BIS JOURNAL
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ БИЗНЕСА
№1 (56) 2025

Владимир МАТЮХИН
По случаю юбилея
Пионеру российской ИБ – 80 лет!
→ 106

Сергей ГУСЕВ
АО «Северсталь Менеджмент»
«Броня крепка, а будет крепче!»
→ 4

БЕЗОПАСНАЯ РАЗРАБОТКА ЭВОЛЮЦИЯ ПО ГОСТУ

Алексей СМИРНОВ
CodeScoring
Open source: безопасное использование
→ 40

Антон БАШАРИН
AppSec Solutions
Безопасность – это ваша прибыль!
→ 44

Дарья ФИГУРКИНА
Swordfish Security
Экспертов с низкой образовательной базой заменит ИИ
→ 48

07.04
2025

ЗАЩИТА ДАННЫХ

Ключевая конференция
о защите данных
на всех этапах
жизненного цикла

DATASEC.
IB-BANK.RU

ХОЛИДЕЙ ИНН СОКОЛЬНИКИ_МОСКВА_07.АПРЕЛЯ

Сергей ПАЗИЗИН
научный редактор
BIS Journal

Долгое время вопросы обеспечения информационной безопасности промышленных предприятий в части сегмента операционных технологий практически не попадали в фокус внимания профильных конференций и периодики. Безусловным лидером и двигателем развития информационной безопасности являлся финансовый сектор, который всегда был привлекателен для киберпреступников, так как позволял обеспечить прямую монетизацию их усилий. Также определенное внимание уделялось сегменту управления предприятием, в котором обрабатываются персональные данные, платежи, информация, составляющая коммерческую тайну.

Последние несколько лет ситуация кардинально изменилась. В операционном сегменте промышленных предприятий расширяется процесс автоматизации, возрастает количество связей с сегментом информационных технологий, широко внедряется роботизация и устройства интернета вещей. Таким образом, операционный сегмент становится более понятен и доступен для злоумышленников. Кроме того, в связи с последними политическими событиями, появился постоянный заказчик для деструктивной деятельности киберпреступников.

С учетом сказанного, в этом году журнал принимает активное участие в организации и проведении конференции «Цифровая устойчивость промышленных систем» 27–28 февраля 2025 г., а тему конференции мы взяли в качестве заглавной темы номера. Наша задача — познакомить читателей с актуальными задачами и особенностями обеспечения информационной безопасности на промышленных предприятиях.

Одной из актуальных проблем обеспечения безопасности, в том числе промышленных предприятий, является задача импортозамещения не только средств защиты информации и системного и прикладного ПО, но автоматизированных систем управления технологическими процессами. Причем, импортозамещенное ПО должно удовлетворять самым высоким требованиям безопасности. Это привело к огромному интересу к методам и средствам разработки безопасного ПО, в том числе, изменению нормативного регулирования в этой области. Поэтому большое внимание в нашем номере мы уделили также теме разработки безопасного ПО.

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 05.02.2025. 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: ЦИФРОВАЯ УСТОЙЧИВОСТЬ ПРОМЫШЛЕННЫХ СИСТЕМ

ИНТЕРВЬЮ НОМЕРА

ТЕМА НОМЕРА — 2: РАЗРАБОТКА БЕЗОПАСНОГО ПО

ТЕМА НОМЕРА — 2: РАЗРАБОТКА БЕЗОПАСНОГО ПО

РЕГУЛЯТОРЫ

УГРОЗЫ И РЕШЕНИЯ

ИНФРАСТРУКТУРА

КИБЕРКУЛЬТУРА

КИБЕРХАБ СКОЛКОВО

ЗА РУБЕЖОМ

СУБЪЕКТЫ

БРОНЯ КРЕПКА!

О СЕКРЕТАХ СПЛАВА ИЗ ТЕХНОЛОГИЙ, МЕНЕДЖМЕНТА И ПРОФЕССИОНАЛИЗМА РАССКАЗЫВАЕТ РУКОВОДИТЕЛЬ ИБ «СЕВЕРСТАЛИ» СЕРГЕЙ ГУСЕВ

Сергей ГУСЕВ
заместитель директора по информационной безопасности — начальник управления АО «Северсталь Менеджмент»

— Сегодня очень важно погрузиться в проблематику ИБ промышленных отраслей, поэтому главная тема этого номера BIS Journal формулируется как «Цифровая устойчивость промышленных систем». Расскажите, пожалуйста, что такое информационная безопасность на металлургических предприятиях? В чём её специфика? Как она устроена, организована?

— Специфика информационной безопасности на промышленных предприятиях ярко проявляется в сложных ИТ-решениях ERP-класса, MES-системах, системах реального времени слежения за производственными процессами и управления технологическими агрегатами. К тому же металлургическое предприятие — потоковое производство, и сбой в любой из цепочек влияет на качество и срок производимых заказов. В настоящее время глубина автоматизации промышленного предприятия достигла таких величин, которые кардинально меняют представление о современном металлургическом заводе или горнодобывающем карьере. Взятый курс на цифровизацию и применение систем на базе искусственного интеллекта вкупе с импортозамещением дополнительно подливают масла в огонь.

Всё это многообразие накладывает отпечаток на процессы обеспечения информационной безопасности. Несмотря на наличие в какой-то части схожих с финтехом киберугроз корпоративного уровня, в производственных компаниях есть и свои отличия, связанные с большим жизненным циклом производственных систем и возможными технологическими окнами для актуализации технических систем защиты. Методы и технологии, которые применяются для этого, разнообразны, и в этом заключается основное различие: нам требуется не только защищать традиционные бизнес-процессы корпоративного уровня, но и фокусироваться на специфичных технологиях АСУП и ТП.

ПРО УГРОЗЫ

— От чего защищают в «Северстали»? Для чего там нужна ИБ? Какой основной набор угроз? Как на него повлияло изменение геополитической обстановки?

— В нашей компании присутствует весь спектр типовых задач по защите от внешних и внутренних угроз для достижения триады верхнеуровневых целей ИБ. А если посмотреть на ценность ИБ со стороны бизнес-ориентированного подхода, то цель простая — создать возможность бизнесу безопасно работать по всем ключевым функциям. В нашей компании мы все угрозы для удобства разделили на типовые, массовые и целевые. Изменения в геополитической обстановке добавили в наш ландшафт угроз очень много новых векторов, которые ранее были присущи другим отраслям. 2024 год для нас прошёл под эгидой обеспечения безопасной собственной разработки и борьбы с мошенничеством и взломами сервис-провайдеров.

ПРО БИЗНЕС И РУКОВОДСТВО

— Кто и как оценивает в «Северстали» системы защиты информации? Эффективность подразделений ИБ? Специалистов ИБ?

— В «Северстали» принят многоуровневый подход к оценке эффективности системы защиты, которые мы разделили с топ-менеджментом компании. Во-первых, мы живём в рамках сервисной модели и с установленными SLA.

Во-вторых, согласно принятой стратегической программе развития, актуальной модели угроз и лучшим практикам принята система метрик защищённости, которая покрывает уровень киберзащиты корпоративных и производственных сегментов, процессы мониторинга и реагирования на киберугрозы, обеспечения уровня комплаенса и защиты данных. Отдельным блоком идут цели по культуре кибербезопасности персонала и подрядчиков.

В-третьих, в компании принята культура ежегодных командных и индивидуальных целей, позволяющая оценить вклад каждого. Несколько лет назад мы успешно внедрили практику по сквозному целеполаганию показателей ИБ с подразделениями, поддерживающими автоматизацию основных производственных и бизнес-процессов, которая доказала свою эффективность.

— Как ИБ связана с бизнесом? Существует ли утверждённая на уровне руководства концепция обеспечения ИБ?

— Напрямую. В «Северстали» существует утверждённая политика ИБ и стратегический план развития. В нашем случае нет никаких отличий в реализации классических принципов СУИБ, один из которых заключается в демонстрации топ-менеджментом «Северстали» своего лидерства и приверженности политикам и стандартам в области информационной безопасности, разделению ответственности и прочее. К тому же сама функция ИБ встроена практически во все ключевые бизнес-процессы, а в рамках сервисной модели наши процессы поддерживаются SLA, согласованным бизнесом.

— Как формируется бюджет на информационную безопасность? По какому критерию вы оцениваете, что выделили достаточно?

— Мы придерживаемся общих корпоративных правил и практик, принятых в финансовой и инвестиционной областях. У нас есть стратегический инвестиционный план развития и так называемый годовой инвестиционный план. Оба плана входят в общий ИТ-бюджет компании в виде отдельного портфеля или программы проектов.

Работа над стратегическим и годовыми бюджетными параметрами начинается с анализа текущих угроз, прогнозируемых в краткосрочной перспективе и на горизонте 3–5 лет. После проведения такого анализа мы проводим оценку доступных методов противодействия этим угрозам, изучаем рынок технологий и оборудования, потенциальных исполнителей. Затем с помощью собственной методики оценки вклада в уровень защищённости проводим моделирование эффекта от реализации мероприятий противодействия угрозам и расстановку приоритетов мероприятий. В зависимости от параметров бюджетного послания определяются финансовые параметры бюджета, отбор проектов и их защита у топ-менеджмента.

В качестве индикатива используется отраслевой бенчмаркинг на соответствие текущим лучшим практикам. В целом мерой достаточности финансового обеспечения функции защиты является оценка способности компании противостоять актуальным угрозам. Главное — делать это разумно и эффективно.

— Легко ли найти взаимопонимание службы ИБ и руководства организации, обосновать расходы на ИБ?

— Нам очень повезло, что топ-руководство компании понимает и разделяет необходимость обеспечения информационной безопасности. Отрадно, что это отношение распространяется и на нижних управленческих уровнях. Расходы, их эффективность и достаточность для коммерческих компаний всегда будут краеугольным камнем. Все необходимые инструменты для обоснования расходов в компании имеются, и как с ними работать, вполне понятно.

— В чём, на ваш взгляд, должен проявляться интерес бизнеса на уровне топ-менеджмента к решениям кибербезопасности и почему он не проявляется?

– Если под интересом к решениям кибербезопасности подразумевать применение этих решений для обеспечения защиты активов компании, то этот интерес проявляется на все 100%. Например, в «Северстали» уже несколько лет развивается культура кибербезопасности. Путём применения различных организационных и технических мероприятий, с привлечением консалтинга и самостоятельно, реализуется масштабный проект, который активно поддерживается топ-менеджментом.

РЕГУЛЯТОРЫ

— Банковским безопасникам по-своему повезло: у них есть прямой регулятор Банк России. На кого ориентируетесь вы? Есть ли у вас свой отраслевой регулятор? Или кто-то ещё выполняет такую функцию?

– Таким отраслевым регулятором выступает Министерство промышленности и торговли Российской Федерации (Минпромторг России), поскольку выполняет функции по выработке государственной политики и нормативно-правовому регулированию в сфере промышленного и оборонно-промышленного комплексов, промышленности строительных материалов (изделий) и строительных конструкций и т.д. В связи с последними изменениями в законодательстве государства в вопросах обеспечения безопасности критической информационной инфраструктуры, взаимодействие с Минпромторгом по вопросам ИБ стало более плотным.

— Проходят ли у вас проверки? Кто проверяет? Какая система наказаний, штрафов или поощрений? Насколько это для вас хлопотно и затратно?

– Как и любое юридическое лицо, находящееся на территории РФ и выполняющее требования федерального законодательства по вопросам информационной безопасности и защите данных, предприятия «Северстали» взаимодействуют с такими регуляторами, как ФСБ, ФСТЭК, РКН, Минпромторг. Опыт полученных результатов проверок считаем положительным.

— Можно ли сказать, что построение системы защиты информации в «Северстали» зарегулировано? Если да, то что это — требования регуляторов или естественные потребности бизнеса?

– Как и любая система управления, СУИБ требует фиксации правил в виде корпоративных и регуляторных нормативных актов. Когда в правилах находят своё отражение сбалансированные требования регуляторов, потребности бизнеса, лучшие практики и собственный опыт – это окно возможностей, которое приносит ещё большую пользу и гарантирует лучший результат в целом для системы менеджмента ИБ.

— Из каких документов берёте требования по безопасности? Насколько это удовлетворительно? Какие плюсы и минусы? Ключевые проблемы?

– Ранее нас полностью удовлетворяла серия международных стандартов ISO 27xxx и других известных фреймворков. Что касается отечественных требований, это, безусловно, требования основных регуляторов (ФСБ, ФСТЭК, РКН, Минпромторг), ГОСТы. Из плюсов хочется отметить, что с каждым годом материалы от регуляторов становятся более ориентированными на текущую ситуацию и помогают бороться с актуальными вызовами на практике.

Из минусов: за последний год принято так много изменений, что без специальной системы для большой компании с ними очень сложно справляться.

НЕПОСРЕДСТВЕННАЯ ПРАКТИКА

— Какие трудности вы испытываете в ходе практической работы?

– Трудности, порождаемые дефицитом: кадровым и технологическим в условиях геополитических ограничений. Реализация регуляторных требований, которые зачастую требуют значительных ресурсов. Но все эти трудности преодолимы. Отдельная трудность – объективное измерение уровня культуры кибербезопасности персонала.

— На кого из коллег вы ориентируетесь в своей работе? Кто или что для вас является Best Practice?

– Это отраслевые лидеры, компании – законодатели мод и с хорошим ресурсом на RND.

— Этот вопрос мы сначала сформулировали так: «Есть ли заметные отличия моделей нарушителя ИБ в современной металлургии от моделей нарушителя в ИБ банков?» Но если у вас нет опыта работы в банковской сфере, вопрос сформулирован некорректно. Давайте проще: какие особенности обеспечения ИБ характерны для предприятий металлургии?

– Основной особенностью ИБ для металлургического предприятия является защита производственных процессов и используемых для этого специализированных технологий, приложений и протоколов обмена информацией. Успешная реализация кибератаки может привести не только к простоям основного технологического оборудования (например, остановка домны является недопустимым событием: её нельзя запустить заново), но и к более значимым последствиям в целом.

— Имеется ли по данной теме специфическая учебно-методическая литература?

– В целом скорее нет, чем да. Основными источниками такой информации для нас являются различные информационные материалы от отраслевых и федеральных конференций, отраслевых сообществ (например, БИП-клуб) и иных организаций. Хотя в последнее время отраслевые журналы тоже становятся значимым источником.

— Кто проводит вам консалтинг в ИБ? Практикуете ли аутсорс?

– Лидирующие компании-интеграторы или производители. Аутсорс мы практикуем, но в меру. Объявления о проведении конкурсных процедур по определению исполнителя в той или иной области ИБ размещаются на наших закупочных онлайн-платформах.

— На некоторых конференциях, например, от «Позитив», проводятся игры, в которых нарушаются/защищаются режимы работы крупных пред-

приятий, в том числе в вашей отрасли. Насколько полезны такие игры?

— Безусловно, полезны. Мы сами практикуем проведение так называемого формата независимого теста на проникновения Red teaming, в рамках которого «красная» команда, состоящая из внутренних/внешних пентестеров, пытается выполнить задание и проникнуть внутрь нашей инфраструктуры, а «синяя» команда противостоит таким попыткам.

ТЕХНОЛОГИИ...

— Какие риски вы видите в использовании в вашей организации продуктов Microsoft и других зарубежных вендоров?

— Первый и самый актуальный для нас — отсутствие возможности получать гарантированные обновления используемых программных продуктов после окончания действий лицензионных соглашений. Второй, в противоположность первому, — потенциальное наличие недекларированных возможностей в пакетах обновлений без каких-либо гарантий доверия со стороны вендора.

— Как используется ИИ в ваших решениях? В частности, используются ли большие языковые модели типа chatGPT и, возможно, близкие отечественные модели?

— В компании активно развивается данное направление. Традиционные ML-модели применяются в качестве цифровых помощников производственному персоналу и автоматизации рутинных операций. Для промышленных процессов используются технологии ИИ, такие как машинное обучение, компьютерное зрение. Уже несколько лет применяются технологии работы с большими данными для предиктивного анализа. Генеративные модели используются пока больше в качестве цифровых помощников для удобства работы с базами знаний, как чат-боты.

В ИБ, помимо инструментов, встраиваемых вендорами в свои решения, мы находимся на стадии апробации таких решений для проведения киберучений, маркировки внесистемно обрабатываемых документов, профилирования и выявления аномалий.

...И ИМПОРТОЗАМЕЩЕНИЕ

— Как идёт процесс импортозамещения? Есть ли проблемы?

— Есть области, где идёт на «ура», в некоторых областях фиксируем неготовность российских решений или потребность в использовании большого количества продуктов для получения требуемого функционала. Проблема в том, что на рынке всё ещё недостаточно конкурентоспособного оборудования для реализации функций защиты, требующих «тяжёлых» вычислений на различных уровнях.

Ещё одна проблема — отказ иностранных производителей от поддержки программного обеспечения и переход на внутреннюю разработку. Это кратно увеличило объём использования свободно распространяемого ПО и программных продуктов собственной разработки. Как следствие, за последний год мы фиксируем десятикратный рост числа уязвимостей в таких продуктах — как случайных, так и умышленно предустановленных. Откликом на эти угрозы стал фокус на выстраивание процессов безопасной разработки. Упор сделан на процессы безопасной разработки новых проектов — порядка 90% всех новых продуктов не имеют критичных уязвимостей, а средний скоринг по их безопасности удалось поднять с трёх до четырёх баллов (пять — максимальный).

КАДРЫ

— Что с кадрами?

— Как и все отрасли, мы ощущаем кадровый голод и недостаток опытных специалистов. Приходится вкладывать значительные усилия в развитие приходящих молодых сотрудников, которые в силу поколенческой специфики своеобразно смотрят на профессиональный и карьерный рост. Кадровый голод и уход квалифицированного персонала приводят к более активному привлечению подрядчиков и внешних сервис-провайдеров.

— Как вы определяете потребность в кадрах ИБ? Как определяете портрет специалиста? Где берёте специалистов и как адаптируете?

— В «Северстали» практикуется применение драйверной модели численности, которая позволяет проводить оценку достаточности персонала для обеспечения бизнес-процессов. Привлечение персонала на вакантные должности в ИБ реализуется сначала из внутренних резервов (работники, желающие поменять область работы), затем идёт поиск готовых специалистов на рынке, и в последнюю очередь мы прибегаем к переквалификации профессионалов из смежных областей. Очень много молодежи из вузов мы привлекаем в качестве стажёров или практикантов. Адаптация проходит по методам, принятым в «Северстали»: кураторство, наставничество, обучение с помощью корпоративных программ и внешних провайдеров.

— Если посмотреть на карту деятельности «Северстали», в неё попадает ряд региональных вузов. Ведётся ли в них подготовка специалистов, в частности, по ИБ по прямым договорам, программам, соглашениям?

— Да, ведётся. Основной фокус работы по подготовке молодых специалистов сосредоточен на Череповецком государственном университете. По нескольким причинам: нахождение в одном городе с основной производственной площадкой — металлургическим комбинатом; наличие кафедры информационной безопасности, отдельные дисциплины студентам которой преподают сотрудники наших подразделений. В настоящее время мы рассматриваем возможности расширения работы с вузами в других регионах присутствия.

Также мы активно приглашаем студентов пройти практику в наших подразделениях, а выпускников — принять участие в программе стажировки. При таком подходе мы присматриваемся к потенциальным сотрудникам, а они оценивают свои возможности и преимущества работодателя. Кроме того, мы заключили соглашение с нашим опорным вузом, в рамках которого на коммерческой основе привлекаем студентов кафедры для выполнения различных задач.

Вопросы задавал
Игорь Некрасов

ПУТЬ К ТЕХНОЛОГИЧЕСКОМУ СУВЕРЕНИТЕТУ АЛРОСА

Вадим ЖЕЛТУХИН
директор по информационным технологиям компании АК АЛРОСА (ПАО)

ОБ АЛРОСА

АЛРОСА — крупнейшая алмазодобывающая компания с почти 70-летней историей, мировой лидер по объёмам добычи и разведанных запасов алмазов и единственная в мире компания полного цикла, которая охватывает все звенья алмазно-бриллиантового производства: от геологоразведки до создания бриллиантов и ювелирных украшений с ними.

В группе АЛРОСА работают свыше 35 тысяч сотрудников, которые обеспечивают более 30 % глобальной и около 90 % российской добычи алмазов. Добывающие активы расположены на территории России — в Республике Саха (Якутия) и в Архангельской области. Компания разрабатывает более 20 коренных и россыпных месторождений алмазов (рис. 1).

АЛРОСА оказывает влияние на рынок во многих сферах. Можно сказать, что она является драйвером перемен, стоит на острие многих инициатив по импортозамещению.

ИТ-функция АЛРОСА помогает автоматизировать производственные и бизнес-процессы, внедрять и поддерживать информационные системы, совершенствовать программные решения и гарантировать безопасность данных.

ИМПОРТОЗАМЕЩЕНИЕ

В АЛРОСА заговорили об импортозамещении ещё в 2018 году — сделали небольшие шаги в этом направлении, заместив иностранные браузеры и системы бизнес-аналитики на российские «Яндекс.Браузер» и Visiology. Три года назад движение в этом направлении усилилось.

В 2022 году наступил этап, когда мы начали выбирать лучшее среди отечественных решений. Мы реши-

Рисунок 1. Компания АЛРОСА — №1 в мире по добыче алмазов

ли не повторять иностранное, а на отечественном стеке собирать более качественные и эффективные решения. Так как для многих компаний и вендоров технологический суверенитет — новый неизведанный путь, у нас не было идеально подходящих отечественных продуктов под наши требования. Мы выбирали самую подходящую основу. Сегодня мы с подрядчиками подстраиваем продукты под АЛРОСА: включаем доработки в дорожную карту продуктов.

Импортозамещение — сложный процесс, который требует досконального анализа. А для этого важно смотреть на внутренние процессы компании, её внутреннюю интегрированность, на то, как она поменялась за десятилетия во время внедрения западных решений, на текущие потребности и на современные технологии. Сделать компанию лучше позволят выбор новой архитектуры и формирование новых требований. Тут стоит сделать акцент, что, прежде всего, это большая трансформация в восприятии не только ИТ-специалистов, но и бизнеса.

Поэтому важно работать с заказчиками, владельцами бизнес-процессов, учитывать риски и в процессах, и в продуктах и искать сбалансированное решение. При этом не повторять под кальку, а делать новый продукт на отечественном стеке.

Известные продукты, ПО, решения во всём мире проходили путь становления не один год: проводились анализы, собиралась и учитывалась обратная связь пользователей, дорабатывались алгоритмы. Всё это совершенствовалось для того, чтобы продукты стали такими, какими мы их видим сегодня. Путь один, и наша задача — его пройти.

ВОЗМОЖНОСТИ И ОГРАНИЧЕНИЯ

Для АЛРОСА импортозамещение сегодня — новая и неотложная задача. У вендоров и компаний пока что не всегда есть однозначное понимание, что правильно, а что нет. Чтобы процесс становился более понятным и прозрачным, государство вводит новые требования, которые призваны создать более оптимальные условия для бизнеса и разработчиков.

ОГРАНИЧЕНИЯ:

- недостаточная совместимость отечественных решений между собой;
- жёсткий подход регуляторов к импортозамещению государственных компаний;
- длительные сроки поставки оборудования;
- указ президента о запрете зарубежного ПО на ЗОКИИ;
- трансформация ФЗ и ФСТЭК по безопасности ИИ;
- финансовая нагрузка на поддержку двух систем на период перехода.

ВОЗМОЖНОСТИ:

- повышение эффективности производства;
- оптимизация бизнес-процессов;
- новые технологии вместо устаревших;
- исключение репутационных и санкционных рисков;
- влияние на становление российского ИТ-рынка.

