессов производства средств производства и последующего применения последних, без ограничений на количество уровней. Например, один 3D-принтер печатает другой, тот — третий — и т.д., а любой из этих принтеров может печатать финальные изделия определённых классов либо их комплектующие. СЛВ обеспечивает порождение всех таких производственных цепочек, а значит, и вариантов построения производственной системы, и селекцию тех из них, которые соответствуют требованиям, указанным в заказе.

Применение мультимножеств в качестве базовой модели данных мультиграмматического фреймворка (МГФ), среди прочих позитивных последствий, позволяет отказаться от древнего матрично-векторного исчисления как математической основы экономических моделей и в перспективе радикально повысить качество макроэкономического планирования и прогнозирования. До настоящего времени межотраслевые балансы рассчитываются посредством операций над матрицами «затраты — выпуск». А теперь попробуйте составить матрицу размерностью хотя бы тысяча на тысячу (для российской экономики это, мягко говоря, не предел), а потом определить на её основе искомые значения модели Леонтьева и оцените, сколько для этого потребуется времени и вычислительных ресурсов. Да ещё с поправкой на хендмейд-ошибки в упомянутых матрицах, которые потом с большим трудом обнаруживаются и исправляются, после чего расчёты необходимо повторять. Насколько мне известно, в Советском Союзе с его высочайшей, уникальной культурой программно-целевого планирования удалось достичь размерности 350 × 350.

МГФ таких проблем в принципе не создаёт, а для проведения необходимых расчётов на практических размерностях (то есть порождения мультимножеств, удовлетворяющих поставленным ограничениям) не нужны никакие суперкомпьютеры. Это позволяет, в частности, легко реализовать перепланирование в случае выявления недостижимости первоначально определённых целей в рамках выполняемого плана (такое возможно в силу изменения текущего состояния технологической и/или ресурсной базы СТС). Либо обоснованно переопределять цели, если их достижение в силу изменившихся условий никакими планами достичь невозможно. Это и есть программно-целевое планирование с обратной связью на основе предсказательного интеллектуального моделирования последствий принимаемых решений и доказательного целеполагания.

ПРЕИМУЩЕСТВА OK AI

Мультиграмматический фреймворк гармонично и эффективно сочетает в себе достоинства технологий конклюзивного ИИ и классической теории оптимизации. Это есть математический фундамент для создания искусственного интеллекта, основанного на объективных знаниях (Objective-Knowledge-based AI, то есть OK AI), в отличие от ИИ, основанного на субъективных знаниях (Subjective-Knowledge-based AI, то есть SK AI) и поэтому наследующего недостатки rules-based экспертных систем 80-х годов, о которых я говорил ранее, и современных нейроимитаторов. В чём преимущество OK AI?

Во-первых, причинно-следственные связи, вносимые в базу знаний, являются верифицированными и юридически значимыми. Во-вторых, система логического вывода, обеспечивающая применение ПСС, также имеет совершенно однозначную, математически строго определённую, а не эвристическую логику. Подобно алгоритмам поиска оптимальных решений в задачах математического программирования. В результате решения, получаемые системами OK AI, как и в классической теории оптимизации, являются доказательно оптимальными и не нуждаются в дополнительном анализе и верификации, что существенно сокращает длительность цикла управления.

С позиций практической реализации и массового применения МГФ — это базовый инструментарий для реализации стека цифровой экономики, от BI до APS/MES. Система логического вывода МГФ естественным образом реализуется на базе мультиагентной модели вычислений и обладает очевидным потенциалом для создания на её основе линейки дешёвых отечественных RISC-процессоров с нетрадиционной архитектурой и максимально возможным параллелизмом. Я бы мог ещё много говорить об МГФ и его перспективах при соответствующем отношении, но, пожалуй, это выходит за рамки нашего интервью.

— Спасибо! Ну, и пару слов в заключение?

— В заключение скажу лишь одно: умного человека ничем не испортишь. Даже искусственным интеллектом.

Вопросы задавала Елена Покатаева, обозреватель BIS Journal

BIS JOURNAL — «ВОПРОСЫ КИБЕРБЕЗОПАСНОСТИ»: ДИАЛОГ ДРУЗЕЙ

В развитие рубрики «Содружество ИБ» предлагаем дайджест из последних наиболее интересных статей журнала «Вопросы кибербезопасности». Тем более что Игорь Анатольевич Шеремет — герой наших «Бесед с Шереметом» — является председателем его редакционного совета.

АЛГОРИТМЫ СОДЕЙСТВУЮТ КОНТРОЛЮ КРИПТОВАЛЮТНЫХ ТРАНЗАКЦИЙ

Одной из главных проблем, связанных с цифровыми финансовыми активами, является их анонимность и невозможность контроля за нецелевым использованием. Это может стать причиной незаконных операций, мошенничества и финансирования терроризма.

В работе **«Методы машинного обучения в задачах контроля криптовалютных транзакций» (Феклин В. Г., Соловьёв В. И., Корчагин С. А., Царегородцев А. В.)** рассмотрены технологические возможности контроля за оборотом цифровых финансовых активов на примере сети Ethereum. Авторы предложили алгоритм автоматизированной системы по выявлению мошеннических транзакций, методологию их анализа, а также реализовали ряд моделей машинного обучения, позволяющих такие операции идентифицировать. Наилучшие результаты показала ансамблевая модель XGBoost, которая и легла в основу прототипа автоматизированной системы.

По мнению авторов исследования, методы машинного обучения являются эффективным инструментом для контроля криптовалютных транзакций. Они позволяют автоматически обнаруживать аномальные операции, которые могут быть связаны с различными незаконными действиями. Тем не менее рассмотренные в работе методы не являются универсальными и требуют тщательной настройки и обучения для каждого конкретного случая.

ПАТТЕРНЫ ДАЮТ ОТПОР АТАКАМ ОТРАВЛЕНИЯ ОБУЧАЮЩИХ ДАННЫХ

Использование новых технологий, связанных с искусственным интеллектом и машинным обучением, ставит вопрос об их безопасности и надёжности. Защите подлежат не только пользователи и их данные, но и функционирование самих алгоритмов.

При наличии многих исследовательских работ есть пробел в разработке универсальных шаблонных механизмов безопасности, называемых паттернами. В статье **«Паттерн для обеспечения безопасности приложения при угрозе модификации модели машинного обучения» (Корнеев Н. В., Котрини Е. С.)** авторы ставят целью разработать соответствующий механизм защиты.

Согласно банку угроз безопасности информации ФСТЭК России, такая угроза безопасности информации называется УБИ 221. Она может быть осуществлена внешним или внутренним нарушителем путём искажения («отравления») обучающих данных.

Авторами построена микросервисная архитектура для обеспечения безопасности для широкого круга приложений в облачной инфраструктуре. Рассмотрен сценарий атаки отравления обучающих данных. Разработан паттерн безопасности для защиты приложения от такой атаки на основе микросервисов, интегрированных в контейнеры. Включённые метрики ошибок дают возможность гибко настраивать сам паттерн и применять его для широкого круга приложений.

ВЫЯВЛЯТЬ КОМПЬЮТЕРНЫЕ АТАКИ ПОСРЕДСТВОМ ФРАКТАЛЬНОГО АНАЛИЗА

Многочисленные исследования статистических характеристик сетевого трафика и сетевых компьютерных атак (КА) показывают наличие у них свойств фрактальности или самоподобия, а также изменчивость по-

казателей, характеризующих фрактальные свойства. Такого мнения придерживаются авторы работы **«Классификация компьютерных атак с использованием мультифрактального спектра фрактальной размерности» (Шелухин О. И., Рыбаков С. Ю., Раковский Д. И.)**.

Методы фрактального анализа широко используются для обнаружения атак и сетевых аномалий. Вместе с тем во многих исследовательских работах в качестве основного рассматривались традиционные асимптотические методы оценки ФР. Однако, используя методы текущей оценки ФР в скользящем окне в реальном масштабе времени, можно усовершенствовать эти алгоритмы.

Учитывая, что свойство самоподобия наблюдается в широких временных масштабах, наличие в сигнале продолжительных атак и аномальной активности изменяет самоподобную природу трафика, приводит к мультифрактальной структуре обрабатываемых процессов.

Информация о различии ФР обрабатываемых процессов при разном разрешении по времени может быть использована для модификации рассмотренных алгоритмов обнаружения КА, приводя к улучшению показателей классификации методами машинного обучения.

ДЛЯ СИСТЕМ ИИ ВАЖЕН УЧЁТ ВСЕХ РИСКОВ

Как утверждает автор работы **«Специальная модель безопасности создания и применения систем искусственного интеллекта» (Гарбук С. В)**, алгоритмы машинного обучения (МО) обеспечивают эффективное решение различных задач в области автоматизированной обработки данных в условиях отсутствия основанных на знаниях моделей наблюдаемых объектов и процессов.

Наряду с универсальностью применения алгоритмы МО обладают также такими особенностями, как отсутствие полной интерпретируемости, возможность дообучения в процессе эксплуатации систем ИИ (СИИ), высокая актуальность вопросов социальной приемлемости применения СИИ, необходимость сравнения функциональных возможностей СИИ и человека-оператора и др.

Автор рассмотрел в статье, как несоответствие различного рода требованиям, предъявляемым к информационным компонентам систем ИИ, влияет на риски, возникающие при создании и применении этих систем. Анализ показал, что эти риски сводятся к ухудшению функциональных характеристик СИИ, увеличению погрешности их оценки эксплуатантом и компрометации данных, обрабатываемых в системе. Предложенная модель безопасности может быть использована для качественной оценки рисков, возникающих при создании и эксплуатации прикладных систем ИИ различного назначения, и организации мер по снижению этих рисков.

ВИДЕТЬ ПРАВОВЫЕ ГОРИЗОНТЫ ТЕХНОЛОГИЙ ИИ

По мнению многих экспертов, термин «искусственный интеллект» не относится к какой-либо конкретной технологии — скорее это собирательный термин для множества технологий использования математико-статистических методов для моделирования когнитивных способностей. В связи с этим важно установить современное понимание ИИ, считают авторы работы **«Правовые горизонты технологий искусственного интеллекта: национальный и международный аспект»** (**Карцхия А. А., Макаренко Г. И**).

На первом международном саммите по безопасности ИИ, прошедшем 1 ноября 2023 г. в Великобритании (Россия не принимала в нём участие) была принята Декларация по вопросам безопасности ИИ (The Bletchley Declaration on AI safety). В ней использован термин Frontier AI, обозначающий высокоэффективные модели ИИ общего назначения. Документ, подписанный странами G7 30 октября 2023 г. в Японии, инициировал Хиросимский процесс. Заявлена цель создать всеобъемлющую политическую основу для разработки безопасных и заслуживающих доверия СИИ.

Россия в отличие от стран коллективного Запада выступает за широкий подход к содержанию понятия международной ИБ, включая в него как технические аспекты, так и значительный круг политико-идеологических вопросов. Национальная стратегия развития ИИ на период до 2030 года нацелена на то, чтобы обеспечить рост благосостояния населения, безопасность и правопорядок, развитие экономики, в том числе лидирующие позиции в мире в области ИИ.

РИСК НАРУШЕНИЯ КОРРЕКТНОСТИ МАШИННОГО ОБУЧЕНИЯ ИИ МОЖНО ОЦЕНИТЬ

Обеспечение безопасности информации СИИ предполагает противодействие злоумышленным угрозам подмены и модификации ММО. Не представляя всей «внутренней кухни» машинного обучения, заказчик и пользователи системы могут воспринимать нарушения её нормального функционирования за обычное техническое несовершенство, считают авторы работы **«Анализ угроз злоумышленной модификации модели машинного обучения для систем с искусственным интеллектом» (Костогрызов А. И., Нистратов А. А.)**.

Для систем, использующих СИИ, из множества различных угроз выделены следующие: угроза подмены ММО (УБИ.222) и угроза модификации ММО путём искажения («отравления») обучающих данных (УБИ.221). В наше время нередко разработчики программных средств (ПС), осуществляющие МО, принадлежат сторонним организациям. Они не хотят раскрывать и передавать заказчику и головному разработчику системы исходные тексты. В этих условиях угрозы, связанные со злоумышленной модификацией ММО, становятся остро актуальными и требуют системного анализа.

Исследователи предлагают подход к решению различных задач по эффективному применению СИИ, включая метод оценки интегрального риска нарушения корректности МО в течение задаваемого периода. Он позволит прогнозировать риски и количественно обосновывать принимаемые решения о стратегии и мерах противодействия рассматриваемым угрозам.

ПРОСТАЯ, ДА НЕПРОСТАЯ!

КАК ЗАЩИЩЕНА ПРОСТАЯ ЭЛЕКТРОННАЯ ПОДПИСЬ

Андрей ЖАРКЕВИЧ
эксперт StartX,
ведущий рубрики

Последнее время в СМИ часто пишут о квантовых компьютерах для взлома шифрования, о постквантовых алгоритмах, на которые в связи с этим нужно срочно переходить. А ещё об импортозамещении алгоритмов шифрования, бэкдорах и уязвимостях, исправленных в популярных криптобиблиотеках. Но вот тему простой электронной подписи (ПЭП) почему-то обходят вниманием.

Между тем ПЭП далеко не так проста, как кажется. Более того, некоторые способы её применения критически небезопасны. В статье рассмотрим связанные с ПЭП угрозы и выясним, существуют ли способы устранения этих угроз.

ЧТО ТАКОЕ ПЭП?

В соответствии с Федеральным законом № 63-ФЗ «Об электронной подписи», простой электронной подписью считаются СМС-коды, одноразовые пароли, переданные по электронной почте или полученные через TOTP-приложения. С их помощью можно открывать счета в банках, подписывать договоры, оформлять кредиты, менять параметры в профиле на Госуслугах и совершать множество других юридически значимых действий.

Это удобно для банков и других организаций, удобно для людей, которым не требуется никаких усилий, чтобы получить желаемое. Но вот о безопасности совершаемых таким образом юридически значимых действий не позаботились. Оговорку «никому не сообщайте этот код» в сообщениях с кодом вряд ли всерьёз можно назвать заботой о безопасности.

ЦИФЕРКИ — ЭТО НЕСЕРЬЁЗНО

Большая часть людей при использовании ПЭП не осознают в полной мере, что совершают юридически значимое действие, равнозначное подписанию договора. Банк просит ввести номер телефона и прислать код для регистрации? Без проблем. Нужен код для выпуска карты? Вот он, пожалуйста. Почему так?

Всё просто. Несколько циферок, которые пришли по СМС в открытом виде, не воспринимаются как что-то важное. Сообщение с ними теряется среди рекламы магазинов, сообщений от МЧС и прочих уведомлений, которые мы привыкли игнорировать. Разве может там быть что-то серьёзное?

Вот если заставить человека поставить три подписи на бумажном документе, да ещё повторить это на 20–30 листах, он волей-неволей соберётся и попытается осознать происходящее. Даже токен с ЭП, который требуется вставить в USB-порт, выглядит как что-то достойное внимания. А циферки в СМС — ввёл и забыл.

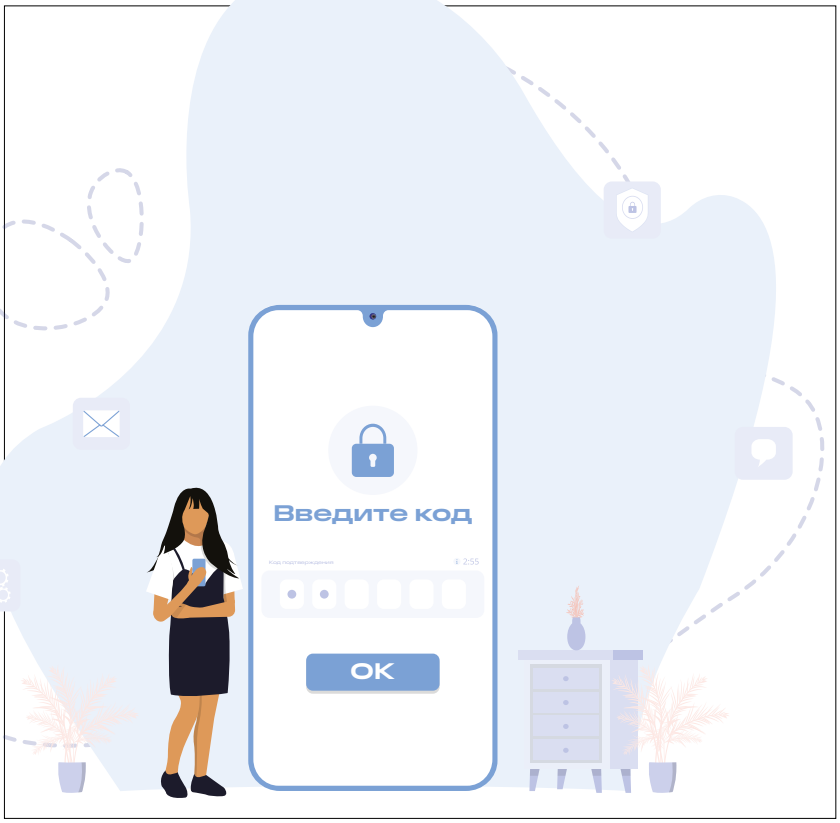
ВЕЗДЕСУЩИЕ КОДЫ

Катализатором легкомысленного отношения к ПЭП становится повсеместное использование номеров телефонов и цифровых кодов для регистрации на различных платформах и сервисах.

Хотите зарегистрироваться в Telegram или VK? Номер телефона и код, пожалуйста. Можем прислать в СМС или позвонить вам, назовите четыре последних цифры номера.

Двухфакторная аутентификация, включённая на многих платформах по умолчанию, также требует ввода кода. Входите в аккаунт с нового устройства? Мы отправим вам код, укажите его, пожалуйста.

Что в итоге? А в итоге происходит путаница. Люди не различают коды для аутентификации и ПЭП. Ведь отличий между ними, откровенно говоря, никаких нет. Что там, что тут — просто циферки. Для подтверждения личности, для подтверждения действия.



Простота превращается в угрозу. Привычка послушно вводить код везде, где его просят, рано или поздно приведёт к печальным последствиям.

ЧЕЙ НОМЕР?

Попробуйте провести эксперимент. Попросите друга или родственника оформить на себя номер телефона и отдать его вам. Затем воспользуйтесь этим номером, чтобы открыть счёт в банке на своё имя. Получилось? Практически не сомневаюсь, что всё прошло успешно.

Теперь вы можете совершать финансовые операции в этом банке и подписывать их с помощью ПЭП. А приходят эти коды на номер телефона, который вам не принадлежит. Теоретически владелец этого номера может сделать замену сим-карты, а затем воспользоваться ей, чтобы получить доступ к вашим счетам. В банке, который не проверяет, кому принадлежит номер, указанный клиентом при открытии счёта.

Стоит уточнить, что сейчас операторы связи при замене сим-карты на сутки блокируют входящие СМС «для безопасности». И разумеется, в большинстве случаев эта «безопасность» лишь доставляет неудобства легальному владельцу номера.

Ещё один неочевидный момент, связанный с ПЭП и телефонными номерами — это номера, которые операторы сотовой связи повторно выставляют в общий доступ. Так происходит с номерами, отключёнными из-за неактивности (через 150 дней) или при закрытии договора по инициативе владельца (через 60 дней).

Получив такую сим-карту, злоумышленники могут проверить, остался ли этот номер телефона привязанным к аккаунтам предыдущего владельца на Госуслугах, в онлайн-банках, маркетплейсах и на других платформах.

Обнаружив совпадение, они могут воспользоваться этой информацией, чтобы оформить кредит на предыдущего владельца сим-карты или похитить деньги с его счетов.

Почему это возможно? Потому что ПЭП подтверждает юридически значимые действия (перевод денег, оформление кредитной карты), а банки не проверяют, кто является владельцем номера, на который отправляют коды простой электронной подписи.

Возникает вопрос: а насколько вообще юридически корректна ситуация, когда при регистрации нового клиента банки принимают его номер телефона без проверки владельца? Ведь получение отправленного СМС-кода вряд ли можно назвать проверкой. Почему законодатели обходят вниманием этот вопрос в процессе борьбы с «дропами»?

ТЕКСТ ПРОТИВ ПОДПИСИ: НЕРАВНЫЙ БОЙ

Ещё одна проблема ПЭП связана с тем, что пользователь не видит или не смотрит, что именно он подписывает. И происходит это не потому, что ему не предлагают прочитать документ, а потому, что читать его неудобно, некогда или банально лень. На мобильном устройстве нам предлагают открыть pdf-ку, изучить написанный мелким шрифтом текст... Вспомните, как часто вы детально изучаете все эти электронные договоры и соглашения.

В случае с бумажными документами мы имеем текст, под которым ставим подпись. С усиленной квалифицированной электронной подписью (УКЭП) ситуация аналогична: мы видим документ и подписываем конкретно его.

А что с ПЭП? Где гарантия, что код, который вы вводите, подтверждает именно то действие, о котором вы думаете? Возьмём текст СМС-сообщения «Код 5503 для подтверждения покупки PG*Avito Dostavka. Никому его не говорите». Здесь нет суммы покупки, которую подтверждает код. В итоге пользователь опирается только на кон-

текст — если он в этот момент что-то покупает, то полагает, что код относится к этой покупке. Но так ли это на самом деле?

Технически ничто не мешает системе запросить у вас код для одной операции, а использовать его для другой. Предположим, к вам на телефон пробрался какой-нибудь вредонос, который подменяет текст СМС-сообщений с подтверждениями. Вы думаете, что подтверждаете перевод 1000 рублей другу, а система использует ваш код, чтобы подтвердить кредит на миллион рублей. Доказать потом, что вы не подтверждали его, будет крайне сложно, ведь формально ПЭП получена.

«РЫБАЛКА» НА ДОВЕРЧИВЫХ

Отдельная категория угроз связана с социальной инженерией. Мошенники активно эксплуатируют привычку людей вводить коды подтверждения. Они звонят, представляются сотрудниками банка, службой безопасности, полицией и под различными предлогами выпрашивают код из СМС.

«На ваше имя пытаются оформить кредит, мы его заблокировали, но для окончательной отмены нужен код, который мы вам отправили» — типичный пример такой манипуляции. Человек получает настоящий код от реального банка (по инициативе мошенника, который начал процедуру оформления кредита) и, не задумываясь, сообщает его звонящему.

Результат? Кредит оформлен, деньги переведены мошенникам, а гражданин остаётся с долгом и испорченной кредитной историей. При этом формально всё сделано по закону — ведь подпись (ПЭП) действительно принадлежит жертве.

ЕСТЬ ЛИ ВЫХОД?

Возможно ли сделать ПЭП более безопасной без потери удобства? Разумеется, да. Можно предложить несколько мер.

Контекстные коды. В СМС должно явно указываться, для чего именно предназначен код. Не просто «Ваш код 123456», а «Код 123456 для подтверждения перевода 1000 руб. на счёт Иванова И. И.». Многие банки и сервисы уже рассылают именно такие СМС, но пока не все.