Рисунок 2. Новые требования и ограничения создают и новые возможности

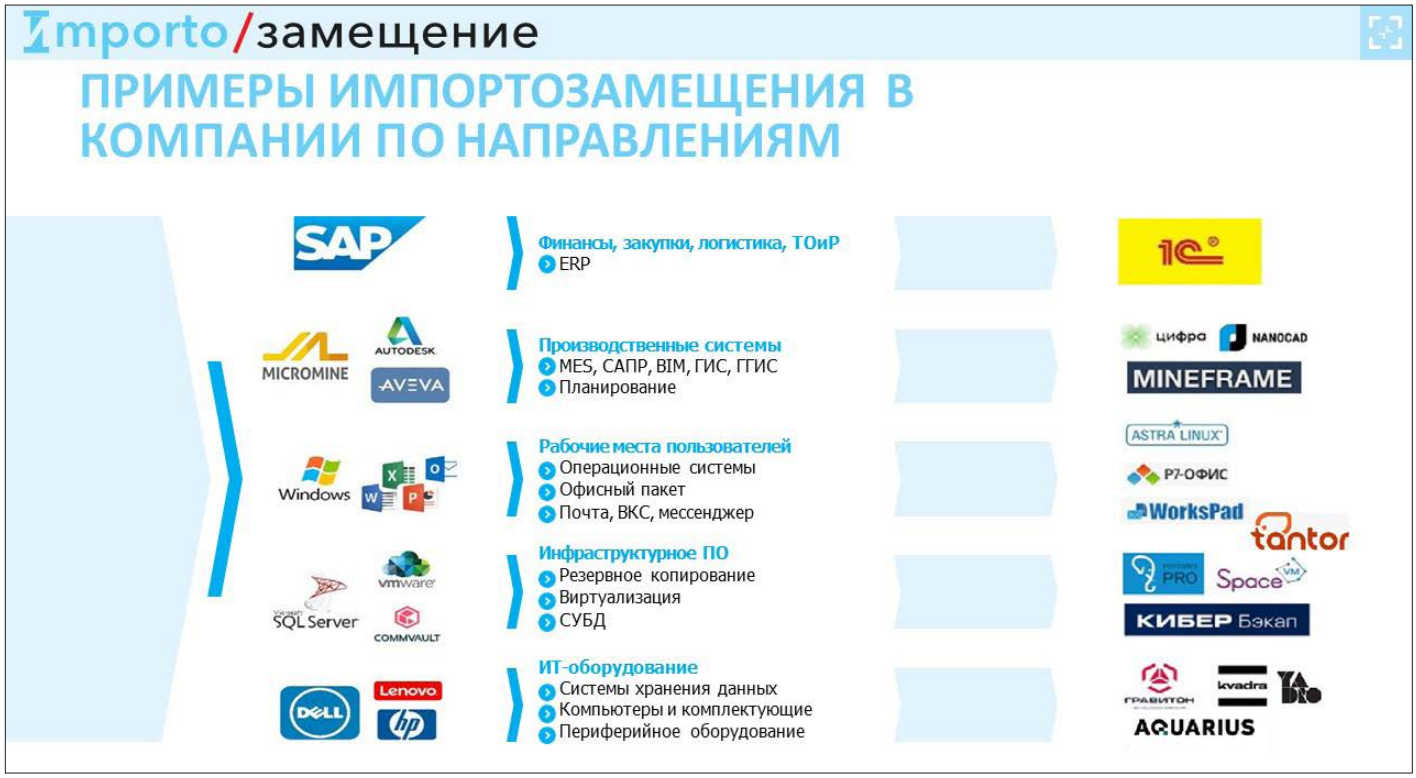


Рисунок 3. Примеры импортозамещения в компании АЛРОСА по направлениям

Трансформация с использованием отечественных технологий — хорошая возможность компаниям посмотреть на себя и процессы внутри, сделать цифровизацию не отдельными «мазками», а внедрить её комплексно — на уровне процессов (рис. 2).

Импортозамещение сегодня имеет ряд очевидных зон роста: сложности с совместимостью отечественных решений между собой, законодательство, степень зрелости вендоров и их компетентность, консолидация рынка. Ожидается, что в ближайшие годы экспертность в части разработки продуктов повысится. Значительный вклад в это делает бизнес, в том числе АЛРОСА. Конструктивная обратная связь — то, на что опираются разработчики и используют в своих дорожных картах, улучшая продукты. В этом плане пользователям следует быть толерантными к тем, кто проходит путь импортозамещения впервые. Только так можно приблизить успех.

ГОСУДАРСТВЕННОЕ УЧАСТИЕ

Государственное участие в компании — это дополнительная ответственность, а также катализатор операционных улучшений. Государство предоставляет возможности для развития, в том числе в части бюджетирования при условии выполнения чётко определённых КПЭ. АЛРОСА ведёт постоянный диалог с различными ведомствами: Минцифры, Минпромторгом и другими, обменивается лучшими практиками с лидерами рынка и предлагает доработки, направленные на улучшение продуктов.

ОТ ПОИСКА ДО ВНЕДРЕНИЯ

Раньше, чтобы производство было высокоэффективным и не давало сбоев, было необходимо выбрать лучшее из 2–3 иностранных решений, которые имели апробацию в отрасли. Для этого можно было организовать референс-визит на производство за границу, получить информацию от глобальных экспертов, снизить свои трудозатраты с помощью готовых работающих решений.

Сегодня мы перешли на качественно новый этап — развиваем и совершенствуем собственные отечественные продукты. Как уже заметили, АЛРОСА ИТ старается выбирать решения, которые изначально максимально подходят требованиям компании — в среднем на 70–80 %. И тут важно учесть фактор развития: насколько компания-производитель готова двигаться по этому пути, насколько она вкладывает ресурсы не только в разработку, но и в поддержку, команду, рынок, образование этих решений, а главное — насколько она готова менять продукт под потребности бизнеса.

ПРИМЕРЫ ИМПОРТОЗАМЕЩЕНИЯ

В этом году АЛРОСА ИТ провели тестирование, отбор и конкурс для определения долгосрочных партнёров — производителей серверов, рабочих станций (рис. 3). Все стандартные модели удалось найти на российском рынке — по адекватной стоимости, сопоставимой с иностранными аналогами.

Российский рынок стремительно развивается, и мы растём и развиваемся вместе с ним: изучаем продукты, совершенствуем их, передаём опыт другим компаниям. Всё это является нашим общим вкладом в цифровую независимость.

РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ В IT- И OT-СЕГМЕНТАХ СЕТИ С РИСК-ОРИЕНТИРОВАННЫМ ПОДХОДОМ

РЕКОМЕНДАЦИИ ОТ SECURITY VISION

Сети предприятий могут включать в себя много объектов, которые можно разделить на два крупных лагеря: информационные и промышленные технологии:

- Промышленный сегмент включает коммутаторы и маршрутизаторы, совместимые с промышленными протоколами (например, Modbus, OPC-UA, Profinet), системы управления процессами (SCADA) для контроллеров и устройств управления (PLC, RTU, DCS и др.), т.е. операционные технологии, OT (Operational Technology);
- Почтовые серверы, мессенджеры, системы управления ресурсами предприятия (ERP) и клиентами (CRM) состоят из классических ИТ-объектов (компьютеров, серверов, баз данных, операционных систем и приложений, маршрутизаторов, коммутаторов и т.д.) и составляют собой сегмент IT (Information Technology).

Отличия между OT и IT сегментами связаны с их назначением, архитектурой, требованиями и особенностями эксплуатации: цель работы первого — управление физическими процессами и оборудованием, в то время как айти сосредотачивается на обработке, хранении и передаче данных. В связи с этим триада «целостность-конфиденциальность-доступность» имеет различный приоритет для сегментов: для OT на первое место выходит доступность процессов, далее их целостность и конфиденциальность (ДЦК), а для IT-сегмента в приоритете — конфиденциальность, триада выглядит как «конфиденциальность-целостность-доступность» (КДЦ) — это учитывается при построении ресурсно-сервисной модули в модуле SV AM.

Промышленный сегмент напоминает в бытовом плане надёжную технику, например, плиту или бойлер, главная задача которых — всегда работать, даже если она устарела (эту технику обновляют редко, а сбой может серьёзно повлиять на повседневную жизнь). IT же можно сравнить с вашим компьютером или смартфоном: вы на нем работаете, храните личные данные и постоянно обновляете программы, чтобы быть защищёнными (этот стек технологий гибок, но уязвим к потерям информации). Поэтому для обеспечения высокого уровня безопасности стоит отталкиваться от особенностей подсетей:

- В промышленности оборудование используется десятилетиями, а совместимость новых решений с устаревшими (legacy) системами — большая проблема. Атаки на OT могут приводить к физическому ущербу, остановке производства или даже риску для здоровья и жизни людей. OT-системы часто изолированы от внешнего мира (air-gapped), но с ростом IoT и Industry 4.0 они становятся все более связанными с IT-сетями. Некоторые системы нельзя выключить для обновления или тестирования, так как это может привести к остановке производства, поэтому и доступность находится на первом месте.
- Главная цель информационных систем — обеспечить безопасное и эффективное управление информацией, нарушение конфиденциальности которой (например, утечка клиентской информации) приводит к репутационным и финансовым потерям. IT сегмент динамичен, технологии и системы обновляются постоянно, новые уязвимости часто закрываются регулярными патчами, а связи с интернетом, облачными платформами и другими сетями делают сегмент более подверженным кибератакам.

Отличия между сегментами Operational Technology и Information Technology связаны с их назначением, архитектурой, требованиями и особенностями эксплуатации

Проговорив отличия, мы выделим несколько точек пересечения, на которых основывается методика построения общего центра киберзащиты SOC:

1. Системы мониторинга OT передают данные в IT для аналитики и управления бизнес-процессами — необходима платформа для интеграции;
2. Устройства Интернета вещей (IoT) связывают IT и OT, создавая новые риски — необходимы средства оркестрации и единого управления процессами;
3. Современные атаки (например, ransomware) могут затрагивать как IT, так и OT-сегменты — поэтому SOC для обоих сегментов основывается на продвинутых способах реагирования с максимальной автоматизацией и единым центром управления.

Эксперты Security Vision подготовили для вас пошаговую инструкцию по построению эффективного центра кибербезопасности:

ШАГ 1: ОЦЕНКА ТЕКУЩЕГО СОСТОЯНИЯ

Проведите аудит сетей IT и OT, чтобы понять их структуру, активы, угрозы и уязвимости. Результатом этого этапа будет определение критичных данных, устройств и систем, мест хранения и обработки информации, приоритетов активов и рисков, готовых для последующего анализа. Управление активами и инвентаризацией (AM/CMDB) и конфигурациями технологических платформ (SPC) стоит выбирать исходя из гибкости, возможностей подключения любых источников данных и гибкости управления конфигурациями, чтобы текущие параметры можно было приводить к эталонным значениям автоматически или по простому нажатию кнопки в интерфейсе.

ШАГ 2: СОЗДАНИЕ ЕДИНОЙ КОМАНДЫ И ПЛАНОВ

Организуйте группу специалистов из IT и OT с чётким распределением ролей (IT-эксперты разбираются в данных и современных угрозах в то время, как OT-специалисты понимают специфику оборудования и критические процессы), разработайте план реагирования на инциденты, который охватывает обе среды с учётом процедур, приоритетов и допустимых сроков восстановления, инструкций по изоляции, восстановлению и эскалации инцидентов. Новейший подход к реагированию с объектно-ориентированным подходом и применение динамических плейбуков, которые подстраиваются под окружение, лежат в основе модуля управления инцидентами (SOAR).

ШАГ 3: СЕГМЕНТАЦИЯ И ЗАЩИТА СЕТЕЙ

Сегментируйте IT и OT-сети, чтобы минимизировать риск распространения атак: внедрите межсетевые экраны с правилами, ограничивающими взаимодействие между IT и OT, используйте VLAN или физическое разделение сетей, установите специализированные системы обнаружения вторжений (IDS), адаптированные для промышленных протоколов (например, Nozomi, Claroty), настройте системы мониторинга событий и корреляции инцидентов (SIEM в составе комплекта NG SOAR) и мониторинг физического оборудования (например, через SCADA). Для защиты сетей также применяются сканеры защищённости (VS) и системы управления уязвимостями (VM), которые поддерживают автопатчинг и автоматическую проверку исполнения задач, как, например соответствующие модули Платформы Security Vision.

ШАГ 4: ЦЕНТРАЛИЗАЦИЯ МОНИТОРИНГА И КОРРЕЛЯЦИИ

Внедрите единую платформу для управления инцидентами (интеграция SIEM и IDS при помощи SOAR), обеспечьте видимость обеих сред через SOC, настройте уведомления и приоритеты для них. Платформенный подход к разработке решений Security Vision позволяет пользователям изменять логику работы отдельных модулей и создавать персональные витрины данных и доступных действий для всех участников процесса.

ШАГ 5: АВТОМАТИЗАЦИЯ РЕАГИРОВАНИЯ

Пропишите правила, когда вмешательство будет происходить автоматически, а когда требуется ручное подтверждение (например, для IT быстрое изолирование заражённых устройств, обновление политик безопасности автоматизируется в первую очередь, а для OT можно автоматизировать переключение на резервное оборудование или снижение мощности оборудования в случае угрозы). При анализе сложных инцидентов в автоматизации также участвуют технологии ИИ: внедрённые в SV SOAR ML-модели позволяют проводить анализ вердиктов и указывают сотрудникам на возможные ложноположительные срабатывания, а интеграция с LLM-моделями в решениях Security Vision делают их (например, ChatGPT и YandexGPT) ИИ-помощниками для аналитиков не только в поиске информации, но и в анализе индикаторов компрометации.

ШАГ 6: ПОСТИНЦИДЕНТНЫЙ АНАЛИЗ И РИСК-ОРИЕНТИРОВАННЫЙ ПОДХОД

Моделирование угроз упрощает анализ рисков (RM) и влияния инцидента на бизнес-процессы, комплаенс и аудит (CM) учитывает особенности объектов КИИ и требования других нормативно-методических документов, а управление непрерывностью (BCP) позволяет проводить разработку планов восстановления деятельности (DRP, Disaster Recovery Plan) и GAP-анализ с оценкой последствий в финансовом выражении: расхождения в показателях RTO (Recovery Time Objective), RPO (RecoveryPoint Objective) и MTPD (Maximum Tolerable Period of Disruption).

* * *

Комплексная система, построенная на основе наших рекомендаций и продвинутых технологий, будет готова к росту инфраструктуры или изменениям в процессе. Это обеспечит не только быстроту и точность реакции, но и минимизацию рисков для бизнеса и процессов.

ЗНАЧИМОСТЬ СТАНДАРТОВ СЕРИИ 57580 В ЦИФРОВОЙ ТРАНСФОРМАЦИИ

Тарас МАКАРЕНКО
руководитель направления Стратегия и риски компании «Информзащита»

Финансовый сектор России активно переходит на цифровые технологии: растёт доля дистанционного обслуживания, появляются новые финтех-сервисы, шире используется облачная инфраструктура. Вместе с этим растут и риски в сфере информационной безопасности, что ставит перед организациями задачу обеспечения устойчивости и непрерывности бизнес-процессов.

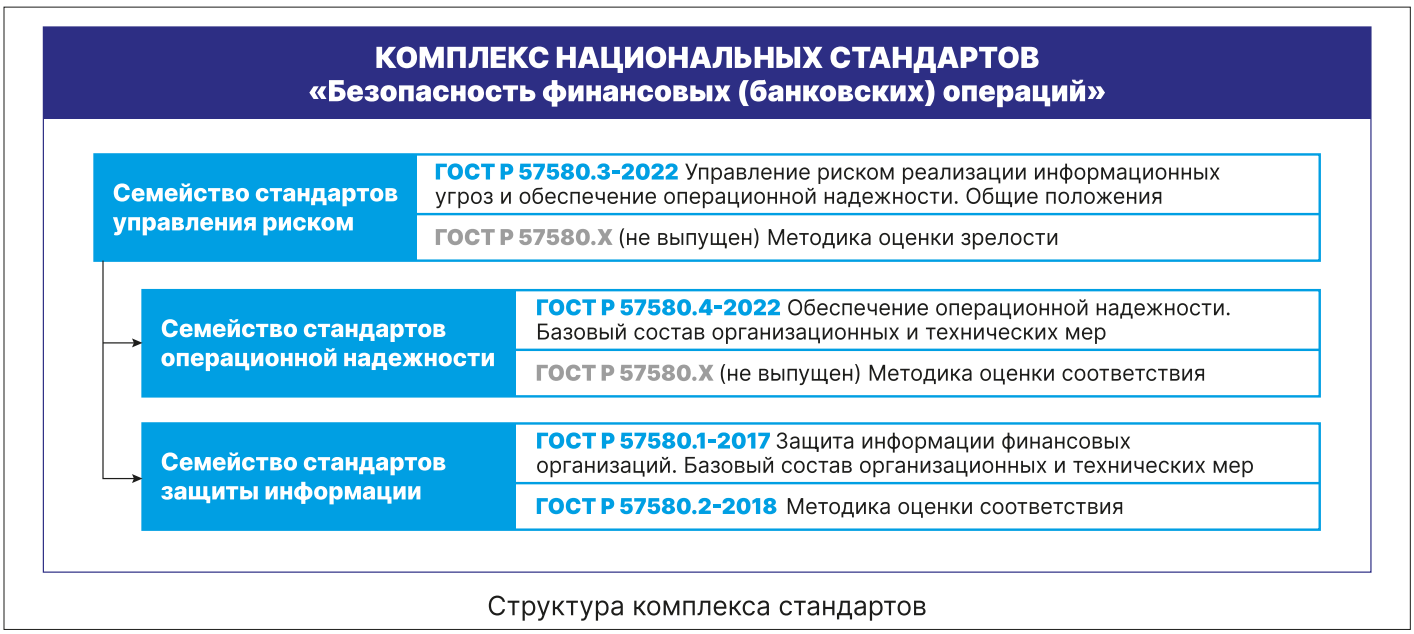
Для решения этих вызовов разработан комплекс национальных стандартов ГОСТ Р 57580 «Безопасность финансовых (банковских) операций». Он охватывает ключевые требования к защите информации, управлению рисками и операционной надёжности. Стандарт создает единую экосистему, где каждый элемент дополняет другой, обеспечивая последовательный подход от оценки рисков до внедрения мер защиты и поддержания непрерывности бизнеса (рис. 1).

ГОСТ Р 57580.3–2022 «Управление риском реализации информационных угроз и обеспечение операционной надёжности. Общие положения» описывает систему управления рисками реализации информационных угроз (СУР РИУ), а ГОСТ Р 57580.4–2022 «Обеспечение операционной надёжности. Базовый состав организационных и технических мер» определяет системы организации, управления и обеспечения операционной надёжности, регламентируя практические аспекты, обеспечивающие устойчивость, надёжность и быстрое восстановление при сбоях или атаках. Эти стандарты также способствуют внедрению действующих положений Банка России в области управления операционным риском и надёжностью (716-П, 779-П, 787-П и др.), обеспечивая практическую поддержку бизнес-процессов.

Реализация информационных угроз в финансовом секторе является объективной реальностью. Организации должны своевременно выявлять угрозы, снижать их вероятность, минимизировать последствия и обеспечивать оперативное восстановление в соответствии с требованиями бизнеса и законодательства. Полностью исключить риск невозможно, однако его можно свести к приемлемому уровню. Для этого в стандартах предусмотрен риск-ориентированный подход к управлению ими.

ГОСТ Р 57580.3–2022

ГОСТ Р 57580.3–2022 является ключевой частью серии стандартов ГОСТ



Структура комплекса стандартов

Рисунок 1. Комплекс национальных стандартов «Безопасность финансовых (банковских) операций»

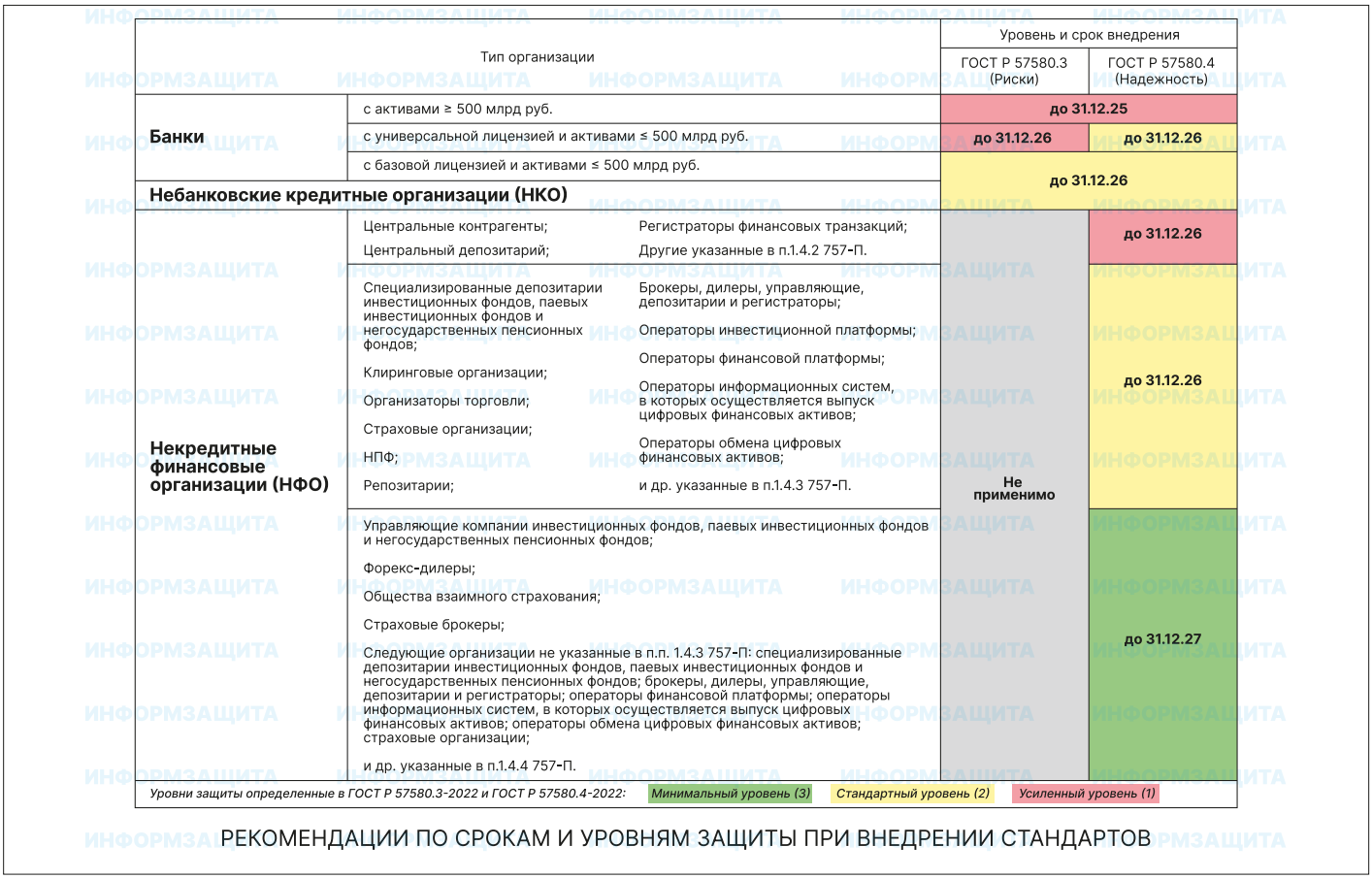


Рисунок 2. Сроки и уровни внедрения стандартов

Р 57580 «Безопасность финансовых (банковских) операций». Стандарт охватывает управление рисками, рассматривая кибербезопасность как неотъемлемую составляющую операционной надёжности и устойчивости бизнеса, и устанавливает единые подходы к управлению рисками реализации информационных угроз. Его цель — организовать планирование, внедрение, контроль и совершенствование системы управления рисками, повысить устойчивость финансовых организаций к киберугрозам за счёт организационных и технических мер, а также стимулировать развитие процессов операционной надёжности и защиты информации.

Стандарт предоставляет методический каркас для управления рисками, описывает назначение, структуру и принципы построения системы, а также её интеграцию с другими стандартами из комплекса ГОСТ Р 57580. Особое внимание уделено риск-ориентированному подходу к выбору мер управления информационными угрозами. В документе представлен перечень направлений, процессов и требований, необходимых для эффективного управления такими рисками.

В восьмой главе стандарта сформулированы требования к СУР РИУ по четырём направлениям: планирование, реализация, контроль и совершенствование. По каждому направлению стандарт определяет рекомендуемые организационные (О), технические (Т) и необязательные (Н) меры. Приложения к стандарту (А–Г) содержат детализированную классификацию событий риска, а в приложениях Д–Е определены ключевые показатели управления рисками (КПУР), которые необходимо отслеживать, с указанием форматов для их представления.

Исходная идея стандарта состоит в том, что полностью устранить ИБ-угрозы невозможно и любая организация должна быть готова постоянно противодействовать им. Главная задача — привести риск к уровню, приемлемому с точки зрения бизнес-стратегии и требований законодательства. Это предполагает регулярную оценку угроз, формирование политики управления рисками и использование компенсирующих мер, когда реализация «штатных» мер оказывается невозможной или слишком затратной.

Стандарт подчёркивает, что СУР РИУ — неотъемлемая часть бизнес-стратегии. Управление рисками информационных угроз и обеспечение операционной надёжности выходит за рамки ответственности исключительно ИТ- или ИБ-подразделений. Важно участие руководства на самом высоком уровне, а также интеграция этой деятельности с общекорпоративной стратегией, целями и политикой управления рисками, которая должна четко определять приоритеты, уровень риск-аппетита к информационным угрозам (приемлемый уровень риска, учитывающий законодательные требования и цели компании), а также принципы распределения ответственности.

ГОСТ Р 57580.4–2022

ГОСТ Р 57580.4–2022 «Обеспечение операционной надёжности. Базовый состав организационных и технических мер» представляет собой практический инструмент для формирования системного подхода к обеспечению операционной надёжности. Стандарт позволяет учитывать и выполнять как внутренние требования организации к уровню отказоустойчивости и надёжности, так и требования регулятора, с учётом уровня риска, масштаба и специфики её деятельности.

Основная задача стандарта — определить ориентиры по мерам, которые необходимы для защиты критичных активов (IT-систем, сетевой инфраструктуры, операционных процессов) и обеспечения непрерывности ключевых операций. Под «критичной архитектурой» в данном контексте понимается совокупность бизнес-процессов и технологических компонентов (серверы, каналы связи, приложения, базы данных), без которых финансовая организация не может выполнять основные функции и обязательства перед клиентами и партнёрами.

Стандарт определяет требования к системе обеспечения операционной надёжности, включающей восемь ключевых процессов:

1. Идентификация критичной архитектуры.
2. Управление изменениями.
3. Выявление, регистрация, реагирование на инциденты и восстановление.
4. Взаимодействие с поставщиками услуг.
5. Тестирование операционной надёжности бизнес- и технологических процессов.
6. Защита критичной архитектуры при дистанционной работе.
7. Управление риском внутреннего нарушителя.
8. Обеспечение осведомлённости об актуальных информационных угрозах.

В центре внимания стандарта — система организации и управления операционной надёжностью, основанная на четырёх направлениях:

1. **Планирование:** постановка целей, определение области применения и выделение ресурсов для защиты и обеспечения доступности критичных активов, бизнес-процессов и услуг.
2. **Реализация:** внедрение организационных и технических мер, обучение персонала и согласование процессов между подразделениями.
3. **Контроль:** мониторинг соблюдения правил, проведение аудитов и стресс-тестов, оценка устойчивости к новым угрозам.
4. **Совершенствование:** анализ инцидентов, корректировка политик и усовершенствование технических решений.

Как и в ГОСТ Р 57580.3, в данном Стандарте подчёркивается, что полностью исключить ИБ риски невозможно, однако их можно уменьшить до уровня, приемлемого для организации и соответствующего её риск-аппетиту. Для этого рекомендуется применять риск-ориентированный подход:

1. Выявлять и классифицировать активы (включая IT-системы, процессы, персонал, инфраструктуру).
2. Оценивать вероятность и последствия возможных угроз.
3. Определять меры безопасности, приоритеты и ресурсы исходя из критичности активов и допустимого уровня риска.

СРОКИ И УРОВНИ ВНЕДРЕНИЯ СТАНДАРТОВ

В марте 2024 года Банк России выпустил Методические рекомендации (7-МР)[1], в которых освещаются сроки внедрения новых стандартов и уровни защиты. В документе регулятор рекомендует уже сейчас приступить к разработке плана реализации стандартов, несмотря на то, что такие планы пока не являются обязательными. Они отражены в 7-МР, но еще не закреплены в законодательных актах Банка России.

Тем не менее, предварительная подготовка позволит не только снизить риски, но и адаптироваться к новым требованиям, пока они не стали обязательными (рис. 2)

ГОСТ Р 57580 может применяться не только финансовыми организациями, но и финтех-компаниями, ИТ-аутсорсерами, а также представителями других отраслей, где требуется системный подход к управлению рисками информационных угроз и обеспечению операционной надёжности. Стандарт предусматривает три уровня защиты, позволяя адаптировать требования под конкретные условия. Минимальный уровень подходит для организаций с некритичными операциями и ограниченным объёмом деятельности. Стандартный уровень предназначен для компаний среднего и крупного масштаба с повышенными требованиями к безопасности и обеспечению непрерывности. Усиленный уровень рассчитан на системно значимых участников, сбои в деятельности которых могут привести к масштабным последствиям.

* * *

Таким образом, стандарты ГОСТ Р 57580 задают системный подход к управлению рисками информационной безопасности и операционной надёжности — как известно, банковская сфера является пионером в создании и совершенствовании систем информационной безопасности в стране и мире. Данный опыт формирования стандартов, безусловно, будет полезен и для построения регуляторики в области безопасности промышленных систем.

[1] Методические рекомендации по управлению риском информационной безопасности и обеспечению операционной надежности» (утв. Банком России 21.03.2024 N 7-МР)

«У НАС УНИКАЛЬНЫЙ ШАНС — ПЕРВЫМИ В МИРЕ СОЗДАТЬ ЭКОСИСТЕМУ РЕШЕНИЙ ОТКРЫТОЙ АСУ ТП»

Сегодня перед российской промышленностью стоит большая задача — технологический рывок на основе цифрового импортозамещения. Это очень сложная комплексная задача. Помочь предприятиям в её решении призвана идея открытой АСУ ТП (ОАСУ ТП). О том, что она представляет собой в теории и на практике, BIS Journal беседует с Антоном Арнаутовым, директором АНО «Открытые системы автоматизации», ответственным секретарём рабочей группы ОАСУ ТП.

Антон АРНАУТОВ
директор АНО «Открытые системы автоматизации», ответственный секретарь рабочей группы ОАСУ ТП

— Антон Георгиевич, что является конечной целью создания открытой АСУ ТП в нашей стране? Стандарты автоматизации и цифровизации промышленных решений?

— Обратите внимание, инициаторами создания нашей рабочей группы по открытой АСУ ТП выступили промышленные компании — лидеры отраслей: «ЕвроХим», «Северсталь», «ЛУКОЙЛ», «АЛРОСА», «Уралхим», «Газпром нефть», «Норильский никель» и др. Но промышленникам нужны не стандарты, а конкретные решения, которые позволят им решать свои насущные задачи по автоматизации технологических процессов. Понятно, что таких задач после ухода из России западных вендоров не просто много, а очень много. Поэтому нашей конечной целью является создание экосистемы решений, основанных на принципах открытой АСУ ТП.

ДРУГАЯ СИТУАЦИЯ

— Этот подход — в русле мирового тренда перехода к открытым решениям АСУ ТП?

— Мы внимательно изучаем международный опыт. Однако наши цели/задачи сегодня отличаются от тех, что декларируют западные коллеги — эксперты из OPAF (Open Process Automation Forum, форум открытой автоматизации), который был создан в 2016 г. на базе Open Group. Они также ставят своей целью переход от проприетарных архитектур АСУ ТП к открытой архитектуре, которая позволит применять новые цифровые технологии, сохраняя при этом возможность использовать проприетарные унаследованные решения. Но основной задачей OPAF является создание стандартов открытой автоматизации — OPAS.

У нас другая ситуация — перед нашим рынком стоит беспрецедентный вызов: надо не только разработать стандарты, но ещё и нарастить вокруг них «плоть и кровь» в виде работающих решений. Это необходимо, поскольку: во многих отраслях доля решений западных вендоров доходит до 97–98%.

СМЕНА ПАРАДИГМЫ — ЭТО ШАНС

— Разве это не главный вызов для перехода на открытые архитектуры?

— Переход на открытые архитектуры является глобальным трендом, он связан с тем, что сегодня весь мир проходит, можно сказать, через смену парадигмы — принципиальное изменение подходов к промышленной автоматизации. И именно это подтолкнуло таких глобальных производителей, как Schneider Electric, ABB, Yokogawa Electric и др., включиться в гонку этого тренда открытости.

— Почему мы говорим о смене парадигмы?

— Промышленная автоматизация, началась очень давно — с электромеханических устройств, никак не связанных с информационными технологиями. И решения АСУ ТП

в наше время, по сути, сохранили свою аппарато-центричность. Эта же логика была перенесена на те решения, которые создаются уже в тесной связи с информационными технологиями. Сегодня разрыв между логикой старых систем промавтоматизации, основанных на аппарато-центричности и закрытости экосистем производителей друг от друга, и логикой мира ИТ, где всё подчиняется идее свободного обмена данными и возможности использовать всю доступную информацию, стал слишком глубоким. Поворот в сторону открытой архитектуры промавтоматизации стал неминуем.

— Так в чём уникальность нашей ситуации?

— После ухода западных вендоров нужно импортозаместить около 90% решений промышленной автоматизации, работающих на российских предприятиях. Иными словами, запрос на отечественные решения АСУ ТП настолько велик, что наши отечественные вендоры при всём желании не смогут его удовлетворить, оставаясь на прежних позициях проприетарности. Нужно придумать, как создавать новые комплексные системы автоматизации, используя программные и аппаратные решения разных вендоров. А сроки жёсткие: к 2030 году все объекты КИИ должны быть автоматизированы с помощью отечественных доверенных ПАКов.

Для нас это исторический шанс: Россия может стать одним из лидеров по созданию новой открытой экосистемы АСУ ТП. Нам максимально быстро необходимо перейти от стандартов и рассуждений о принципах к внедрению конкретных решений.

ЗАРУБЕЖНЫЙ ОПЫТ

— Зарубежный опыт стандартизации открытых решений АСУ ТП может быть полезен?

— Конечно. В России есть практика перевода и адаптации международных стандартов, в том числе — стандартов, которые разрабатывает Международная электротехническая комиссия (МЭК). Например, для создания распределённых систем управления (РСУ, DCS — Distributed Control System) полезен стандарт IEC61499 Он определяет архитектуру и методы программирования промышленных систем, а также описывает методы создания гибких, масштабируемых и реконфигурируемых систем управления на основе программируемых логических контроллеров (ПЛК).

Над стандартами работают также NAMUR, международная ассоциация пользователей технологий автоматизации в промышленности, UniversalAutomation, OPC Foundation и др.

OPAF отличается тем, что они создают «стандарт стандартов» — O-PAS, то есть берут «кирпичики» уже имеющихся стандартов МЭК, ISA, NAMUR и т.д. и строят из них новую конструкцию: O-PAS — это набор стандартов для открытой, совместимой и безопасной архитектуры систем автоматизации.

По сути, подход OPAF подразумевает максимальное использование того, что уже существует и хорошо работает. Например, в части стандартизации разработки прикладных частей используется международный стандарт МЭК 61131–3. Он описывает языки программирования для ПЛК: три графических и два текстовых.

— А у нас?

— У нас стоит такая же задача — максимально переиспользовать имеющиеся наработки. Так, коллеги, работающие в подгруппе полевых протоколов, взяли за основу одну, на наш взгляд, из наиболее перспективных технологий — Ethernet APL. Она обеспечивает непрерывную связь и быструю передачу данных с полевого уровня в систему управления технологическим процессом.

Кроме того, мы понимаем, что в недалёком будущем предстоит выход на глобальные рынки дружественных стран. Очевидно, что российские решения должны иметь возможность поддержки оборудования и софта, произведённых в других странах. А это означает совместимость с международными стандартами.

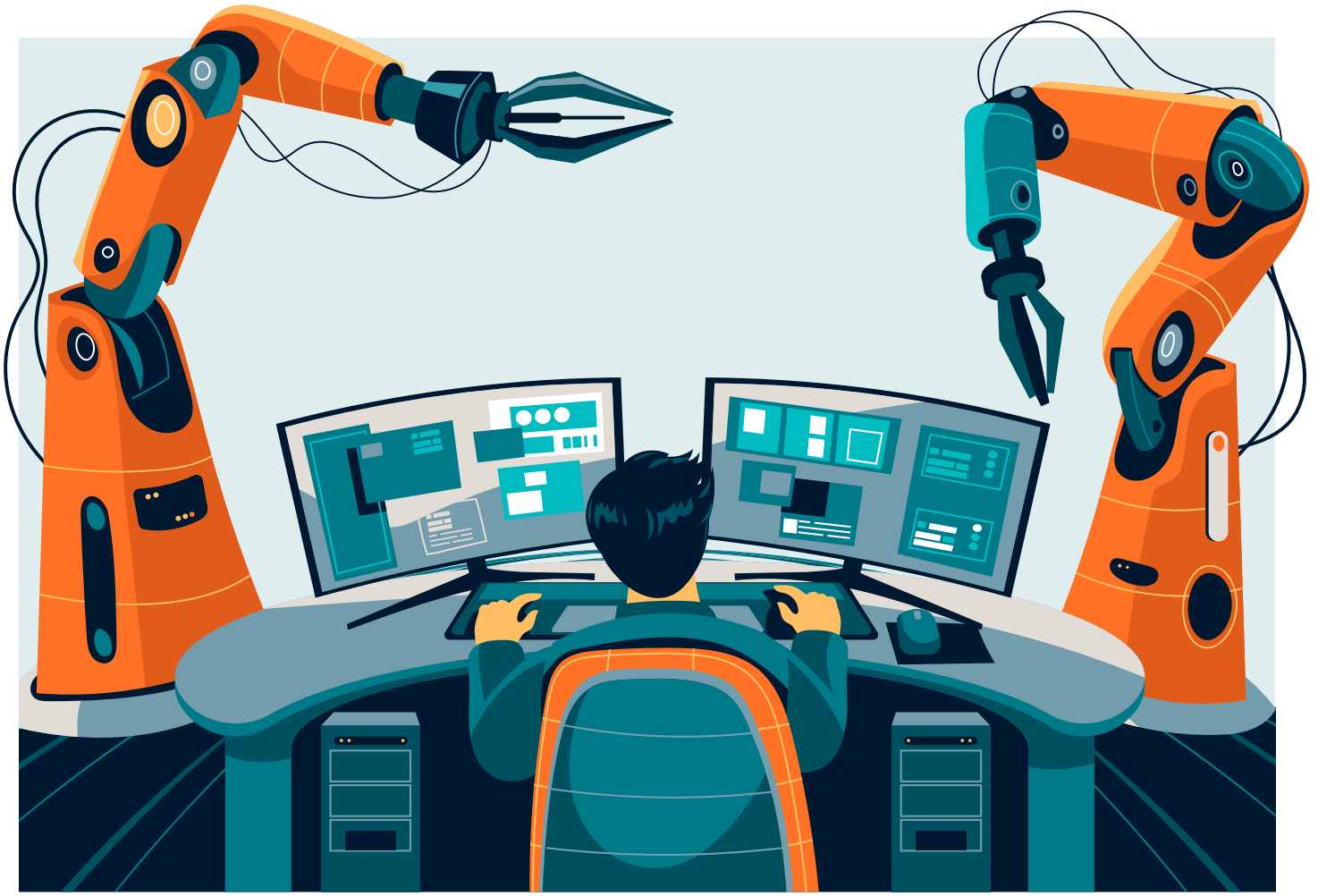
Поэтому в настоящее время в нашей стране активно идёт перевод и творческая переработка стандартов O-PAS, созданы проекты предварительных национальных стандартов. И не обязательно эти стандарты должны носить характер ГОСТов, держателями этих стандартов могут стать такие отраслевые организации, как ИНТИ (Институт нефтегазовых технологических инициатив).

О КЛЮЧЕВЫХ ПРИНЦИПАХ

— Речь идёт о создании принципиально новой архитектуры. И какие принципы положены в её основу?

— В основу архитектуры ОАСУ ТП заложены принципы открытости, совместимости, интероперабельности. Мы в своей работе выделяем целый ряд атрибутов открытости АСУ ТП:

- интероперабельность — переносимость информации между компонентами системы;



◆ модульность: любой кусочек РСУ (модуль) можно заменить модулем любого другого производителя. Это полезно, в частности, для повышения надёжности системы: очень легко заменить модуль, вышедший из строя;

◆ масштабируемость: систему автоматизированного управления можно наращивать с помощью модулей от уровня одного агрегата до уровня АСУ ТП цеха или целого предприятия. и др.

ОСОБЕННОСТИ АРХИТЕКТУРЫ ОАСУ ТП

— За счёт чего достигается интероперабельность компонентов АСУ ТП?

— Интероперабельность компонентов открытой АСУ ТП, основанной на стандарте OPA-S (Open Process Automation Standard), достигается благодаря использованию открытых стандартов, унифицированных интерфейсов и современных технологий, которые обеспечивают бесшовную интеграцию различных устройств и систем в рамках единой инфраструктуры. Архитектура этой системы строится вокруг нескольких ключевых элементов, каждый из которых выполняет свою роль в обеспечении совместимости и взаимодействия всех компонентов.

Одним из основных элементов архитектуры является OCF (Open Communications Framework) — коммуникационный фреймворк, который обеспечивает стандартный обмен данными между всеми компонентами системы. OCF позволяет использовать широко распространенные промышленные протоколы, такие как OPC UA и MQTT, а также Ethernet TSN, что делает систему гибкой и совместимой с различными устройствами и программным обеспечением от разных производителей. Благодаря интеграции протоколов для обмена данными в реальном времени, таких как Ethernet TSN (Time-Sensitive Networking), OCF обеспечивает высокоскоростную и точную передачу данных между компонентами системы. Это позволяет гарантировать синхронизацию и эффективное взаимодействие всех узлов в реальном времени, что критически важно для задач промышленной автоматизации. За счет поддержки открытых стандартов и протоколов, таких как OPC UA, комму-

никационный фреймворк предоставляет возможность легко интегрировать устройства, независимо от их производителя, обеспечивая необходимую совместимость и безопасность передачи данных. При этом OCF включает механизмы шифрования и аутентификации, что также повышает уровень кибербезопасности.

Другим важным компонентом является DCN (Distributed Control Node) — узел управления, который реализует распределенную модель управления технологическими процессами. Каждый DCN управляет локальными процессами, получая данные от сенсоров и исполнительных механизмов, обрабатывает их и передает управляющие сигналы на устройства. Эти узлы могут работать автономно, даже в случае потери связи с центральной системой, что гарантирует бесперебойную работу всей системы. Важно отметить, что DCN могут быть разного исполнения: они могут быть как аппаратными, так и программными. Аппаратные DCN представляют собой специализированные устройства, которые обеспечивают высокую производительность и надежность при выполнении задач управления. Они могут включать в себя вычислительные ресурсы и интерфейсы связи, оптимизированные для специфических задач. В свою очередь, программные DCN — это виртуализированные узлы управления, которые могут работать на стандартных серверных платформах, используя вычислительные ресурсы более общего назначения. Программные DCN обладают большей гибкостью и позволяют легко масштабировать систему, адаптируя её под изменяющиеся условия работы. Коммуникация между DCN осуществляется через OCF, что гарантирует стандартизированный обмен данными и бесшовную интеграцию узлов управления в общую систему. Все DCN взаимодействуют между собой, а также с другими элементами системы, такими как ACP, с использованием тех же открытых протоколов и механизмов, что и другие компоненты системы, обеспечивая необходимую совместимость и безопасность передачи данных.

ACP (Advanced Computing Platform) — серверная платформа, которая является центральным вычислительным узлом в системе. ACP отвечает за обработку данных, координацию работы всех узлов управления и интеграцию с внешними информационными системами, такими как ERP или MES. Благодаря использованию контейнеризации и виртуализации, ACP обеспечивает гибкость и масштабируемость всей системы. Это также способствует улучшению интероперабельности, так как различные компоненты системы могут работать в независимых контейнерах, а их взаимодействие происходит через стандартизированные интерфейсы. ACP также включает мощные аналитические и прогнозирующие возможности, используя искусственный интеллект и машинное обучение для обработки больших данных, что улучшает управление технологическими процессами.

Для того чтобы вся система функционировала как единое целое, необходим оркестратор, который управляет всей инфраструктурой и конфигурирует ландшафт системы. Оркестратор автоматизирует процессы развертывания, настройки и обновления всех компонентов, включая DCN, ACP и другие устройства. Он координирует работу всех элементов, настраивает их взаимодействие и следит за состоянием системы в реальном времени. Таким образом, благодаря использованию открытых стандартов, унифицированных интерфейсов и оркестрации, компоненты системы АСУ ТП на базе OPA-S могут легко взаимодействовать друг с другом, обеспечивая необходимую интероперабельность.

Открытость архитектуры, поддержка стандартных протоколов и механизмов кибербезопасности позволяют строить высокоэффективные и надежные системы управления, которые могут интегрировать устройства и решения от различных производителей, создавая гибкие, масштабируемые и безопасные решения для промышленной автоматизации.

ОАСУ ТП И РАЗНЫЕ ТИПЫ ПРОИЗВОДСТВ

— Важная особенность промышленности — различные типы производств: непрерывные, дискретные, гибридные. Как эта особенность сказывается на подходах к реализации ОАСУ ТП на предприятиях?

— В мире интерес к разработке открытых стандартов начинался в отраслях с непрерывными типами производства — нефтегазовой, химической... Это происходило потому, что именно там сразу становятся заметны преимущества и экономические эффекты, которые даёт переход на принципы открытой архитектуры: как с точки зрения стоимости на всех этапах жизненного цикла, так и с точки зрения более эффективного управления сквозными информацион-

ными потоками. Но, возвращаясь к нашей уникальной ситуации, импортозамещение требуется всем предприятиям со всеми типами производств. И тут именно ОАСУ ТП помогает справиться со всеми «снежными комами» вопросов, возникающими при замене западных ПЛК в поле: совместимость протоколов, взаимозаменяемость устройств и т.д. Так что процессы перехода к системам с открытой архитектурой АСУ ТП, которые на Западе в гибридных и дискретных производствах пока идут не так активно, у нас могут пойти гораздо активнее.

ОСОБЕННОСТИ ИБ

— Какие специфические черты информационной безопасности обусловливает переход на открытую платформу АСУ ТП?