Проверка владельца телефона. Банки могут и должны проверять, действительно ли номер телефона принадлежит тому человеку, который его указывает. Например, через ЕСИА (Госуслуги) или путём запроса у операторов связи.

Специальные приложения для ПЭП. Вместо СМС можно использовать защищённые приложения, которые показывают детали подписываемой операции и требуют дополнительного подтверждения (например, отпечатком пальца).

Образовательная работа. Банки и государство должны проводить кампании по повышению цифровой грамотности населения, объясняя, что такое ПЭП и какие риски она несёт.

Законодательное ограничение. Возможно, стоит ограничить список операций, которые можно подтверждать с помощью ПЭП, исключив наиболее рискованные (например, оформление кредитов). Работы в этом направлении уже проводятся. Тот же самозапрет на кредиты — вполне эффективная мера. Но, к сожалению, её можно обойти с помощью социальной инженерии. Например, убедить жертву снять это ограничение.

Исключить слабое звено. Полностью отказаться от СМС для рассылки кодов ПЭП и от идентификации человека по номеру телефона. Перехват СМС с помощью вредоносного ПО и социальной инженерии, нелегальные замены сим-карт и использование чужих номеров в качестве контактных для доступа к банкам и другим сервисам — это не просто гипотетический недостаток, а вполне реальная и чрезвычайно опасная архитектурная уязвимость.

ОТВЕТСТВЕННОСТЬ НА ПЛЕЧАХ ПОЛЬЗОВАТЕЛЯ

Пока все эти меры не внедрены повсеместно, ответственность за безопасность ПЭП лежит на плечах пользователей. Проявляйте бдительность при получении кодов, никому их не сообщайте, внимательно читайте текст СМС-сообщений.

Если вы меняете номер телефона — обязательно отвяжите старый от всех сервисов, где он использовался для ПЭП. Если потеряли телефон — немедленно блокируйте сим-карту.

Помните, что ПЭП — это не просто набор цифр, а полноценная юридически значимая подпись. Относитесь к ней с тем же вниманием, с каким относились бы к своей рукописной подписи под важным документом.

К сожалению, сегодня мы наблюдаем парадоксальную ситуацию: с одной стороны, законодатели и финансовые регуляторы ужесточают требования к идентификации клиентов, а с другой — сохраняют юридическую значимость инструмента, который не обеспечивает даже базового уровня защиты. Пока этот парадокс не разрешён, каждый из нас должен самостоятельно заботиться о своей безопасности в цифровом мире.

МНОГОЛИКИЙ ДИНАМИЧЕСКИЙ АНАЛИЗ

Дмитрий ПОНОМАРЕВ
заместитель генерального директора – директор департамента внедрения и развития практик РБПО ООО НТЦ «Фобос-НТ», сотрудник ИСП РАН, преподаватель МГТУ им. Н. Э. Баумана, модератор испытаний статических анализаторов исходного кода

Второй блок статей из серии «Три кита РБПО» посвящен технологиям и инструментам динамического анализа программного обеспечения. На первый взгляд интуитивно понятное определение «динамический анализ» на практике оказывается одним из самых «крепких орешков» при выборе подходов и инструментов динамических исследований программного обеспечения. Определение их применимости и достаточности, в условиях ограниченности ресурсов (и кадров), с учетом необходимости выполнения регуляторных требований, является типовой задачей, регулярно решаемой как разработчиками ПО, так и специалистами в области ИБ и РБПО, в том числе сотрудниками испытательных лабораторий. В статье приведен обобщенный взгляд на существующие технологии динамического анализа (далее – ДА), требования и особенности их применения. Цель статьи – подготовить читателя к последующему знакомству с конкретными инструментами динамического анализа, помочь в определении их полезности и применимости.

Раздумывая несколько месяцев над наполнением статьи, я в очередной раз столкнулся с обозначенной в аннотации проблемой. Казалось бы тривиальный в понимании термин «динамический анализ», или, в соответствии с ГОСТ Р 56939–2024[1] «динамический анализ кода программы», определяемый как *«вид работ по инструментальному исследованию программы, основанный на анализе кода программы в режиме непосредственного исполнения (функционирования) кода»*, на самом деле не дает ответа на большую часть практических вопросов, возникающих у исследователя, которому поставлена задача по проведению ДА. Пытаться ответить на них все единолично в рамках одной небольшой статьи, ещё и в формате стройной, формально-выверенной картины – задача заведомо нерешаемая. Поэтому решено действовать другим – уже проверенным в предшествующих материалах[2] – способом, а именно перечислить типовые вопросы, с которыми уважаемые разработчики периодически «влетают» в эксперта испытательной лаборатории, а также некоторые апробированные временем и практикой тезисы ответов.

1. ДИНАМИЧЕСКИЙ АНАЛИЗ ЭТО ЖЕ DAST?

Мой «любимый» тезис, регулярно всплывающий при общении с представителями разработчиков и исследователей безопасности кода. Сильно упрощая, для большого числа инженеров-безопасников ДА примерно тождественен «походить по API с помощью условного OWASP Zap»[3]. Действительно, являясь одним из полезных и распространенных видов ДА, комплекс подходов и инструментов анализа, в обиходе известный как DAST, сконцентрирован в первую и основную очередь на анализе API (в первую очередь в отношении web-фреймворков). Данный комплекс, как правило, ориентирован на поиск известных уязвимостей – как составляющих API компонентов, так и безопасности их конфигураций – либо, на выявление «нехороших» API (Shadow, Orphan и Zombie[4]) и их параметров. Практики и инструменты DAST в наибольшей степени применимы при работе команд пентестеров (RedTeam), а также при создании и постоянном контроле защищенности микросервисных (зачастую разрабатываемых в парадигме API-First) приложений, по своей природе предполагающих частые внесения изменений. Тем не менее вышеуказанные практики состав-

[1] https://clck.ru/3Ncr6J

[2] РБПО-2024. Итоги и перспективы // BIS Journal. – 2025. – № 1 (56). – С. 23–25.

[3] Видеозапись моего выступления на Kaspersky Certification Day: https://certificationday.kaspersky.com/ (08:08:00)

[4] https://habr.com/ru/companies/webmonitorx/articles/804489/

ляют только подмножество существующих и требуемых в ряде случаев практик ДА.

2. ЧТО ТРЕБУЕТ И ЧТО НЕ ТРЕБУЕТ ФСТЭК РОССИИ, КОГДА УПОМИНАЕТ ДИНАМИЧЕСКИЙ АНАЛИЗ?

Дискутируя с коллегами, мы, как правило, делим РБПО-практики на «вширь» и «вглубь»[5]. «Вширь» определяется ГОСТ Р 56939–2024, в котором вводятся 25 процессов, составляющих комплексный процесс РБПО, при этом сами описания процессов достаточно верхнеуровые и зачастую оставляют на усмотрение разработчика выбор инструментов и детали (в т.ч. численные критерии) реализации процессов. «Вглубь» — а именно более конкретные требования к технологическим возможностям инструментов и численные критерии — определяется Методикой выявления уязвимостей и недекларированных возможностей в ПО ФСТЭК России[6], доступной для использования в работе лицензиатам ФСТЭК России, а также частично приказом № 76 ФСТЭК России «Требования, устанавливающие уровни доверия...».

В область требуемых практик ДА с точки зрения Методики (для испытаний по 4 — самому типовому — уровню контроля) попадают как минимум:

- функциональное тестирование (иначе: «пользовательское» тестирование функций безопасности);
- модульное тестирование (основным доп. требованием которого является запуск тестов с комплектами датчиков срабатывания ошибок в тех случаях, когда это применимо);
- генетическое фаззинг-тестирование (о нем ниже);
- комплексный сбор информации об объекте в динамике оценки, совмещенный с тестированием на проникновение (на пальцах этот процесс можно охарактеризовать как совмещение практик DAST и анализа в песочнице);
- а также ряд специальных практик, таких как динамический анализ потоков распространения чувствительных данных (в т.ч. полносистемный).

В область требуемых практик ДА с точки зрения ГОСТ явно попадают динамический анализ (процесс № 11) и функциональное тестирование (процесс № 18). При этом в процессе № 11 в явном виде упоминается необходимость фаззинг-тестирования, пусть и без указания требования «генетического» свойства, однако с введением комплексного примечания, в настоящей редакции ГОСТ пока что рекомендующего добровольно подходить к решению задачи ДА с должным энтузиазмом:

«Используемые методы динамического анализа могут позволять осуществлять динамический анализ кода программы путем подачи заведомо некорректных входных данных, динамического профилирования, путем отладки программы, путем поиска защищаемой информации (в оперативной памяти, других местах среды исполнения кода), путем исследования поведения программы с использованием встраиваемых инструментальных датчиков срабатывания ошибок (санитайзеров) или инструментированных с использованием средств динамического двоичного инструментирования, другими применимыми методами, в том числе определенными соответствующими национальными стандартами»

Также процессы определения поверхности атаки (процесс № 7) и нефункционального тестирования (процесс № 19) не требуют, но подразумевают использование различных, характерных для ДА, подходов.

Начиная с апреля 2025 ФСТЭК России также публикует методические рекомендации по проведению тех или иных видов испытаний в Телеграм-канале @sdl_inform, входящем в группу информационных ресурсов РБПО-сообщества ФСТЭК России и ИСП РАН[7]. Вопросы применимости и требований методик и инструментов динамического анализа рассмотрены представителем ФСТЭК России И. С. Гефнер в рамках большого эфира[8], посвященного тематике РБПО.

3. ФАЗЗИНГ, ЧТО ЭТО ЗА ЗВЕРЬ?

Самое простое определение фаззинга — это подача на вход тестируемому объекту случайных данных (в надежде обнаружить какое-либо неожиданное — вплоть до аварийного завершения — поведение тестируемого объекта или даже системы в целом). Простейшие инструменты фаззинга — мутаторы значений параметров запросов, как правило, включены в комплект поставки упоминавшихся выше DAST-инструментов.

Однако, в силу принципиального отсутствия в мире технологических и вычислительных возможностей доказать формальную корректность какого-либо типового кода (даже для нескольких сотен тысяч исполняемых инструкций, за исключением частных случаев тривиального кода), вероятность найти все случаи неожиданного поведения методом подачи полностью случайных данных практически нулевая. Такой метод, разумеется, позволяет находить некоторые конкретные нештатные ситуации, однако существенно отстает от возможностей исследователя, вооруженного более продвинутыми инструментами, такими как генетические фаззеры. Инструменты данного типа могут автоматически оценивать эффективность собственной работы, выражающуюся в открытии новых состояний тестируемой программы, и до некоторой степени автоматически корректировать стратегию мутаций.

Как правило, в тех случаях, когда регуляторикой требуется фаззинг, подразумевается именно генетический фаззинг. Более подробный рассказ о данной технологии будет представлен в статье ИСП РАН в данном

---

[5] Выступление Елены Быхановой (НТЦ Фобос-НТ): https://arppsoft.ru/ie/19556/. Видео доступно по ссылке: https://t.me/sdl_community/8690

[6] Ссылка на презентацию: https://www.tbforum.ru/2025/program/information-security, ссылка на просмотр: https://clck.ru/3NcrPB

[7] https://t.me/sdl_community/7859

[8] https://t.me/sdl_community/8407

блоке, также различные материалы публикуются в Телеграм-канале @sdl_dynamic[9]. При этом важность (и сложность) технологии в целом подчеркивает в том числе тот факт, что именно упоминанию вопросов генетического фаззинга посвящено наибольшее число методических рекомендаций ФСТЭК России, публикуемых в Телеграм-канале @sdl_inform.

4. МОЖЕТ БЫТЬ ВСЕ-ТАКИ СДЕЛАТЬ ЕДИНЫЙ СТАНДАРТ ПО ДИНАМИЧЕСКОМУ АНАЛИЗУ?

Отличное предложение! В настоящий момент помимо «большого» ГОСТ Р 56939–2024 вступили в силу и действуют «инструментальные» ГОСТы: статический анализ исходного кода[10]; безопасный компилятор языков Си/Си++[11]. Также на финальной стадии подготовки находится стандарт по композиционному анализу программного обеспечения[12]. В планах ТК362 на 2025 год среди прочих значится разработка стандарта «Динамический анализ программного обеспечения»[13], автором стандарта является ИСП РАН. Работа над первой редакцией стандарта уже ведётся, на текущий момент с высокой степенью вероятности можно утверждать о попадании в редакцию стандарта как минимум следующих областей динамического анализа: модульное (и возможно комплексное функциональное) тестирование, фаззинг-тестирование, анализ потоков помеченных данных (как для уточнения поверхности атаки, так и для выявления утечек чувствительных данных).

5. И ЭТО ВСЁ? А КАК ЖЕ X, Y И ИИ?

Разумеется, нет! Список типов инструментов, выполняющих виды динамического анализа, полезные как на этапе создания ПО, так и на этапе его эксплуатации, можно продолжать достаточно долго — упомянем для примера следующие из них:

[9] https://t.me/sdl_dynamic/9103

[10] https://docs.cntd.ru/document/1304734159

[11] https://docs.cntd.ru/document/1304734158

[12] https://t.me/sdl_community/8716

[13] https://fstec.ru/tk-362/deyatelnost-tk362/plany-rabot/plan-raboty-na-2025-god

ЗАМЕТКИ О ХОДЕ ИСПЫТАНИЙ СТАТИЧЕСКИХ АНАЛИЗАТОРОВ ИСХОДНОГО КОДА

5 августа 2025 г. на площадке кафедры ИУ10 МГТУ им. Н. Э. Баумана стартовал основной этап испытаний открытых и коммерческих статических анализаторов исходных кодов компилируемых и динамических языков программирования под патронажем ФСТЭК России.

Подробнее о целях и задачах испытаний, а также о функциональных возможностях участвующих в испытаниях инструментов статического анализа, вы можете узнать, ознакомившись с материалом «Испытания статических анализаторов»[1]. В материале «Итоги этапа «Домашнее задание» испытаний статических анализаторов под патронажем ФСТЭК России»[2] приведена краткая характеристика инструментов, сформированная по итогам выполнения первого из двух этапов испытаний, а также обозначены планы организаторов испытаний по развитию публичного репозитория комплектов тестов и стандартизации варианта формата SARIF, допускающего обмен результатами испытаний инструментов в рамках работ Центра исследований безопасности системного ПО ФСТЭК России[3].

Представление результатов испытаний ожидается в декабре 2025 года на полях Открытой конференции ИСП РАН в инновационном кластере «Ломоносов»[4] — главного ежегодного отечественного события в области безопасной и качественной разработки и традиционной площадки встреч участников РБПО-сообщества ФСТЭК России и ИСП РАН.

[1] Испытания статических анализаторов // BIS Journal. — 2025. — № 2 (57). — С. 72–74.

[2] https://ib-bank.ru/bisjournal/post/2508

[3] https://portal.linuxtesting.ru/

[4] https://www.isprasopen.ru/

- инструменты динамического определения поверхности атаки по коду (например, Natch от ИСП РАН);
- платформы контроля и безопасности контейнерной инфраструктуры, использующие движок eBPF (например, Luntry от Лантри);
- инструменты комплексного динамического исследования REST API (например, ПроAPI от Вебмониторэкс);
- полноценные песочницы, совмещенные со средствами антивирусной защиты (например, Sandbox от Лаборатории Касперского).

Отдельным и весьма актуальным является создаваемый прямо на наших глазах тип инструментов ДА, предназначенный для различных динамических исследований работы моделей систем искусственного интеллекта. Составить верхнеуровневое представление о созданных и развивающихся методах и инструментах анализа можно на основе доклада Вартана Падаряна (ИСП РАН) «Разработка безопасных технологий искусственного интеллекта»[14].

* * *

Далеко не все перечисленные инструменты в настоящий момент явно требуются во всех видах испытаний, либо подходят для анализа и защиты всех видов программных продуктов и систем. Однако темпы развития общей инженерной культуры, равно как и соответствующие темпы развития регуляторных требований, не оставляют сомнения в том, что все полезные и применимые технологии анализа и защиты скорее рано, чем поздно будут введены в обязательный набор требований. И, разумеется, никто не запрещает ответственным разработчикам и эксплуатантам, заинтересованным в качестве, безопасности и надежности кода, ПО и систем, а также в повышении общей эффективности процессов их создания и эксплуатации, применять указанные средства анализа уже сейчас!

[14] https://www.itsecexpo.ru/2025/program/ai-tools-for-coding

Состоявшийся 5–6 августа запуск основного этапа испытаний в целом признан успешным. Несмотря на потребовавшийся от участников испытаний, членов жюри, площадки и организаторов испытаний существенный объем ресурсных вложений — в первую очередь в разработку комплектов тестов и репозитория их хранения, а также в создание портала централизованной разметки и адаптацию инструментов для взаимодействия с ним — основная часть коллективов приняла активнейшее участие в процессе подготовки. К указанным категориям участников испытаний добавилась новая категория — эксперты, в зоне ответственности которых первичная разметка и кросс-верификация срабатываний инструментов. В данную категорию включены представители Ассоциации ФинТех, АО «ИнфоТеКС», ООО «Постгрес Профессиональный», ООО «Свордфиш Секьюрити», АО Центр «Атомзащитаинформ».

На запуске основного этапа присутствовали представители ФСТЭК России и всех участвующих в испытаниях компаний и организаций. Почетная обязанность определить порядок начала испытаний инструментов была предоставлена Михаилу Павловичу Сычеву — основателю и бессменному лидеру кафедры ИУ10 «Защита информации». Основной задачей, успешно решенной всеми участниками испытаний 5–6 августа, являлось проведение статического анализа в отношении комплекта компонентов с открытым исходным кодом, сформированного организаторами испытаний на основе предложений жюри, и загрузка данных результатов на портал централизованной разметки — работы под кодовым названием «Блок Б». Начиная с 11 августа и до 1 ноября 2025 будет выполняться разметка и кросс-верификация разметки, результаты которой станут основой для подготовки итоговых отчетных материалов.

В середине сентября участники и жюри вновь соберутся в МГТУ для выполнения комплекта тестов под кодовым названием «Блок А». В состав данного комплекта входят тесты, позволяющие проверить реализацию инструментами различных свойств методов статического анализа, наличие у инструментов технологических возможностей по перехвату сборочного процесса и созданию собственных спецификаций на источники помеченных данных, а также возможность инструментов успешно анализировать крупные проекты в установленные ГОСТ Р 71207–2024[5] предельные временные рамки — нагрузочное тестирование.

М. П. Сычев

[5] https://docs.cntd.ru/document/1304734159

ДИНАМИЧЕСКИЙ АНАЛИЗ

КАК ВАЖНЫЙ ЭТАП РАЗРАБОТКИ БЕЗОПАСНОГО ПО

Вартан ПАДАРЯН
заведующий лабораторией ИСП РАН, руководитель органа по сертификации процессов РБПО

ИСП РАН уже более пятнадцати лет проводит фундаментальные и прикладные исследования, связанные с разработкой и применением технологий анализа программ для обеспечения кибербезопасности. Результаты исследований реализованы в виде комплекса инструментов, обеспечивающих разработку безопасного ПО. Наряду с широко известными инструментами статического анализа программ, такими как Svace[1] и Svacer[2], в ИСП РАН разработан ряд решений по динамическому анализу (ДА) ПО.

Одним из передовых способов ДА на текущий момент является гибридный фаззинг. Это сочетание классического фаззинг-тестирования с методами динамического символьного исполнения (ДСИ). ДСИ выполняет анализ программы, опираясь на ее логику и внутреннюю структуру. Для этого реальные входные данные заменяются на символьные переменные, с использованием которых происходит интерпретация бинарного кода и построение математической модели исполнения программы. На основе данной модели генерируются новые входные данные, которые приводят к увеличению тестового покрытия или воспроизведению ошибок.

Гибридный фаззинг зарекомендовал себя как наиболее эффективный метод тестирования. Он объединяет в себе скорость классического фаззинга и способность к открытию труднодостижимых участков кода ДСИ. Тем самым быстрее достигает большего покрытия и обнаруживает больше ошибок, чем оба метода по отдельности.

Комплекс Sydr-Fuzz[3], разрабатываемый в ИСП РАН, позволяет организовывать гибридный фаззинг бинарных программ с помощью открытых инструментов фаззинга (libFuzzer, AFL++, Honggfuzz) и инструмента ДСИ Sydr. Sydr-Fuzz одновременно запускает заданное число процессов фаззинга и символьного исполнения и по ходу работы синхронизирует корпуса данных между ними: отсеивает лучшие пути для анализа методом ДСИ и отбирает полезные входные данные для фаззера. Sydr-Fuzz также контролирует работу инструментов, отслеживает статистику их работы и условия для завершения фаззинга.

Инструмент ДСИ Sydr, для увеличения покрытия генерирует новые входные данные для анализируемой программы путем инвертирования условных переходов, зависящих от входных данных. Также Sydr осуществляет целенаправленный поиск ошибок с помощью символьных предикатов безопасности. Sydr определяет потенциально опасные участки в бинарном коде и пытается подобрать входные данные для воспроизведения ошибки. В Sydr поддерживаются предикаты безопасности для обнаружения разыменования нулевого указателя, деления на ноль, переполнения буфера, целочисленного переполнения и усечения, инъекции форматной и командной строки.

Sydr-Fuzz поддерживает гибридный фаззинг для компилируемых программ на языках C/C++/Rust/Go и C# (при использовании компиляции Native AOT) на ОС семейства Linux. Также, в нем реализована поддержка анализа на архитектурах x86/x86–64, ARM64 (в т.ч. Байкал) и RISC–V.

Sydr-Fuzz поддерживает пайплайн ДА для компилируемого кода, включая следующие этапы: анализ, минимизация итогового корпуса входных данных, сбор покрытия и анализ аварийных завершений. Также реализована поддержка программ на Python/Java/JavaScript/Lua. Вместо гибридного фаззинга на этапе анализа для таких проектов выполняется обычное фаззинг-тестирование с использованием открытых инструментов Atheris, Jazzer, Jazzer.js, Sharpfuzz, luzer. Sydr-Fuzz реализует процедуры запуска фаззинга, минимизации корпуса, сбора покрытия и анализа аварийных завершений для каждого тулчейна, что сильно облегчает процесс автоматизации ДА.

Для автоматического анализа аварийных завершений Sydr-Fuzz использует инструмент CASR[4]. Он позволяет генерировать отчеты о каждой обнаруженной в процессе анализа ошибке, удалять дубликаты и кластеризовать оставшиеся ошибки по степени похожести стека вызовов. Отчеты об ошибках генерируются на основе информации от санитайзеров или gdb и содержат всю необходимую информацию для аналитика, в т.ч. стек вызовов и участок исходного кода с ошибкой. CASR являет-

[1] https://www.ispras.ru/technologies/svace/
[2] https://www.ispras.ru/technologies/svacer/
[3] https://www.ispras.ru/technologies/sydr/
[4] https://www.ispras.ru/technologies/casr/

ся мощным инструментом, позволяющий существенно облегчить разбор результатов фаззинга, где зачастую могут находиться сотни различных аварийных завершений.