— С возрастанием роли информационных технологий на производстве, взаимопроникновением мира OT и IT, риски, связанные с кибербезопасностью, существенно возрастают. Не секрет, что наша страна сегодня — одна из самых атакуемых стран в мире. Традиционно, вопросы информационной безопасности решаются за счет наложенных и встроенных средств безопасности, а также — за счет максимальной изоляции систем предприятия от внешнего мира. При этом, концепция открытой АСУ ТП ориентирована на доступность технологических данных за счёт применения открытых протоколов. Понятно, что ситуация требует применения средств информационной безопасности. Но более важно то, что принципы информационной безопасности должны изначально закладываться в саму архитектуру решений. Принцип Security by design должен быть свойствен решениям, создаваемым в рамках экосистемы открытой АСУ ТП.

У нас есть Техническая рабочая группа, которая занимаются формированием требований к информационной безопасности компонентов ОАСУ ТП, описанием типовых угроз и др. В рамках этой группы мы активно сотрудничаем с ведущими российскими вендорами: Positive Technologies, «Лаборатория Касперского» и т.д. Они, в частности, занимаются разработкой концепции безопасности открытых систем и средств защиты именно для открытой архитектуры. То есть идёт согласованное движение: создаётся решение открытой АСУ ТП, а специалисты по безопасности планируют меры защиты.

Одной из идей, которые прорабатываются в группе, является идея создания конвейера проверки решений открытой АСУ ТП на информационные уязвимости — отраслевого Bug Bounty.

Надо отметить, что на данном этапе мы видим ограничения применимости открытой АСУ ТП. Стандарты O-PAS не претендуют на то, чтобы охватить абсолютно всё производство, включая устройства противоаварийной защиты (ПАЗы), где действуют максимально жёсткие требования к функциональной безопасности. Мы не предлагаем в обозримом будущем перевести ПАЗы на открытую архитектуру. Развитие открытой АСУ ТП должно идти поступательно: от отдельных опытных установок — на уровень предприятия и распределённых систем управления, и параллельно эти решения будут взрослеть с точки зрения безопасности.

РЕПОЗИТОРИЙ

— Если подразумевается универсальность платформы по отношению к отраслевым практикам автоматизации, значит, следует говорить о некоторой библиотеке стандартных программных модулей, базовых элементов автоматизации?

— Естественно, при таком подходе напрашивается некий репозиторий или доверенная витрина, где хранятся библиотеки готовых модулей, совместимых, с подтверждённым качеством разработки и опытом использования, сведениями о совместимых продуктах и т.д. Это отдельный большой круг вопросов, которыми также в настоящее время занимается наша рабочая группа. Скажу больше: не просто занимается, а идут горячие дискуссии о том, как наилучшим образом подойти к решению этих задач: хранению информации, организации библиотек, алгоритмов и т.д. Кто держатель этого репозитория? Кто будет сопровождать его функционирование?

Как организовать весь процесс, чтобы помочь и крупным, и мелким производителям выйти на рынок? Чтобы всем им было интересно работать в этом секторе, а инновационные новинки продвигались, несмотря на малый объём внедрений. Вопросов очень много, и все они — предмет активных дискуссий.

— Не слишком ли много задач для одной рабочей группы?

— Действительно, приходится действовать по принципу «всё и сразу». Но по-другому нельзя. Ситуация сейчас такая — уникальная: у нас нет времени решать отдельные задачи последовательно, мы вынуждены одновременно бежать во все стороны. И это, возможно, даёт нам уникальный шанс — выполнить

амбициозную задачу по созданию экосистемы работоспособных решений ОАСУ ТП. Но внутри каждого направления мы действуем последовательно. Например, в ближайшее время мы собираемся запустить прототип доверенной витрины решений для экосистемы открытой АСУ ТП. Со временем эта витрина, где изначально будет располагаться только информация о решениях, должна превратится в репозиторий, где будут реализованы правила проверки библиотек и готовых решений на предмет соответствия стандартам и требованиям ОАСУ ТП, а также требованиям ИБ..

«ЛОСКУТНАЯ АВТОМАТИЗАЦИЯ»

— Если смотреть на современные цифровые системы в промышленности, возникает ощущение «лоскутной автоматизации»: в них на разных уровнях и участках производства используются различные системы управления, в том числе интеллектуальные. Единый архитектурный подход ОАСУ ТП поможет справиться с этой «лоскутностью»?

— Несомненно! Идея открытой архитектуры АСУ ТП — это ответ на современный вызов: различные умные системы, например APC (Advanced Process Control), в российской терминологии — СУУ ТП (Система усовершенствованного управления технологическим процессом), системы RTO (Real-Time Optimization, оптимизация в режиме реального времени), вынуждены реализовываться как наложенные информационные системы. Они вынужденно находятся не внутри АСУ ТП, а где-то рядом, и при этом происходит дублирование процессов, возникает много проблем с передачей данных, и в целом это очень неудобно в управлении. В чём причина такого положения дел?

Нынешние системы — закрытые, проприетарные решения — нацелены на решение конкретной задачи, с которой они прекрасно справляются. И это очень важно для заказчика — там реализована именно та функциональность, которая даёт возможность легко и удобно эксплуатировать внедрённую систему управления технологическими процессами определённого типа. Но как только возникает задача изменения технологического процесса, развития, внедрения инноваций в управление, скажем, цифровых двойников, тут начинаются проблемы

с адаптацией таких решений под действующую систему АСУ ТП, реализацией функцией конфигурирования, настройкой решений и т.д. А вот идея открытой АСУ ТП как раз подразумевает возможность запуска любых новых инновационных решений на уровне АСР — это заложено в архитектуре изначально. В самой архитектуре описано, как запустить своё приложение в среде ОАСУ ТП и каким требованиям для этого должно соответствовать приложение. А значит, вендору смежных решений не придётся ломать голову над обеспечением их совместимости: можно использовать готовые решения, поддерживающие стандарты ОАСУТП, и постепенно наращивать объём внедряемых умных систем управления по всей цепочке производства. Открытая архитектура АСУ ТП это всё обеспечивает. И тогда тот самый небольшой разработчик решений, которых у нас должно быть очень много (спрос сейчас многократно превышает предложение), сможет сфокусировать свои усилия на том, что он умеет делать лучше всего: проектировать «железо» или писать функциональный софт, а остальные компоненты готового решения можно взять у других производителей, и они будут совместимы между собой.

О СТИРАНИИ ГРАНИЦ

— Получается, что все вопросы управления в автоматизированных промышленных системах в конце концов сходятся к управлению данными?

— Вы видите, как на практике происходит тот самый сдвиг парадигмы промышленной автоматизации, о котором я говорил выше: функции, которые ранее выносились за пределы АСУ ТП, теперь втягиваются в её периметр: микросервисная архитектура, сервисы Advanced Process Control, Real Time Optimization и т.д. становятся частью экосистемы АСУ ТП. Даже часть классических функций MES уходит туда. Мы видим, что на наших глазах происходит смешивание двух больших областей: ИТ и промышленной автоматизации, которые ранее развивались независимо друг от друга. И это даёт более эффективное использование принципов управления технологическими процессами. При этом не стоит сводить открытую АСУ ТП к платформе. С функциональной точки зрения ОАСУ ТП — это не платформа, а экосистема, который помогает создавать комплексные системы управления технологическими процессами на основе открытой архитектуры. Эта экосистема имеет несколько уровней: стандарты, витрина, репозиторий, система сертификации (кто-то должен определять, действительно ли данное решение соответствует открытой архитектуре ОАСУ ТП), тестовые лаборатории и др. Отдельные платформы и решения — это, скорее, прерогатива проектировщиков, вендоров и интеграторов.

КАК ОАСУТП ИЗМЕНИТ РЫНОК

— Их деятельность, думается, претерпит существенные изменения с появлением на рынке экосистемы ОАСУ ТП?

— Вообще, очень интересно, что будет происходить на рынке, потому что в новых условиях ОАСУ ТП принципиально меняется роль интеграторов и вендоров. По факту создаётся новая рыночная реальность.

— Насколько рынок готов принять эту новую реальность?

— Это ещё один интересный вопрос в списке тех, что мы сегодня обсуждаем. Вопрос в том, как убедить бизнес-заказчиков в целесообразности перехода на открытую архитектуру? Требования государства, хоть и представляют собой мощный аргумент, всё-таки не являются главным стимулом. Самое важное в практическом применении ОАСУ ТП — то, что даже на отдельных участках производства, не говоря о внедрении всей совокупности этих решений, стоимость владения снижается на существенное количество процентов. Обращаю ваше внимание: даже на отдельных участках внедрения отдельных решений, связанных с открытой архитектурой, удаётся добиться понятных и вполне просчитываемых экономических эффектов. Именно поэтому она в итоге и победит. Хочется еще отметить, что открытой является не только архитектура АСУ ТП, но и наша рабочая группа. Мы очень заинтересованы в интеллектуальных ресурсах, которые готовы включиться прямо сегодня в создание этой новой реальности и новой экосистемы. Приглашаем к диалогу всех. Приглашаем промышленные компании поработать вместе над техническими требованиями к решению ОАСУ ТП, принять участие в тестировании и создавать у себя первые промышленные установки, основанные на открытой архитектуре. Приглашаем вендоров, которым предстоит воплощать идеи ОАСУ ТП в «железе» и софте. Приглашаем интеграторов, ведь им предстоит играть центральную роль на этом формирующемся рынке. Предлагаем им тесное взаимодействие для того, чтобы контуры этого рынка начали практически оформляться.

Вопросы задавала Елена Покатаева, обозреватель BIS Journal

«РБПО — не для ФСТЭКа. РБПО — для безопасности и качества вашего ПО».
Представитель ФСТЭК России

РБПО-2024. ИТОГИ И ПЕРСПЕКТИВЫ

АКТУАЛЬНОСТЬ ТЕМАТИКИ РБПО

Дмитрий ПОНОМАРЁВ
заместитель генерального директора — директор департамента внедрения и развития практик РБПО ООО НТЦ «Фобос-НТ», сотрудник ИСП РАН, преподаватель МГТУ им. Н. Э. Баумана

Если задаться целью проанализировать, какие именно слова были наиболее популярными в 2024 году в области, связанной с разработкой и поддержкой программ и систем, акроним РБПО с высокой вероятностью займёт лидирующую позицию[1]. Бесспорно, никуда не делся, хотя и несколько снизил темпы маркетинговой экспансии «искусственный интеллект». Резкий всплеск внимания к термину NGFW — все стремятся «застолбить поляну», правила работы на которой ещё толком не определены. Всё больше внимания обращается на микросервисные программные решения: «облака», сервисы банков и маркетплейсов и даже средства защиты информации — в контейнерном исполнении, в том числе функционирующие в кластерах под управлением kubernetes.

Но все эти понятия и слова в итоге подразумевают под собой определённые типы и особенности эксплуатации ПО. А где ПО — там и необходимость его создания и поддержки. Качественно, безопасно, управляемо и, что немаловажно, в соответствии с парадигмой действующей и перспективной регуляторики. «Комплаенс» — мощнейший стимул становиться лучше, особенно в современных условиях стратегической турбулентности и уже никому не требующих доказательства фактов непрестанных атак на отечественную IT-инфраструктуру. При этом необходимо отметить: несмотря на все сложности последних лет, мы не находимся в уникальной ситуации. Рост рынка киберпреступности в мире оценивается в «триллионы рублей в год»[2], степень информатизации становится всё выше, а атаки — всё изощреннее.

Реакцией на давление киберпреступности — как «частной», так и инициируемой на уровне недружественных государств (не все APT-группировки только лишь «про деньги») — является рост системности и проработанности различных требований в области информационной безопасности и, как следствие, рост технологий, инструментов и методик РБПО, а также вовлечённого в эти процессы сообщества инженеров, экспертов, чиновников и руководителей. Все эти факторы приводят к трансформации отечественных рынков ИБ и ИТ в целом. Парадигма «Внедрённые процессы РБПО — показатель зрелости компании и бизнес-преимущество XXI века» становится всё более распространённой, а в ряде сегментов — безальтернативной. Развиваются имеющиеся и возникают новые классы инструментов анализа. Пресса и профильные конференции пестрят анонсами о важности РБПО и предложениями продуктов и услуг. Безотносительно к тому, написаны они заинтересованными специалистами-инженерами или «ванильными маркетологами» с целью набить цену собственной компании, информационный поток становится всё более значимым, и из «темы для избранных» вопросы РПБО за единицы лет стали настоящим мейнстримом.

Эта статья пополнит копилку материалов «по теме» и, надеемся, окажется полезной читателям. В ней я постарался осветить некоторые типовые вопросы, возникающие у разработчиков — лицензиатов ФСТЭК России — при внедрении инструментов и развитии практик РБПО и последующем выводе собственных решений на сертификацию. Материал можно рассматривать в качестве логического продолжения опубликованной в 2024 г. статьи «6 мифов о безопасной разработке и сертификации ПО»[3].

[1] Во время написания статьи вышел материал (https://habr.com/ru/news/860268/), не подтверждающий данную гипотезу для сферы ИТ в целом. Тем не менее автор оставляет за собой право считать утверждение верным в отношении компаний-лицензиатов отечественных регуляторов.

[2] https://www.statista.com/hart/28878/expected-cost-of-cybercrime-until-2027/

[3] https://cs.groteck.com/IB_2_2024/60/

ТИПОВЫЕ «ПРОБЛЕМЫ» ЗАЯВИТЕЛЯ

Примерно с 2020 года развитие отрасли создания средств защиты информации можно охарактеризовать в том числе следующими тезисами:

- растёт число лицензиатов ФСТЭК, равно как и число заявителей на сертификацию СЗИ;
- растёт число малых команд, приходящих на сертификацию с одним небольшим продуктом и имеющих околонулевой опыт в сертификации; при этом многие команды ничего не слышали о требованиях РБПО и считают, что сертификация — это «что-то записанное в контракт по остаточному принципу, сделаем за 3–6 месяцев, не напрягаясь»;
- всё больший процент кодовой базы СЗИ составляют компоненты с открытым исходным кодом; у некоторых решений он достигает 100%, а на долю разработчика остаются компоновка, конфигурирование, маркетинг и поддержка;
- всё большую долю кодовой базы составляют интерпретируемые языки программирования / языки с «управляемой памятью» (Python, JS, C#, Java и т.д.);
- более половины приходящих на сертификацию продуктов составляют «СЗИ в контейнерном исполнении[4]», выполняющиеся в контексте средств контейнеризации (в том числе оркестратора kubernetes).

Наряду с иными веяниями времени вышеуказанное приводит к типовым «проблемам», возникающим у разработчиков, впервые оказывающихся в гостях у въедливой испытательной лаборатории:

- разработчик не умеет собирать своё решение из исходников, использует бинарные пресобранные компоненты из произвольных источников; нарушение базового принципа «весь код СЗИ === ваш код»;
- не ведётся контроль наличия уязвимых версий компонентов либо ведётся по остаточному принципу, поскольку: «их так много, мы же всё не поправим», «да оно не эксплуатируемо», «да наше ПО будет применяться только в доверенном контуре, никаких внутренних врагов нет»;
- у разработчика СЗИ в контейнерном исполнении, а значит: «у нас всё в контейнерах, значит, всё безопасно и вообще, упадёт — переподнимем», «что это вы такое придумали — контейнеры самому собирать и анализировать код компонентов... Это же Alpine с DockerHub, там всё отлично и безопасно»;
- разработчики СЗИ относятся к пакетной базе репозиториев отечественных сертифицированных ОС (~50 000 пакетов) так же, как к самому сертифицированному дистрибутиву (~300 пакетов): «разработчик ОС сказал, что в репе тоже всё доверенное, берите, чего в дистрибутиве не хватает».

Ещё одной типовой проблемой организации и контроля процессов РБПО является «разнобой» в используемых инструментах анализа, в том числе между разработчиками СЗИ и испытательными лабораториями. Часть разработчиков клюёт на активность маркетологов и приобретает за большие деньги «самый раскрученный», но не самый качественный инструмент, часть — принципиально экономит на платных инструментах, используя открытые, безотносительно к качеству их работы, зачастую только ради формального выполнения требования о проведении соответствующего вида анализа. Наиболее жаркие «дискуссии» в отрасли традиционно идут вокруг средств поиска известных уязвимостей и ошибок конфигурирования компонентов системы. Второе же место, бесспорно, принадлежит проблематике выбора инструментов статического анализа исходного кода. Данная практика анализа является широко распространённой и одной из базовых при построении процессов РБПО. Неслучайно требования ФСТЭК России к процессу статического анализа в части методики проведения сертификационных испытаний, равно как и в части комплектования испытательных лабораторий инструментами анализа, являются одними из наиболее проработанных.

Вышеуказанные факторы в совокупности с существенной разницей в компетенциях испытательных лабораторий, а также отсутствием прямых и конкретных разъяснений в нормативно-правовой базе по каждому возможному подвопросу (парадигма «писать рамочные требования — рассчитывать на сознательность и заинтересованность разработчика в безопасности и качестве», к сожалению, работает далеко не всегда) приводят к частому непониманию разработчиками СЗИ, «что именно, как и на какую глубину» требуется выполнить. Что, в свою очередь, порождает риски неопределённости для бизнеса, зависящие во многом от позиции конкретных экспертов, их персональных трактовок требований регулятора.

АКТУАЛИЗАЦИЯ РЕГУЛЯТОРИКИ И СООБЩЕСТВО РБПО

Ответом на вызовы времени явилось активное развитие в 2024 году нормативно-правовой базы ФСТЭК России. Ниже кратко описаны наиболее значимые изменения и сопровождавшие их события.

1. Информационным письмом «О порядке испытаний и поддержки безопасности средств защиты информации» изменён порядок исследования критичных компонентов с открытым исходным кодом при подготовке и проведении испытаний. При подаче заявки на сертификационные испытания заявители должны предоставить Перечень Программных Компонентов (ППК aka SBoM) в составе СЗИ и далее осуществлять их поддержку безопасности. Глубина и качество анализа компонентов, равно как и распределение нагрузки по анализу компонентов между разработчиками, определяются в рамках консорциума Центра исследований безопасности системного ПО ФСТЭК России и ИСП РАН[5].

2. Информационным письмом (от 25.10.2024)[6] уточнён порядок анализа компонентов, реализую-

[4] https://clck.ru/3GAsaP

[5] https://portal.linuxtesting.ru/index.html#regulations

[6] https://clck.ru/3GAsim

щих функции серверов приложений, веб-серверов и интерпретаторов. Функции безопасности данных компонентов должны быть корректно заявлены в формулярах СЗИ и проверены в ходе испытаний, при этом разработчик СЗИ должен сформулировать рекомендации по безопасной настройке указанных компонентов, а также минимизировать поверхность атаки на компонент посредством удаления из комплекта поставки функциональных возможностей, не предполагаемых к использованию. В первую очередь данные требования затрагивают разработчиков ОС, традиционно включающих в составы своих дистрибутивов значительное число таких компонентов[7].

3. На ноябрьских сборах ФСТЭК России с разработчиками СЗИ, испытательными лабораториями и органами по сертификации значимый акцент сделан на том, что компоненты СЗИ, упакованные в контейнеры различных форматов, в полной мере подлежат соответствующим уровню доверия проверкам в случае вхождения в состав поверхности атаки / реализации ими функций безопасности. Контейнеры должны формироваться из доверенной компонентной базы либо в полном объёме компоноваться разработчиком самостоятельно, с полной ответственностью за безопасность исходного и исполняемого кода.

4. В ноябре ФСТЭК России запустила программу аттестации экспертов испытательных лабораторий. Типовые задания аттестации предполагают не только знание нормативно-правовой базы регулятора, но и — в первую очередь — проверку навыков эксперта в выполнении различных видов статического и динамического анализа. Основной упор в процессе аттестации делается именно на выполнение практических заданий, что лишний раз подчёркивает факт отхода регулятором от примата вопросов «бумажной безопасности» к верховенству вопросов практического РБПО.

5. Принятый в 2024 году ГОСТ Р 71207–2024 (статический анализ программного обеспечения)[8] фактически явился первым из целого семейства ГОСТ в области РБПО, запланированных к принятию в 2024–2026 годах. Одной из задач данного ГОСТа является регламентация процесса оценки качества инструмента статического анализа. Анонс испытаний отечественных статических анализаторов был сделан заместителем начальника 2 управления ФСТЭК России И.С.Гефнер[9] в ходе Открытой конференции ИСП РАН 11 декабря[10]. В настоящий момент осуществляется формирование жюри испытаний, комплекта тестов. К участию в испытаниях приглашаются все отечественные компании — разработчики статических анализаторов, а также заинтересованные участники сообщества. В качестве инфраструктурной основы организации тестирования предполагается использование наработок, полученных в рамках создания Унифицированной среды безопасной разработки ПО[11].

6. Сообщество РБПО центра компетенций ФСТЭК России и ИСП РАН[12] активно развивается и прирастает новыми участниками. Целями сообщества являются:

- популяризация системного, фундаментально-инженерного подхода к организации безопасной и качественной разработки и подготовке кадров;
- популяризация отечественных технологий и школ, в том числе в части лучших практик и регуляторики; поддержка и продвижение отечественной «культуры»;
- формирование «грибницы» доверенных, кросс-верифицированных горизонтальных связей. Ядро сообщества составляют «технари» (бизнесмены, инженеры, чиновники). В сообществе не приветствуется «*маркетологическая маркетология*».

Крупнейшая ежегодная встреча участников сообщества состоялась на полях уже упомянутой выше Открытой конференции ФСТЭК России и ИСП РАН.

Основные информационные ресурсы сообщества в «Телеграме», посвящённые вопросам инструментального анализа, объединения усилий по анализу разделяемой компонентной базы, организации просветительских мероприятий, превысили число в 1500 участников. Узнать подробности про семейство чатов сообщества вы можете, перейдя по приведённому QR-коду или по ссылке[13]:

ПОДВОДЯ ИТОГ

2024-й выдался чрезвычайно насыщенным на различные события в области ИТ, ИБ и регуляторики. «За скобками» статьи остались такие важнейшие для отрасли вопросы, как, например, сертификация процессов РБПО на соответствие обновлённому ГОСТ Р 56939–2024 или публикация проекта обновлений 17-го приказа и многие другие. Реальное влияние анонсированных и принятых решений в полной мере отрасль ощутит в 2025–2026 годах. Со своей стороны традиционно могу пожелать читателям всех рангов как можно скорее осознать безальтернативность парадигмы безопасной и качественной разработки ПО в современных реалиях, трансформации отечественной регуляторики в технологичный и полезный инженеру свод рекомендаций и требований, а также тезис о том, что «внедрённые процессы безопасной и качественной разработки — гарантия эффективного прохождения сертификационных испытаний и конкурентное преимущество XXI века»!

[7] https://clck.ru/3GAsaP

[8] https://protect.gost.ru/document1.aspx?control=31&baseC=6&page=3&month=2&year=2024&search=&id=257752

[9] https://t.me/sdl_community/7343

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

[11] https://www.tbforum.ru/hubfs/Digital/SS/SS_ADAPT/TBF24_14-02-24_Падарян.pdf

[12] https://cs.groteck.com/IB_3_2023/40/

[13] https://t.me/sdl_community

ЗАКОНОДАТЕЛЬНЫЕ ИНИЦИАТИВЫ В ОБЛАСТИ РБПО

ТРЕНДЫ И ПРАКТИКА. ОБЗОР

Альбина АСКЕРОВА
руководитель направления взаимодействия с регуляторами Swordfish Security

ВВЕДЕНИЕ: ЧТО ЕСТЬ В ОБЛАСТИ РЕГУЛИРОВАНИЯ РБПО

Практика РБПО давно вышла за рамки традиционного DevOps с интегрированной безопасностью. Сегодня это уже полноценная идеология, в которой безопасность выступает как правило хорошего тона, часть этикета и гигиены.