Все инструменты ДА программы позволяют анализировать только тот код, который был реально выполнен. Поэтому важно выбрать такой набор тестов или сценариев работы, который покрывал бы все важные функции.

Для сбора сведений о выполнении программы, ее прерывают, обеспечив работу инструментального кода. Для этого анализатор заведомо замедляет целевую программу. Инструментальный код встраивается в код программы на этапе компиляции или предобработки бинарного файла перед запуском (статическое инструментирование). Другой подход — это добавление инструментального кода непосредственно во время выполнения фрагментов целевой программы (динамическое инструментирование).

В ИСП РАН разработан инструмент Natch[5], предназначенный для определения поверхности атаки (ПА) приложений. Он построен на основе виртуальной машины QEMU и использует динамическое инструментирование.

ПА ПО — это те интерфейсы или программные компоненты (функции, модули, программы, библиотеки), которые получают данные из недоверенных источников. Так как при отправке модифицированных данных на интерфейсы или в программные компоненты возможно нарушить работу программы.

Разработчики определяют поверхность атаки своего ПО для тестирования (в том числе с помощью фаззинга) этих функций. Также поиск поверхности атаки необходим для того, чтобы найти зависимости от лишних или устаревших библиотек и пр.

Для определения ПА можно применить статический анализ (построение зависимостей функций, просмотр кода через IDE) или ДА (поиск покрытия кода набором тестов). При этом, статический анализ не способен в принципе находить некоторые типы зависимостей, к примеру, из-за динамического связывания, с чем может помочь Natch. А ДА (при достаточно хорошем наборе тестов) находит именно тот код, который выполнялся. Но сведения о выполненных функциях (и строках кода) недостаточно точно отражают характер этих функций. Такой метод не создает ясности зависят ли функции от входных данных. Например, код инициализации выполняется всегда, но злоумышленник редко может на него повлиять. Поэтому этот код не должен быть включён в ПА. Для определения более точной ПА необходимо отследить те программные модули, которые взаимодействовали со входными данными из недоверенных источников, в чем полезен Natch.

Гибридный фаззинг зарекомендовал себя как наиболее эффективный метод тестирования. Он объединяет скорость классического фаззинга и способность к открытию труднодостижимых участков кода ДСИ

Чтобы выделить из множества выполненных функций только те, что относятся к ПА (то есть обрабатывающие небезопасные данные), Natch помечает входные данные из недоверенных источников, специфицированных пользователем, а затем средствами эмулятора отслеживает их распространение по памяти виртуальной машины. Каждая процессорная инструкция, копирующая помеченные данные, копирует также и пометку. Что позволяет узнать, куда передавались и где обрабатывались входные данные и получить поверхность атаки, интересующую аналитика.

Natch анализирует не отдельные приложения, а виртуальную машину целиком, что позволяет проследить работу с данными, перетекающими между сервисами. При этом необходимо: помещать исследуемую программу в контролируемое окружение (виртуальную машину), а также разделять выполняемый в виртуальной машине код между высокоуровневыми сущностями (процессами, модулями) для представления пользователю.

В базовой версии QEMU включен только эмулятор gdb-сервера для подключения отладчика и логирование выполняющихся инструкций. Для того, какие именно приложения выполняются в гостевой системе, этого недостаточно. Поэтому Natch загружает в QEMU плагины, которые инструментируют выполняемый код. С помощью этого в гостевой системе определяются обращения к файлам, переключение между процессами. Восстанавливается стек вызовов всех приложений, собирается информация о покрытии кода. Также Natch умеет распознавать выполнение функций из программ на Python и JavaScript и даже скомпилированного байт-кода Java.

Natch может анализировать виртуальные машины под управлением Linux, Windows или FreeBSD для архитектур x86_64 и AArch64. Генерация ПА и стека вызовов работает для компилируемых языков типа C/C++, а также Go, Python, Java, C# и JavaScript.

ИСП РАН продолжает исследования безопасности ПО и развитие технологий ДА, в том числе ИСП Crush[6], Блесна[7] и пр. О новых подходах и развитии технологий исследований безопасности ПО можно узнать на официальном сайте ИСП РАН[8].

[5] Описание: https://www.ispras.ru/technologies/natch/. Запись доклада на ТБ Форум 25: https://clck.ru/3Necyo. Слайды доклада на ТБ Форум 25: https://clck.ru/3Neczn

[6] https://www.ispras.ru/technologies/crusher/

[7] https://www.ispras.ru/technologies/blesna/

[8] https://www.ispras.ru/news/

ПРОБЛЕМЫ ДИНАМИЧЕСКОГО АНАЛИЗА ВЕБ-ПРИЛОЖЕНИЙ И API

КАК МЫ ИХ РЕШАЕМ

Валерий КУВАЕВ
руководитель направления защищенной разработки группы компаний SolidLab

Чтобы использовать DAST на практике, заказчик должен понимать, как работает этот класс решений, для каких целей его нужно выбирать, какие приложения и в каких сценариях необходимо анализировать и, наконец, как работают собственные сканируемые приложения. В этой статье мы разберем некоторые аспекты динамического анализа веб-приложений с упором на актуальный опыт применения и пилотирования нашего решения по динамическому анализу SolidPoint DAST.

РАЗБИРАЕМ ТЕРМИНЫ

Следует разграничить термины «DAST», «динамический анализ», «сканер уязвимостей» и «сканер безопасности». Путаницу в терминах я встречал как в формальных взаимодействиях с заказчиками, так и в личных беседах, конечно, она осложняет взаимопонимание, и может приводить к ложным ожиданиям.

Если говорить о терминах проще, то:

- «Динамический анализ» — общее название методов анализа ПО во время его выполнения. Сюда входит не только безопасность, но и проверка производительности и функциональности, анализ поведения ПО, сетевая активность, работа с памятью и другие категории.
- «Сканеры уязвимостей» — это подкласс «сканеров безопасности». Они используют разные методы, включая динамические, для поиска уязвимостей в широком стеке инфраструктуры и ПО. Чаще всего сканеры отрабатывают уязвимости из классификатора CVE. При этом «сканеры безопасности» могут идентифицировать более широкую номенклатуру рисков. Оба термина применяются достаточно вольно для обозначения инструментов, представленных на рынке.
- «DAST» — наиболее узкий термин. Он указывает на класс сканеров, применяющих динамический анализ для идентификации недостатков безопасности веб-приложений и API без доступа к коду, методом «черного ящика». Результатом работы DAST, как правило, является список выявленных недостатков ПО, категорированных по CWE.

Таким образом, под DAST мы понимаем специфический класс инструментов для анализа безопасности веб-приложений и API. Хотелось бы, чтобы на рынке вся терминология становилась более унифицированной. Разница в понимании ведёт к потере времени при переговорах, что критично в условиях срочных запросов и интенсивных коммуникаций. Сейчас мы рекомендуем согласовать все термины ещё на старте.

Нередко мы встречаем конкурсные процедуры, где указаны широкие требования для сканеров уязвимостей, например, по поддержке протоколов, не имеющих отношения к вебу. При этом конкурс заявлен на выбор инструмента DAST. Добавлю, что есть некоторая надежда на то, что ожидаемый новый ГОСТ по динамическому анализу зафиксирует терминологию и взаимодействие станет проще.

ЧТО ЗНАЧИТ ПРАВИЛЬНАЯ ПОДГОТОВКА К СКАНИРОВАНИЮ

Основное, если вы не знаете, как устроено ваше приложение, которое вы хотите сканировать, а также инфраструктура его доставки, то эффективности от DAST'а ожидать не приходиться. Опыт пилотных внедрений показал, что успешное сканирование требует тщательной подготовки. Были случаи, когда мы сталкивались со сложностями при сборе информации о приложении и при проведении первичного сканирования: недостоверная устаревшая или неполная информация, систематические ошибки в полученных «на руки» данных, низкий показатель стабильности и доступности стендов.

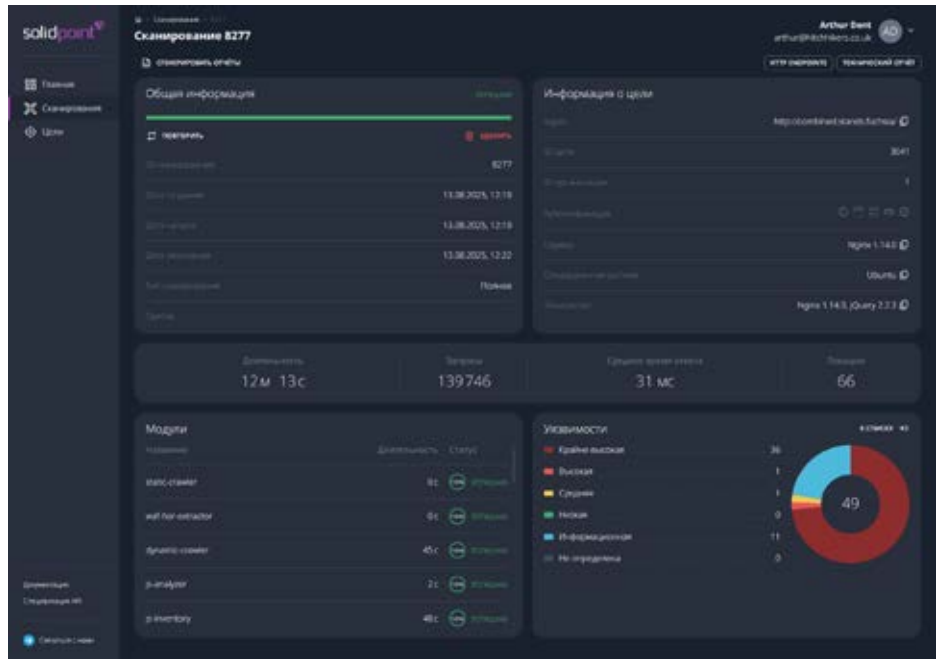
По сути, инструменты DAST умеют сканировать приложения без ка-

кой-либо подготовки, даже без данных для аутентификации. Но обычно всё интересное закрыто от доступа, поэтому первое, с чем необходимо определиться, — это какую инсталляцию приложения мы сканируем, какие данные по аутентификации нам нужны, достаточно ли сканирования под одной ролью или нужно под разными, как работает механизм аутентификации, ограничено ли время сессии, и если да, то как конкретно? Зачастую типы аутентификации и применяемые методы могут смешиваться, тогда инструмент должен уметь их применить «по месту».

С помощью SolidPoint DAST мы поддерживаем различные механизмы: аутентификация по кукам, токенам, HTTP Basic, по клиентским сертификатам, через локальное хранилище браузера (localStorage). Наконец, существуют более сложные сценарии — запись браузерного скрипта с данными аутентификации и метод аутентификации по HTTP-запросу, например, для работы с JWT-токенами и для обновления короткоживущих сессий. При этом для сканируемого приложения можно задать целую группу данных аутентификации для основного приложения и для входящих в приложение API, находящихся на соседних URL, — сканер сам применяет эти данные.

Для подготовки сканирования следом идут дополнительные вопросы, есть ли CAPTCHA, OTP, SMS, можно ли как-то зафиксировать их значения в тестовых средах и что делать с ними в продуктивной среде, поскольку динамически подгрузить их в запущенное сканирование может оказаться проблематичным. Следующий вопрос — как ограничена нагрузка в продуктивной или в тестовой среде? Зачастую тестовые среды сами по себе менее мощные, а в продуктивной не хочется влиять на производственный процесс. Важно понять предел нагрузки, сколько условных RPS можно разрешить сканеру, этот же параметр, кстати, напрямую повлияет на время сканирования.

Есть ли WAF или иные системы, блокирующие трафик? Если да, необходимо внести сканер в белый список.



Также, нужно выявить, какие конечные точки приложения нельзя затрагивать сканированием. В первую очередь, это касается конечных точек, приводящих к выходу из сессии — «разлогину». Еще в продуктивных приложениях это могут быть конечные точки, связанные с вызовом внешних интеграций, например, SMSGateway — мы же не хотим исчерпать весь бюджет платного сервиса, отправив тысячи SMS в никуда? Также могут быть конечные точки, связанные с критическим бизнес-процессом, например, с кнопкой «оплатить». Обычно на сайте это последний этап воронки продаж, и он должен работать идеально.

Сканирование — это отправка множества запросов, не всегда корректных функционально, для проверки того, как приложение отреагирует. Приложение может начать регистрировать поток ошибок. В ситуации, когда сканер внесён в белый список и средства защиты пропускают его трафик, это может неожиданно для всех привести к реальным операционным рискам, например, вызвав DoS. Но чаще всего регистрируемые ошибки могут замаскировать сопутствующую реальную проблему, и служба мониторинга имеет все шансы за штормом событий её пропустить, нарушив SLA и, как следствие, не выполнив KPI.

Также возникает вопрос о длительности сканирования. Как правило, время зависит от размера приложения, сложности конечных точек приложения — количества параметров в каждой, а также от скорости сети и выбранного RPS. При сканировании составляется карта приложения и различными методами проверяется каждый выявленный объект: конечная точка или ресурс на сайте, атаки посылаются по каждому выявленному параметру. Все эти факторы в совокупности влияют непредсказуемо сложно, и чтобы ответить точно, потребуется провести первое полноценное сканирование.

Вытекающий вопрос из предыдущего — а сколько узлов сканирования понадобиться для реальной промышленной инсталляции? До первого полноценного сканирования каждого приложения и API ответить сложно, т.е. это становится понятным в середине внедрения. По этой причине в сканере SolidPoint DAST поддерживается горизонтальное масштабирование и количество узлов не ограничено лицензией.

Таким образом польза от DAST прямо пропорциональна степени подготовки к анализу и коректности настройки сканирования, которые невозможны без глубокого понимания сканируемого приложения, его

механизмов и инфраструктуры доставки. Свой вклад в полезность несут и инструменты, и на мой взгляд недооцененной является сложность составления карты поверхности атаки — списка конечных точек и ресурсов с помощью которых возможно взаимодействие с сервером.

ТЕХНИЧЕСКИЕ ПРОБЛЕМЫ АНАЛИЗА ПОВЕРХНОСТИ АТАКИ

Несмотря на то, что DAST как класс решений работает с приложениями как с «черным ящиком» (т.е. через его внешние интерфейсы), влияние технологий разработки сканируемого приложения все же сказывается на результатах сканирования. Так было при появлении SPA приложений, после чего сканеры на рынке дружно заявили о всяческой поддержке SPA — почти сразу, как ее реализовали.

Возникает вопрос, насколько качественно средства динамического анализа определяют поверхность атаки? Ответ не очевиден, ведь недостаточное покрытие не приводит к ложным срабатываниям, на которые можно указать, а приводит к ложно негативным результатам, оставляя реальный скоуп приложения и уязвимости без внимания. Ведь чтобы просканировать функцию на стороне сервера, надо сначала найти, как ее вызвать — узнать формат запроса, параметров, а дальше уже проверять на уязвимости; если инструмент не умеет с хорошей полнотой идентифицировать функции на стороне сервера — т.е. поверхность атаки — до этапа тестирования на уязвимости этой функции инструмент даже не доберется, т.е. фактически приложение останется просто непроанализированным. Эти проблемы характерны для современных приложений с изощренной сложностью интерфейсов и глубокой зависимостью от разнообразных JS-фреймворков.

В исследовании “The Security Tools Gap”[1], проведенном компанией Axeinos в марте 2025 года, прямо сказано, что при определении поверхности атаки BlackBox сканеры очень быстро сдаются, оставляя значительную часть приложения неисследованной, причем чем выше сложность приложения, тем больше эта проблема. Получается, что изначально, сканеры ищут уязвимости и ошибки не в приложении, а в его малой части, при этом существующие технологии динамического краулинга не могут компенсировать это упущение, нужно что-то иное.

Значительно ранее, проводя многочисленные пентесты для наших заказчиков, мы обнаружили, что периодически встречаются запросы, хранящиеся в коде JS, не имеющие соответствующей части в UI. Стало понятно, что классические методы динамического краулинга, не способны их найти. Кроме того, у них есть дополнительные ограничения: страницы приложения могут создаваться динамически, что удлиняет и иногда зацикливает анализ, не всегда элементы управления и связанные с ними функции получается идентифицировать, не все введенные краулером данные оказываются корректными, чтобы приложение перешло на следующий экран. По этой причине при разработке своего сканера мы уделили особое внимание этой проблеме, разработав специальный модуль статико-динамического анализа клиентского кода — анализатор JavaScript-кода[2]. Мы рассказывали об этой технологии на Standoff в 2022 году[3]. Удобными особенностями JS-анализатора являются относительная быстрота анализа, игнорирование ветвлений, т.е. весь загруженный код может быть проанализирован без ограничений логики работы приложения, и в нем могут быть найдены необходимые вызовы, включая необходимый формат и параметры. Также, если приложение отдает сразу весь JS-код, появляется возможность без авторизации получить полную карту конечных точек, включая связанные с административными функциями. Также этот анализ интересен пентестерам, с его помощью можно быстро получить информацию о поверхности атаки приложения заказчика.

Таким образом, в SolidPoint DAST проблема обнаружения возможной поверхности атаки и как следствие, проблема сужения проверяемого скоупа приложения эффективно решаются спектром инструментов: статическим и динамическим краулерами, дирбастингом, и уникальным JS-анализатором. Для получения дополнительной информации о конечных точках приложения сканер может интегрироваться с SolidWall WAF, а также способен импортировать спецификацию OpenAPI/Swagger, SOAP, GraphQL сервиса.

О РЕШЕНИИ SOLIDPOINT DAST

SolidPoint DAST входит в реестр отечественного ПО. Разработчиком кода является компания «СолидСофт», которая активно развивает продукт с оглядкой на потребности российских заказчиков.

Мы предлагаем внедрять инструмент SolidPoint DAST как централизованную систему автоматического динамического анализа веб-приложений и API, которая включает возможности масштабирования задач сканирования с единым центром управления и поддержкой горизонтального масштабирования мощностей сканирования. Централизованное управление и разделение доступов позволяют организовать работу множества подразделений одновременно, оптимизируя потребляемые ресурсы. SolidPoint DAST из коробки поддерживает интеграции в различные автоматизированные процессы, как для анализа продуктивных сред, так и для интеграции в среды разработки, с помощью REST API или CLI, взаимодействующего с REST API. Также можно автоматизировать выгрузку результатов сканирования во внешние системы ASOC или интегрироваться с системами управления задачами, например Jira, Redmine и т.п. Таким образом, SolidPoint DAST может решать большой спектр задач автоматизированного сканирования веб-приложений и API на практике.

[1] http://web.archive.org/web/20250424002323/https://axeinos.co/report/The%20Security%20Tools%20Gap.pdf

[2] http://journals.tsu.ru/engine/download.php?id=223281&area=files

[3] https://www.youtube.com/watch?v=vG0EzOr81pE

kaspersky активируй будущее

Защита организации от сложных и целевых атак

Kaspersky Anti Targeted Attack

с модулем NDR

ДиалогНаука

СИСТЕМНАЯ ИНТЕГРАЦИЯ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

dialognauka.ru

С ФОКУСОМ НА БЕЗОПАСНОСТЬ ПРИЛОЖЕНИЙ

ВКЛЮЧАТЬ DAST В ПРОЦЕССЫ СТОИТ РАЗУМНО И ПОСТЕПЕННО

Анна МЕЛЕХОВА
Senior Security Architect, Kaspersky OS

Если вы интересуетесь темой безопасной разработки, то, наверняка читали прошлый выпуск РБПО, посвящённый статическим анализаторам. Сегодня мы поговорим о следующей практике безопасной разработки – динамическом анализе кода (DAST). В статье сосредоточусь на санитайзерах (sanitizers), подклассе инструментов динамического анализа в инструментарии C/C++ разработчиков.

СУТЬ ДЕЛА

Так что же такое динамический анализ и чем он отличается от статического? В первую очередь это процесс тестирования уже скомпилированного кода (либо его частей) в динамике (во время исполнения). Как это происходит? Создаём специальную «санитизированную» сборку с помощью всего лишь дополнительных опций компилятора (-fsanitize=). Такая сборка будет содержать дополнительную инструментацию — некие универсальные проверки, которые будут отрабатывать в ходе выполнения приложения. Тестирование подготовленной сборки и есть процесс динамического анализа.

ПРОВЕРКИ

Сразу становится интересным: какие могут быть проверки, которые не зависят от задач и позволяют санитайзерам быть полезными и для hello_world, и для условного SAP. Это проверки некоторых низкоуровневых инвариантов, нарушение которых приводит к серьёзным ошибкам. И, поскольку мы говорим о безопасном программировании, то речь об ошибках, которые могут использовать атакующие. Например, санитайзер встроит проверку, что к освобождённой памяти не будет обращения (защищая от UAF — use-after-free). Или предотвратит обращение за границу массива на стеке (OOB — out-of-

bound). Также можно проверить на утечки, работу с памятью, надёжность многопоточной работы, отсутствие неопределённого поведения и другое. С помощью опций компилятора можно настроить не только объём проверок, но и поведение программы в случае срабатывания. В зависимости от способа использования динамического анализа в вашей компании разные варианты реакций могут быть полезны — от автоматического оповещения SOC до тихого подавления или рестарта приложения.

О СКРЫТЫХ ПРОБЛЕМАХ

Итак, есть универсальные полезные проверки. И чтобы включить их, нужно лишь добавить флаги компиляции. Значит, достаточно небольшого изменения в пайплайне сборки, чтобы динамический анализ работал и повышал безопасность продукта? И неужели нет скрытых проблем? Конечно, есть.

Во-первых, полезность санитайзеров прямо пропорциональна качеству ваших тестов, обычных и фаззинговых. Если санитайзеры включены для теста с покрытием 1%, вероятность найти утечку памяти или UAF существенно снижается, в отличие от статического анализа. Если до юнит-тестирования вы пока не добрались, браться за DAST нецелесообразно.

Во-вторых, санитайзеры существенно замедляют работу: от 1,5 до 5–6 раз (!) в зависимости от объёма инструментации и характера нагрузки. А значит, многие тесты будут завершаться аварийно по time-out и разработчик будет злиться на краснеющий пайплайн. Когда пайплайны существенно замедлятся, разработчик ради стабильности и надёжности отключит динамический анализ для части тестов. От этого естественным образом снизится и полезность DAST, смотри пункт первый. Ну и при таких замедлениях и речи не идёт о том, чтобы включать динамический анализ в «релизе».

ДВЕ НОВОСТИ

Выходит, что полагаться только на динамический анализ нерационально? Да, но есть и хорошая новость. Некоторые проверки можно выполнить другими средствами. Например, чтобы обнаружить переполнение целочисленного знакового, можно использовать как динамический (-fsanitize=signed-integer-overflow), так и статический анализ. Статический анализ способен найти доступ к неинициализированной переменной. Однако статический анализ тоже раздражает разработчиков: для некоторых правил он выдаёт до 30% ложноположительных срабатываний. Случаются и ложноотрицательные, когда реальная проблема упускается.

Также некоторые проверки из арсенала динамического анализа можно выполнять через харденинги — другой вид инструментирования приложения. При скромном замедлении на 3–10% мы защитим приложение не только от ошибок разработчика, но и от намеренных повреждений при распространении атаки. Например, опция компилятора FORTIFY_SOURCE заменяет обращение к «небезопасным» функциям стандартной библиотеки дополнительными безопасными вставками и так позволяет избегать доступа вне диапазона (OOB). Аппаратный механизм MTE (memory tagging extension) с некоторой вероятностью защищает и от OOB и ошибок вида type confusion. Однако, этот механизм доступен не на всех аппаратных платформах.

УВЫ, НУЖЕН!

Так динамический анализ не нужен? Увы, нужен. Многие проверки не сделаешь иначе как санитайзерами. Это большая часть случаев undefined behavior, утечки памяти и нарушения memory safety разных сортов на «старых» аппаратных платформах или в виртуализованных окружениях. Фаззинговые тесты вообще бесполезны, если не настроены проверки инвариантов, и самая простая из них — инструментирование от санитайзеров, тот самый динамический анализ. Но включать DAST в процессы стоит разумно и постепенно. Я предлагаю идти по пирамиде: тесты, харденинг, статический анализ, динамический анализ, фаззинг (см. рис.). Так вы балансируете уровни пользы и затрат, настраивая проверки под себя для оптимального результата.

* * *

А если искать баланс между разными инструментами и их настройками слишком сложно, можно ориентироваться на систему, созданную с фокусом на безопасность приложений. Мы, разрабатывая KasperskyOS, выстроили всю систему в парадигме конструктивной безопасности и адаптировали инструменты разработки, чтобы сформировать целостный подход к безопасности приложений.

СОВРЕМЕННЫЕ МЕТОДЫ ДИНАМИЧЕСКОГО АНАЛИЗА КОДА

ФАЗЗИНГ-ТЕСТИРОВАНИЕ И ЕГО КЛАССИФИКАЦИЯ

Илья АНТИПОВ
руководитель группы Центра оценки соответствия и тестирования АО «НПО «Эшелон»

Роберт АРУСТАМЯН
заместитель директора Центра оценки соответствия и тестирования АО «НПО «Эшелон»

Нелли МАГАКЕЛОВА
руководитель группы Центра оценки соответствия и тестирования АО «НПО «Эшелон»

ВВЕДЕНИЕ

Динамический анализ безопасности приложений (Dynamic Application Security Testing, DAST) прочно закрепился в арсенале средств обеспечения безопасности информации как метод оценки работающего приложения «извне», с позиции злоумышленника. Традиционные DAST-инструменты эффективно выявляют широкий спектр известных уязвимостей (таких как инъекции, уязвимости конфигурации, небезопасные десериализации), используя предопределённые наборы тестовых векторов и сигнатур, основанных на знаниях о распространённых атаках и уязвимых шаблонах. Тем не менее, несмотря на свою эффективность, классический DAST обладает существенным недостатком: он часто полагается на базы данных уже известных уязвимостей. Это делает его менее эффективным в обнаружении принципиально новых (zero-day) уязвимостей, сложных логических ошибок или уязвимостей, возникающих при обработке специфических, нестандартных или некорректно сформированных входных данных.

Фаззинг-тестирование, в свою очередь, представляет собой методику обеспечения безопасности, основанную на автоматизированной подаче в тестируемую систему большого объёма полуслучайных, искажённых или мутированных входных данных («корпусов») с целью спровоцировать сбои, аварийные завершения или иные неожиданные поведения программы. Именно способность фаззинга исследовать «пограничные случаи» и «неизведанные пути» выполнения кода делает его незаменимым для обнаружения уязвимостей, которые остаются невидимыми для традиционных, сигнатурно-ориентированных методов.

Целью данной статьи является детальное рассмотрение фаззинг-тестирования как активного метода поиска неожиданного поведения программы. В рамках статьи будут рассмотрены методологические аспекты фаззинг-тестирования, его виды, а также преимущества и недостатки.

Способность фаззинга исследовать «пограничные случаи» и «неизведанные пути» выполнения кода делает его незаменимым для обнаружения уязвимостей, которые остаются невидимыми для традиционных методов

ФАЗЗИНГ-ТЕСТИРОВАНИЕ ПРИЛОЖЕНИЙ

Фаззинг-тестирование представляет собой метод динамического анализа безопасности и устойчивости программного обеспечения путём подачи на его вход неверных, неожиданных или случайным образом сгенерированных данных. Его основная цель — выявление ошибок реализации, приводящих к сбоям (крашам), уязвимостям безопасности (таким как переполнение буфера), утечкам памяти или некорректному поведению программы. В соответствии с современными требованиями к надёжности ПО фаззинг-тестирование рекомендуется применять как к собственному коду, так и к интегрируемым сторонним компонентам (биб-

лиотекам, исполняемым файлам), доступным для тестирования в скомпилированном виде.

Первые подходы, схожие с фаззинг-тестированием, заключались в ручном или полуавтоматическом вводе некорректных данных для проверки реакции программы. Это могли быть попытки подачи на вход очень длинных строк, бинарного «мусора», невалидных параметров командной строки или файлов с повреждённой структурой. Подобные методы были трудоёмкими, несистемными и охватывали лишь малую часть возможных аномальных сценариев. По мере развития методологии появились специализированные инструменты, способные автоматически генерировать большие объёмы случайных или структурированных аномальных входных данных («корпусов») и массово подавать их на тестируемую программу, отслеживая её состояние на предмет сбоев. Изначально фокус этих инструментов смещался в сторону улучшения общего качества кода, но со временем акцент сменился на поиск критических уязвимостей безопасности. Это стало возможным благодаря чёткой постановке целей.

Эволюция фаззинг-тестирования от простых методов к сложным инструментам привела к появлению различных методик, классифицируемых по уровню инсайдерской информации, доступной тестеру. Этот уровень доступа напрямую определяет глубину анализа и эффективность поиска уязвимостей. Одним из ключевых критериев классификации фаззинг-тестирования является уровень доступа к внутренней информации тестируемой программы и степень её инструментирования. В зависимости от этого критерия выделяют следующие основные виды.

Фаззинг-тестирование методом чёрного ящика (black-box). Включает взаимодействие с программой исключительно через её стандартные интерфейсы (ввод/вывод, файлы, сеть) без какого-либо доступа к внутренней структуре. Ошибки выявляются путём наблюдения за внешними реакциями системы (падения, зависания, ошибки), моделируя атаку внешнего злоумышленника.

Выбор между black-box, grey-box и white-box фаззингом задаёт рамки возможностей, однако внутри каждой из этих методик критическую роль играет конкретная стратегия формирования входных данных, подаваемых на программу

Фаззинг-тестирование методом серого ящика (grey-box). Включает инструментирование программы для сбора ограниченной внутренней информации, прежде всего о покрытии кода (какие базовые блоки или переходы были выполнены). Эта информация используется для управления генерацией/мутацией данных, отдавая приоритет входам, которые приводят к выполнению новых путей кода, что значительно повышает эффективность поиска глубоких уязвимостей.

Фаззинг-тестирование методом белого ящика (white-box). Включает полный доступ к исходному коду и состоянию программы. Использует методы динамического анализа (включая символьное выполнение) для построения ограничений на путях выполнения и целенаправленной генерации входных данных, удовлетворяющих этим ограничениям, теоретически позволяя находить самые сложные уязвимости, но требует детального изучения исходных текстов программы.

Выбор между black-box, grey-box и white-box фаззингом задаёт рамки возможностей, однако внутри каждой из этих методик критическую роль играет конкретная стратегия формирования входных данных, подаваемых на программу. Именно алгоритм генерации или модификации этих данных во многом определяет, какие участки кода будут протестированы и насколько глубоко. Ключевым аспектом фаззинг-тестирования является стратегия генерации входных данных. По этому критерию выделяют два основных подхода.

Генерационный фаззинг. Включает использование формальной модели или спецификации ожидаемого формата входных данных (грамматика файла, протокола, API). Тестовые данные создаются «с нуля» на основе этой модели, целенаправленно формируя синтаксически корректные, но семантически аномальные входы для проверки глубоких ветвей кода и сложных состояний программы.

Мутационный фаззинг. Включает использование набора валидных входных данных (начальный корпус — seed corpus). Тестовые данные генерируются путём применения случайных искажений (битовые перевороты, замена/удаление/вставка байтов, изменение длины) к этим образцам, позволяя быстро находить ошибки обработки на поверхностном уровне. Для мутации (искажения) используются данные, полученные с помощью обратной связи от приложения. Примерами таких данных могут служить: информация об увеличении покрытия, сведения о новых путях исполнения кода или время выполнения программы.

Эффективность любой стратегии генерации данных — будь то генерационный или мутационный подход — необходимо измерять. Наиболее объективной метрикой здесь выступает покрытие кода, показывающее, какая часть программы была фактически протестирована фаззером. Разные способы расчёта покрытия дают существенно отличающуюся картину тестирования. С точки зрения получения информации по покры-

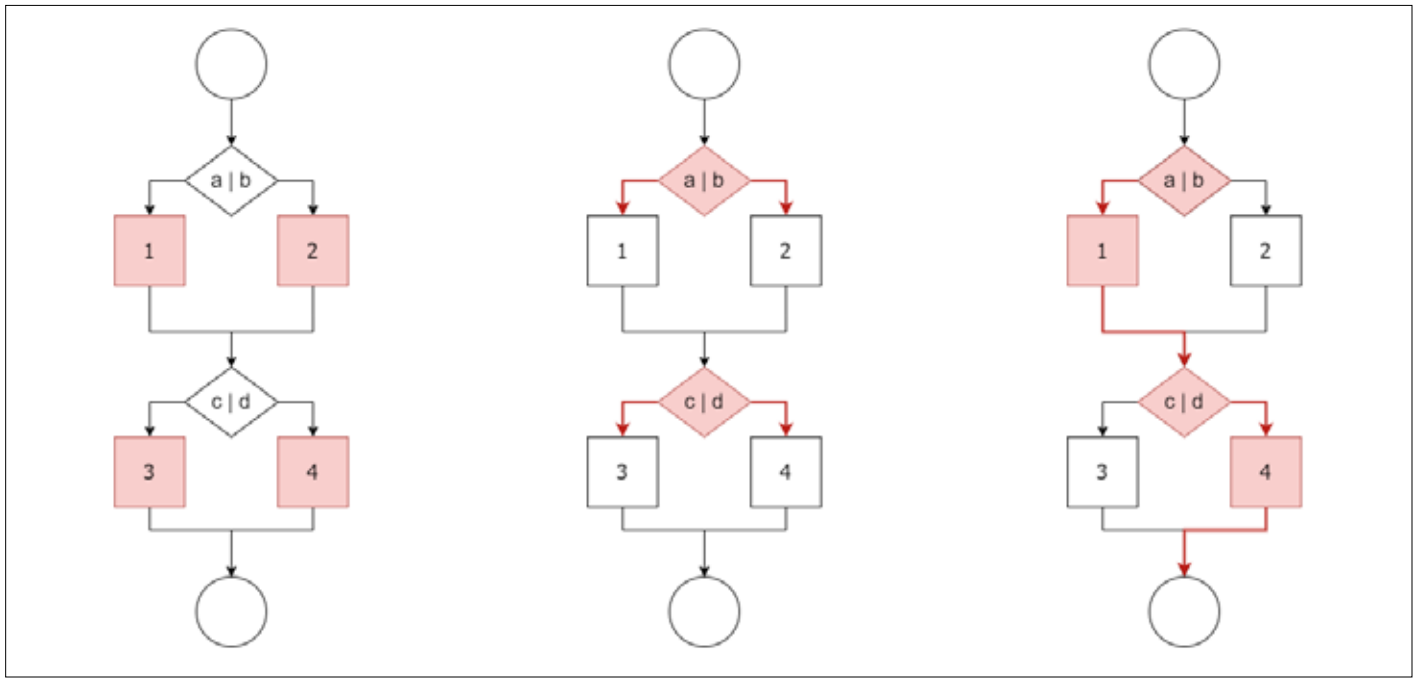


Рисунок 1. (а) — тестовое покрытие по базовым блокам, (б) — тестовое покрытие по ветвям условных переходов, (в) — тестовое покрытие по путям исполнения в программе

тию, которое получается в результате проведения фаззинг-тестирования, выделяются три подхода (рис. 1).

При этом в зависимости от способа сбора тестового покрытия процент, которого достиг фаззер, будет сильно меняться. Если входное значение прошло по блокам 1 и 4, то по базовым блокам мы достигли 50% покрытия (блоки 1 и 4), по условным ветвям мы достигли 50% покрытия (условные переходы a и d), по путям исполнения мы достигли только 25% покрытия (путь a-1-d-4).

Показатели покрытия — важный, но не единственный критерий оценки фаззинга. Для понимания реальной ценности этого метода для тестирования безопасности необходимо взвесить все его сильные и слабые стороны в сравнении с другими подходами. Говоря об эффективности фаззинг-тестирования, стоит учитывать и недостатки. Далее представлена таблица с преимуществами и недостатками фаззинг-тестирования по сравнению с иными подходами к обнаружению ошибок в программах.

Преимущества	Недостатки
Нахождение проблем безопасности, которые невозможно обнаружить при других анализах	Сложность настройки и анализа
Высокая степень автоматизации	Сильная зависимость от инструментации
Эффективность для сложных форматов данных	Низкая эффективность при наличии в программе большого количества входных данных
Высокая масштабируемость	Возможность пропуска редких путей выполнения
Работа на конкретном наборе входных данных	Трудоёмкость и сильные временные затраты
Возможность проведения без наличия исходных текстов программы	Ресурсоёмкость и высокие вычислительные мощности

Таблица. Преимущества и недостатки фаззинг-тестирования

ВЫВОД

Инструменты динамического анализа, и особенно фаззинг-тестирование, играют критически важную роль в обеспечении безопасности и надёжности программного обеспечения, выявляя уязвимости, проявляющиеся исключительно во время выполнения. В отличие от статического анализа, который исследует код, не подразумевая его исполнения, динамический анализ проверяет поведение работающей программы в реальных или близких к реальным условиях. Его ключевая особенность — способность находить сложные, эксплуатируемые баги в обработчиках недоверенных данных (парсерах, протоколах, API), которые часто ускользают от других методов тестирования. Несмотря на свою ресурсоёмкость и необходимость настройки, фаззинг-тестирование является незаменимым элементом современного подхода к разработке безопасного программного обеспечения, дополняя статический анализ и обеспечивая выявление критических уязвимостей на этапе тестирования.

ФАЗЗИНГ-ТЕСТИРОВАНИЕ

ОТ ПРОСТОГО К СЛОЖНОМУ

Степан ХАРИТОНОВ
руководитель направления
безопасной разработки ООО «НПЦ «КСБ»

С августа 2024 года проектом OSS-Fuzz зарегистрировано не менее 750 подтверждённых уязвимостей в open-source-компонентах. Более 30 исправлений ошибок и уязвимостей в коде за этот же период внесено Центром исследования безопасности системного ПО, сформированным при участии отечественных экспертов. Эти цифры объединяет одно: данные уязвимости выявлены видом динамического анализа кода под названием «фаззинг». Тестировщики, которые впервые с ним знакомятся, ассоциируют его с анализом граничных значений, оценкой на основе эквивалентных классов, тестированием property-based. Действительно, эти виды тестирования отчасти покрываются в ходе фаззинга, но всплывают и нюансы, которые делают процедуру не такой уж и простой.

ФАЗЗИНГ: ЧТО ЭТО?

Фаззинг — подход к анализу кода во время его исполнения, основанный на оценке работы программы в ответ на подачу на вход множества невалидных значений. Гибкость в его проведении достигается широкими возможностями:

- в зависимости от оценки выполнения кода фаззинг проводится по принципам «белого», «серого» или «чёрного» ящиков;
- подход к формированию входных значений (семплов) может быть генерационным — не связанным с процессом фаззинга — или мутационным — основанным на получаемом покрытии кода;
- целью исследования может быть как конечный исполняемый файл, так и конкретная библиотечная функция.

Большой ассортимент существующих инструментов, фаззеров, «даёт разгуляться». Однако такая вариативность создаёт определённую сложность в реализации фаззинг-тестирования.

С ЧЕГО НАЧАТЬ?

Простой фаззинг можно запустить «на коленке», достаточно определить цель. В таком случае вы с легкостью сможете выполнить генерационный фаззинг методом «чёрного» ящика: входные семплы генерируются случайно, информации о покрытии кода нет, целью выступает конечный исполняемый процесс, который можно запустить и вручную. Такой подход зачастую применим при фаззинге веб-приложений: программа-клиент отправляет на сервер запросы, в их содержимое подставляются случайные данные. Результат ожидаемо «сырой»: искать «вредные» семплы необходимо самостоятельно.

К ЧЕМУ СТРЕМИТЬСЯ?

Освоение мутационного фаззинга методом «серого» ящика удобно начать с формирования на базе юнит-тестов «фаззинг-обёрток» — программ, вызывающих исследуемый код и подающих на вход данные от фаззера. Интересными целями выступают библиотечные функции: строкочувствительные, утилитарные, с высокой цикломатической сложностью, парсеры, десериализаторы и т.п. Их тест завязан на трёх элементах:

- проинструментированная библиотека;
- фаззер;
- скомпилированная обёртка с входным набором данных, обеспечивающих стартовое покрытие.

Дополнить процесс можно:

- мутаторами, увеличивающими входной набор данных;
- словарями, насыщающими семплы значениями, влияющими на ход выполнения кода.

Работа фаззера сводится к увеличению числа уникальных путей исполнения кода. Но следует помнить, что важен не только конечный уровень покрытия, но и общее число запусков цели. Также для повышения эффективности поиска дефектов при фаззинге, предлагается использовать средства отлова ошибок — санитайзеры, способные фиксировать отклонения от штатного выполнения программы.

ИГРА СТОИТ СВЕЧ

Фаззинг давно доказал свою эффективность, как технология, способствующая повышению качества и безопасности продуктов. Современные тенденции превращают внедрение этой разновидности динамического анализа кода из опционального метода тестирования в устойчивую практику, демонстрирующую практический эффект в поиске ошибок и уязвимостей, которая уже сейчас применяется отечественными разработчиками.

АНАЛИЗАТОР КОДА ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ АК-ВС 3

ИНСТРУМЕНТ, КОТОРЫЙ СОВМЕЩАЕТ В СЕБЕ ТРИ ВИДА ДИНАМИЧЕСКОГО АНАЛИЗА

Виталий ВАРЕНИЦА
заместитель генерального директора АО «НПО «Эшелон»

ВВЕДЕНИЕ

«АК-ВС 3» представляет собой инструмент, предназначенный для автоматизации процесса проведения испытаний при сертификации в соответствии с требованиями различных регуляторов, а также для выполнения периодических проверок в рамках разработки безопасного программного обеспечения. Инструмент объединяет три ключевых метода динамического анализа, которые позволяют детально исследовать поведение программы в условиях реального исполнения, обнаруживать как типовые, так и трудноуловимые ошибки, и обеспечивать соответствие современным требованиям к безопасности программного обеспечения.

ДИНАМИЧЕСКИЙ АНАЛИЗ БЕЗОПАСНОСТИ ПРИЛОЖЕНИЙ (DAST)

Динамический анализ безопасности приложений представляет собой процесс выявления уязвимостей в режиме выполнения (run-time) программного обеспечения. Основные методы динамического анализа включают общий сбор путей выполнения (трассировку выполнения), полносистемный анализ и фаззинг-тестирование.

Общий сбор путей выполнения включает проведение сборки исходных текстов, в которые будут интегрированы специальные датчики. Эти датчики отслеживают проходящие через них вызовы функций и осуществляют запись логов в файл, на основе которых впоследствии осуществляется анализ и формируется трасса выполнения. Это позволяет определить, какие блоки кода были вызваны, а какие остались неиспользованными, а также проследить за прохождением по веткам выполнения.

Таким образом, можно выделить следующие этапы трассировки выполнения:

1. Сбор логов по динамическому выполнению проекта.
2. Обнаружение путей ветвления и исполнения проекта на основе реального выполнения.
3. Определение модулей и функций, через которые проходило выполнение.
4. Выявление мест возникновения ошибок и сбоев.

Данный подход в АК-ВС 3 позволяет выявить наиболее используемые участки кода, а при наличии всех возможных сценариев работы программы с помощью данного метода возможно найти «мёртвый код». В результате данный анализ позволяет из всей кодовой базы выделить именно те участки кода, которые требуют тщательного анализа безопасности кода.

ПОЛНОСИСТЕМНЫЙ ДИНАМИЧЕСКИЙ АНАЛИЗ (КОД2)

АК-ВС 3 обеспечивает эффективное выполнение полносистемного динамического анализа благодаря способности записывать и воспроизводить сценарии работы системы в контролируемой виртуальной среде. Это осуществляется за счёт использования специализированной платформы QEMU и возможностей виртуализации, предоставляемых инструментом. Виртуализация позволяет фиксировать состояние системы на любом этапе, что, в свою очередь, упрощает диагностику сложных и скрытых проблем.

Одной из ключевых особенностей АК-ВС 3 является автоматизированное отслеживание и анализ «помеченных данных» и функций, изменяющих их, что позволяет оперативно выявлять источники и пути распространения «чувствительной» информации и проверять корректность обращения с секретами путём поиска их следов в артефактах работы программы — от переменных окружения до оперативной памяти.

АК-ВС 3 также обеспечивает визуальное представление результатов анализа. Например, с помощью таких инструментов, как граф процессов и flame-граф, пользователи могут легко интерпретировать результаты, видеть конкретные места возникновения проблем безопасности и оперативно устранять их. Это значительно сокращает время анализа и повышает эффективность работы специалистов.