В эволюционном развитии такого подхода всё происходит по классическим законам экономики: спрос рождает предложение. Если ранее большинство экспертов фокусировались на анализе кода, то сейчас мировоззрение меняется, и в поле зрения попадают и те аспкеты, которые требуют проведения ИБ-проверок — от проектирования архитектуры и бизнес-логики до харденинга инфраструктуры и анализа цепочки поставок ПО. Может ли система изначально быть идеальной, или жизненные циклы создания ПО таковы, что хороший результат можно достичь только при комплексном применении всех практик безопасной разработки?

С таким широким запросом на спектр практик мы обращаемся к регуляторике и изучаем, что уже существует в этой области. Порой эксперты не замечают требования, если напрямую не указано: «Чтобы построить РБПО — делай раз, два, три». А по сути, если знать, из чего состоит РБПО и в каких документах оно описано, то можно найти множество регуляторных требований и рекомендаций о том, как правильно выстраивать процессы.

Итак, посмотрим.

Наши основные регуляторы в данном вопросе — ФСТЭК России и Банк России. Есть ещё отраслевые требования, но они, как правило, издаются как ответвление к основным, например, требования Минцифры России к госсистемам, размещаемым на ЕЦП «ГосТех», или требования Минэнерго к объектам электроэнергетики.

Помимо регуляторных, есть требования, утверждаемые президентом, — федеральные законы, указы.

Также существуют документы общего рекомендательного характера — ГОСТы (они являются рекомендательными до момента, пока о необходимости их исполнения не будет сказано в обязательных к исполнению документах).

Кроме «источника» нормативного документа, регулирование можно также классифицировать по отраслям. Обычно специалисты по ИБ именно так и формулируют свой запрос, так как решают задачу по защите объектов в конкретной сфере экономики.

Можно выделить несколько ключевых направлений регулирования: для финтеха (кредитные и некредитные организации и ряд других организационно-правовых форм в финансовой сфере), для объектов КИИ (критической информационной инфраструктуры), для ГИС (государственных информационных систем), для информационных систем обработки ПДн (персональных данных).

Важно отметить, что одна сфера регулирования не исключает другую и при выборе набора требований необходимо знать всё об объекте — его бизнес-задачи, обрабатываемые данные и их объём, нюансы взаимодействия с внешними системами и многие другие аспекты. Может получиться так, что в отношении объекта нужно принимать меры защиты и для финтеха, и для КИИ, и для ПДн, и для ГИС.

Иногда компании планируют сертифицировать свои программные продукты во ФСТЭК России, и этот процесс предполагает проверку внедрения процедур безопасной разработки ПО.

Также важна информация о том, где будут размещаться вычислительные ресурсы. Если объект будет работать на платформе ГосТех, то для ГИС необходимо будет соблюдать не только требования ФСТЭК России, но и Минцифры РФ.

Таким образом, для специалистов по безопасности нет единого универсального набора регуляторных требований — это всегда набор, формирующийся из особенностей защищаемого объекта.

Из описанного выше можно предложить некоторый алгоритм выбора требований из всего множества:

1. Является ли защищаемый объект КИИ и/или ГИС, и/или ИСПДн, и/или финтех?
2. Если несколько «да», то важно изучить и учесть особенности регулирования для каждого. Например, если программный продукт является объектом КИИ, это не всегда говорит о том, что он значимый. Также,

если приложение обрабатывает ПДн, нет необходимости без разбора выполнять все требования в полном объёме. В каждой отрасли есть свои «уровни безопасности», назовём таким общим термином разные наборы требований.

3. Если ГИС, то планируется ли размещать её на платформе ГосТех?

4. Если значимый объект относится к КИИ — это электроэнергетика или, может, АСУ ТП?

5. Есть ли задача по сертификации продуктов во ФСТЭК России?

6. Если финтех, то кредитная или некредитная организация? Или, может, бюро кредитных историй?

ОСНОВНАЯ ЧАСТЬ: РЕТРОСПЕКТИВА — ЧТО БЫЛО И ЕСТЬ В НПА РБПО

Теперь рассмотрим конкретные упоминания РБПО в регуляторике.

Общие нормы, которые применимы или могут быть опционально применимы к любой отрасли:

- Указ Президента РФ от 18.06.2024 № 529 «Об утверждении приоритетных направлений научно-технологического развития и перечня важнейших наукоёмких технологий»
- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации
- ГОСТ Р 56939–2024 «Разработка безопасного программного обеспечения. Общие требования»
- ГОСТ Р 15408–3–2013 «Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий»
- ГОСТ Р 58412–2019 «Разработка безопасного программного обеспечения. Угрозы безопасности информации при разработке программного обеспечения»
- Приказ ФСТЭК России от 03.04.2018 № 55 «Об утверждении Положения о системе сертификации средств защиты информации»
- Приказ ФСТЭК России от 02.06.2020 № 76 «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий»

Нормы для субъектов критической информационной инфраструктуры (КИИ):

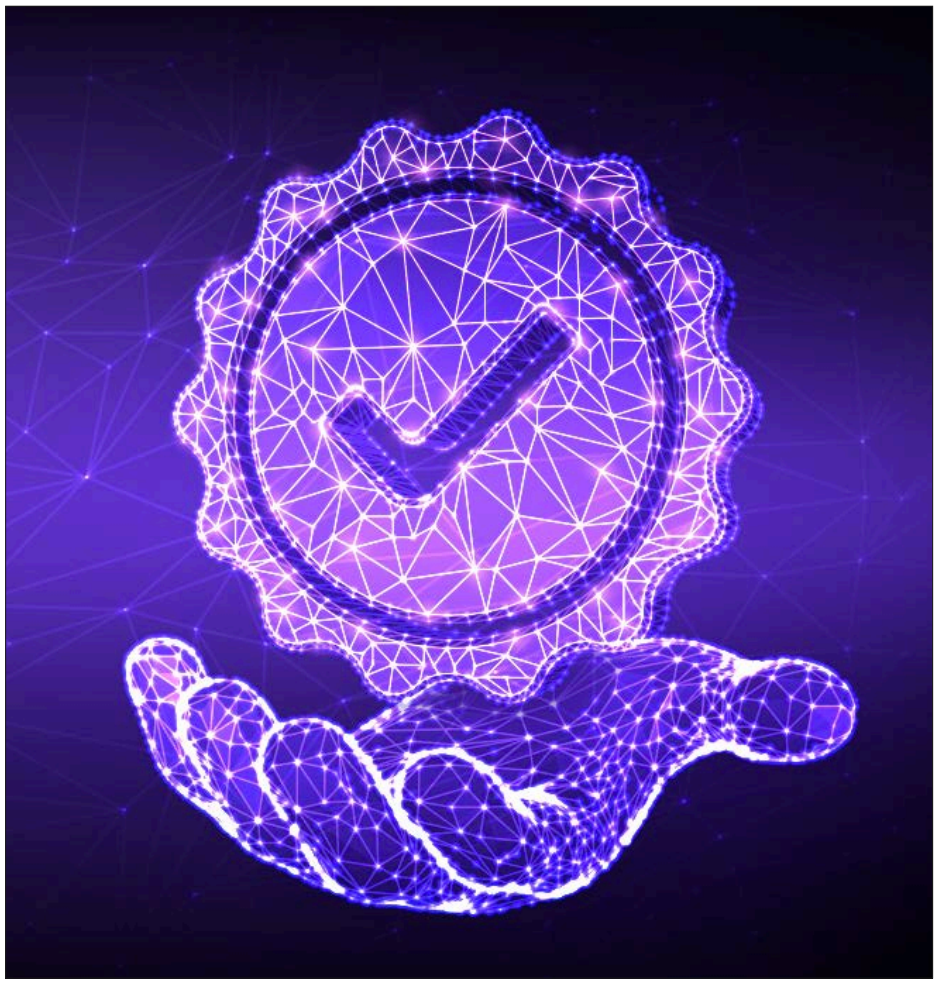
- Указ Президента РФ от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»
- Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»
- Приказ ФСТЭК России от 14.03.2014 № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»
- Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»

Нормы для систем обработки персональных данных:

- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»
- Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

Нормы для финтеха:

- ГОСТ Р 57580.1–2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер»
- Положение Банка России от 17.04.2019 № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента»
- Положение Банка России от 08.04.2020 № 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе»
- Положение Банка России от 20.04.2021 № 757-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций»
- Положение Банка России от 15.11.2021 № 779-П «Об установлении обязательных для некредитных финансовых организаций требований к операционной надёжности при осуществлении видов деятельности»
- Положение Банка России от 12.01.2022 № 787-П «Об обязательных для кредитных организаций требованиях к операционной надёжности при осуществлении банковской деятельности в целях обеспечения непрерывности оказания банковских услуг»
- Положение Банка России от 25.07.2022 № 802-П «О требованиях к защите информации в платёжной системе Банка России»
- Положение Банка России от 17.10.2022 № 808-П «О требованиях к обеспечению защиты информации при осуществлении деятельности в сфере оказания профессиональных услуг на финансовом рынке в целях противодействия осуществлению незаконных финансовых операций...»
- Положение Банка России от 03.08.2023 № 820-П «О платформе цифрового рубля»
- Положение Банка России от 17.08.2023 № 821-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств»
- Положение Банка России от 07.12.2023 № 833-П «О требованиях к обеспечению защиты информации



для участников платформы цифрового рубля»

◆ Методический документ Банка России от 2021 года «Профиль защиты прикладного программного обеспечения автоматизированных систем и приложений кредитных организаций и некредитных финансовых организаций»

◆ Стандарт Банка России СТО БР ФАПИ.СЕК-1.6-2024. Безопасность финансовых (банковских) операций. Прикладные программные интерфейсы обеспечения безопасности финансовых сервисов на основе протокола OpenID Connect

◆ Стандарт Банка России СТО БР ФАПИ.ПАОК-1.0-2024. Безопасность финансовых (банковских) операций. Прикладные программные интерфейсы. Обеспечение безопасности финансовых сервисов при инициации OpenID Connect клиентом потока аутентификации по отдельному каналу.

◆ Методические рекомендации Банка России от 30.09.2024 № 16-МР по организации взаимодействия информационных систем организаций финансового рынка с инфраструктурой, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме

◆ Методические рекомендации Банка России от 22.01.2025 № 2-МР по проведению тестирования на проникновение и анализа уязвимостей информационной безопасности объектов информационной инфраструктуры организаций финансового рынка

Предметные нормы для сферы энергетики:

◆ Приказ Минэнерго России от 26.12.2023 № 1215 «Об утверждении дополнительных требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры, функционирующих в сфере электроэнергетики, при организации и осуществлении дистанционного управления технологическими режимами работы и эксплуатационным состоянием объектов электроэнергетики из диспетчерских центров субъекта оперативно-диспетчерского управления в электроэнергетике»

Требования для государственных информационных систем:

◆ Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»

◆ Методические рекомендации по обеспечению безопасности при разработке программного обеспечения с использованием компонентов Единой цифровой платформы «ГосТех» (утверждено протоколом Президиума Правительственной комиссии от 08.12.2022 № 54)

◆ Концепция разработки безопасного ПО на платформе «ГосТех» (утверждено протоколом Президиума Правительственной комиссии от 04.05.2023 № 20)

ЧТО БУДЕТ МЕНЯТЬСЯ?

Указом от 18.06.2024 № 529 Президент России определил приоритетные направления научно-технологического развития и перечень важнейших наукоёмких технологий. «Безопасность получения, хранения, передачи и обработки информации» определена как приоритет научно-технологического развития, а в числе важнейших наукоёмких технологий мы видим «технологии создания доверенного и защищённого системного и прикладного программного обеспечения». Таким образом речь идёт о стратегическом направлении развития нашей страны, в котором РПБО занимает важное место.

Изменения происходят во всех сферах.

Произошедшее уже изменение — это пересмотр в полном объёме базо-

вого ГОСТ Р 56939–2024. Вместо 9 мер по разработке безопасного ПО, которые были с 2016 года, вводится 25 мер, которые в сумме содержат более 100 требований к процессу РБПО.

Среди нового перечня мер выделяются те, которые, как правило, требуют экспертных компетенций в области безопасной разработки: экспертиза и статистический анализ исходного кода, динамический анализ кода программы, использование безопасной системы сборки программного обеспечения, обеспечение безопасности используемых секретов, проверка кода на предмет внедрения вредоносного ПО через цепочки поставок и ряд других.

В развитие ГОСТ 56939-2024 сейчас ФСТЭК и экспертное сообщество ведут работу над разработкой ГОСТ по методике оценке уровня реализации процессов разработки безопасного ПО. Данным ГОСТ планируется зафиксировать подходы к оценке соответствия процессов ГОСТ 56939.

Еще в скором времени ФСТЭК планирует выпустить ГОСТ по композиционному анализу ПО, в котором будут описаны и процессы, и требования к инструментам, и требования по формированию перечня программным компонентов (перечень зависимостей, библиотек и других элементов, имеющих отношение к продукту).

В новой редакции ФСТЭК России планирует выпустить приказ от 11.02.2013 № 17 (проект изменений опубликован на сайте ФСТЭК России 08.08.2024) о защите информации в госсистемах. Положения о внедрении практик безопасной разработки добавлены в явном, акцентированном виде. В частности, не допускается использование ПО без проведения работ по экспертизе, тестированию и (или) исследованиям исходного кода, в том числе без проведения статического и динамического анализа кода программ, а также композиционного анализа программного обеспечения.

Также важно, что регулятор планирует утвердить эти требования не только для систем в статусе ГИС, но и в целом для всех объектов, которые эксплуатируют госорганизации.

Также и Банк России планирует пересмотреть положения № 821-П и № 757-П. Операторы по переводу денежных средств, банковские платёжные агенты (субагенты), некредитные финансовые организации получат право не проводить контроль каждой версии ПО, если они имеют «заключение проверяющей организации о том, что реализуемые процессы разработки программного обеспечения и приложений включают меры обеспечения безопасного жизненного цикла разработки программного обеспечения и приложений». То есть безопасная разработка позволит избежать контроля ПО (в том числе, если это объект КИИ, судя по действующим проектам новых редакций положений) — это достаточно революционный подход.

Такой же концептуально новый подход ФСТЭК России уже утвердила в 2023 году приказом № 240, в котором допускается вместо сертификации новых версий СрЗИ иметь сертифицированный процесс разработки этого СрЗИ.

Также, думаю, и с принятием закона «об оборотных штрафах» за утечки ПДн всё больше внимания будет уделяться безопасности ПО, обрабатывающего ПДн.

ТОП-3 КЛЮЧЕВЫХ ТРЕНДА

Какие тренды безопасной разработки в России можно выделить с учетом вектора развития регуляторики:

1. Импортозамещение и доверие. Open Source по-прежнему популярен, но в современных реалиях для критических сфер в российской экономике использовать его небезопасно (недавний прецедент с ядром Linux яркий тому пример) , и наблюдается тренд перехода на отечественные решения и инструменты для реализации и автоматизации практик РБПО.

2. Повышение компетенций ИТ-специалистов. Относится к разработчикам, ИБ-специалистам, сетевикам и всем, кто обеспечивает эксплуатацию объекта, для которого внедряется РБПО.

Этот тренд, как результат осознанного перехода к концепции Secure by Design, свидетельствует и о максимальном «смещении влево» в обеспечении безопасности программных продуктов компаний.

3. Применение ИИ и машинного обучения. Использование технологий доверенного искусственного интеллекта для выявления уязвимостей, анализа поведения приложений и предотвращения атак. Машинное обучение помогает в прогнозировании угроз и автоматизации процессов тестирования на безопасность.

Ключевое слово тут «доверенный» — применением ИИ сейчас никого не удивишь, но можем ли мы на 100% довериться ему в защите своих критических ресурсов? Подходы и принципы «доверия» к ИИ, а также регулирование этой технологии сейчас являются практически основной повесткой всех дискуссий профессионального сообщества.

ЗАКЛЮЧЕНИЕ: НОРМАТИВНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ РБПО — НЕОБХОДИМО ДЛЯ ОБЕСПЕЧЕНИЯ КИБЕРУСТОЙЧИВОСТИ

Очень часто от регуляторики требуют меньше бюрократии, бумажной безопасности и больше практической пользы, описанной лаконично, просто и с конкретным набором действий.

Но, по сути, наши регуляторы уже давно уделяют этому много внимания, выпуская пояснения, методические материалы, да и в целом отвечая на прямые вопросы офлайн или онлайн, а также привлекая профессионалов и экспертов из коммерческих организаций для совместной работы над регуляторикой.

Безопасность всегда была и остаётся процессом, только сейчас точка старта смещается влево у всё большего числа компаний, а не только у крупнейших корпораций.

Государство в лице регуляторов задаёт и корректирует вектор развития процессов и технологий разработки безопасного ПО, помогая сохранить баланс между скоростью выпуска программных продуктов в эксплуатацию и защищённостью чувствительной информации.

СОВРЕМЕННЫЕ ПРАКТИКИ РБПО ДЛЯ ФИНАНСОВОГО СЕКТОРА

Андрей ПРОХОРЕНКО
руководитель отдела аудита и консалтинга
по безопасной разработке компании Swordfish

Госдума ужесточила санкции за утечку персональных данных. Теперь штрафы достигают 15 миллионов рублей, а в случае повторной утечки компании будут вынуждены платить уже оборотные штрафы. Эта новость особенно важна для бизнеса, который напрямую несёт ответственность не только за персональные данные, но и за финансы клиентов. Разберёмся, как избежать проблем и убытков при помощи грамотного построения безопасной разработки.

Финансовый сектор — один из самых регулируемых в мире, особое внимание уделяется защите финансовых активов физических и юридических лиц. С ростом зависимости бизнеса от количества используемых технологий, длинных цепочек поставок и цифровизации соблюдение требований по обеспечению безопасности приложений становится ещё более критичным, чем когда-либо.

Несоблюдение этих требований может привести к значительным финансовым потерям и потере доверия клиентов. Так, согласно исследованию IBM «Cost of Data Breach Report» за 2024 год средняя стоимость утечки данных по финансовому сектору в мире постоянно растёт и за последний год выросла на 3%. При этом суммарная стоимость потерь бизнеса в результате успешных атак выросла почти на 11% по сравнению с 2023 годом. Потери бизнеса включают в себя потерю выручки из-за простоя в работе сервисов, стоимость оттока активных клиентов и принесённый ущерб репутации (рис. 1).

Отказоустойчивость сервисов не единственный показатель надежности финансовых систем , важна и защита информации (персональные данные, финансовые операции, коммерческая тайна и др.). Так, Россия уже несколько лет находится в лидерах мирового антирейтинга стран по количеству утечек персональных данных. Об этом, кстати, свидетельствует рост предложений по украденным базам на теневом рынке.

К счастью, мы видим, что компании всё больше внимания уделяют практикам безопасной разработки и начинают активнее применять меры, руководствуясь наилучшими практиками. К слову о наилучших практиках: 20.12.2024 введён в действие ГОСТ Р 56939–2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования» — последняя редакция одного из основополагающих документов по разработке безопасного ПО (далее – РБПО). Компаниям, которые только начинают свой путь построения безопасной разработки, рекомендуем прежде всего ориентироваться именно на этот документ.

С ЧЕГО НАЧИНАЕТСЯ РАЗВИТИЕ РБПО?

В первую очередь организация должна определить перечень предъявляемых ей регулятором требований. В отличие от других секторов, финансовый сектор строго контролируется регулирующими органами. Необходимо применять сертифицированное ПО или ПО, которое соответствует ОУД (оценочному уровню доверия).

Следующим шагом будет аудит и оценка уровня зрелости текущих процессов РБПО. Аудит и оценку можно провести собственными силами, например, руководствуясь международными (BSIMM, OWASP SAMM, Microsoft SDL, NIST SP 800–64) и отечественными стандартами (ГОСТ Р 56939–2024, ГОСТ Р 71207–2024). При детальном рассмотрении можно заметить, что большая часть международных стандартов основывается на одной и той же базе, и лишь немногие содержат уникальные рекомендации и практики в зависимости от направленности конкретного стандарта. У каждого стандарта есть свои преимущества и недостатки, так как же нам понять, с чего начать?

Компании из финансового сектора могут сочетать элементы разных стандартов для создания дорожной карты развития инициатив РБПО, соответствующей их уникальным потребностям, и гибко адаптировать лучшие мировые практики к российским реалиям. Не у всех есть необходимый набор компетенций, а зачастую и время, чтобы разбираться предметно в вопросе. Тогда можно обратиться к экспертам.

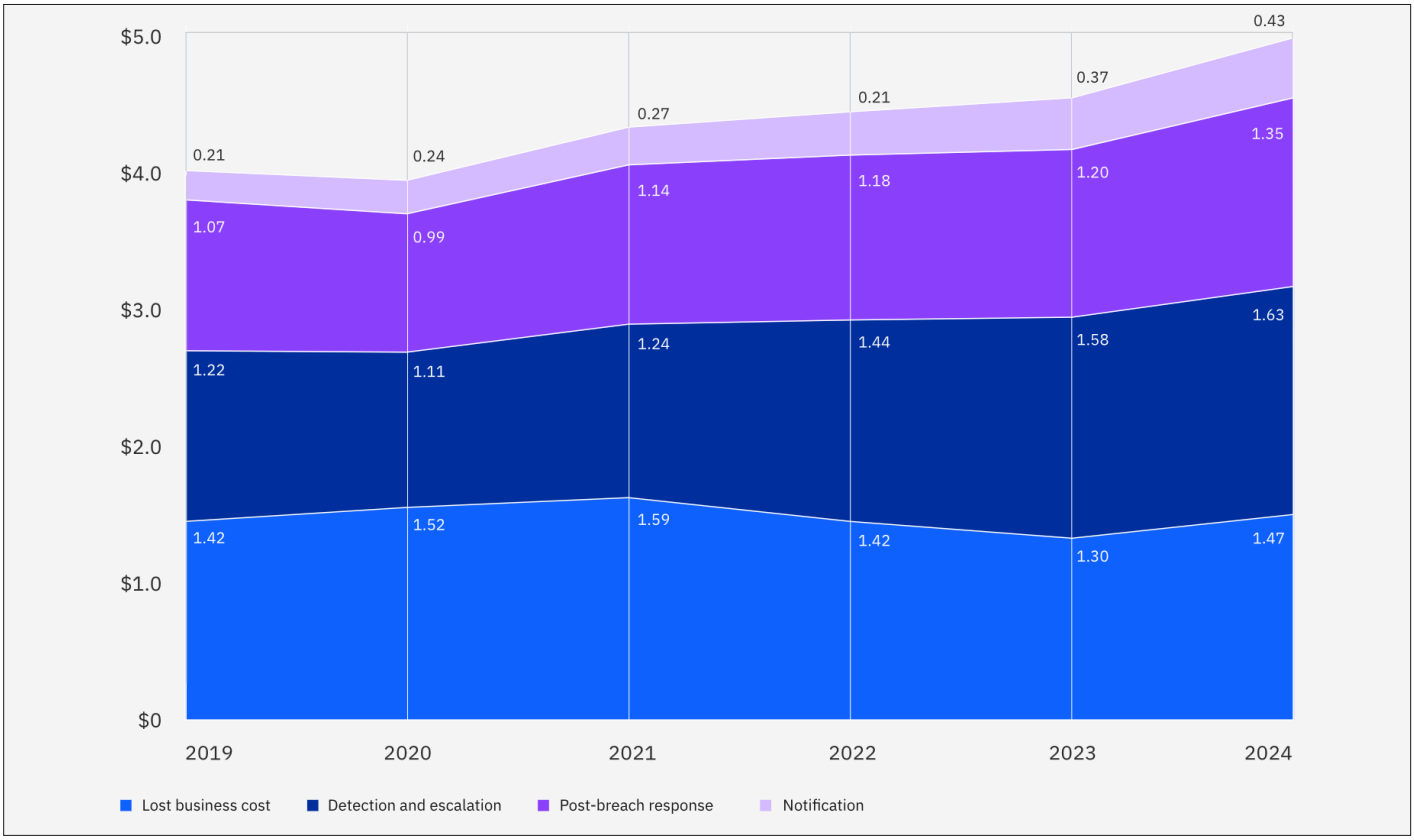


Рисунок 1. Средняя стоимость утечки данных (млн долл. США)

ПОДХОД К ВНЕДРЕНИЮ

По нашему опыту, внедрение вышеперечисленных стандартов или их комбинаций базируется на трёх основных элементах:

- технологии;
- люди;
- процессы.

Из этих элементов складывается корпоративная культура безопасной разработки, и в разрезе этих трёх ключевых элементов проводится аудит/оценка отправной точки.

Под технологиями мы подразумеваем прежде всего используемые в компании инструменты жизненного цикла безопасной разработки таких классов, как OSA, SCA, SAST, DAST, MAST, CS, ASPM.

При этом, инструмент бесполезен без знаний о том, как его правильно установить, настроить и интегрировать в производственный цикл. Именно люди обладают навыками, опытом и компетенциями, необходимыми для корректного и эффективного использования инструментов. Без опыта и экспертизы обработки результатов сканирования технический долг команд разработки будет только расти от релиза к релизу.

Одной из самых острых проблем сегодня является дефицит квалифицированных сотрудников, поэтому крайне важно не только оценивать текущие навыки и компетенции сотрудников, но и сформировать программу обучения специалистов. Обучение поможет облегчить введение в контекст безопасной разработки для новых сотрудников и закрыть отдельные пробелы в их знаниях.

Для обеспечения эффективной передачи экспертного опыта компаниям зачастую необходимо пересмотреть текущую ролевую модель сотрудников с целью определения недостающих ролей, а также формирования налаженного процесса взаимодействия между структурными единицами. Наличие знаний в головах, безусловно, хорошо, однако не хватает последней составляющей — чётко выстроенного процесса безопасной разработки, в основу которого ложится регламентирование и методологическое сопровождение. Без отработанных процедур невозможно добиться эффективной и результативной работы практик безопасной разработки.

ПОДЫТОЖИМ

Развитие практик РБПО актуально для финансовых организаций любой категории, но в разном объёме, есть индивидуальные особенности. При этом необходимо сфокусироваться на нескольких ключевых элементах:

- внедрении инструментов анализа безопасности;
- обучении сотрудников практикам безопасной разработки и вводе их в эксплуатацию;
- выстраивании и регламентации процессов, определяющих эффективное взаимодействие между командами.

На начальном уровне основные процессы и регламенты безопасной разработки в небольшой компании можно выстроить приблизительно за 1 год при должном уровне экспертного опыта специалистов. Достижение зрелого состояния безопасной разработки занимает, по нашему опыту, около трёх лет, но здесь всё может быть сильно индивидуально.

ПОИСК УЯЗВИМОСТЕЙ ПО ОТКРЫТЫМ ИСТОЧНИКАМ

В РАМКАХ ЦИКЛА РАЗРАБОТКИ БЕЗОПАСНОГО ПО

Виталий ВАРЕНИЦА
кандидат технических наук, доцент МГТУ имени Н. Э. Баумана

Сас АРУСТАМЯН
старший преподаватель МГТУ имени Н. Э. Баумана

Илья АНТИПОВ
аспирант МГТУ имени Н. Э. Баумана

Нелли МАГАКЕЛОВА
студентка Финансового университета при Правительстве РФ

В условиях стремительного роста технологий и всеобъемлющей зависимости от программного обеспечения с открытым исходным кодом безопасность становится приоритетом для разработчиков и организаций. В данной статье рассматриваются методы и инструменты анализа уязвимостей по открытым источникам, их применение для повышения уровня безопасности ПО и лучшие практики их интеграции в процесс разработки. Отдельное внимание отведено композиционному анализу, который представляет собой мощный инструмент для выявления уязвимостей в программном обеспечении, включая библиотеки и компоненты, используемые в разработке. Разработка безопасного программного обеспечения на данный момент в Российской Федерации применяется в соответствии с требованиями ГОСТ Р 56939–2024.

ВВЕДЕНИЕ

С увеличением сложности программных систем и распространением программного обеспечения с открытым исходным кодом (ПО с ОИС) уязвимости становятся всё более распространённой проблемой. Согласно исследованию, большинство атак на программное обеспечение происходит через уязвимости в сторонних библиотеках и компонентах. Это связано с тем, что доступность исходного кода позволяет злоумышленникам легко анализировать и выявлять слабые места, что, в свою очередь, ставит под угрозу безопасность многих систем, использующих такие решения. Открытость исходного кода, несмотря на её преимущества в обеспечении прозрачности и возможности проведения аудита, также создаёт риски для безопасности, если разработчики не придерживаются надлежащих практик защиты информации.

Анализ по открытым источникам информации позволяет разработчикам идентифицировать и управлять этими рисками. Различные источники указывают, что поиск уязвимостей в ПО с ОИС становится необходимым элементом цикла разработки безопасного программного обеспечения (SSDLC). Цель данной статьи — рассмотреть преимущества использования инструментов данного анализа в процессе разработки безопасного ПО.

МЕТОДИКА ПРОВЕДЕНИЯ АНАЛИЗА УЯЗВИМОСТЕЙ ПО ОТКРЫТЫМ ИСТОЧНИКАМ

Анализ сторонних компонентов программного обеспечения на предмет известных уязвимостей может быть проведён несколькими способами:

1. Ручной поиск уязвимостей по базам данных уязвимостей, который включает в себя поиск информации о компонентах в различных источниках информации, таких как:
   - ◆ национальные базы данных:
     - Банк данных угроз безопасности информации (БДУ ФСТЭК России);
   - ◆ зарубежные базы данных уязвимостей и недостатков (ошибок):
     - Common Vulnerabilities and Exposures (CVE);
     - CVE Details;
     - National Vulnerability Database;
     - Vulners.
   - ◆ публикации и тематические форумы;
   - ◆ результаты исследований, полученные сторонними исследователями;
   - ◆ официальный сайт производителей компонентов с открытым исходным кодом.

Этот подход позволяет идентифицировать известные уязвимости, однако требует значительных временных затрат, особенно при большом количестве компонентов и сложных зависимостях. Это делает его неэффективным для больших проектов или при необходимости быстрого анализа. Таким образом, эффективность и скорость ручного поиска уступают автоматизированным методам, и даже тщательный ручной поиск не гарантирует обнаружения всех уязвимостей.

2. Статический анализ исходного кода (SAST — Static Application Security Testing) — вид работ, который включает в себя поиск дефектов в исходном коде без его фактического выполнения.

3. Динамический анализ исходного кода (DAST — Dynamic Application Security Testing) — вид работ, который включает в себя поиск уязвимостей в процессе выполнения кода.

4. Нефункциональное тестирование — вид работ, который включает в себя проверки, не относящиеся к тестированию функциональных возможностей ПО. Данный термин был введён в ГОСТ Р 56939–2024 и в первую очередь является заменой понятия тестирования на проникновение. Однако, в отличие от классического пентеста, нефункциональное тестирование — более широкое понятие, включающее в себя также другие проверки, которые требуется проводить в соответствии с промышленными требованиями разработчика. В контексте анализа заимствованных компонентов авторы данной статьи подразумевают именно тестирование на проникновение.

5. Композиционный анализ (SCA — Software Composition Analysis) — вид работ, основанный на формировании перечня зависимостей ПО, определении лицензионной чистоты используемых компонентов и выявлении наличия уязвимостей и/или иных недостатков в зависимостях ПО.

Стоит дополнительно отметить, что статический анализ, динамический анализ и нефункциональное тестирование в отношении заимствованных компонентов требуют гораздо больших трудозатрат с точки зрения проведения, поскольку необходимо разработать уникальную методику тестирования каждого компонента. Соответственно, данные виды анализов целесообразно проводить на этапе тестирования программного обеспечения, когда состав заимствованных компонентов уже сформирован. Важно также подчеркнуть, что в процессе тестирования можно выявить zero-day-уязвимости. Это уязвимости, которые не были ранее известны разработчикам или производителям программного обеспечения, и, следовательно, на них отсутствуют патчи или средства защиты.

В свою очередь, ручной анализ по открытым базам данных и композиционный анализ рекомендуется интегрировать в жизненный цикл разработки программного обеспечения на более ранних этапах, включая стадии проектирования и разработки. Это поможет заведомо выявить проблемы, связанные с безопасностью, и не допустить использования в составе программных компонентов библиотек с подтверждёнными уязвимостями. Поскольку композиционный анализ является логическим продолжением анализа по открытым источникам, в дальнейшем стоит сделать акцент именно на нём.

Многие проекты используют пакетные менеджеры зависимостей (например, npm, maven, pip). Анализ списка зависимостей позволяет идентифицировать используемые компоненты и проверить их на наличие уязвимостей в вышеупомянутых базах данных. Инструменты для анализа состава компонентов помогают автоматизировать данный процесс.

Процесс разработки программного обеспечения, включающий использование компонентов с открытым исходным кодом, формирует определённую цепочку поставок, состоящую из аналогичных проектов с ОИС. Эти проекты могут ссылаться на дополнительные библиотеки с открытым исходным кодом, что приводит к образованию длинной последовательности зависимостей. В связи с этим возникает необходимость в проведении проверки этих зависимостей на наличие известных подтверждённых уязвимостей.

Этапы композиционного анализа традиционно включают в себя:

1. Идентификацию компонентов, которая определяет все внешние библиотеки и зависимости, используемые в проекте.

2. Выявление известных уязвимостей в этих компонентах с использованием различных баз данных уязвимостей, таких как CVE (Common Vulnerabilities and Exposures).

3. Проверка лицензионных соглашений используемых компонентов на предмет соответствия требованиям проекта.

Для прохождения первого этапа необходимо сгенерировать SBOM-файл (Software Bill of Materials) — файл, который содержит в себе спецификацию в виде машиночитаемого формата, в котором перечислены библиотеки и их версии.

Взаимодействие между программными компонентами определяется через граф зависимостей, вершины которого представляют компоненты, а рёбра — зависимости между ними. Зависимости делятся на прямые (direct dependencies) и транзитивные (transitive dependencies). Прямая зависимость устанавливается, если компонент A явно использует компонент B, что обычно отображается в метаданных проекта (например, package.json, requirements.txt). Транзитивная зависимость возникает, когда компонент A зависит от компонента B, а B, в свою очередь, зависит от компонента C. В этом случае C является транзитивной зависимостью для компонента A (рис. 1).

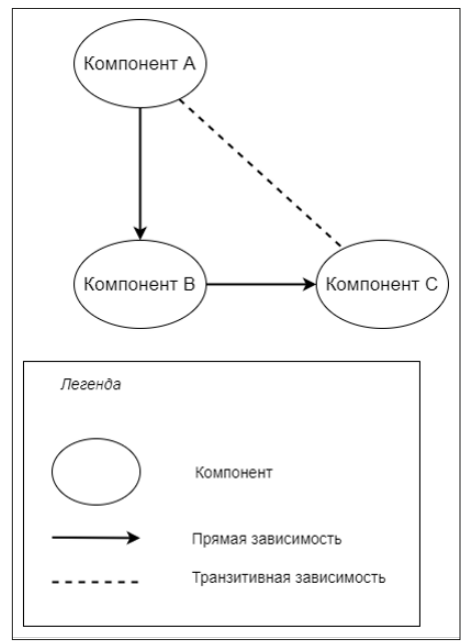


Рисунок 1. Транзитивная зависимость

ТРЕБОВАНИЯ РЕГУЛЯТОРОВ

Анализ компонентов открытого программного обеспечения на наличие известных уязвимостей является обязательным требованием множества отечественных и международных нормативных документов. Несмотря на повсеместную необходимость выявления уязвимостей в заимствованных компонентах (часто сводящуюся к поиску информации в открытых источниках для идентификации потенциальных угроз), явное указание на композиционный анализ как специфический метод проверки присутствует лишь в национальном стандарте ГОСТ Р 56939–2024 (таблица 1). Остальные рассмотренные стандарты (ГОСТ Р 56939–2016, ГОСТ Р ИСО/МЭК 15408–3–2013, «Профиль защиты прикладного программного обеспечения автоматизированных систем и приложений кредитных организаций и некредитных финансовых организаций», стандарт PCI DSS, NIST SP 800–171) описывают требования к анализу ПО с ОИС, однако не конкретизируют методологию.

Анализ требований, представленных в таблице далее по тексту, демонстрирует неоднородность подходов к анализу заимствованных компонентов по открытым источникам информации. В то время как необходимость такого анализа признаётся во всех рассмотренных документах, только ГОСТ Р 56939–2024 указывает на композиционный анализ как наиболее эффективный метод. Это свидетельствует на недостаток стандартизации в области оценки безопасности заимствованных компонентов, что может привести к неполному покрытию уязвимостей и повышенному риску компрометации системы. Дальнейшие исследования должны быть направлены на разработку более чётких и унифицированных методик, учитывающих специфику различных областей применения программного обеспечения.

Нормативный источник	Номер меры	Указание требований по композиционному анализу в явном виде
ГОСТ Р 56939–2016	п. 5.3.3.4, п. 5.3.3.5, п. 5.4.3.2, п. 5.4.3.3, п. 5.4.3.4, п. 5.6.3.4	Нет
ГОСТ Р 56939–2024	п. 5.12, п. 5.15, п. 5.16	Да
ГОСТ Р ИСО/МЭК 15408–3–2013	AVA_VAN.1.2E — AVA_VAN.5.2E, ACO_VUL.1.3E — ACO_VUL.3.3E	Нет
«Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (утв. приказом ФСТЭК России от 2 июня 2020 г. № 76)	п. 12.2, п. 22.1	Нет
Методический документ «Профиль защиты прикладного программного обеспечения автоматизированных систем и приложений кредитных организаций и некредитных финансовых организаций» (утв. Банком России)	AVA_VAN.5.2E	Нет
Стандарт PCI DSS	Requirement 11.3.1.1	Нет
NIST SP 800–171	3.11.2	Нет

Таблица 1. Требования регуляторов

ИНСТРУМЕНТЫ, ПРИМЕНЯЕМЫЕ ПРИ КОМПОЗИЦИОННОМ АНАЛИЗЕ

Использование CI/CD позволяет автоматизировать процесс анализа зависимостей, что снижает вероятность возникновения человеческой ошибки и обеспечивает регулярное обновление информации о безопасности.

Для композиционного анализа наиболее популярными решениями являются OWASP Dependency Track и OWASP Dependency Check. Далее более подробно рассмотрим пример использования OWASP Dependency Track.

Для автоматизированного использования данного инструмента необходимо подготовить файл определённой структуры, в котором содержатся зависимые компоненты и информация о них (SBOM-файл). Необходимо выбирать утилиту для генерации файла в соответствии с используемыми языками программирования. Наиболее распространённая утилита генерации — CycloneDX (cdxgen).

После анализа SBOM-файла в OWASP Dependency Track можно отслеживать не только сами выявленные уязвимости (рис. 2), но и изменение количества уязвимостей в проекте, который инкрементально исследуется (рис. 3).

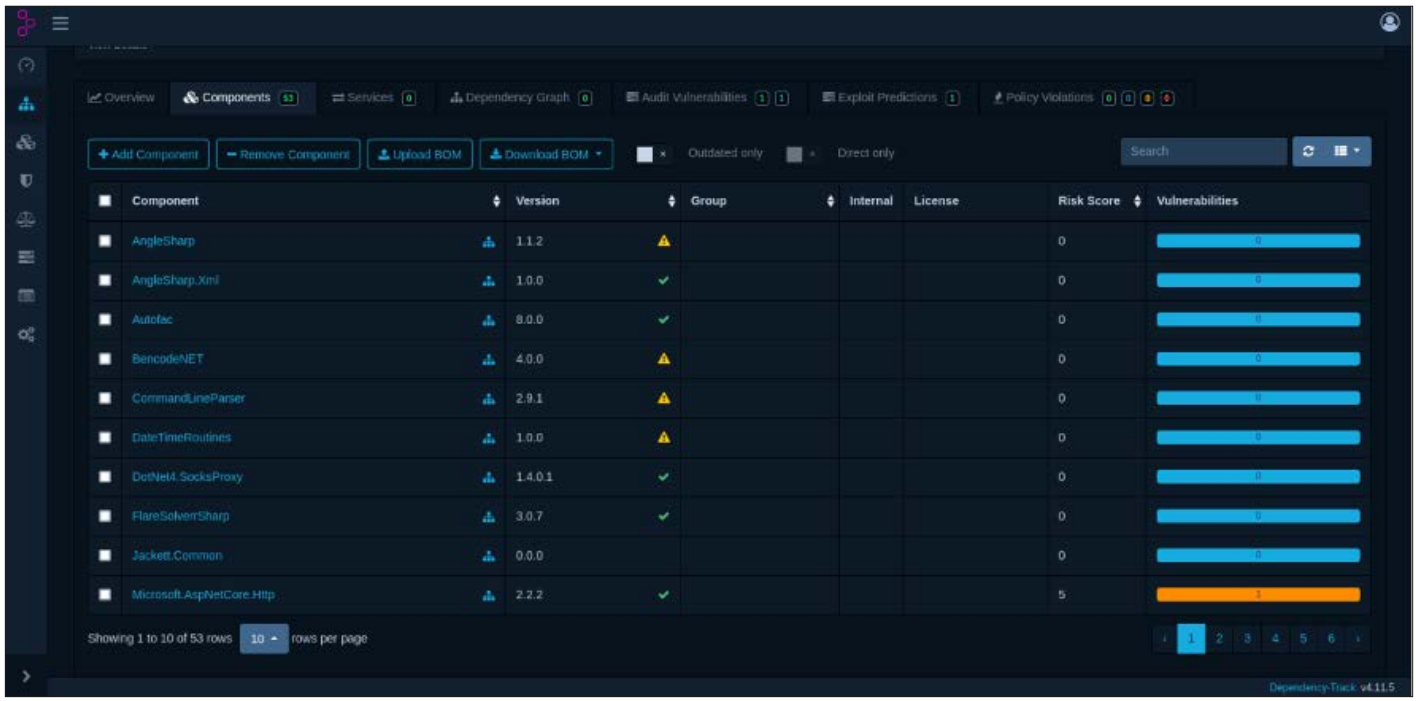


Рисунок 2. Выявленные уязвимости

Рисунок 3. График зависимости количества выявленных уязвимостей от версии проекта

ВЫВОД

Современная разработка с использованием ПО с ОИС требует особого внимания к вопросам безопасности. Применение методов и инструментов анализа уязвимостей, включая композиционный анализ, позволяет существенно снизить риски, связанные с использованием уязвимых библиотек и компонентов. Интеграция таких практик в процесс разработки способствует созданию надёжного ПО, соответствующего как международным стандартам, так и требованиям ГОСТ Р 56939–2024, актуального для Российской Федерации. Постоянное совершенствование подходов к обеспечению безопасности и внедрение инновационных решений позволяют разработчикам и организациям быть готовыми к вызовам стремительно меняющегося технологического ландшафта.

ПОСТРОЕНИЕ КОНТУРА РАЗРАБОТКИ БЕЗОПАСНОГО ПО

Виталий ВАРЕНИЦА
кандидат технических наук, доцент МГТУ имени Н. Э. Баумана

Сас АРУСТАМЯН
старший преподаватель МГТУ имени Н. Э. Баумана

Илья АНТИПОВ
аспирант МГТУ имени Н. Э. Баумана

Нелли МАГАКЕЛОВА
студентка Финансового университета при Правительстве РФ

В данной статье представлен подход к созданию контура разработки безопасного программного обеспечения, который применяется для создания инфраструктуры по разработке программного обеспечения, предусматривающей предотвращение появления проблем безопасности информации, а также их эффективное обнаружение и устранение. На текущий момент разработка безопасного программного обеспечения в Российской Федерации осуществляется в соответствии с требованиями национального стандарта ГОСТ Р 56939–2024.

ВВЕДЕНИЕ

В настоящее время разработка безопасного ПО становится всё более актуальной задачей. Это связано с тем, что всё больше разработчиков обращают внимание не только на оптимизацию и функциональные возможности продуктов, но и на их безопасность.

Эта проблема широко освещается в различных источниках. Например, в источниках подробно расписываются конкретные методики внедрения процессов разработки безопасного ПО. В работах специалистов отмечается необходимость минимизации различных проблем безопасности, которые возникают на этапе разработки.

ЖИЗНЕННЫЙ ЦИКЛ РАЗРАБОТКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ (SDLC) И БЕЗОПАСНЫЙ ЖИЗНЕННЫЙ ЦИКЛ РАЗРАБОТКИ ПО (SSDLC)

SDLC (Software Development Life Cycle) — это процесс разработки программного обеспечения, который включает в себя последовательность этапов, начиная от первоначального предъявления требований и заканчивая поддержкой и обслуживанием готового продукта.

Цикл SDLC состоит из следующих этапов:

- анализ требований;
- планирование;
- проектирование и дизайн;
- разработка ПО;
- тестирование;
- развёртывание;
- эксплуатация.

Анализ требований подразумевает процесс выявления, определения и документирования требований к разрабатываемому продукту.

Планирование подразумевает процесс составления плана разработки программного обеспечения, который включает определение требуемых ресурсов для реализации плана разработки ПО, подготовки бюджета и формирование команд разработки.

Проектирование и дизайн подразумевает процесс продумывания всей архитектуры продукта в детализированном виде, а также анализ рисков.

Разработка программного обеспечения подразумевает процесс написания исходного кода, а также создания системы на основе требований и проекта архитектуры.

Тестирование подразумевает процесс проверки продукта на предмет несоответствий заявленным требованиям.

Развёртывание подразумевает процесс установки и настройки программного обеспечения, создание баз данных, конфигурирование сетевых настроек и других действий, необходимых для работы ПО.

Эксплуатация подразумевает процесс технической поддержки ПО, а также процесс обновления ПО в случае внесения изменений и (или) выявления ошибок в ходе эксплуатации.

Как можно заметить, в данном цикле основное внимание уделяется процессу разработки, который является ключевой задачей. Вопросы информационной безопасности не рассматриваются отдельно. Следовательно, для разработки безопасного программного обеспечения необходимо доработать этот цикл, интегрировав в него аспекты, связанные с безопасностью. Таким образом, цикл SSDLC (Secure Software Development Life Cycle) представляет собой модификацию цикла SDLC, в которую включены специфические методы, направленные на обеспечение безопасности. Более под-

Этап жизненного цикла ПО	Номер процесса	Описание процесса (ГОСТ Р 56939–2024)
Анализ требований	5.3	Формирование и предъявление требований безопасности к программному обеспечению
Планирование	5.1	Планирование процессов разработки безопасного программного обеспечения
	5.2	Обучение сотрудников
Проектирование и дизайн	5.4	Управление конфигурацией программного обеспечения
	5.6	Разработка, уточнение и анализ архитектуры программного обеспечения
	5.7	Моделирование угроз и разработка описания поверхности атаки
Разработка ПО	5.5	Управление недостатками и запросами на изменение программного обеспечения
	5.8	Формирование и поддержание в актуальном состоянии правил кодирования
	5.9	Экспертиза исходного кода
	5.10	Статический анализ исходного кода
	5.12	Использование безопасной системы сборки программного обеспечения
	5.13	Обеспечение безопасности сборочной среды программного обеспечения
	5.14	Управление доступом и контроль целостности кода при разработке программного обеспечения
	5.15	Обеспечение безопасности используемых секретов
	5.16	Использование инструментов композиционного анализа
	5.17	Проверка кода на предмет внедрения вредоносного программного обеспечения через цепочки поставок
Тестирование	5.11	Динамический анализ кода программы
	5.18	Функциональное тестирование
	5.19	Нефункциональное тестирование
Развёртывание	5.20	Обеспечение безопасности при выпуске готовой к эксплуатации версии программного обеспечения
	5.21	Безопасная поставка программного обеспечения пользователям
Эксплуатация	5.22	Обеспечение поддержки программного обеспечения при эксплуатации пользователями
	5.23	Обеспечение реагирования на информацию об уязвимостях
	5.24	Поиск уязвимостей в эксплуатирующемся программном обеспечении
	5.25	Обеспечение безопасности при выводе программного обеспечения из эксплуатации

Таблица 1. Дополнительные меры в цикле SSDLC

робно данные методы, а также сопоставление с текущими требованиями национального стандарта ГОСТ Р 56939–2024 указаны в таблице ниже (таблица 1).