Важным преимуществом инструмента является высокая точность и глубина анализа, достигаемая за счёт сочетания динамического подхода с возможностью детального просмо-

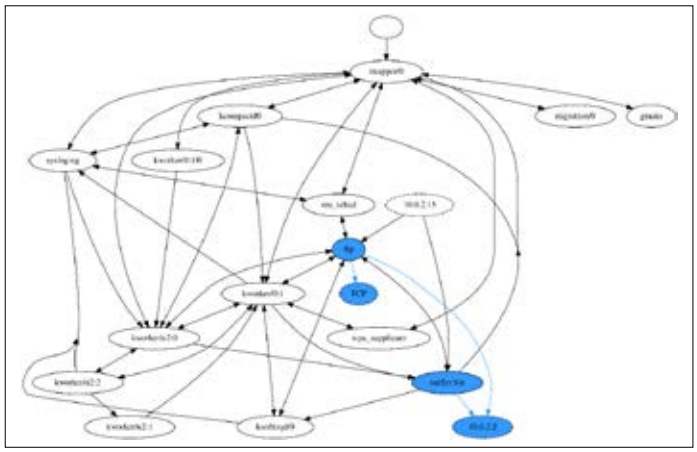


Рисунок 1. Граф, отражающий последовательность вызова функций/программ. Синим отмечены «заражённые» объекты, в которых модифицируются помеченные данные

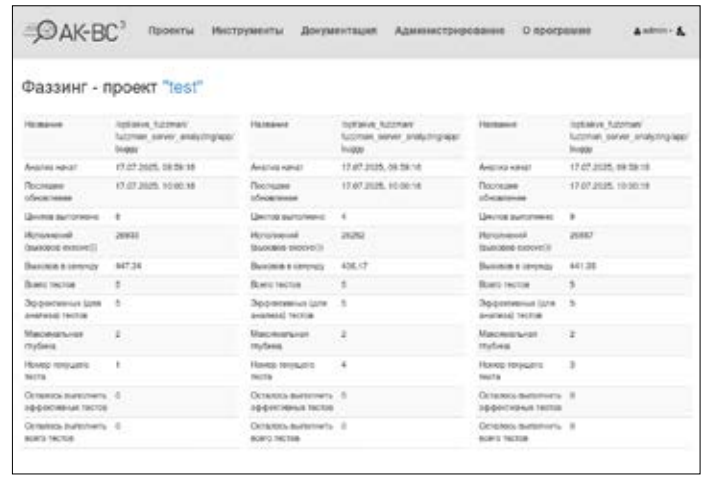


Рисунок 2. Статистика о выполнении фаззинг-тестирования в АК-БС 3

тра состояния памяти и сети на момент выполнения сценария.

Этапы полносистемного анализа включают:

- полносистемный анализ трассы выполнения кода;
- запись данных всей системы с отслеживанием каждого элемента;
- поиск утечек данных и критической информации.

ФАЗЗИНГ-ТЕСТИРОВАНИЕ

Фаззинг-тестирование представляет собой метод исследования, при котором на вход программы подаются случайные данные. В АК-БС 3 реализован современный подход фаззинг-тестирования, основанный на использовании обратной связи (feedback-based fuzzing). Данный подход значительно увеличивает качество проводимого тестирования, так как в данном случае инструмент получает информацию о том, как случайные данные влияют на систему. Стоит отметить, что для получения наиболее точной информации о внутреннем состоянии программы данный подход требует доступа к исходному коду программы. Однако также предусмотрена возможность фаззинг-тестирования без статического инструментирования, если доступ к исходным текстам ограничен. Входные данные генерируются с использованием как мутационных, так и генерационных методов. Для повышения качества генерируемых данных возможно использование динамического символьного выполнения — метода, при котором внутренние и внешние данные программы оцениваются как абстрактные символьные переменные, а не как конкретные значения.

АК-БС 3 содержит в себе все необходимые модули для качественного проведения фаззинг-тестирования:

- различные виды компиляторов для инструментации исходных текстов (при необходимости инструментации);
- модуль фаззера;
- специальные датчики, которые находят ошибки в поведении программы, которые не может выявить оригинальный AFL++;
- инструмент динамического символьного выполнения.

Также необходимо отметить удобство использования веб-интерфейса АК-БС 3 — одна из тех деталей, которые превращают фаззинг в прозрачный рабочий процесс. Достаточно открыть браузер, выбрать проект, и вы сразу видите живую картину: как меняется интенсивность прогона по времени, сколько найдено уникальных сбоев и другую сводку результатов фаззинг-тестирования (рис. 2).

ЗАКЛЮЧЕНИЕ

АК-БС 3 — комплексное решение для обеспечения безопасности программного обеспечения, объединяющее современные методы анализа и механизмы соблюдения нормативных требований. Благодаря гибкой архитектуре и интеграции с конвейерами CI/CD продукт легко встраивается в процессы разработки и выступает единой мощной платформой тестирования. На одной площадке можно проводить разные виды проверок и выполнять регулярный анализ безопасности на протяжении всего жизненного цикла ПО. Клиент-серверная архитектура обеспечивает быструю интеграцию, масштабируемость и удобное сопровождение, позволяя централизованно управлять проектами и распределять вычислительную нагрузку между несколькими узлами в инфраструктуре разработчика.

* * *

Для отслеживания последних новостей в сфере информационной безопасности подписывайтесь на наш телеграм-канал Echelon Eyes (*t.me/EchelonEyes*):

ЦИФРОВОЙ РУБЛЬ В ТЕЛЕФОНЕ

ЧТО ГОВОРИТ СТАНДАРТ ЦР ПРО МОБИЛЬНЫЕ ПРИЛОЖЕНИЯ И ПРИ ЧЁМ ТУТ ТРАССА ВЫЗОВОВ?

Юрий ШАБАЛИН
директор продукта AppSec.Sting

Платформа цифрового рубля постепенно превращается из концепции в реальность. Переводы между физическими лицами, оплата в торговых точках, работа кассы мерчанта — все эти сценарии должны быть интуитивно доступны со смартфона в ближайшее время. В этой парадигме мобильное приложение, в которое участники платформы встраивают Программный модуль Банка России (ПМ БР), становится не просто интерфейсом, а ключевым звеном в этой цепочке. Именно поэтому мобильное приложение с интегрированным ПМ БР становится центральным элементом всей архитектуры платформы. Однако эта центральная роль делает мобильное приложение и самым уязвимым звеном. Здесь пересекаются требования пользовательского опыта, криптографической стойкости и регуляторного соответствия. Любое изменение в коде приложения потенциально может повлиять на работу ПМ БР, что автоматически требует дополнительных проверок со стороны надзорных органов.

ЧТО В СТАНДАРТЕ?

Опубликованный «Стандарт Платформы цифрового рубля» от 20 ноября 2024 года (далее — Стандарт) чётко определяет статус мобильного приложения с интегрированным ПМ БР: он относится к средствам криптографической защиты информации. Это означает, что каждое обновление приложения формально требует прохождения процедуры оценки влияния изменений в аккредитованной лаборатории.

Но понимая, что мобильные приложения обновляются значительно чаще традиционного программного обеспечения и изменения в приложениях могут не затрагивать функционал, связанный с цифровым рублём, регулятор предусмотрел компромиссное решение: если в новой версии МП сохранились «неизменность трасс вызовов и порядка вызовов ПМ БР», то повторная оценка влияния не нужна, достаточно предоставить материалы, подтверждающие эту неизменность.

Если посмотреть детальнее, то Стандарт предъявляет к мобильным приложениям два основных требования:

1. Фиксировать и сравнивать трассы вызовов встроенного ПМ БР для каждой новой сборки.
2. Доказывать, что публичная сборка, размещённая в магазине приложений, идентична той, что была проверена в аккредитованной лаборатории.

Стандарт констатирует, что нужно получить (граф вызовов, контрольные суммы), но умалчивает, как этого достичь в реалиях современной мобильной разработки. В этой статье мы последовательно разберём эти вопросы и представим проектные методики, которые закрывают технические и организационные меры, позволяя автоматизировать получение необходимой информации для соблюдения регуляторных норм.

ТРАССЫ ВЫЗОВОВ, ЧТО ЭТО И КАК ПОЛУЧИТЬ?

Итак, для того, чтобы упростить себе жизнь, нам необходимо построить трассу вызовов и при каждом обновлении приложения доказывать её неизменность. Вроде бы ничего сложного, но давайте разберёмся.

Для начала определим, что же такое «Трасса вызовов». По сути, это последовательность инструкций и функций, которые выполняются при обращении к Программному модулю Банка России.

Как же построить эту трассу? Это один из главных вопросов, на который ответа пока что нет, Стандарт прямо требует, чтобы «неизменность трасс вызовов и порядка вызовов ПМ БР в составе МП» подтверждалась при каждом релизе; при этом сами трассы «разрабатываются (согласовываются) совместно с испытательной лабораторией». Формально метод оставлен на усмотрение разработчика и лаборатории, поэтому практика только складывается.

На первый взгляд задача кажется простой: запусти любой популярный сканер, получи граф вызовов и сравни с эталоном. Но основная сложность построения трасс вызовов заключается в том, что современные мобильные приложения представляют собой сложные многослойные системы. Android-приложения могут содержать код одновременно на Kotlin, Java, использовать динамическую загрузку модулей. iOS-приложения сочетают Swift, Objective-C, также могут включать нативные компоненты.

Ну а множество современных фреймворков с «синтаксическим сахаром» делают разработку удобнее, но анализ такого кода сильно затрудняется[1]. Классические инструменты статического анализа очень плохо справляются с задачей построения полного графа вызовов в таких сложных и разнообразных системах. Они могут проанализировать код на одном языке, но теряют связи на границах между языками, не понимают динамически создаваемые вызовы, не всегда поддерживают всё многообразие фреймворков и путаются при использовании в коде «сахара».

Что делать в том случае, когда статические анализаторы не справляются? На мой взгляд, тут на помощь приходит анализ уже скомпилированного кода. После компиляции весь «синтаксический сахар» разворачивается компилятором в стандартные конструкции, Java и Kotlin унифицируется в один формат для корректного восприятия виртуальной машиной Android, все трансграничные вещи между Objective-C и Swift имеют точную и явную связь и отображение в бинарном файле. То есть вместо запутанного, сложного и непредсказуемого кода можно использовать унифицированный и единый формат представления после компиляции.

Таким образом, практическое решение задачи построения трасс вызовов требует комплексного подхода, объединяющего несколько технологий и методик. Процесс методически можно разбить на четыре ключевых этапа, каждый из которых решает определённую техническую задачу.

ЭТАП 1: ПОДГОТОВКА «ЧИСТОЙ» СБОРКИ

Первый шаг — получение приложения в форме, пригодной для анализа. Для Android это означает APK или AAB без обфускации. Для iOS требуется IPA-файл с сохранёнными dSYM-символами, содержащими отладочную информацию. Эти артефакты должны быть подписаны тем же ключом, который будет использоваться для финальной сборки, чтобы исключить возможность подмены.

ЭТАП 2: ПОСТРОЕНИЕ ОРИЕНТИРОВАННОГО ГРАФА

Второй этап заключается в построении полного ориентированного графа вызовов, где каждая вершина представляет метод или функцию, а каждое направленное ребро — возможный вызов. Граф сохраняется в стандартизированном формате (GraphML, Mermaid и других), что обеспечивает совместимость с раз-

[1] Синтаксический сахар в программировании — упрощённые формы записи конструкций языка, которые не меняют логику работы программы, но делают код более читаемым и удобным для написания. Это своего рода «дополнительные возможности» в синтаксисе, которые позволяют выражать те же идеи более лаконично и понятно для разработчика.

личными инструментами анализа и визуализации.

ЭТАП 3: ФИЛЬТРАЦИЯ И ВЫДЕЛЕНИЕ ТРАСС ПМ БР

Критически важным является третий этап — фильтрация полного графа с целью выделения только тех путей, которые связаны с ПМ БР. Из полного графа, содержащего десятки тысяч вершин, необходимо выделить подграфы, описывающие все возможные пути обращения к методам ПМ БР. Алгоритм фильтрации начинает с известных точек входа в ПМ БР и рекурсивно обходит граф в обратном направлении, находя все методы, которые прямо или косвенно могут привести к вызову модуля.

ЭТАП 4: СРАВНЕНИЕ С ЭТАЛОНОМ

Финальный этап — сравнение полученных трасс с эталонными, зафиксированными при первичной экспертизе. Алгоритм сравнения ищет структурные различия: добавленные или удалённые вершины, изменившиеся связи, новые пути вызовов. Любые изменения, затрагивающие цепочки, ведущие к ПМ БР, классифицируются как «критичные» и требуют дополнительного анализа.

В результате мы получаем гарантированно повторяемый и стабильный результат по составлению и контролю трассы вызовов, который подсвечивает любые изменения или новые трассы до методов ПМ БР, что полностью соответствует описанным требованиям в Стандарте.

ДОКАЗАТЕЛЬСТВО ИДЕНТИЧНОСТИ СБОРОК

Но остаётся ещё один вопрос: как доказать, что приложение, которое передаётся на анализ в испытательную лабораторию, соответствует тому, что выкладывается в магазины приложений?

Казалось бы, сравни два файла, посчитай хеш-суммы и убедись в идентичности. Но как оказывается, это совсем не тривиальная задача, так как при сборке даже из одного и того же кода приложение будет иметь разные хеш-суммы по разным причинам. Это и различные создаваемые во время сборки файлы, и уникальные для каждой сборки идентификаторы (рекламные, аналитические и другие). Более того, магазины приложений сами вносят изменения в приложения. Например, Google Play с 2021 года требует загрузки приложений в формате AAB (Android App Bundle), который затем автоматически разделяется на device-специфичные пакеты и переподписывается ключами, сгенерированными на стороне Google. Apple же применяет к приложениям FairPlay-шифрование, которое кардинально изменяет структуру исполняемого файла. В результате контрольная сумма приложения в магазине никогда не совпадает с контрольной суммой исходной сборки. А если разработчик приложения применяет усиленные меры шифрования для своих сборок — это отдельная история.

Дополнительную сложность создаёт обфускация кода. Для анализа в лаборатории требуется «чистая» сборка без обфускации, но финальная версия для публикации в магазинах приложений обязательно проходит процедуры минификации и запутывания кода. И все эти, и другие неупомянутые нюансы делают проверку соответствия между версиями совершенно нетривиальной задачей.

Решение этой проблемы лежит в плоскости организационно-технических мер, сочетающих технические маркеры с процедурными гарантиями. Ключевая идея заключается в том, чтобы вместо контроля каждого байта исполняемого файла фиксировать «отпечаток происхождения» — набор метаданных, который остаётся неизменным на всём пути от исходного кода до финального приложения. Такой подход предполагает автоматическое внедрение в каждую сборку уникальных идентификаторов.

Организационная составляющая решения требует строгого контроля доступа к релизным ключам и переменным сборочного конвейера. Все операции должны выполняться автоматически и только в CI/CD-системе, исключая возможность ручного вмешательства. Перечень лиц, имеющих доступ к критически важным компонентам, должен быть документально зафиксирован и ограничен техническими средствами. Такое решение позволяет владельцу ПО скачать приложение из магазина, извлечь из него метаданные происхождения и сопоставить их с данными из лабораторного протокола. Организационные меры обеспечивают, что эти метаданные не могли быть подделаны благодаря защищённому процессу сборки и ограниченному доступу к ключам подписи.

ЗАКЛЮЧЕНИЕ

Стандарт цифрового рубля ставит перед рынком правильные цели — обеспечить безопасность и контроль над критически важным компонентом, ПМ БР. На данный момент два ключевых требования, контроль неизменности трасс вызовов ПМ БР и доказательство идентичности сборок, сформулированы на концептуальном уровне, далее необходимы конкретные методические рекомендации и технические спецификации.

Индустрия мобильной разработки уже располагает технологиями, методиками и экспертизой, необходимыми для создания эффективных решений данной задачи. Предложенный в статье комплексный подход демонстрирует, как современные DevSecOps-практики могут быть адаптированы для соответствия требованиям финансового регулятора без ущерба для скорости и качества разработки.

Ключевые принципы предложенного решения, автоматизация рутинных операций, стандартизация форматов данных, прозрачность процессов и разделение ответственности между техническими и организационными мерами, превращают регуляторные требования из потенциального увеличения Time2Market в катализатор технологического развития отрасли.

Дальнейшее развитие предложенного подхода требует тесного взаимодействия между тремя ключевыми группами участников: технологическими командами, создающими инструменты и методики, регуляторными органами, формализующими требования и процедуры, и бизнес-сообществом, обеспечивающим реальное внедрение решений в коммерческую практику.

МОБИЛЬНЫЕ ПРИЛОЖЕНИЯ ВЫХОДЯТ НА НОВЫЙ УРОВЕНЬ. НО ХАКЕРЫ ОПЕРЕЖАЮТ

Юрий ШАБАЛИН
директор продукта AppSec.Sting

95% клиентов банков пользуются финтех-услугами посредством мобильных приложений — это статистика крупнейших банков России. При этом 90% мобильных приложений для ФинТех содержат серьезные уязвимости. Такой результат показало исследование мобильных приложений, проведенное платформой AppSec.Sting компании AppSec Solutions, опубликованное в 2025 году. Уязвимостей высокого и критического уровня становится больше, несмотря на активное развитие безопасной разработки. Директор по продукту AppSec.Sting Юрий Шабалин рассказал об основных трендах в безопасности мобильных приложений в 2025 году.

— Звучит как парадокс: мобильные приложения — самый быстроразвивающийся сервис, но и самый уязвимый, почему?

— Мобильные приложения — самый молодой клиентский продукт, в отличие от веба, которому уже больше 40 лет, приложения появились лет 15 назад. Раньше они были просто витринами данных: отображали информацию, поступающую с бэкэнда, и на этом всё — никакой особой логики внутри не было. Сейчас же мобильные приложения представляют собой самостоятельные, сложные системы со своими фреймворками, архитектурой, межпроцессным взаимодействием. Внутри одного приложения может быть очень сложный архитектурный код, со своими проблемами в бизнес-логике — и всё это на стороне клиента, на самом устройстве пользователя. При этом очень немногие понимают, как на самом деле устроен процесс дистрибуции мобильных приложений, то есть каким образом они попадают к пользователю. Немало возможностей хакерам предоставляет использование сторонних сервисов. Например, отправка push-уведомлений, установка точек банкоматов на карте и многое другое.

— Возьмем, например, финтех. В чем основное отличие в области безопасности?

— Если уязвимость обнаружена на веб-сайте, срабатывает традиционная система защиты данных: ИБ-инженеры применяют наложенные средства защиты, Web Application Firewall, чтобы не дать злоумышленникам использовать уязвимость. Это своего рода «пластырь на ране». Затем нужно «обработать рану»: устранением проблемы компания занимается во внутреннем контуре. Инженеры полностью контролируют среду выполнения: это их серверы, они знают, где они находятся, кто к ним имеет доступ, как их обновлять. А в случае с приложением мы не контролируем среду, и даже если удастся выявить и оперативно вылечить уязвимость, придется ждать модерации исправленной версии и выхода обновления приложения.

— Достаточно ли в распоряжении компаний средств для этого?

— В распоряжении коммерческого сектора не так много продуктов, которые позволяют выполнять проверку приложений комплексно. На сегодняшний день, единственная платформа автоматизированного анализа мобильных приложений, которая сочетает несколько видов анализа — это AppSec.Sting.

Ручной анализ мобильного приложения обычно занимает около двух дней, а платформа справляется с этим за два часа. Это автоматизированный и повторяемый процесс, который можно встроить в цикл разработки. После каждой сборки вы получаете отчёт о безопасности и понимаете, какие уязвимости есть в приложении, что именно выходит в релиз. Это значительно ускоряет анализ и сокращает затраты на обеспечение безопасности.

Кроме того, благодаря AppSec.Sting специалист по тестированию на проникновение сможет сосредоточиться на тех проблемах, которые невозможно обнаружить автоматически.

Наш продукт обеспечивает максимальное покрытие за счёт различных практик анализа. Мы смотрим на приложение со всех сторон: анализируем его в статике — исходный код, декомпилированный или восстановленный, — запускаем на устройстве, наблюдаем за его поведением, отслеживаем сетевые запросы, выясняем, куда и какие данные уходят, и как приложение взаимодействует с внешними сервисами, так называемыми third-party.

Платформа проводит и компонентный анализ: определяем, какие библиотеки используются в приложении, и оцениваем их уязвимость. То есть AppSec.Sting позволяет охватить практически все аспекты безопасности.

ИНЖЕНЕРНЫЙ ПОДХОД К БЕЗОПАСНОСТИ В IDECO

АРХИТЕКТУРА, ПРОЦЕССЫ, ИНТЕРФЕЙС

Владимир ИВЧЕНКО
системный архитектор Ideco

Илья СОБОЛЕВ
менеджер по продукту Ideco NGFW

Марк КОРЕНБЕРГ
CTO Ideco

Создание корпоративного NGFW требует не только абстрактного подхода, но и конкретных инженерных решений, учитывающих реалии эксплуатации. В Ideco архитектура проекта строится на кейсах заказчиков, внутренних ценностей и опыте эксплуатации в сложных инфраструктурах. Ниже — обзор принципов, которыми мы руководствуемся в разработке.

ИСХОДНАЯ ТОЧКА — ПОЛЬЗОВАТЕЛЬСКИЕ СЦЕНАРИИ

Технические решения не принимаются вслепую. Помимо собственных компетенций и изучения конкурентных решений, мы регулярно проводим интервью с заказчиками: собираем обратную связь с пилотов, из поддержки, от пресейлов. Анализируем не только «что нужно», но и «как это используется». Это позволяет понять ограничения, с которыми живёт инфраструктура заказчика, и то, как наша архитектура должна адаптироваться к потребностям. Интерфейс, модули, структура, способ реализации — всё строится от задачи, а не от абстрактного идеала. Иногда это означает усложнение архитектуры ради простоты в эксплуатации — но это разумный обмен.

ИЗОЛЯЦИЯ CONTROL PLANE И DATA PLANE — НЕ ОПЦИЯ, А ТРЕБОВАНИЕ

В корпоративной архитектуре сети управления и сети передачи данных жёстко разделены — они имеют разную адресацию и разные политики доступа. Управляющий трафик считается доверенным, а пользовательский — потенциально враждебным. Поэтому изоляция Control Plane и Data Plane — это не вопрос удобства, а требование безопасности.

В Ideco NGFW это реализовано через изолированные контейнеры VCE: управляющая и трафиковая части работают раздельно, с разными ресурсами и изоляцией на уровне сети и процессов. В других решениях это достигается через отдельные ВМ или даже разные платы (как у Check Point).

Control Plane и Data Plane имеют разные архитектурные требования: к языкам, отказоустойчивости, производительности и логике взаимодействия. Такое разделение позволяет сохранить управляемость NGFW даже при атаке на Data Plane — и наоборот. Это критично при восстановлении, отладке или экстренной смене конфигурации.

КОНТЕЙНЕРНАЯ МОДЕЛЬ С VCE: ЭТО ПРО МАСШТАБИРУЕМОСТЬ

Каждый VCE (Virtual Context Engine) — это логически сетевая изолированная среда, фактически это копия NGFW (отдельно запущенные копии всех программ для обработки сети со своей копией сетевого стека). Она используется для разделения политик доступа, зон безопасности. Это не просто удобство, а механизм управления сложной инфраструктурой. VCE позволяет оптимизировать потребление ресурсов: у каждого контекста своя адресация, маршруты, сессии и журналирование. Ранее отчётность хранилась внутри каждого VCE, но это привело к росту потребления памяти. С сентября 2025 года мы централизуем хранение данных в корневом контексте, чтобы уменьшить нагрузку и упростить поддержку. Этот переход стал логичным продолжением пути оптимизации, и мы не исключаем, что в будущем подобная консолидация затронет и другие тяжёлые сервисы.