Стоит принять во внимание, что некоторые из приведённых процессов невозможно отнести к конкретному этапу, поскольку они являются итеративными и могут пересекаться сразу с несколькими этапами жизненного цикла. Это связано с тем, что разработка программного обеспечения является цикличным процессом, где результаты одного этапа могут быть использованы для пересмотра предыдущих этапов.

Так, процесс «обучение сотрудников» по вопросам безопасности должен быть непрерывным процессом, охватывающим все стадии разработки ПО, который встраивается в корпоративную культуру. Это требует регулярных обновлений и пересмотров программ обучения, что выходит за рамки определённого этапа жизненного цикла. Поскольку первичное создание обучающих мероприятий осуществляется на ранних стадиях жизненного цикла ПО, данное требование было отнесено к этапу планирования.

Аналогично процесс «управление недостатками и запросами на изменение программного обеспечения» может возникать на разных этапах жизненного цикла ПО. Он включает в себя выявление, анализ и обработку недостатков, которые могут быть обнаружены как в процессе разработки (тестировщиками, разработчиками), так и в процессе эксплуатации (конечными пользователями).

ИНСТРУМЕНТЫ, ИСПОЛЬЗУЕМЫЕ В ПРОЦЕССЕ РАЗРАБОТКИ БЕЗОПАСНОГО ПО

Выполнение требований к разработке безопасного ПО подразумевает под собой комплекс организационных и технических мер. Помимо регламентов, которые необходимы для каждой из внедряемых мер, контур разработки подразумевает внедрение в инфраструктуру разработки инструментов, позволяющих эффек-

Этап жизненного цикла ПО	Номер процесса	Используемые инструменты	Пример инструментов
Анализ требований	5.3	Системы хранения документов проекта	Jira
Планирование	5.1	Системы планирования работ и управления задачами	Confluence
	5.2	–	–
Проектирование и дизайн	5.4	Аналогично п. 5.1, 5.3, 5.5, 5.9, 5.12, 5.21, 5.22	Аналогично п. 5.1, 5.3, 5.5, 5.9, 5.12, 5.21, 5.22
	5.6	Инструмент визуального моделирования и проектирования	Sparx Systems Enterprise Architect, Archimate
	5.7	Инструмент для определения поверхности атак	Natch
Разработка ПО	5.5	Системы управления изменениями	Jira, Bugzilla, Redmine, Azure DevOps, GitHub, GitLab, Bitbucket
	5.8	Линтеры	ESLint, Pylint
	5.9	Интегрированная среда разработки	Visual Studio Code, JetBrains IDE, Эшелониум
	5.10	Статические анализаторы	АК-ВС 3, Sonarqube, Svace, Horusec, Cppcheck, Clang SA
	5.12	Средства сборки	Apache Maven, Gradle, Make, CMake
		Инструмент контейнеризации	Docker
		Система для оркестрации	Kubernetes
	5.13	Аналогично п. 5.12	Аналогично п. 5.12
	5.14	Аналогично п. 5.5	Аналогично п. 5.5
	5.15	Статические анализаторы	АК-ВС 3, Sonarqube, Svace, Horusec, Cppcheck, Clang SA
		Инструменты сканирования для поиска секретов	Git-Secrets, gitLeaks, Git-all-secrets, Detect-secrets, Gittyleaks
	5.16	Инструменты композиционного анализа	OWASP Dependency-Check, OWASP Dependency-Track, CodeScoring
	5.17	Средства антивирусной защиты информации	Kaspersky Endpoint Security, Dr.Web Enterprise Security Suite, PT MultiScanner, Secret Net Studio 8
Тестирование	5.11	Инструменты динамического анализа	АК-ВС 3, Блесна
		Фаззеры	АК-ВС 3, AFL++, WinAFL, Crusher, Libfuzzer, Peach Fuzzer, Sharpfuzz, jazzer
	5.18	–	–
	5.19	Инструменты тестирования на проникновение	Burp Suite, OWASP ZAP, sqlmap, Metasploit
		Сетевые сканеры безопасности	Сканер-ВС, Nessus, Nmap
Развёртывание	5.20	Средства контрольного суммирования	ФИКС, ФИКС-Unix, Трафарет, ПИК Эшелон, gostsum
	5.21	Аналогично п. 5.20	Аналогично п. 5.20
		Инструменты резервного копирования	Citprotect, Rewind, BackupLABS, Veeam Backup Agent
Эксплуатация	5.22	Системы отслеживания и регистрации ошибок	Jira, Redmine, Azure DevOps, Bugzilla
	5.23	Аналогично п. 5.1, 5.5, 5.22	Аналогично п. 5.1, 5.5, 5.22
	5.24	Аналогично п. 5.8, 5.9, 5.11, 5.16, 5.19	Аналогично п. 5.8, 5.9, 5.11, 5.16, 5.19
	5.25	–	–

Таблица 2. Используемые инструменты в цикле SSDLC

тивно бороться с различными проблемами безопасности, возникающих по вине разработчика на этапе создания продукта. В таблице ниже (таблица 2) представлен перечень инструментов, требуемых для успешной реализации процессов РБПО.

СОСТАВ КОМАНД, НЕОБХОДИМЫХ НА КАЖДОМ ЭТАПЕ ЖИЗНЕННОГО ЦИКЛА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

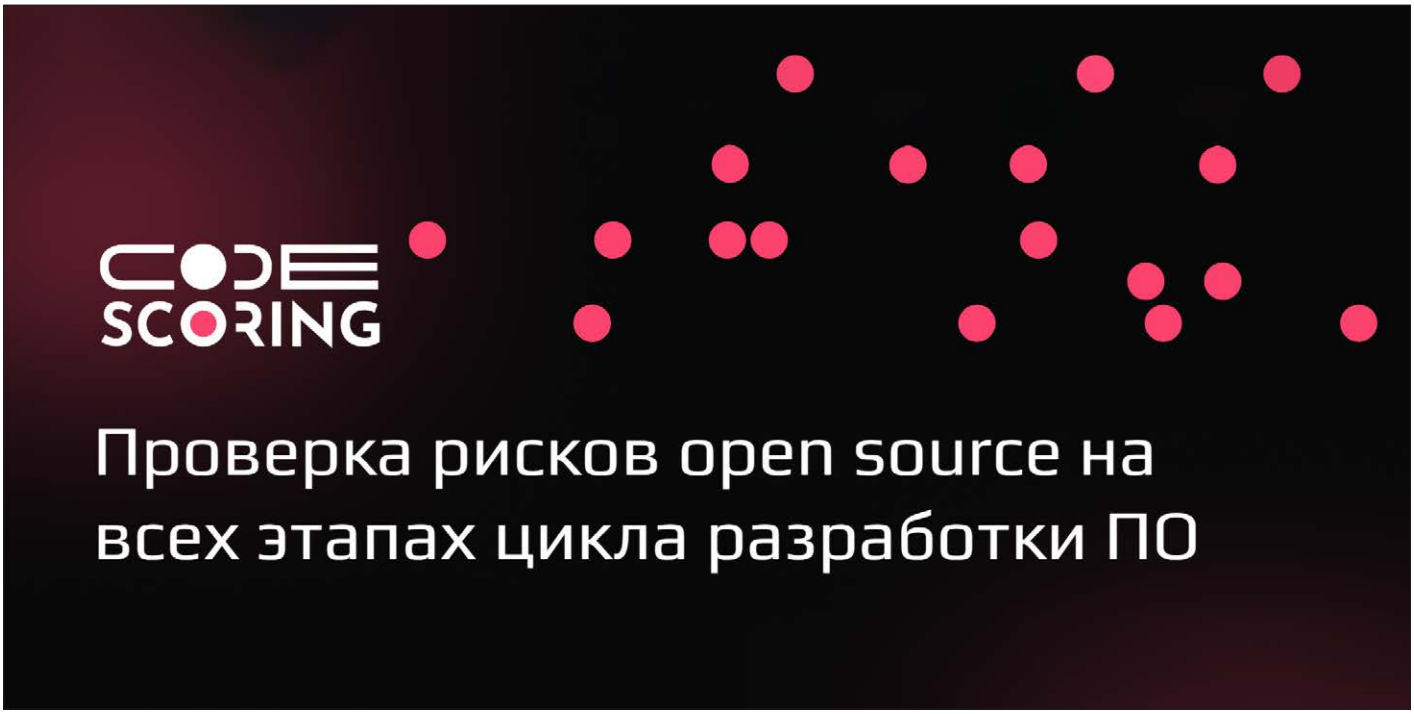
Для успешной реализации процессов разработки безопасного программного обеспечения в соответствии с ГОСТ Р 56939–2024 организациям необходимо сформировать команду, включающую различные роли, способные эффективно выполнять свои функции на каждом этапе жизненного цикла программного обеспечения. В процессе построения конвейера безопасной разработки крайне важно соблюдать принцип разделения полномочий и чётко определить для каждого члена команды конкретные элементы конфигурации, находящиеся в их зоне ответственности. Количество специалистов и их роли, представленные в таблице далее по тексту, являются усреднёнными значениями для компании и могут варьироваться в зависимости от специфики организации, масштаба разрабатываемого продукта и прочих факторов (таблица 3).

ВЫВОД

В статье рассматриваются особенности построения контура разработки безопасного программного обеспечения, который включает в себя интеграцию процессов, направленных на обеспечение безопасности, внедрение инструментария, применяемого в процессе разработки, а также вовлечение в выстроенные процессы команд, необходимых на каждом этапе жизненного цикла программного обеспечения. Подобный системный подход к организации всех указанных элементов является ключевым фактором для достижения высокого уровня безопасности программного обеспечения в организации.

Этап жизненного цикла ПО	Роль	Количество специалистов	Процессы из ГОСТ Р 56939–2024
Анализ требований	Product Owner	1 человек + заместитель	5.3
	Аналитик	2–3 человека	
Планирование	Руководитель проекта	1–2 человека	5.1, 5.2
	SCRUM–Master	2–3 человека	
Проектирование и дизайн	Архитектор	2–4 человека	5.6
	Архитектор по безопасности	2–3 человека	5.6, 5.7
Разработка ПО	Team leader	Для каждой команды разработки 1 человек	5.5, 5.8, 5.9, 5.10, 5.12
	Команда разработки	Различные команды от 5 человек	5.4, 5.5, 5.8, 5.9, 5.10, 5.16
	DevOps-специалист	На каждую команду разработки 1–2 человека	5.4, 5.5, 5.13
	Специалист по безопасности	На каждую команду разработки 1–2 человека	5.14, 5.15, 5.17, 5.18, 5.19, 5.24
Тестирование	Руководитель тестирования	Для каждой команды тестирования 1 человек	5.11, 5.18, 5.19, 5.24
	Команда тестирования	На каждый вид тестирования 3–5 человек	5.11, 5.18, 5.19, 5.24
Развёртывание	Специалист функционального сопровождения	2–3 человека на каждый продукт	5.20, 5.21, 5.25
	Специалист отдела внедрения и сопровождения (технической поддержки)	3–4 человека на каждый продукт	5.22, 5.23
	Инженер по сборке	2–3 человека на каждый продукт	5.4, 5.5, 5.13
	Инженер инфраструктуры	2–3 человека на каждый продукт	5.4, 5.5, 5.14
	Технический писатель	1–2 человека	5.4
Эксплуатация	Специалист по технической поддержке	3–5 человека на каждый продукт	5.22, 5.23
	Специалист по мониторингу и управлению инцидентами	1–2 человека на каждый продукт	5.23, 5.24

Таблица 3. Кадровый подбор для реализации требований ГОСТ Р 56939–2024



OPEN SOURCE: БЕЗОПАСНОЕ ИСПОЛЬЗОВАНИЕ

О БАЗОВЫХ ПРАКТИКАХ ЗАЩИТЫ ЦЕПОЧКИ ПОСТАВКИ, КОМПОЗИЦИОННОМ АНАЛИЗЕ ПО И ПОЧЕМУ ЭТО ПОЛЕЗНО ДЛЯ РАЗРАБОТКИ

Алексей СМИРНОВ
основатель CodeScoring

Обновлённый стандарт безопасной разработки (ГОСТ Р 56939–2024) определил практики, которые не были отражены в прежней версии стандарта. В частности, в отношении работы со сторонними компонентами описываются подходы к защите цепочки поставки и необходимости применения композиционного анализа ПО.

Контроль сторонних компонентов играет важную роль с точки зрения безопасности, поскольку важно следить за тем, что включается в состав вашего ПО. В статье рассматривается проблематика и действенные подходы, которые позволяют контролировать использование сторонних компонентов ПО от стадии выбора компонентов до особенностей их применения в продуктивных средах.

ПРОБЛЕМАТИКА

Открытого кода в программных продуктах становится всё больше, а культура ответственного потребления сторонних компонентов, к сожалению, отстаёт. Бизнесу нужно быстрее разрабатывать, а с техническим долгом и особенностями библиотек «мы разберёмся позже». Вместе с открытым кодом в ПО попадают недостатки, связанные не только с базовым качеством, но и с безопасностью. Важно помнить, что открытый код известен, исследуем и идентифицируем в составе ПО, которое может попасть в прицел злоумышленника. Кроме того, открытые компоненты обладают своими лицензионными соглашениями, ко-

торые читают, увы, не все пользователи, что может привести к последующей переработке кода и замене используемой библиотеки.

Помимо базовых вопросов безопасности и качества компонентов, в их отношении нарастает количество атак на цепочку поставки. Подобное происходит, когда злоумышленник намеренно выпускает версию пакета с полезной нагрузкой, что приводит к утечке параметров окружения (в частности, компрометации конвейера сборки), появлению бэкдоров в продуктах, занесению шифровальщиков в контур и иным последствиям.

Самые популярные способы подобной «доставки» — это:

- typosquatting — публикация компонента с заведомой опечаткой в названии;
- dependency confusion — эксплуатация механизмов управления компонентами;
- malicious code injection — инъекция вредоносного кода в тело легитимного пакета.

Кроме того, в последние годы обострилась ситуация с закладками и политизированным саботажем авторов компонентов.

СТАТИСТИКА

Команда CodeScoring обладает собственной экспертностью в части анализа данных о мировом Open Source, чем регулярно делится с сообществом РБПО. Приведём сокращённую статистику:

- ~100 уязвимостей и вредоносных активностей в компонентах обнаруживается ежедневно;
- ~900 вредоносных пакетов выявляется ежемесячно;
- 8 млн — мировая база открытых компонентов;
- 90 млн разработчиков участвуют в открытых проектах;
- ~2500 типов открытых лицензий со своими видами ограничений и разрешений.

ХРАНЕНИЕ КОМПОНЕНТОВ В КОНТУРЕ ОРГАНИЗАЦИИ

Если вы не храните компоненты, из которых производится или производилась сборка, пора начать делать это.

Для этого существует отдельный класс решений в виде **репозиториев артефактов**, которые позволяют не только хранить компоненты, но и интегрировать их в процессы сборки ПО с учётом модели разграничения доступа организации.

Одним из ключевых примеров здесь является открытый Nexus Repository OSS.

Теперь, если компонент пропадёт из интернета, вы всё равно сможете произвести сборку.

КОНТРОЛИРУЕМЫЙ РЕПОЗИТОРИЙ АРТЕФАКТОВ

Что касается безопасности компонентов, важно не только хранить их у себя, но и проверять на вредонос, публичные уязвимости, разрешённые лицензии и иные особенности компонентов, которые допущены к использованию внутри организации.

Такую проверку можно организовать для каждого запроса компонента пользователем.

Например, наше решение для защиты цепочки поставки CodeScoring. OSA позволяет встроиться в процесс запроса компонента разработчиком и произвести проверку на соответствие политике безопасности организации. В случае если компонент нарушает принятые политики, он блокируется, а разработчику даются подробные пояснения, почему так вышло и что делать дальше.

Узнать больше про защиту цепочки поставки с CodeScoring.OSA

https://codescoring.ru/osa

КОМПОЗИЦИОННЫЙ АНАЛИЗ, ИЛИ «ИЗ ЧЕГО СОСТОИТ ВАШЕ ПО»

Понятие композиционного анализа на отечественных SDL-пространствах является довольно молодым, но важным и встаёт в один ряд со статическим и динамическим анализами.

Если коротко, то этот вид анализа позволяет ответить на вопрос: «из чего состоит ваш продукт?» и проверить риски.

Если более развёрнуто, то композиционный анализ основан на инвентаризации сторонних компонентов ПО, определении особенностей их использования, составлении перечня известных уязвимостей и/или иных недостатков компонентов.

В общей практике применения композиционный анализ разделяется на три части:

1. Инвентаризация всех компонентов в составе ПО. Это крайне важная стадия, которая должна быть выполнена точным образом, с учётом особенностей применяемых языков программирования и окружений сборки. Для ПО на разных языках могут быть свои особенности определения компонентов, например для C/C++.

2. Анализ компонентов
Обогащение информации о компонентах данными об уязвимостях и лицензиях и иными известными факторами компонента: возраст, авторы, количество версий и пр.

3.Рекомендация и действие
После получения результатов анализа производится проверка политик безопасности и может быть выполнено действие: например, заблокировать сборку. Результаты проверки политик должны сопровождаться информацией о выявленных проблемах и предлагать решение, например безопасную версию компонента.

Важным артефактом реализации этапа инвентаризации и анализа является перечень программных компонентов (ППК или SBoM, Software Bill of Materials). Это машиночитаемый документ, который обеспечивает фиксацию результатов в едином формате. Им можно поделиться с коллегами или заказчиком в рамках поставки. Существует два основных формата

обмена данными: CycloneDX (OWASP) и SPDX (Linux Foundation). В России больше распространён первый.

Полезный аспект реализации практики композиционного анализа — рекуррентность процесса. В уже выпущенных компонентах уязвимости не появляются, уязвимости обнаруживаются.

За год в продукте без обновлений накапливается ~100 уязвимостей от сторонних компонентов

Это означает, что в отношении ранее выпущенного ПО нужно не только регулярно проводить композиционный анализ в целях выявления новых проблем, но также следует наладить процесс обновлений своего ПО так, чтобы иметь возможность выпустить безопасную сборку при обнаружении рисков.

Узнать больше про композиционный анализ с CodeScoring.SCA

https://codescoring.ru/sca

ПОЛЬЗА ПРИМЕНЕНИЯ КОМПОЗИЦИОННОГО АНАЛИЗА ДЛЯ РАЗРАБОТЧИКОВ

Применение практики композиционного анализа позволяет разработке комплексно следить за компонентами, которые заносятся в разрабатываемые продукты.

Своевременная актуализация компонентного состава позволяет иметь меньше проблем с обратной совместимостью со старыми версиями компонентов.

Опыт работы с известными уязвимостями в сторонних компонентах повышает уровень знаний разработчиков в области безопасности кода и позволяет быть более подготовленными к практикам статического и динамического анализа.

НА ЧТО ОБРАТИТЬ ВНИМАНИЕ ПРИ ВЫБОРЕ ИНСТРУМЕНТА КОМПОЗИЦИОННОГО АНАЛИЗА

Наличие своего агента для инвентаризации компонентов. Наличие своего агента для инвентаризации компонентов, как правило, даёт более полноценную, глубокую, комплексную интеграцию со всем решением. Агент важен для встраивания в систему сборки для получения более точного результата анализа. Использование открытых инструментов, таких как Trivy, cdxgen или dep-scan, накладывает ограничения: вендору приходится учитывать их особенности и зависеть от направления развития этих проектов. Наличие функций, нацеленных на сокращение издержек по работе с инструментом: точность анализа, гибкие политики безопасности, удобство работы с инвентарём и качественные рекомендации. Встраиваемость в действующую автоматизацию разработки. Наличие агента, программных интерфейсов, вебхуков существенно упростит.

ЗАКЛЮЧЕНИЕ

Наладив правильные процессы проверки сторонних компонентов для своих продуктов, вы получите основу и фундамент для построения безопасных процессов разработки:

- защиту цепочки поставки стороннего ПО;
- безопасность компонентной базы в первом приближении;
- информированность об уязвимостях в ранее выпущенных версиях ПО;
- понимание и контроль лицензионной чистоты;
- контроль актуальности компонентной базы выпускаемого ПО.

СПРАВКА О CODESCORING

Платформа CodeScoring представлена на рынке с начала 2021 года и сегодня решает задачи банков, телеком-операторов, ИТ-компаний и других организаций, для которых важны вопросы кибербезопасности и качества собственных продуктов.

CodeScoring сегодня:

- вся ключевая функциональность собственной разработки;
- анализ 15 языков программирования и Docker-образов;
- более 20 интегрированных баз уязвимостей;
- собственная база знаний про мировой open source;
- интеграция на всех этапах разработки ПО;
- широкий набор политик отслеживания и блокирования рисков;
- интеграция с отечественными ASOC/ASPM-платформами;
- интеграция с Kaspersky Open Source Software Threats Data Feed;
- применение машинного обучения для удобства пользователей.

Мы остаёмся одними из немногих производителей средств безопасной разработки, кто ведёт открытый Changelog и доступную документацию.

КОД БЕЗ СЕКРЕТОВ: ПОЧЕМУ ЭТО ВАЖНО?

К ЧЕМУ ПРИВОДИТ НАЛИЧИЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В КОДЕ ПРОДУКТОВ И КАК С ЭТИМ БЫТЬ

Алексей СМИРНОВ
основатель
CodeScoring

ЧТО ТАКОЕ СЕКРЕТ?

ГОСТ Р 56939–2024 под секретами определяет «данные, которые могут использоваться для обеспечения аутентификации и/или целостности и/или конфиденциальности информации (пароли, цифровые сертификаты и т.п.)».

Секреты могут быть представлены также и иными данными, например платёжными: номерами карт, счетов, пинами и пр. Подобную «живую» информацию хранить в коде, конфигурационных файлах или фикстурах совершенно нежелательно.

ПОЧЕМУ ЭТО ВАЖНО

Исходные коды приложений находятся под стражей специалистов по безопасности. Тем не менее приложения, собранные из этих кодов, регулярно разворачиваются на сторонние площадки или публикуются (очевидный пример — мобильные приложения), а сами исходные коды хранятся на рабочей технике разработчиков. Угроза внутреннего злоумышленника и утечки исходных кодов сохраняется актуальной для любой организации.

Наличие чувствительной информации в приложении может позволить злоумышленнику использовать её для получения доступов в целях кражи персональных данных, поддержания цепочки взломов, фишинга, распространения вредоносного ПО или иных целей.