АТОМАРНОСТЬ КОНФИГУРАЦИЙ КАК СРЕДСТВО ОТКАЗОУСТОЙЧИВОСТИ

Состояние системы не должно зависеть от того, прервалась ли сессия администратора во время внесения изменений, отключилось ли питание. В Ideco NGFW изменение конфигурации либо полностью применяется, либо откатывается. Это принцип архитектуры, а не «удобная фича». Цель — исключить рассогласованность между подсистемами. Атомарность конфигураций позволяет выполнять обновление в автоматическом режиме в течение 5–10 минут. В перспективе рассматриваем переход к транзакционному применению настроек — по аналогии с подходами западных вендоров, когда изменения группируются и применяются только по подтверждению администратора.

OPEN SOURCE — С АДАПТАЦИЕЙ И КОНТРОЛЕМ

Использование внешнего кода — нормальная практика. Но мы не переносим чужие проекты в чистом виде. Библиотеки анализируются, интегрируются как модули, подвергаются фаззингу, покрываются тестами. Некоторые подсистемы (например, Suricata) доработаны вручную. Всё, что попадает в сборку, проходит через наш CI, и мы исключаем неконтролируемые зависимости. Также в разработке применяются внутренние политики: мы не используем.tar.gz из интернета, не доверяем сторонним бинарным репозиториям, не допускаем автоматических зависимостей без ручной ревизии. Такой подход может показаться избыточным, но он позволяет избежать классических проблем supply chain-инцидентов, которые в последние годы затронули десятки вендоров.

Мы не делаем «коробочное решение с галочками». Мы делаем систему, которая не теряет управляемость тогда, когда это критично. И именно поэтому в наших приоритетах — не только функциональность, но и прозрачность, отказоустойчивость и операционная предсказуемость

CI/CD-ПРОЦЕСС: СТРОГАЯ РЕГЛАМЕНТАЦИЯ ВМЕСТО «БЫСТРОГО РЕЛИЗА»

Релизы каждый месяц возможны только при стабильной инфраструктуре. Каждая фича живёт в своей ветке до полной готовности. DroneCI, шаблоны jsonnet, автоматические сборки, автотесты в VK и Yandex Cloud, ручные проверки, статус-контроль версий — всё это выстроено в пайплайн. Мы не делаем «релиз по флагу», а стабилизируем каждый образ перед публикацией. Важной особенностью является то, что вся сборочная инфраструктура — собственная. Мы не полагаемся на SaaS-инструменты и разворачиваем весь процесс внутри облаков, которыми управляем самостоятельно. Это позволяет не только быстрее реагировать на ошибки, но и гарантировать предсказуемость среды сборки.

ИНТЕРФЕЙС КАК ИНСТРУМЕНТ УМЕНЬШЕНИЯ ОШИБОК

Понятный интерфейс снижает порог ошибок. Дашборды по пользователям, контекстное создание объектов, фильтры, drag & drop — это не декоративные элементы. Это способ быстрее диагностировать, кто генерирует аномальный трафик и как на него реагировать. Мы постепенно выносим в UI те настройки, которые раньше были доступны только через терминал. Это не упрощение, а повышение управляемости. Интерфейс становится частью инженерной дисциплины: он не заменяет документацию, но позволяет ускорить принятие решений в условиях инцидента.

ЗАКЛЮЧЕНИЕ

Ideco NGFW — это набор архитектурных решений, принятых для того, чтобы продукт был предсказуемым в эксплуатации, масштабируемым в инфраструктуре и устойчивым к сбоям. Мы не делаем «коробочное решение с галочками». Мы делаем систему, которая не теряет управляемость тогда, когда это критично. И именно поэтому в наших приоритетах — не только функциональность, но и прозрачность, отказоустойчивость и операционная предсказуемость. Это не лозунги, а результат конкретных инженерных решений, о которых мы честно рассказываем.

ТРИ ВОПРОСА МЕНТОРУ

КТО ПОМОГАЕТ ИБ-СТАРТАПАМ ДОБИТЬСЯ УСПЕХА

BIS Journal продолжает рубрику, посвящённую ИБ-стартапам Киберхаба Фонда «Сколково». Сегодня представляем в лицах деятельность менторов, помогающих новорождённым компаниям найти свой курс в бушующем море рынка.

Игорь БИРЮКОВ
руководитель Киберхаба Фонда «Сколково»

Суть стартапа заключается в коммерциализации инновационного решения. Перед начинающими предпринимателями возникает много проблем: надо определить объём рынка, целевую аудиторию (кто клиент), позиционирование продукта, его окупаемость и многое другое. И логичный вопрос: а откуда это всё узнать и куда обратиться за помощью?

Мы все знаем, что новые решения создают в первую очередь инженеры ИБ с разработчиками, и про коммерциализацию продукта им мало что известно. Новые технологии — это замечательно, но работать на благо клиента и государства получится только через продажу.

В России существует множество институтов развития, и они содействуют продвижению инновационных решений льготами и поддержкой менторов. Киберхаб «Сколково» также предоставляет менторов, являющихся опытными специалистами в конкретной отрасли. Они готовы ответить на все вопросы как в начале пути стартапа, так и на этапе бурного развития, уберечь от ошибок.

Предлагаю познакомиться с нашими менторами. Мы попросили их ответить на три вопроса: в чём суть их работы? Почему они этим занимаются? Что для них является мерилом успеха?

Анна ЛУЧНИК
специалист в сфере разработки ПО

«УСПЕХ — КОГДА МЕНТОР БОЛЬШЕ НЕ НУЖЕН»

Главная задача ментора — ускорить развитие стартапа-резидента и повысить его шансы на коммерческий успех, помогая избежать типичных ошибок. Часто его путают с консультантом, который принесёт готовое решение. Ментор показывает правильное направление, но не даёт проработанных документов со стратегией или готовых ответов.

Часто приходится быть переводчиком с языка стартапа (особенно технологического) на язык инвесторов и бизнеса. Иногда основатель жалуется на «плохих инвесторов» или «незрелых клиентов», а проблема в том, что он сам не может внятно объяснить свою бизнес-модель или преимущества продукта.

Мне важно, чтобы проект меня зацепил — либо амбициозностью задачи, либо нестандартным подходом, либо харизмой команды. Отказываюсь от проектов, где основатели не готовы честно смотреть на свои ошибки и меняться, чтобы достичь результатов, которые сами заявляют. Также не беру команды, которые ищут не ментора, а «волшебную палочку» для решения их проблемы без их участия.

Для меня успех — это когда ментор меняет у основателя видение проблемы и иногда даже картину мира. Другой критерий успеха — когда я становлюсь ненужной. Это значит, что основатель не просто решил конкретную проблему, а освоил методологию. После успешных сессий с ментором стартап начинает задавать правильные вопросы, разрушающие иллюзии, и смотреть на проблемы шире, вне рамок решения базовой задачи. Мне нравятся кейсы, где небольшими, недорогими изменениями удаётся перевернуть череду неудачных взаимодействий с клиентами, инвесторами или собственной технической командой.

Елена НЕПОЧАТОВА
специалист в сфере продаж

«МЕНТОРСТВО ДЛЯ МЕНЯ ПОДОБНО ИНВЕСТИРОВАНИЮ»

Главная задача ментора — создать условия, при которых цели владельца бизнеса могут быть достигнуты. А для этого важно двигаться шаг за шагом, ступенька за ступенькой. И на каждом этапе надо правильно сформулировать запрос, а потом, при достижении результата, детализировать, оцифровать этот результат. И только после этого стартап может сделать следующий шаг, перейти к следующему этапу своего развития. Построение бизнеса — эволюционный процесс, и перескочить через ступеньку тут не получится.

Я сразу говорю ребятам, где знаю, что делать, потому что делала, а где нет, и тут будет элемент творчества и эксперимента. Вообще, менторство для меня очень похоже на инвестирование: очень рискованно инвестировать в темы, где собственной экспертизы мало, однако, если стартап готов рискнуть, а тема для меня интересная, всегда возникает эффект синергии.

Всегда есть момент перелома: у ребят вроде и продукт хороший, и горы они готовы свернуть, но пока команда не дозрела ментально до желаемого масштабирования, она, словно подросток, упорно «гнёт свою линию», которая — со стороны это очевидно — ни к чему хорошему не приведёт. Об успехе можно говорить, только когда владелец точно понял, чего хочет и как к этому прийти. После этого можно перейти от активного общения к формату единичных консультаций. Корабль, как говорится, пошёл своим курсом.

Оксана ТКАЧЁВА
специалист в сфере HR

«СИЛЬНОЕ ЯДРО КОМАНДЫ КОМПЕНСИРУЕТ ДЕФИЦИТ РЕСУРСОВ»

По моему мнению, менторы — это профессионалы, обладающие высокой степенью насмотренности и демонстрирующие на опыте тиражируемый успех. Их задача — используя свой многогранный опыт, обеспечить молодых предпринимателей прикладными знаниями, применимыми на практике.

Основатели стартапов обычно обращаются ко мне с такими запросами, как формирование команды, организационный дизайн, решение вопросов найма и мотивации. Я понимаю глубоко ИТ-отрасль и могу быть в ней максимально полезна. Определяю со стартапом образ результата совместной работы, и это для нас становится ориентиром. Если результат не достигнут, то разбираемся в причинах и меняем курс к его достижению.

Одна из тем работы с ментором — регулярный менеджмент. У собственников стартапов есть видение вектора движения бизнеса, но, когда доходит до тактической реализации, возникают проблемы с управлением целями и командой, что приводит к нарушению сроков, снижению качества, конфликтам.

Мерилом успеха для меня являются переход от команды единомышленников в развивающуюся компанию с устойчивой выручкой. На этом пути приходится реализовывать пересборку команды и повышать прозрачность процессов внутри неё. При дефиците ресурсов очень важно формировать сильное ядро команды, которое способно привести стартап к достижению стратегических целей.

Татьяна БЕЛЕЙ
специалист в сфере маркетинга

«ФОКУСИРУЕМСЯ НА ТОМ, ЧТО ДЕЛАЕТ УСПЕХ ВОЗМОЖНЫМ»

Основная задача — помочь стартапам преодолеть технические и бизнес-проблемы, а также ускорить рост и выход на рынок. Такой запрос присутствует всегда. Например, на конференции Skolkovo Startup Village в конце мая ко мне с такой просьбой обратилось 16 стартапов. Там работало ещё более десятка менторов, у них спрашивали о том же.

Успех зависит от множества факторов, и наличие только классной технологии не гарантирует его достижения. Ментор может помочь оценить рынок, дать рекомендации, как отстроиться от конкурентов, на чём делать акценты и т.д. Самое главное, если ты веришь в своё решение, надо действовать. Вместо того чтобы объяснять, почему что-то невозможно, нужно придумать и сфокусироваться на том, как сделать это возможным. В этом и могут помочь менторы.

Технические и маркетинговые знания, а также большой опыт работы в вендорах и интеграторах дают мне возможность разговаривать на одном языке с техническими специалистами, экспертно оценивать рынок, делать глубокие исследования и писать стратегии. Рынок турбулентный, все пытаются оперативно решить, как действовать дальше. И тут внешняя экспертиза даёт другой взгляд, новый опыт. Важно и отсутствие страха, умение говорить собственнику «как есть», задавать неожиданные, часто неудобные вопросы. В итоге я и моя команда вместе находим новые возможности для развития и роста продаж.

ДОЛЖНОСТЬ — ПЕРЕВОДЧИК С ИТ-ШНОГО

ВОПРОС С ЗАРПЛАТОЙ РЕШАЕТСЯ

Дарья ПЕНЗЕВА
корреспондент BIS Journal

Ирина СМИРНОВА
корреспондент BIS Journal

Знакомая журналистка рассказывала случай: послала её редакция писать репортаж с круглого стола, где собрались одни ИТ-специалисты. Материал не вышел, поскольку, по словам коллеги, все выступающие говорили на каком-то «птичьем» языке, где понятны только предлоги. «Мне тогда был нужен переводчик с ИТ-шного», — пошутила она. Но в каждой шутке лишь доля шутки. И при сегодняшних темпах цифровизации различных отраслей, когда информационная безопасность стала критически важной для выживания бизнеса, всё больше компаний внедряют в штатное расписание «переводчиков с ИТ-шного». Эта профессия, находящаяся на стыке ИТ, психологии и коммуникации, обещает стать ключом к эффективному взаимодействию ИТ-специалистов с самыми разными людьми, не понимающими «птичьего» языка: от сотрудников других подразделений до клиентов или студентов вузов.

ДЛЯ КОГО ПЕРЕВОДИМ?

Потребность в подобном переводчике может возникнуть у самых разных компаний и в различных ситуациях, но объединяет ИТ-переводчиков одна общая цель — дешифровать сложные термины и объяснить их неспециалистам в ИТ «на пальцах».

«Например, во многих банках для подтверждения операций используется технология мобильной цифровой подписи, построенная на асимметричной криптографии и представляющая собой достаточно непростую штуку с точки зрения технологий, — рассказывает генеральный директор SafeTech Group Денис Калемберг. — ИТ-специалисты банка прекрасно понимают, как это работает, но пояснения для клиентов будут построены таким образом, чтобы граждане могли понять надёжность и безопасность технологии, не испугавшись при этом зубодробительных терминов».

Впрочем, переводчик с ИТ-шного нужен и внутри команды. «Например, ИТ или ИБ-компания запускает принципиально новый технически сложный продукт, который будут продавать сейлы этой организации или компаний-партнёров, — рассуждает технический директор „Спикателя“ Евгений Пудовкин. — И тут тоже потребуется „переводчик“, который пояснит коллегам, в чём преимущество решения, как оно работает, отфильтровывая лишние технические подробности и оставляя лишь суть». Эксперт признался, что за последние полгода компания существенно увеличила штат ИТ-специалистов и вывела на рынок несколько новых для себя продуктов. В планах — усиление команды за счёт тех, кто будет эти продукты продвигать. «И да, мне нужен будет человек, кто сможет чётко и понятно донести коммерческому блоку и маркетологам, что мы делаем, всю суть и пользу тех или иных обновлений, разных фич», — указал эксперт.

ПРИМЕР

Ещё один сценарий, когда «переводчик» необходим, — если компания в сотрудничестве с вузами и другими учебными заведениями работает со студентами, готовит для них курсы по работе со своими продуктами, лекции. Пример тому — компания Servicepipe, которая запустила образовательный проект, направленный на подготовку специалистов в сфере информационной безопасности с акцентом на защиту от ботовых и DDoS-атак. Одно из направлений этого проекта — курс для студентов технических вузов, благодаря которому ребята изучают азы защиты от DDoS-атак и попробуют себя в роли безопасника, работая с ПО DosGate и Flow Collector. «Когда появилась идея курса, встал вопрос: кто будет учить? — рассказывает директор по продуктам Servicepipe Михаил Хлебунов. — Было очевидно,

что нужен человек, который сможет „перевести“ достаточно сложную техническую документацию по продуктам для студентов, выявить, какие именно понятия или термины им незнакомы, и разъяснить на понятном для обучающихся на 2–3-м курсе языке». То есть такой уникальный специалист, работающий на стыке технологий и лингвистики.

ИТ-переводчиком для молодёжи в компании стал Иван Горячев, студент 2-го курса МГТУ им. Баумана. Он также является сотрудником Servicepipe и менеджером образовательного проекта. В своей работе Иван решает задачи, включающие в себя элементы ИТ-перевода. В частности, он преобразует техническую информацию в доступные объяснения для студентов, упрощает и адаптирует технические тексты для образовательных целей, а также участвует в разработке учебных материалов, которые эффективно передают знания об ИТ-продуктах компании. Как отмечает сам Иван Горячев: «В ИТ-сфере информация устаревает очень быстро, поэтому умение оперативно и точно переводить технические тексты, адаптировать их для разной аудитории, становится критически важным. Моя задача — не просто переводить слова, а делать сложные вещи понятными для молодёжи».

СПРОС ПРЕВЫСИТ ПРЕДЛОЖЕНИЯ

По словам HR-специалистов, спрос на переводчиков с ИТ-шного уже есть. «Профессия „переводчик с ИТ-шного“ — это не просто тренд, а критически необходимое развитие рынка, — указывает HR-директор ИТ-интегратора „Телеком биржа“ Катерина Смирнова. — Сейчас мы видим огромный разрыв между тем, что могут создавать разработчики, и тем, что способно воспринимать большинство пользователей. Эта пропасть порождает недопонимание, снижает эффективность, тормозит внедрение инноваций». Специалист, свободно владеющий как техническим языком, так и литературным, способен не просто переводить текст, а формировать понятную и убедительную коммуникацию о сложных технологиях, указывает она. Это важно для маркетинга, для подготовки документации, взаимодействия с клиентами, создания обучающих материалов — везде, где требуется адаптировать сложный технический контент для широкой аудитории, резюмировала Катерина Смирнова.

Опрошенные эксперты также сходятся во мнении, что спрос на этих специалистов будет только расти. «Я не удивлюсь, если даже появятся отдельные рекрутеры, специализирующиеся на подборе ИТ-переводчиков, будут созданы профессиональные ассоциации и сообщества, — рассуждает Евгений Пудовкин. — Чем более сложную информацию необходимо „перевести“, тем сложнее будет найти специалиста с глубоким пониманием технологий и лингвистики, и ИТ и ИБ-компании будут готовы платить высокую зарплату специалистам с таким набором навыков».

По словам Катерины Смирновой, ИТ-переводчики уже работают в компаниях-лидерах рынка — просто их должности пока называются по-разному: Product Evangelist, Solutions Architect с фокусом на коммуникацию, Technical Product Marketing Manager, IT Business Partner. Их ценность — в предотвращении потери времени, денег и нервов, когда «миры» перестают понимать друг с друга. «Я уверена, эта профессия станет массово востребованной, — указывает Катерина Смирнова. — Это естественная эволюция отрасли».

СПЛАВ ТЕХНАРЯ И ГУМАНИТАРИЯ

Какими знаниями и скилами должен обладать ИТ-переводчик? По словам Катерины Смирновой, идеальный кандидат — «редкий гибрид»: бывший разработчик или инженер с развитыми софт-скилами или сильный гуманитарий (журналист, технический писатель), погрузившийся в ИТ до уровня понимания архитектурных решений. Ключевое — любопытство (чтобы копаться в коде и задавать «глупые» вопросы) и эмпатия (чтобы чувствовать боль и «язык» обеих сторон). Это не про «банальное упрощение», а про точную трансляцию смыслов.

По словам Дениса Калемберга, для ИТ-переводчика также нужны аналитические способности и некоторая творческая составляющая, что позволит находить нестандартные решения и предлагать инновационные подходы к решению задач. «Переводчик с ИТ-шного» должен владеть иностранными языками (английским) в случае необходимости работы с англоязычной технической документацией.

По словам Ивана Горячева, также обязательно уметь работать с ИИ (DeepSeek, ChatGPT и т.д.), которые помогают снять часть «глупых» вопросов. «Конечно, „перевод“ ИИ не сделает, но позволит хотя бы не дёргать коллег с просьбой пояснить тот или иной термин или аббревиатуру», — говорит он.

МЕЖДУНАРОДНЫЙ ОПЫТ

В чистом виде переводчиков с ИТ в мировом опыте пока нет. Но есть специалисты, которые решают схожие задачи. Подобные навыки в других странах включает в себя должность Technical Evangelist, специалиста, который продвигает новые технологии и решения, объясняя их преимущества простым и понятным языком. Также существует должность Solution Architect, специалиста, который проектирует ИТ-системы, учитывая потребности бизнеса и технические возможности. Ещё есть Technical Writer — специалист, который создаёт техническую документацию, понятную для пользователей разного уровня подготовки, а также Knowledge Manager — специалист, управляющий знаниями в организации, обеспечивая их доступность и актуальность.

Успешные примеры включают в себя создание должности Developer Advocate в компании Google, который занимается продвижением Google Cloud Platform среди разработчиков, объясняя им, как использовать облачные сервисы для решения своих задач. В компании Microsoft существует программа Microsoft Certified Trainer, на которой ИТ-специалистов обучают использованию продуктов Microsoft.

ОТ СКЕПСИСА ДО ШТАТНОГО РАСПИСАНИЯ

По словам опрошенных экспертов, внедрение новой профессии сопряжено с рядом вызовов. На сегодняшний день во многих компаниях подобный «перевод» является как бы дополнительной нагрузкой без выделения в профессию. И во многих случаях может просто не оказаться нужного фронта работ, чтоб создавать отдельную ставку. Плюс профессия новая, и пока нет примеров чётких должностных инструкций и метрик эффективности. То есть существует риск, что в этом деле придётся быть пионером. Кроме того, в первое время возможен некий скепсис со стороны настоящих ИТ-специалистов к этому «недоайтишнику-переводчику», который пытается зачем-то пересказывать совершенно понятные, с точки зрения разработчиков-сеньоров, вещи.

По словам Евгения Пудовкина, все эти сложности преодолимы, если компания чётко понимает, для чего ей нужен переводчик, какие задачи он будет решать. «Тем более что суть не в названии должности, человеко-часах и даже не в нагрузке, а в пользе для компании от такого специалиста, — указывает эксперт. — И есть ощущение, что с каждым годом всё больше компаний будут понимать, что ИТ-переводчик — это не лишние траты, а то, что позволяет компании увеличивать выручку, расти и развиваться».

ГРУЗИЯ

ОБЗОР ЗАКОНОДАТЕЛЬСТВА В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Александр ВИНОГРАДОВ
ФГУП «ЦНИИХМ»

Сергей МЕНЬШИКОВ
основатель Belarusian InfoSecurity Community

Андрей СИТНОВ
независимый эксперт

Наталья КАЗАНЦЕВА
независимый эксперт

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

В 2005 году Грузия ратифицировала Конвенцию о защите физических лиц в отношении автоматизированной обработки персональных данных и взяла на себя обязательство по формированию соответствующих правовых основ защиты персональных данных, в 2011 году приняла Закон «О защите персональных данных».

Указанный закон утратил силу в 2023 году в связи с принятием нового **Закона «О защите персональных данных» от 14.06.2023** № 3144-XIმს-Xმპ (далее — Закон о защите персональных данных).

Действие Закона распространяется на обработку данных на территории Грузии при помощи автоматических и полуавтоматических средств, обработку при помощи неавтоматических средств данных, являющихся частью файловой системы или обрабатываемых для внесения в файловую систему, а также обработку данных лицом, ответственным за обработку, зарегистрированным за пределами границ Грузии, при помощи технических средств, имеющихся в Грузии, за исключением случая, когда технические средства используются только для транзита данных.

Персональными данными является любая информация, связанная с идентифицированным или идентифицируемым физическим лицом. При этом физическое лицо является идентифицируемым тогда, когда возможно его идентифицировать прямо или косвенно, в том числе по имени, фамилии, идентификационному номеру, геолокационным данным, данным, идентифицирующим электронную коммуникацию, физическим, физиологическим, психическим, психологическим, генетическим, экономическим, культурным или социальным характеристикам.

Персональные данные делятся на данные особой категории, данные, касающиеся здоровья, биометрические данные и генетические данные.

Обработка персональных данных предполагает выполнение в отношении них любых действий, в том числе их сбор, получение, доступ к ним, их фотографирование, видеомониторинг или (и) аудиомониторинг, организацию, группировку, взаимосвязь, хранение, изменение, восстановление, истребование, использование, блокировку, удаление или уничтожение, а также разглашение данных путём их передачи, обнародования, распространения либо обеспечения доступа к ним иным образом.

СОБЛЮДЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Установление прав и обязанностей публичного и частного секторов в сфере соблюдения информационной безопасности, а также определение механизмов государственного контроля за осуществлением политики информационной безопасности предусмотрено **Законом Грузии «Об информационной безопасности» от 05.06.2012** № 6391-Iს (далее — Закон об информационной безопасности).

Законом об информационной безопасности предусмотрены отдельные понятия и термины.

Информационная безопасность — деятельность, обеспечивающая соблюдение правил доступа, единства, аутентичности, конфиденциальности информации и информационных систем и их работы в течение длительного времени.

Политика информационной безопасности — совокупность норм и принципов, а также практики, предусмотренных Законом об информационной безопасности, другими нормативными актами и международными соглашениями Грузии, служащих обеспечению информационной безопасности и соответствующих международным стандартам, установленным в сфере их соблюдения.

Киберпространство — пространство, особенностью которого является использование электронных устройств и электромагнитного спектра посредством связанных в сети систем и вспомогательной физической инфраструктуры для хранения, замены или обмена данными.

Кибератака — деяние, во время совершения которого электронное устройство или (и) связанная с ним сеть либо система используется вследствие нарушения, создания препятствий или уничтожения систем, имущества или функций, входящих в критическую информационную систему, либо путём незаконного добывания информации.

Компьютерный инцидент — реальное или потенциальное нарушение в сфере политики информационной безопасности в результате использования информационных технологий, влекущее доступ, разглашение информации без разрешения на то, её повреждение или создание помех либо завладение информационным ресурсом.

Информационная система — любая комбинация информационных технологий и действий, осуществлённых с использованием данных технологий, содействующих управлению или (и) принятию решения.

Особенностью Закона об информационной безопасности является то, что он распространяется только на юридические лица и государственные органы, являющиеся субъектами критической информационной системы, а также на организации и ведомства, которые

Список субъектов критической информационной системы, классификация критичности соответствующего субъекта устанавливается постановлением Правительства Грузии, проект которого представляет Министерство юстиции Грузии по согласованию с Министерством обороны Грузии и Министерством внутренних дел Грузии и Службой государственной безопасности Грузии.

Для составления списка имеют значение следующие критерии:

- тяжесть и масштаб предполагаемых последствий работы информационной системы с помехами или её выхода из строя;
- тяжесть предполагаемого экономического ущерба для субъекта или (и) государства;
- необходимость оказания информационной системой услуг для нормального функционирования общества;
- число пользователей информационной системы;
- материальное положение субъекта и размер предполагаемых расходов вследствие возложения на него обязательств исходя из Закона об информационной безопасности.

Действие Закона об информационной безопасности не распространяется на массмедиа, редакции изданий, научные, образовательные, религиозные и общественные организации и политические партии независимо от степени значимости их деятельности для обороны или (и) экономической безопасности страны, сохранения государственной власти или (и) общественной жизни.

Любое юридическое лицо и орган государственной власти, не являющиеся субъектами критической информационной системы, вправе в добровольном порядке взять на себя обязательства, вытекающие из Закона об информационной безопасности.

Субъект критической информационной системы обязан принять правила информационной безопасности для внутрислужебного пользования, которые служат исполнению положений Закона об информационной безопасности и определяют политику информационной безопасности организации.

Политика информационной безопасности должна удовлетворять минимальным требованиям информационной безопасности (с учётом классификации критичности субъекта критической информационной системы), определённым Агентством по обмену данными (юридическое лицо публичного права, действующее в сфере управления Министерства юстиции Грузии), в соответствии со стандартами и требованиями, установленными Международной организацией стандартизации (ISO) и Ассоциацией аудита и контроля информационных систем (ISACA).

Рассмотрение правил информационной безопасности для внутрислужебного пользования осуществляет Агентство по обмену данными.

Также Агентство по обмену данными с согласия субъекта критической информационной системы проводит аудит информационной безопасности — оценку соответствия правил информационной безопасности для внутрислужебного пользования (политики информационной безопасности) минимальным стандартам безопасности, установленным Агентством по обмену данными. Допускается аудит информационной безопасности проводить лицом либо организацией, выбранной субъектом критической информационной системы из авторизованных Агентством по обмену данными лиц.

подчиняются субъекту критической информационной системы или связаны с данным субъектом отношениями в сфере занятости, стажировки, договорными или иными отношениями и которые обеспечивают доступ к информационным активам в пределах данных отношений.

Под критической информационной системой понимается информационная система, непрерывное функционирование которой имеет важное значение для обороны или (и) экономической безопасности страны, нормального функционирования органов государственной власти или (и) общества.

Конфиденциальная информация — информация, посягательство на конфиденциальность, целостность или доступность которой может повлечь значительный вред в отношении функций субъекта критической информационной системы и целью классификации которой в качестве конфиденциальной информации является обеспечение правил управления информационными активами, за исключением правил, согласно которым определяется доступность публичной информации.

Информация для внутрислужебного пользования — информация, предназначенная только для сотрудников субъекта критической информационной системы или (и) для лиц, имеющих с ним договорные отношения, посягательство на конфиденциальность, целостность или доступность которой может повлечь создание существенных препятствий при выполнении субъектом критической информационной системы своих функций либо нанести ущерб безопасности органа государственной власти, государственным интересам или деловой репутации частных лиц и целью классификации которой в качестве информации для внутрислужебного пользования является обеспечение правил управления информационными активами, за исключением правил, согласно которым определяется доступность публичной информации.

Понятие публичной информации определяется **Общим административным кодексом Грузии от 25.06.1999** № 2181-IIс и представляет официальный документ (в том числе — чертежи, макеты, планы, схемы, фотоснимки, электронная информация, видео- и аудиозаписи), то есть информацию, хранящуюся в публичном учреждении, а также полученную, обработанную, созданную или направленную публичным учреждением или служащим в связи со служебной деятельностью и проактивно опубликованную публичным учреждением.

Публичная информация является открытой, за исключением предусмотренных законом случаев и информации, в установленном порядке отнесённой к государственной, коммерческой или профессиональной тайне или персональным данным. Публичное учреждение обязано обеспечить проактивное опубликование публичной информации, представляющей общественный интерес, на электронных ресурсах в порядке, установленном соответствующим подзаконным нормативным актом.

Субъект критической информационной системы обязан:

1. Определить менеджера информационной безопасности — конкретное лицо или сотрудника, который ответствен за выполнение требований информационной безопасности субъекта критической информационной системы.

К обязанностям менеджера информационной безопасности относятся: ежедневный мониторинг выполнения требований политики информационной безопасности; описание информационных активов и доступа к ним; подготовка внутриведомственной документации в связи с политикой информационной безопасности; сбор информации об инцидентах в сфере информационной безопасности и мониторинг реагирования на них; другие обязанности.

Менеджер информационной безопасности подотчётен перед руководителем субъекта критической информационной системы или соответственно уполномоченным им сотрудником либо группой лиц с полномочиями на осуществление политики информационной безопасности (коллегиальным органом).

2. Определить специалиста по компьютерной безопасности — конкретное лицо или сотрудника, который ответствен за практическое обеспечение безопасности компьютерных систем субъекта критической информационной системы.

К обязанностям специалиста по компьютерной безопасности относятся: ежедневный мониторинг и оценка компьютерных систем; идентификация компьютерных инцидентов и реагирование на них; анализ и отчётность компьютерных инцидентов и мер безопасности; другие обязанности.

Специалист по компьютерной безопасности подотчётен перед руководителем службы информационных технологий субъек-

та критической информационной системы или соответственно уполномоченным им сотрудником.

ГРУППА ПОМОЩИ

В целях управления инцидентами против информационной безопасности в киберпространстве Грузии создана Группа помощи Агентства по обмену данными по реагированию на компьютерные инциденты — CERT.GOV.GE, которая служит устранению первостепенных угроз кибербезопасности:

- кибератак, создающих угрозу жизни и здоровью людей, государственным интересам или обороноспособности страны;
- кибератак против информационных систем субъекта критической информационной системы;
- кибератак, создающих угрозу финансовым ресурсам или (и) праву собственности в отношении государства, организации или частного лица;
- всех остальных деяний, которые исходя из характера, цели, источника, объёма или размера либо из объёма ресурсов, необходимых для пресечения указанных деяний, представляют значительную угрозу для нормального функционирования критической информационной системы.

В СФЕРЕ ОБОРОНЫ

Законом об информационной безопасности предусмотрен особый порядок для субъектов критической информационной системы в сфере обороны.

Минимальные требования информационной безопасности в сфере обороны (с учётом классификации критичности субъекта критической информационной системы в сфере обороны) определяет Бюро кибербезопасности в соответствии с ISO и ISACA.

Бюро кибербезопасности — юридическое лицо публичного права, действующее в сфере управления Министерства обороны Грузии. Сфера действия Бюро кибербезопасности не распространяется на Агентство по обмену данными.

Перечень субъектов критической информационной системы в сфере обороны, классификация критичности соответствующего субъекта устанавливается соответствующим актом Правительства Грузии, проект которого представляет Министерство юстиции Грузии по согласованию с Министерством обороны Грузии, Министерством внутренних дел Грузии и Службой государственной безопасности Грузии.

Для составления списка имеют значение следующие критерии:

- тяжесть и масштаб предполагаемых последствий работы информационной системы с помехами или её выхода из строя с точки зрения обороноспособности государства;
- тяжесть предполагаемого экономического ущерба для субъектов или (и) государства;
- необходимость оказания информационной системой услуг для беспрепятственного функционирования в сфере обороноспособности государства;
- число пользователей информационной системы;
- материальное положение субъекта и размер предполагаемых расходов вследствие возложения на него соответствующих обязательств.

Управление кибератаками на субъекты критической информационной системы в сфере обороны, создающими угрозу жизни и здоровью человека, государственным интересам и обороноспособности страны, а также другими инцидентами, направленными против информационной безопасности, и связанную с этим деятельность осуществляет Группа помощи Бюро кибербезопасности по реагированию на компьютерные инциденты — CERT.MOD.GOV.GE.

В ФИНАНСОВОЙ СФЕРЕ

В соответствии с **Законом Грузии «О Национальном банке Грузии» от 24.09.2009** форматы и стандарты по вопросам информационной безопасности устанавливаются в соответствующем порядке Национальным банком Грузии или Агентством финансового надзора Грузии в пределах их компетенции, передаются коммерческим банкам и небанковским депозитным учреждениям в индивидуальном порядке.

Положения о банковской тайне предусмотрены **Законом Грузии «О деятельности коммерческих банков» от 23.02.1996** (далее — Закон о коммерческих банках) — никто не вправе допускать кого-либо к конфиденциальной информации, разглашать и распространять такую информацию или использовать её для личной выгоды. Конфиденциальная информация может предоставляться только Национальному банку и Комиссии по рассмотрению споров при Национальном банке в пределах их компетенции.

Информация о любых сделках (в том числе в случае попытки заключения сделки), осуществлённых платёжных операциях, сче-

тах, операциях, осуществлённых со счетов, и остатках, имеющихся на счетах, может предоставляться:

- сторонам, участвующим в соответствующих сделках, при осуществлении платёжной операции;
- выплачивающему лицу или (и) получающему лицу, владельцам соответствующих счетов и их представителям, в случаях, предусмотренных законодательством Грузии;
- Службе финансового мониторинга Грузии и лицам, правомочным исполнять подлежащие исполнению акты, определённые Законом Грузии «Об исполнительных производствах», в процессе их исполнения;
- Службе защиты персональных данных при осуществлении проверки, предусмотренной Законом Грузии «О защите персональных данных»;
- налоговому органу на основании судебного решения, предусмотренного Административно-процессуальным кодексом Грузии, и Соглашения между Правительством Соединённых Штатов Америки и Правительством Грузии об улучшении исполнения международных налоговых обязательств и исполнении Акта о налоговом соответствии иностранных счетов (FATCA);
- юридическому лицу публичного права Агентству по страхованию депозитов в случае, предусмотренном **Законом Грузии «О системе страхования депозитов» от 17.05.2017** № 852-IIს.

Указанная информация может предоставляться также на основании соответствующего определения суда.

Законом о коммерческих банках также предусмотрено, что коммерческий банк вправе разрабатывать и представлять Национальному банку для согласования политику безопасности использования электронной подписи при оказании им конкретных банковских услуг.

При оказании коммерческим банком конкретной банковской услуги, согласованной с Национальным банком, электронная подпись, использованная при оказании конкретной банковской услуги, на основании политики безопасности использования электронной подписи имеет юридическую силу, равную личной подписи, выполненной на материальном документе. Электронный документ, удостоверенный указанной электронной подписью, может быть использован во всех случаях, когда законодательство Грузии требует представления материального документа.

Политика безопасности использования электронной подписи может не представляться Национальному банку в случае, если коммерческий банк при оказании банковских услуг использует подпись, выполненную посредством электронного удостоверения личности, выпущенного уполномоченным административным органом в соответствии с законодательством Грузии, или подпись, сертификат которой выдан в соответствии с требованиями Закона Грузии «Об электронном документе и надёжном электронном обслуживании» от 23.12.2017 № 639-IIს (далее — Закон об электронном документе).

При этом право коммерческого банка при оказании банковских услуг использовать электронную подпись не ограничивается в силу Закона об электронном документе, устанавливающего, что, если между физическими лицами или (и) юридическими лицами частного права существует соглашение, электронный документ и электронная подпись для этих лиц имеют равную юридическую силу соответственно с материальным документом и личной подписью.

В этом случае Национальный банк правомочен требовать у коммерческого банка согласования с Национальным банком политики безопасности электронной подписи, использованной в соответствии с настоящим пунктом. Если Национальный банк после оценки политики безопасности использования электронной подписи, представленной коммерческим банком, заявит об отказе в согласовании политики безопасности использования электронной подписи, коммерческий банк обязан прекратить использование такой электронной подписи.

Законом об электронном документе установлено исключение, согласно которому при осуществлении деятельности представителями Национального банка Грузии и финансового сектора в соответствии с условиями, отличающимися от Закона об электронном документе, электронный документ и электронная подпись, выполненные в порядке, установленном Национальным банком Грузии, имеют равную юридическую силу соответственно с материальным документом и личной подписью.

* * *

Надеемся, что данная статья поможет вам не заблудиться в законодательстве Грузии. Мы постарались облегчить путь изучения и применения на практике законов и подзаконных актов в области ИБ. В следующем номере будет представлено законодательство Молдовы.

Окрестности Рейхстага. Май 1945 г.

«МАЙСКИМИ КОРОТКИМИ НОЧАМИ, ОТГРЕМЕВ, ЗАКОНЧИЛИСЬ БОИ»

БОИ ВЕЛИКОЙ ОТЕЧЕСТВЕННОЙ ВОЙНЫ, ЗАВЕРШИВШИЕСЯ ПОБЕДОЙ, ОТГРЕМЕЛИ УЖЕ 80 ЛЕТ НАЗАД, НО ДОКУМЕНТЫ ПРОШЛОГО ПО-ПРЕЖНЕМУ ПРИТЯГАТЕЛЬНЫ И ПОУЧИТЕЛЬНЫ

Борис СТОЛПАКОВ
историк криптографии

За четыре военных года экономика СССР и его вооружённые силы претерпели существенную модернизацию. Зримые перемены вызывали гордость граждан страны и впечатляли как союзников, так и врагов. Одним из заметных проявлений модернизации стало создание современно оснащённых войск связи, включавших в себя в 1945 г. до 10 % личного состава действующей армии.

ЗАДАЧА: ОБЕСПЕЧИТЬ БЕЗОПАСНОСТЬ СВЯЗИ ПО ВСЕЙ СТРАНЕ

Особой государственной заботой являлось и является обеспечение секретности при передаче собственной важной информации по каналам связи. За годы ВОВ только шифровальная служба Генштаба КА разослала нижестоящим штабам и войскам порядка 3,2 млн комплектов шифрдокументов. В армейских и флотских штабах за шифровальную деятельность отвечали их 8-е отделы.

Но потребности в засекречивании сообщений были гораздо значительнее. Криптографы противоборствовавших сторон проделали гигантскую работу по обеспечению безопасности проводной связи и радиосвязи для военных и гражданских нужд в масштабах значительной части земного шара. Ведь шифрование применялось даже в такой, казалось бы, неожиданной области, как передача метеосводок и прогнозов погоды.

«В ЦЕЛЯХ СОХРАНЕНИЯ В ТАЙНЕ ОТ ПРОТИВНИКА...»

Метеосводки, передаваемые по каналам связи в СССР, подлежали засекречиванию ввиду их ценности для обеих воевавших сторон.

В первых пунктах инструкции о порядке использования и хранения гидрометеорологических шифров указывалось:

«1. В целях сохранения в тайне от противника сведений о фактическом и ожидаемом состоянии погоды и гидрорежима метеорологические, аэрологические и т.п. сводки, а также гидрометеорологические прогнозы, обзоры, консультации, заранее составленные по общеизвестным международным или общесоюзным кодам, дополнительно перешифровываются при помощи специальных секретных таблиц, именуемых гидрометеорологическими шифрами.

2. Разработка и издание г/м шифров производится Главным Управлением Гидрометеорологической службы Красной Армии по согласованию с 5 Управлением НКВД СССР.

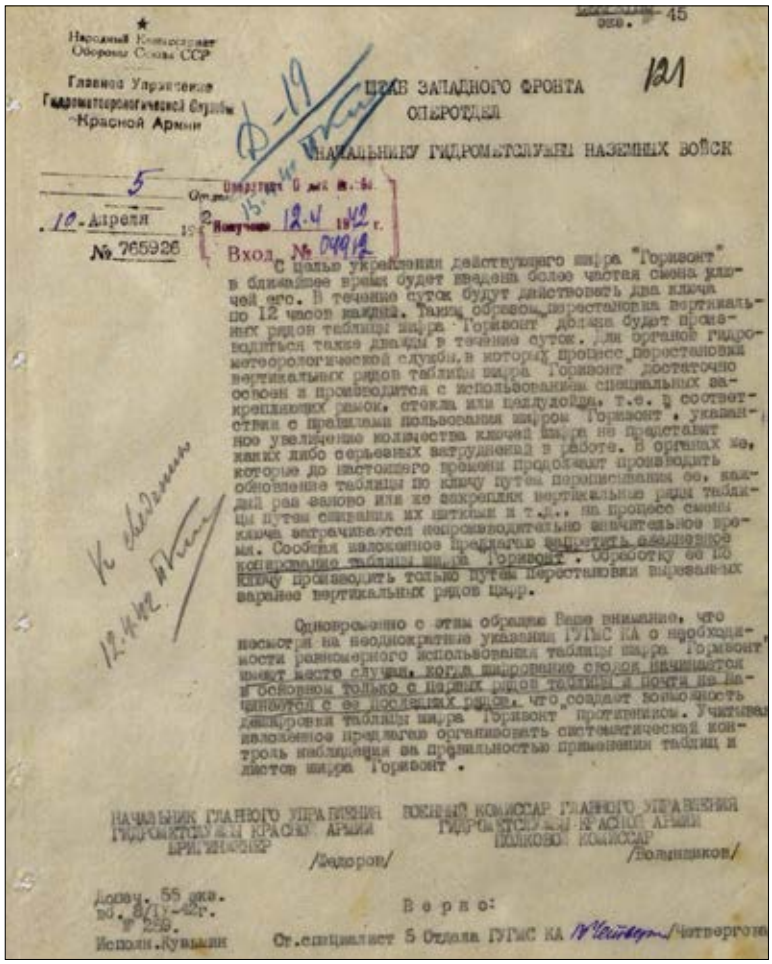
3. Гидрометеорологическими шифрами обеспечиваются <...> также органы службы погоды, находящиеся в ведении других наркоматов или главных управлений (НКПС, ГУСМП, Дальстрой) <...>».

Документ с илл. 2, относящийся к апрелю 1942 г., свидетельствует о принятии мер по эффективному использованию г/м шифров.

Впрочем, защищённая радиосвязь тоже может таить опасности.

РАДИОИГРЫ С ВОЕННЫМ ПРОТИВНИКОМ

Уже во время Первой мировой войны был разработан способ использования чужой радиостанции в противоборстве — радиоигра с противником. С началом ВОВ советские контрразведчики тоже взяли на вооружение практику радиоигр.



Народный Комиссариат Обороны Союза ССР
Главное Управление Гидрометеорологической службы Красной Армии

НАЧ ЗАПАДНОГО ФРОНТА
ОПЕРОТДЕЛ

НАЧАЛЬНИКУ ГИДРОМЕТОТДЕЛА НАЗЕМНЫХ ВОЙСК

10 Апреля 1942 г.
№ 265926

Вход. № 04912

Ст.специалист 5 Отдела ГУГМС КА

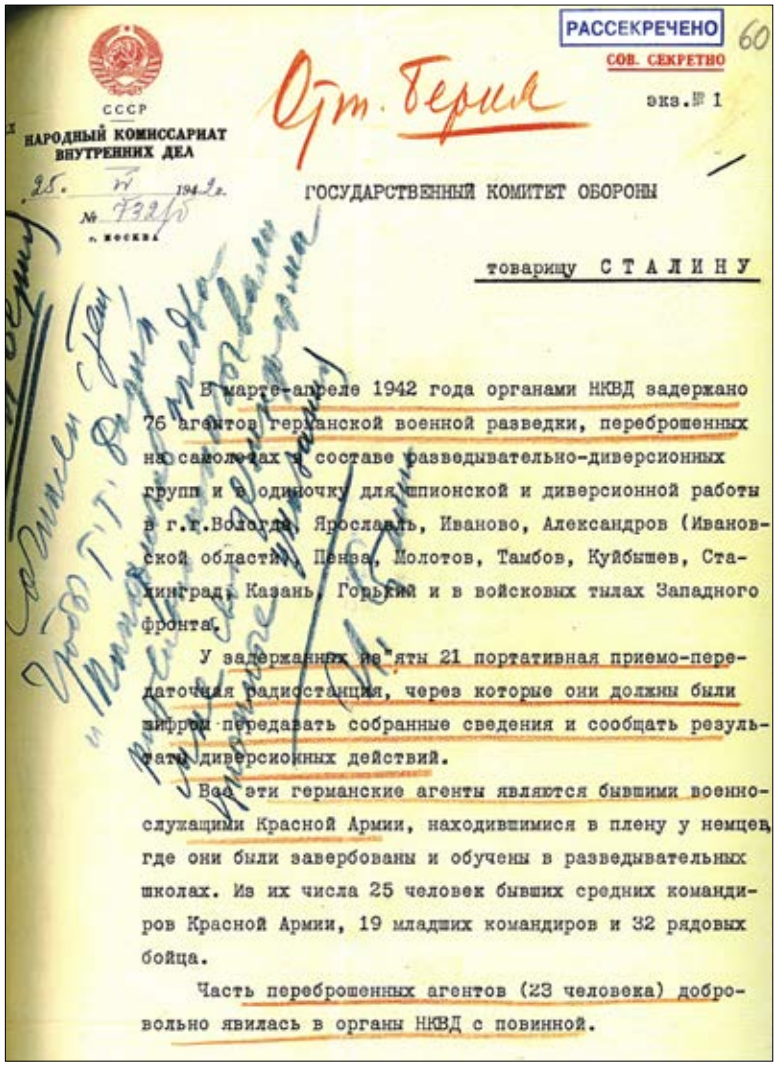
Иллюстрация 2. Директива ГУГМС Красной Армии

Знаковым событием стало представление в ГКО докладной записки Л. П. Берия от 25 апреля 1942 г. о задержанных немецких агентах с рациями.

«В марте-апреле 1942 г. органами НКВД задержано 76 агентов германской военной разведки, переброшенных на самолётах в составе разведывательно-диверсионных групп и в одиночку для шпионской и диверсионной работы в г.г. Вологда, Ярославль, Иваново, Александров (Ивановской области), Пенза, Молотов, Тамбов, Куйбышев, Сталинград, Казань, Горький и в войсковых тылах Западного фронта.

У задержанных изъяты 21 портативная приёмо-передаточная радиостанция, через которые они должны были шифром передавать собранные сведения и сообщать результаты диверсионных действий.

Все эти германские агенты являются бывшими военнослужащими Красной Армии, находившимися в плену у немцев, где они были завербованы и обучены в разведывательных школах. Из их числа 25 бывших средних командиров Красной Армии, 19 младших командиров и 32 рядовых бойца. Часть переброшенных агентов (23 человека) добровольно явилась в органы НКВД с повинной.



СССР
НАРОДНЫЙ КОМИССАРИАТ ВНУТРЕННИХ ДЕЛА
25. IV 1942 г.
№ 732/б
г. МОСКВА

РАССЕКРЕЧЕНО
СОВ. СЕКРЕТНО
60
От. Берия
экз. № 1

ГОСУДАРСТВЕННЫЙ КОМИТЕТ ОБОРОНЫ

товарищу С Т А Л И Н У

В марте-апреле 1942 года органами НКВД задержано 76 агентов германской военной разведки, переброшенных на самолетах в составе разведывательно-диверсионных групп и в одиночку для шпионской и диверсионной работы в г.г.Вологда, Ярославль, Иваново, Александров (Ивановской области), Пенза, Молотов, Тамбов, Куйбышев, Сталинград, Казань, Горький и в войсковых тылах Западного фронта.

У задержанных изъяты 21 портативная приемо-передаточная радиостанция, через которые они должны были шифром передавать собранные сведения и сообщать результаты диверсионных действий.

Все эти германские агенты являются бывшими военнослужащими Красной Армии, находившимися в плену у немцев, где они были завербованы и обучены в разведывательных школах. Из их числа 25 человек бывших средних командиров Красной Армии, 19 младших командиров и 32 рядовых бойца.

Часть переброшенных агентов (23 человека) добровольно явилась в органы НКВД с повинной.

Иллюстрация 3. Докладная записка Л. П. Берия

В целях ограничения активности германских разведывательных органов в указанных выше городах и создания видимости работы переброшенных шпионских групп и одиночек по заданиям германской разведки, по 12 захваченным радиостанциям противника нам удалось установить радиосвязь с немецкими разведывательными органами в г.г. Варшава (центр военной германской разведки), Псков, Дно, Смоленск, Минск, Харьков, Полтава.

НКВД СССР считает, что захваченные немецкие радиостанции можно использовать в интересах Главного командования Красной Армии для дезинформации противника в отношении дислокации и перегруппировок частей Красной Армии.

Поэтому, если данное мероприятие будет признано Вами целесообразным, считаем необходимым поручить Начальнику Оперативного Управления ГШ КА тов. Бодину и Начальнику Главного Разведывательного Управления тов. Панфилову выработать порядок разработки материалов по дезинформации противника и передачи их в НКВД СССР для реализации через захваченные немецкие радиостанции.

Передача дезинформации противнику через захваченные рации будет обеспечиваться надёжным контролем. Прошу Ваших указаний».

На документе можно видеть и резолюцию: «Согласен с тем, чтобы т.т. Бодин и Панфилов предварительно показывали мне свои дезинформационные указания. И. Сталин» (илл. 3).

Этим документом был подведён итог работы радиоконтрразведчиков по обезвреживанию вражеской агентуры в начальный период войны. Известно, что после поражения немцев под Москвой Гитлер выразил неудовольствие качеством информации об СССР, предоставленной военной разведкой — абвером. В ответ её начальник, В. Канарис, сделал ставку на массовую засылку агентов. В Германии и на оккупированных территориях были созданы 60 школ для их подготовки.

Данные о замыслах абвера и донесения его агентуры удавалось выяснять по перехваченным и дешифрованным радиограммам. Так, один из документов свидетельствует: «В конце января 1942 г. контрольно-слежечными радиостанциями 2-го спецотдела НКВД СССР была зафиксирована новая учебно-тренировочная линия радиосвязи между двумя подцентрами германской разведки.

Дальнейшее наблюдение показало, что в первой половине февраля после краткого перерыва одна из точек изменила характер работы, и, по данным пеленгаторной сети, местонахождение её определялось на нашей территории.

Одновременно дешифровальная группа 2-го спецотдела НКВД СССР раскрыла шифр, применявшийся при обмене, и обеспечила расшифровку перехватываемых телеграмм. Это в сочетании с работой оперативно-разыскной группы 2-го спецотдела НКВД СССР, выехавшей в район действия радиостанции, позволило с помощью одного из оперативных управлений и частей НКВД арестовать большую группу агентов германской разведки».

РОЖДЕНИЕ «СМЕРШ»

Секретным постановлением СНК СССР от 19 апреля 1943 г. на базе Управления особых отделов НКВД СССР было создано Главное управление контрразведки (ГУКР) «Смерш» Наркомата обороны, оно подчинялось непосредственно наркому обороны И. В. Сталину.

В ГУКР «Смерш» был организован 3-й отдел, на который возложили функции по розыску вражеской агентуры на советской территории и проведению радиоигр с использованием захваченных агентов-радистов противника.

ПЕРВЫЕ ИТОГИ

Уже 29 мая 1943 г. начальник ГУКР «Смерш» В. С. Абакумов обобщил для ГКО накопленный опыт работы по радиоиграм:

«За период отечественной войны органами контрразведки задержано 1040 германских шпионов-парашютистов, переброшенных противником на нашу сторону, из которых 263 разведчика были снабжены портативными коротковолновыми радиостанциями. После перевербовки некоторой части агентов-парашютистов нашими органами было включено в радиоигру с противником 89 изъятых радиостанций.

Из этого количества 65 раций были в разное время из игры выведены из-за потери к ним оперативного интереса, опасности провала наших мероприятий, вследствие длительного срока работы станций и по техническим причинам.

Остальные 24 радиостанции работают по настоящее время и размещены в разных местах Советского Союза, так как при переброске разведчиков на нашу сторону немцы указывали им пункты для оседания.

8 работающих ныне станций функционируют с 1942 года, а остальные с 1943 года, причём 2 начали работать с февраля с.г., 2 — с марта и 12 — с мая 1943 г.

Из числа арестованных шпионов-парашютистов — 305 человек расстреляно, остальные содержатся под стражей.

С помощью работающих радиостанций Главное Управление контрразведки «Смерш» осуществляет мероприятия по вызову агентуры противника на нашу сторону для её перехвата и в этих же целях передаётся немцам дезинформация военного характера, которая согласовывается с Генеральным штабом Красной Армии.

За время войны арестовано присланных немцами 16 агентов-связников, захвачено 19 посылок, сброшенных противником с самолётов, в которых находились рации, документы, одежда, продукты питания и 824 000 рублей советских денег».

ОТРАБАТЫВАЛОСЬ ВСЁ ДО МЕЛОЧЕЙ

В отличие от немецких радиоигр, игры ГУКР «Смерш» проводились централизованно, с участием Генерального штаба. Отрабатывалось всё до мелочей. В инструкции «по организации и проведению радиоигр с противником», введённой в действие в первые дни Курской битвы, особо отмечалось: «Включение захваченной вражеской агентурной рации в радиоигру, все тексты радиограмм, передаваемые по этим станциям, санкционируются лично Начальником ГУКР НКО „Смерш“».

ЦЕЛЬ — ПАРАЛИЗОВАТЬ ДЕЯТЕЛЬНОСТЬ РАЗВЕДКИ ПРОТИВНИКА

За военные годы ГУКР «Смерш» провело 186 радиоигр с германской, финской, болгарской и другими разведывательными службами противника. Согласно тексту инструкции, «радиоигры, организуемые органами «Смерш», преследуют основную цель — проведение агентурных комбинаций, направленных к парализации деятельности разведывательных органов противника». И в период сталинградских боёв, и на Курской дуге, и в операции «Багратион» радиоконтрразведчики неизменно стремились к своей цели, затрудняя германской агентуре сбор информации и проведение диверсий. Порой они добивались ослабления фронтовых возможностей противника. В этой связи показательна радиоигра «Березино».

ЛЕГЕНДА ПОДПОЛКОВНИКА ШЕРХОРНА

18 августа 1944 г. через сеть радиоигры «Престол» немцам было передано сообщение, что хорошо известный им и авторитетный агент добыл важную информацию. Этот агент, прибывший из Белоруссии в Москву в командировку, рассказал о якобы ставшем ему известном крупном немецком соединении (более 1500 человек), застрявшем в тылу советских войск. Командир соединения — некий подполковник Г. Шерхорн. Немцы после некоторых сомнений приказали тому же агенту (советскому разведчику А. П. Демьянову) попытаться установить связь с Шерхорном.

Демьянову, разумеется, «удалось» установить контакт с Шерхорном. Числившийся у немцев пропавшим без вести, тот попал в плен под Минском и был размещён контрразведчиками «Смерш» в окрестностях селения Березино, в 100 км западнее Могилёва. Вместе с Шерхорном там находилась и его «группа» — небольшая группа военнопленных немцев, согласившихся сотрудничать с советской контрразведкой.

Демьянов передал немецкой разведке координаты «группы» Шерхорна для сброса радиста и грузов. По легенде у Шерхорна имелось много раненых и были проблемы с боеприпасами и продовольствием. Так началась операция «Березино»».

ЗАСЛУЖЕННОЕ ДОВЕРИЕ И ЕГО ПЛОДЫ

Немцы решили проверить полученную информацию и послали две группы агентов на поиски «группы» Шерхорна. Выручила предусмотрительность командования: лес, где обитала «группа» Шерхорна, был тщательно блокирован. Всех прибывших агентов удалось задержать. Контрразведчикам достались в целости и сохранности радиостанции, коды и шифрблокноты. Это позволило включить в радиоигру проверочные группы. После сеансов связи с ними немцы окончательно поверили Шерхорну.

В состав захваченных проверочных групп входили и подчинённые О. Скорцени. Он тоже участвовал в руководстве операцией по снабжению «группы» Шерхорна. В её расположение было сброшено 255 мест груза с вооружением, боеприпасами, ме-

дикаментами, продовольствием, зимним обмундированием. К Шерхорну направили 25 разных специалистов, часть из них погибла, часть — задержали. Семь захваченных при них радиостанций включили в радиоигру.

Помимо прорыва на запад, Шерхорну была поставлена задача попутной разведки. Её «выполнили», и немцы стали регулярно получать дезинформацию. Сеансы связи продолжались до самого конца войны.

В ТАКОЙ УСПЕХ БЫЛО ТРУДНО ПОВЕРИТЬ

Всего, по данным советских источников, немцы совершили к Шерхорну 67 самолёто-вылетов. Последний груз был принят 17 апреля 1945 г. Здесь следует отметить, что после потери румынских нефтепромыслов осенью 1944 г. ценность горючего, особенно авиационного бензина, резко выросла. Каждый вылет транспортного самолёта к Шерхорну оставлял на земле немецкие истребители и штурмовики, ослабляя таким образом германский фронт.

Когда в послевоенное время в прессе были раскрыты некоторые подробности, связанные с Шерхорном, не все смогли в них поверить. Так, Скорцени написал в своих мемуарах: «В апреле и мае 1945 г., а также во время пребывания в тюрьме я часто думал о Шерхорне. Меня мучила неопределённость. Сообщениям Шерхорна и наших радиотелеграфистов всегда предшествовал специальный шифр, постоянно менявшийся согласно предварительной договорённости. Все полученные нами радиограммы соответствовали принятым принципам... Я задавал себе вопрос: не проводила ли советская разведслужба с нами всё это время так называемую радиоигру. Позже, когда немецкая коммунистическая пресса опубликовала по делу Шерхорна большие репортажи, озаглавленные «Советы надули Скорцени», знание мной советских методов работы позволило сделать вывод, что мои опасения были напрасными». Таким образом, Скорцени не поверил разоблачительным публикациям о «группе» Шерхорна.

Отметим, что в операции «Березино» работой советских и перевербованных немецких радистов руководил Вильям Генрихович Фишер, широко известный позже под псевдонимом Рудольф Иванович Абель. Можно констатировать, что он одержал интеллектуальную победу в игре со Скорцени.

ПЕРЕД ШТУРМОМ БЕРЛИНА

Последней репетицией перед штурмом Берлина стало взятие советскими войсками в апреле 1945 г. «бастиона германского духа», каким считался Кёнигсберг (ныне Калининград). Там, а не в столичном Берлине короновали последнего короля Пруссии Вильгельма I, впервые создавшего в 1871 г. единое германское государство — Германскую империю. В основном с той поры и утвердилось представление о Кёнигсберге как о духовном бастионе. Чему вполне соответствовали и мощнейшие форты, опоясавшие главный город Восточной Пруссии в конце XIX столетия.

ИСТОЧНИК КАДРОВ И ИДЕЙ

Вместе с тем Кёнигсберг издавна был связан с культурной жизнью соседних стран, в том числе России. Когда в 1724 г. в Петербурге занялись организацией Академии наук, из Кёнигсберга туда потянулась профессура местного университета, претендуя на академические звания. Достаточно упомянуть хорошо известного всем интересующимся математикой и криптографией Христиана Гольдбаха. С его именем связан первый громкий успех российских дешифровальщиков дипломатической корреспонденции, заметно отразившийся во внешней государственной политике. Другой петербургский академик, великий Леонард Эйлер, прославил Кёнигсберг своей статьёй о его мостах, положившей начало новой математической дисциплины — теории графов.

К ШТУРМУ ГОТОВИЛИСЬ ТЩАТЕЛЬНО

В конце января 1945 г. советские войска приблизились к Кёнигсбергу и прервали его сухопутное сообщение с остальной Германией. Пришло время «бастиону германского духа» почувствовать мощь удара Красной Армии, совершенно изменившейся за четыре военных года.

Штурм готовили войска 3-го Белорусского фронта под командованием маршала А. М. Василевского. Все понимали моральное значение Кёнигсберга для немцев и важность быстрого успеха при штурме города. Несколько десятков разведгрупп занимались разведкой Кёнигсберга и его пригородов, каждая на своём участке территории. Разведчики действовали под видом власовских или немецких подразделений.

Сведения, доставленные всеми видами разведки, после их анализа послужили основой для изготовления натурного макета. Его использовали при составлении плана штурмовой операции. Одновременно запланировали сковывающий удар по Земландской группировке противника в направлении военно-морской крепости Пиллау (ныне Балтийск). На подступах и в самом Кёнигсберге предстояло преодолеть три мощных рубежа обороны с водными преградами. При планировании уличных боёв упор был сделан на 26 штурмовых отрядов и 104 штурмовые группы. По этим подразделениям распределили большое количество огнемётчиков, добавили по 1–2 танка и самоходному орудию. Перед штурмом со 2 по 5 апреля (4 дня!) была проведена необычно мощная артиллерийская подготовка. Авиация при этом использовалась слабо из-за дождливой погоды. Вступили в бой постановщики радиопомех. Известно, что на-

Иллюстрация 4. Замок прусских королей в поверженном Кёнигсберге

кануне штурма Кёнигсберга только 131-й и 226-й отдельные радиодивизионы ОсНаз эффективно заглушили 175 радиостанций противостоящих частей врага, хотя те пытались вести работу в 30 радиосетях на 300 радиочастотах. Гражданское население до самого штурма имело возможность покинуть город в направлении балтийского побережья и Пиллау, чем большинство и воспользовалось.

БЕЗОГОВОРОЧНАЯ КАПИТУЛЯЦИЯ ЧЕРЕЗ ЧЕТЫРЕ ДНЯ

Штурм Кёнигсберга начался утром 6 апреля. Генерал О. Ляш, командовавший его обороной, отметил в своих воспоминаниях: «Все средства связи были сразу же уничтожены, и лишь пешие связные пробирались на ощупь сквозь груды развалин к своим командным пунктам или позициям». Утром 9 апреля под контролем немецких войск остался лишь небольшой плацдарм в центре города, насквозь простреливаемый советской артиллерией. Стала улучшаться погода, и авиация смогла совершить около 1500 вылетов на бомбардировку и штурмовку врага. Уже в 23:30 9 апреля 1945 г. Москва салютовала войскам 3-го Белорусского фронта, овладевшим крепостью Кёнигсберг. Знаменательно, что приказ генерала О. Ляша о безоговорочной капитуляции был передан его войскам именно радиостанциями радиодивизионов ОсНаз.

* * *

После небольшой передышки 3-й Белорусский фронт ликвидировал и Земландскую группировку противника, овладев 25 апреля 1945 г. городом Пиллау. В тот же день начался штурм Берлина.

БОЛЬШЕ РЕЕСТРОВ, ХОРОШИХ И РАЗНЫХ

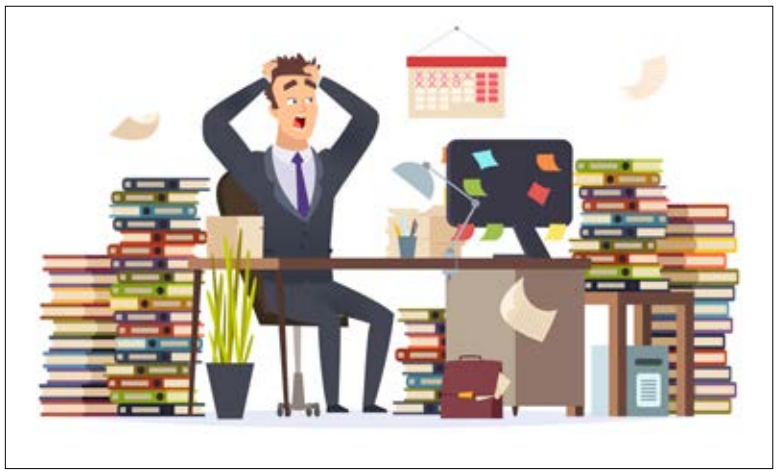
ЗАМЕТКИ БЕЗОПАСНИКА

Александр ИГОНИН
эксперт BIS Journal,
ведущий рубрики

В прошлых заметках мы поговорили о реестрах пользователей и хостов, а также некоторых других объектов. Сегодня хотелось бы закрыть тему с реестрами, поговорив о более диковинных из них. Начнём с тех, которые были лишь вскользь упомянуты ранее.

Во-первых, это реестр подсетей. Создать актуальный реестр хостов с владельцами каждого из них — задача очень непростая; если сил, времени и иных ресурсов на это не хватает — стоит задуматься о реестре подсетей, когда за каждой подсетью закрепляется ответственный сотрудник. Так в случае чего можно будет быстро найти человека, который хотя бы в общем понимает, что происходит в этой подсети.

Следующий момент — это доступные из интернета ресурсы: межсетевые экраны, веб-порталы, API-шлюзы и так далее. Для каждого такого устройства хочется знать как минимум публичный IP-адрес и краткое описание предоставляемого сервиса. Неплохо также иметь сведения об операционной системе и ключевых её компонентах: это очень актуально в момент выхода очередного «зеродея».



Хорошо бы ясно понимать, куда поступает внешний трафик и через какие промежуточные точки он проходит. В большинстве случаев здесь используется технология NAT, когда публичный IP-адрес преобразуется во внутренний. Однако всё может быть сложнее: например, опубликованный в интернете портал компании может находиться под защитой анти-DDoS сервиса, когда трафик вначале поступает на внешние сервера этого сервиса — и лишь затем, после «очистки», попадает в нашу инфраструктуру. При этом оригинальный адрес клиента-источника запроса может быть скрыт.

Если не очень опытный сотрудник, увидев подозрительный запрос, решит заблокировать «вредоносный» IP-адрес, с которого этот запрос пришёл, это может сделать ресурс недоступным для всех внешних пользователей. Конечно, со временем такие подробности становятся известны всем безопасникам — однако очень часто они хранятся и передаются в формате «устных народных преданий». А хочется видеть больше структуры и организованности, которые спасают сотрудников от излишнего стресса, а компанию порой и от серьёзных убытков (вспомним февральскую историю, где сотрудники Cloudflare «удачно» заблокировали фишинговую ссылку, в результате чего почти на час перестали работать некоторые их сервисы).

В завершение цикла упомяну реестр информационных систем. Как показывает практика, бизнес периодически прибегает с вопросами «А хорошо ли защищены наши критичные бизнес-системы?» — и на этот случай хорошо бы заранее договориться, какие системы мы считаем критичными, а какие имеют более низкий приоритет. Для каждой критичной системы надо знать её бизнес-владельца, верховного администратора, а также список входящих в неё хостов.

* * *

Тема с реестрами получилась довольно объёмной потому, что при реагировании на инциденты способность быстро определить, с каким хостом, системой и пользователем мы имеем дело, трудно переоценить. К сожалению, понимание этого часто приходит слишком поздно. Надеюсь, что вас, уважаемый читатель, такая участь обойдёт стороной.

SOC Tech

Технологии SOC

киберзастава

7 ОКТ 2025

Москва, LOFT #1

SOC Tech 2025 – это мероприятие нового типа
Оригинальные форматы откроют возможности сверхэффективного взаимодействия между участниками, спикерами и партнерами.

Регистрация: ib-bank.ru/soctech

Kaspersky
NGFW

Kaspersky NGFW уже в продаже!

kaspersky.ru/enterprise-security/ngfw

kaspersky активируй будущее

www.kaspersky.ru