Одним из примеров реализации подобного вида атаки является декомпиляция мобильных приложений из публичных площадок с целью извлечения доступов к его публикации, размещённых разработчиками по неосторожности, что позволяет подменить оригинальное приложение приложением с полезной нагрузкой. Аналогичным образом получаются доступы к API используемых сервисов, sms-шлюзам, ключам доступа к платёжным сервисам, которые случайно забыла разработка.

СТАТИСТИКА

Показательной является статистика открытого кода из свежего отчёта The State of Secrets Sprawl 2024:

- 12,8 млн новых секретов обнаружено в публичных коммитах на GitHub за 2023 год;
- 90 % секретов оставались валидными и через 5 дней после утечки;
- каждый десятый разработчик случайно добавляет секрет в код.

К сожалению, ревью кода и средства идентификации секретов в коде до публикации изменений применяются не всеми и совершить подобную ошибку случайного добавления может каждый.

ПОСТРОЕНИЕ БАЗОВЫХ ПРОЦЕССОВ РАБОТЫ С СЕКРЕТАМИ

Важно контролировать, чтобы секреты не попадали в исходные коды приложений, хранились и обрабатывались соответствующим образом.

Во-первых, должно быть организовано пространство хранения и предоставления секретов смежным приложениям. Для этого есть специальные системы управления секретами («паролешницы»), например открытый Vault.

Во-вторых, следует настроить блокирующую проверку секретов на стороне разработки. Это могут быть такие открытые и «лёгкие» статические анализаторы, как GitLeaks, TruffleHog, DeepSecrets или иные, которые уже устоялись в экспертной практике и позволяют легко настраивать правила анализа. Независимо от уровня применяемого инструмента следует приготовиться к разбору ложноположительных срабатываний, если не предлагается специальных механизмов интеллектуального анализа. К примеру, наша лаборатория показала, что можно натренировать модель машинного обучения, которая с ходу идентифицирует 50–70 % ложноположительных срабатываний. А если проводить дообучение этой модели на контекстных данных проектов, то результат стремится к 90–95 %, что существенно экономит время специалистов РБПО на разбор срабатываний.

В-третьих, если всё-таки утекло или возникли подозрения, то должна быть разработана чёткая процедура отзыва и инвалидации утёкших секретов. Не говоря уже о том, что секреты должны ротироваться и вообще подчиняться определённой ролевой модели использования.

Безусловно, всё, что вы придумаете и настроите, должно быть закреплено в регламенте по работе с секретами. Или наоборот, но регламент должен работать, а не лежать.

ВЫВОДЫ

Можно разработчику сильно не доказывать, что секреты в коде — это неправильная инженерная культура. Ошибки совершают все. Но правильный процесс и инструментарий для контроля секретов должны быть реализованы.

БЕЗОПАСНОСТЬ — ЭТО ВАША ПРИБЫЛЬ

КАК УПРАВЛЕНИЕ БЕЗОПАСНОЙ РАЗРАБОТКОЙ НА ОСНОВЕ ДАННЫХ СОКРАЩАЕТ TIME-TO-MARKET

Антон БАШАРИН
старший управляющий партнёр AppSec Solutions

Разработка программного обеспечения, в том числе мобильных приложений, давно стала необходимой частью бизнес-процессов как в b2c-, так и в b2b-сегменте — в особенности это касается крупного и среднего бизнеса. В то же время некоторые организации относятся к вопросам кибербезопасности, включая разработку безопасного ПО, по остаточному принципу. В результате общий ущерб экономике России от действий злоумышленников в 2023–2024 годах, по оценкам Сбербанка, может превысить 1 триллион рублей, а в открытом доступе находятся данные 90% взрослых россиян. На этом фоне государство заметно и обоснованно будет ужесточать санкции за уязвимости в ПО, а клиенты — выбирать более безопасные сервисы.

Таким образом, разработка безопасного программного обеспечения, или DevSecOps, — это не затраты, а инвестиции. Сделать их максимально эффективными помогает использование методов управления Data Driven и принципа Shift Left. Объясним, что это и как работает.

ЗАЧЕМ НУЖЕН DEVSECOPS БИЗНЕСУ

Для начала разберёмся, как работает неэффективное управление процессами разработки и во что оно обходится бизнесу. Для этого очень хорошо подходит метрика Time-to-Market, или скорость вывода продукта на рынок — до конечного пользователя. Другими словами, чем раньше будет релиз, тем быстрее мы начнём зарабатывать. Поскольку прибыль от выведенного на рынок продукта остаётся примерно одинаковой, любые задержки разработки увеличивают затраты, что снижает рентабельность. Ошибки, выявленные на поздних этапах создания ПО, требуют больше ресурсов на исправление, поскольку при этом задействуются высокооплачиваемые специалисты: разработчики, системные архитекторы, техлиды и другие. Это особенно критично для уязвимостей информационной безопасности, поиск которых требует привлечения ИБ-инженеров или подрядчиков, что само по себе связано с крупными финансовыми вложениями. А устранение таких уязвимостей на поздних этапах значительно увеличивает трудозатраты, делая раннее их выявление и предотвращение ключевым фактором эффективности процесса.

Что означает доработка на позднем этапе? Это аврал, отвлечение ключевых специалистов от других задач и проектов, сверхурочная работа. Представьте: у вас всего два ИБ-инженера, а тестирование выявило 500 серьёзных уязвимостей. Очевидно, что они физически не смогут справиться с таким объёмом за две недели, даже если предложить им дополнительные выплаты. Привлечение ещё 10 специалистов практически нереально, так как это сверхдефицитная специальность. В результате сроки проекта неизбежно сдвинутся на неопределённое время, затраты станут неконтролируемыми, и возникнет реальный риск того, что проект в итоге окажется нерентабельным.

К сожалению, такой результат возможен даже в том случае, если в компании применяются отдельные практики разработки безопасного программного обеспечения, например, в силу требований регулятора или если замруководителя по ИТ в целом фокусируется на информационной безопасности. Какие-то регламенты принимаются, те же сканеры закупаются. Но если средний менеджмент и сами разработчики относятся к требованиям безопасности как к навязанным извне задачам, которые нужно выполнить «для галочки», провалы неизбежны.

Именно поэтому важно внедрять принципы DevSecOps с акцентом на подход Shift Left. Этот подход предполагает смещение практик обеспечения безопасности влево по таймлайну проекта — с этапа приёмки на этапы разработки или даже проектирования. Это критично, поскольку именно на ранних этапах создание и обнаружение новых рисков информационной безопасности наиболее вероятно, а их устранение обходится значительно дешевле, чем на более поздних стадиях.

На ранних этапах разработки нужно внедрять сканеры, которые сразу анализируют уязвимости в исходном коде. Они же становятся фактическим барьером для попадания вредоносных элементов при использовании источников Open Source. На следующих этапах применяется уже динамический анализ. Например, сканируется API, то есть программный (API) и пользовательский (UI) интерфейс.

То есть анализ идёт на каждом этапе разработки, и в финальной сбор-

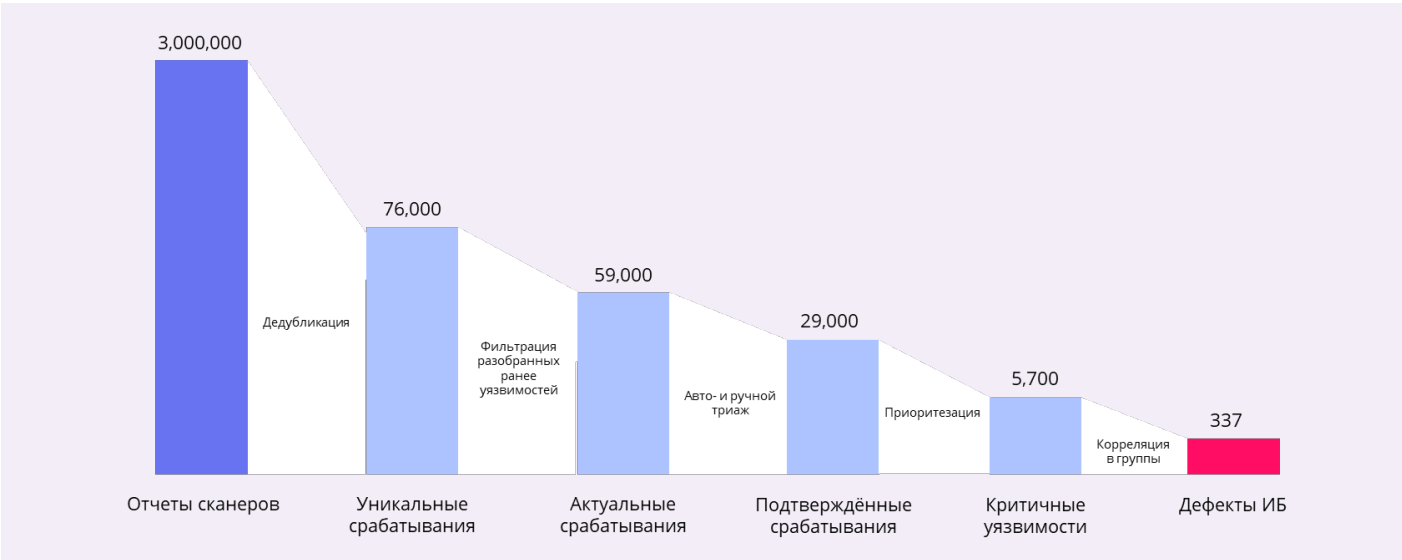


Рисунок 1. Эффективность обработки результатов сканирования ASPM-платформы AppSec.Hub

ке могут остаться единицы уязвимостей, а не сотни, как могло бы произойти без применения принципов DevSecOps.

Организация комплексного контроля и аналитики безопасной разработки может существенно ускорить и упростить создание программных решений. Она позволяет сформировать своего рода единый центр управления сканированием уязвимостей, оценкой рисков и анализом состояния кода.

ДЛЯ ЧЕГО НУЖНЫ ASPM-РЕШЕНИЯ

ASPM (Application Security Posture Management) — это класс систем для управления безопасностью приложений, который помогает организациям оценивать, управлять и улучшать свою безопасность приложений на всех этапах жизненного цикла разработки. Платформа ASPM предоставляет инструменты и средства для анализа уязвимостей, контроля за соблюдением стандартов безопасности, управления инцидентами и выполнения аудитов. Основные функции ASPM-решения:

1. Оценка и приоритизация уязвимостей. Помощь в выявлении слабых мест в приложениях, включая сортировку уязвимостей, оценку всех данных со сканеров.

2. Контроль за соблюдением стандартов. Проверка соответствия приложений положениям нормативных актов и корпоративным стандартам кибербезопасности.

3. Управление рисками. Помощь в оценке рисков, связанных с уязвимостями и угрозами, для более осмысленных решений в области безопасности.

4. Определение корреляций и аналитика. Визуализация данных по уязвимостям и контроль процессов РБПО на основе прозрачной системы метрик.

Давайте разберём, из чего состоит типовой процесс управления безопасностью приложений с помощью ASPM. Пройдя через все стадии автоматической и ручной обработки, анализа, приоритизации и корреляции, уязвимости преобразуются в дефекты, экспортируемые в дефект-трекинговую систему команды разработки для исправления.

Основные стадии обработки результатов сканирования:

- дедубликация,
- применение автоматических правил обработки,
- триаж,
- приоритизация,
- корреляция.

Примером такой системы является российская платформа AppSec.Hub (рис. 1). Это централизованная платформа для интеграции различных инструментов безопасности и процессов. Основные преимущества AppSec.Hub:

1. Единая точка управления. AppSec.Hub обеспечивает централизованное управление всеми инструментами безопасности, что упрощает процесс мониторинга и обеспечения безопасности приложений.

2. Интеграция инструментов. Позволяет объединять данные из различных источников и инструментов, используемых для анализа безопасности приложений, и предоставляет полную картину безопасности.

3. Аналитика и отчётность. Упрощает процесс анализа уязвимостей и генерирует отчёты, которые могут быть использованы для принятия решений и управления рисками.

4. Прозрачность и контроль на основе метрик. Предоставляет командам разработки и безопасности возможность видеть состояние безопасности всех приложений и управлять им из одного интерфейса.

Особо отмечу, что все рутинные операции автоматизируются в том числе с применением искусственного интеллекта, как, например, в нашем продукте AppSec.Hub с помощью модуля AppSec.CoPilot. Это позволяет отсеивать ложные срабатывания — как правило, это более 90 % того, что выдают сканеры. Время ваших специалистов в таком случае тратится на решение действительно сложных и необходи-

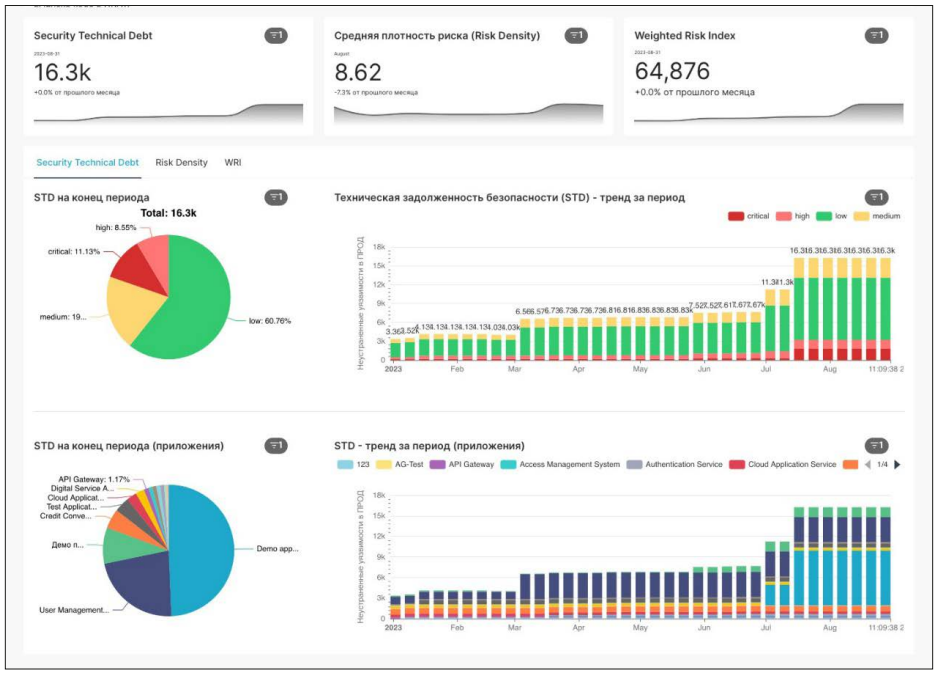


Рисунок 2. Дашборд операционных показателей ASPM-платформы AppSec.Hub

мых задач, а алгоритмы ИИ не требуют почасовой оплаты.

Принцип Shift Left и автоматизация делают методологию DevSecOps максимально эффективной. В идеале все инструменты ИБ интегрируются в среду разработки, проще говоря, на рабочий стол специалиста. В реальности проверки ИБ встраиваются в CI/CD- или DevOps-процесс, который запускается автоматически после публикации изменений разработчиком. Одновременно формируется аналитика, представление которой должно быть адаптировано под уровень получателя. Например, руководитель проекта должен видеть подробную динамику выявленных и закрытых уязвимостей. А вице-президенту по ИТ или гендиректору достаточно светофора: если процессы проекта идут в «зелёной зоне», ему не нужно вмешиваться, а если попадают в «жёлтую» или вдруг включается «красный», то нужно тормозить и решать выявленные проблемы на данном этапе, а не в конце, потому что потом это обойдётся намного дороже.

DevSecOps — это не набор определённых инструментов и правил их использования, а именно бизнес-подход.

Представим основные метрики аналитики уязвимостей в виде пирамиды по уровням принятия решений в бизнесе от инженерных команд к ценности продукта.

◆ На её острие будет уровень топ-менеджмента (Executive). С точки зрения руководителя компании он влияет на следующие ключевые метрики: Time-to-Market (о чём мы уже говорили подробно), Digital Business Continuity & Security (защищённость и непрерывность цифрового бизнеса), Compliance (соответствие требованиям регулятора), Software Development Maturity (зрелость процесса разработки). Все эти параметры составляют общую ценность от внедрения безопасной разработки.

◆ «Вторым слоем» пирамиды мы представляем себе управленческий уровень (Management). На нём расположены метрики, на которые влияет управленческая команда проекта. Например, менеджмент контролирует time-to-market для определённого релиза, покрытие продуктовых команд практиками Application Security, устранение уязвимостей в программном продукте и т.д.

◆ Операционный уровень (Operations) — информационный слой, являющийся производным от параметров телеметрии. В зоне ответственности операционного уровня такие метрики, как объём технического долга, плотность дефектов, среднее время жизни дефекта и т.д. Параметры этого уровня, как правило, контролируются на уровне отдельных команд (рис. 2).

◆ База пирамиды — уровень телеметрии (Telemetry) — это вся информация, которая поступает от сканеров из DevOps- или CI/CD-процессов, из репозиториев исходного кода и артефактов сборки. Это гигантский объём данных, с которым работает команда. Но все они нуждаются в структуре и приоритизации — без этого невозможно подняться на уровень выше. Мы собираем информацию в специально разработанном и структурированном хранилище. Интерпретация и представление данных в виде удобных и понятных диаграмм на дашбордах для разных уровней управления — это фишка AppSec.Hub. Этот продукт позволяет реализовать полноценный подход Data Driven к управлению DevSecOps-процессом, эффективность которого будет только расти по мере усиления роли и функционала AI-инструментов.

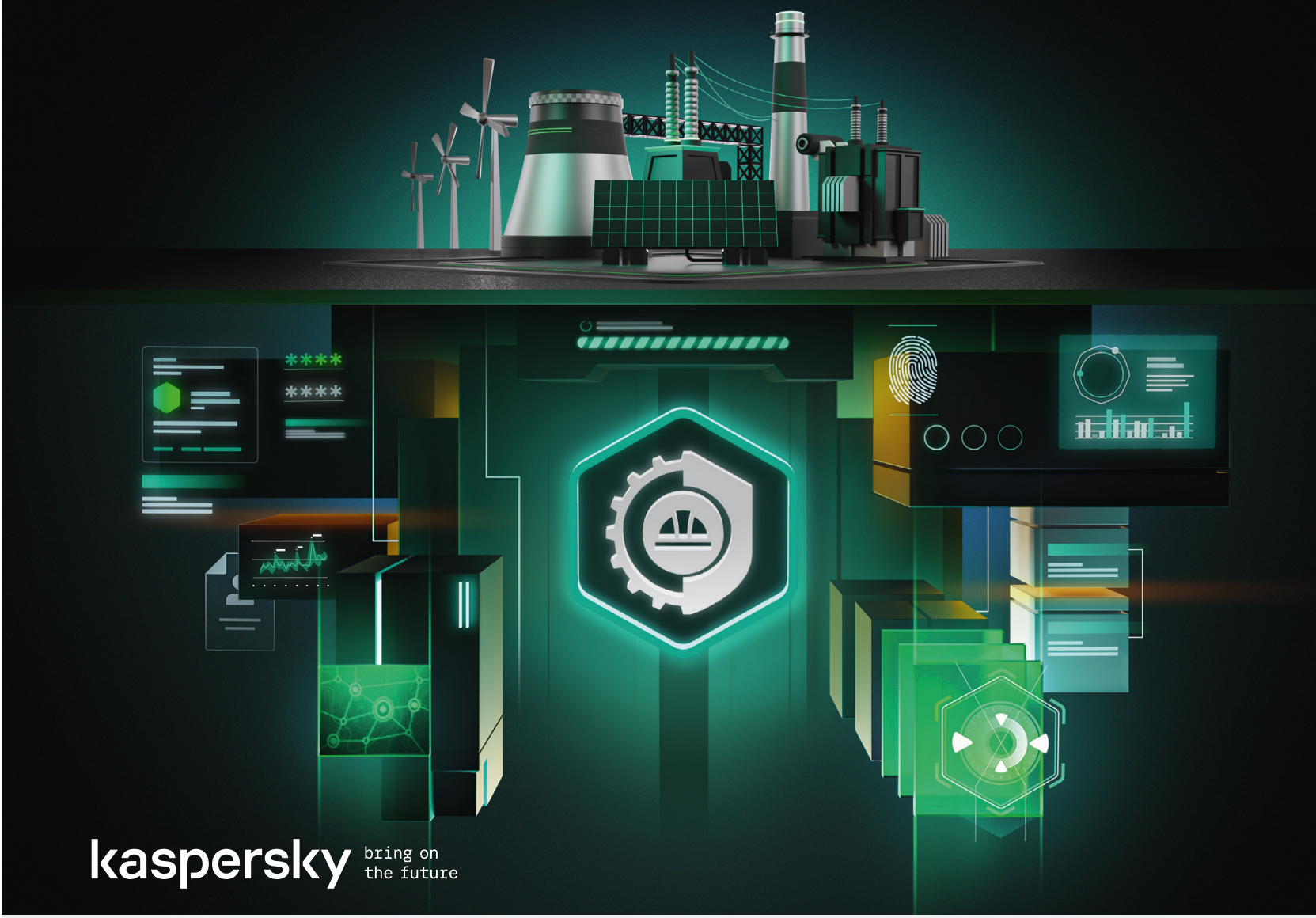
* * *

Разработка безопасного программного обеспечения является неотъемлемой частью современного бизнеса, независимо от его масштабов и сферы деятельности. Анализ ситуации на рынке показывает, что игнорирование вопросов информационной безопасности может привести к колоссальным экономическим потерям и утечкам данных, что ставит под угрозу не только бизнес, но и доверие клиентов. Применение принципов DevSecOps и Shift Left в процессах разработки закономерно приводит к снижению рисков и затрат на исправление уязвимостей. При этом ASPM-решения становятся гибкими инструментами, которые помогают организациям измерять, управлять и улучшать безопасность приложений в течение всего жизненного цикла разработки.

Кибербезопасность полного цикла

Kaspersky
OT CyberSecurity

Kaspersky OT CyberSecurity для промышленной кибербезопасности. Защита каждого элемента инфраструктуры: от оборудования и АСУ ТП до информационных систем



kaspersky bring on the future

ДиалогНаука

СИСТЕМНАЯ ИНТЕГРАЦИЯ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

dialognauka.ru

ЭКСПЕРТОВ С НИЗКОЙ ОБРАЗОВАТЕЛЬНОЙ БАЗОЙ ЗАМЕНИТ ИИ

НО СПРОС НА ТАЛАНТЫ БУДЕТ ТОЛЬКО РАСТИ

Дарья ФИГУРКИНА
директор по талантам Swordfish Security

1 миллион человек — примерно столько профессионалов не хватает ИТ-отрасли России. В кибербезопасности этот дефицит ещё острее. Причин этому две. Во-первых, технологии развиваются быстрее образовательных программ, во-вторых, нет доступа к рынку ИТ-кочевников, которые находятся за пределами страны. Кибербезопасность, пожалуй, самая чувствительная отрасль в сфере разработки, поскольку её основная задача — обеспечить цифровую защищённость критической инфраструктуры и коммерческих компаний внутри России.

Дефицит кадров в отрасли будет только усугубляться. Число вакансий для узких специалистов, например для редчайших ML-инженеров, за последний год стало больше на 53% (по данным hh.ru — *прим. автора*), а зарплатное предложение для ИБ-инженеров за год подросло на 1/5. Сложное время для HR, зато потрясающее — для молодых и талантливых инженеров, которые только входят в профессию, ведь для них сегодня открыты все двери, в них готовы инвестировать работодатели и доращивать их внутри своих команд. Пожалуй, DevSecOps наименее требовательна к базовому образованию за счёт высокой мобильности внутри профессии.

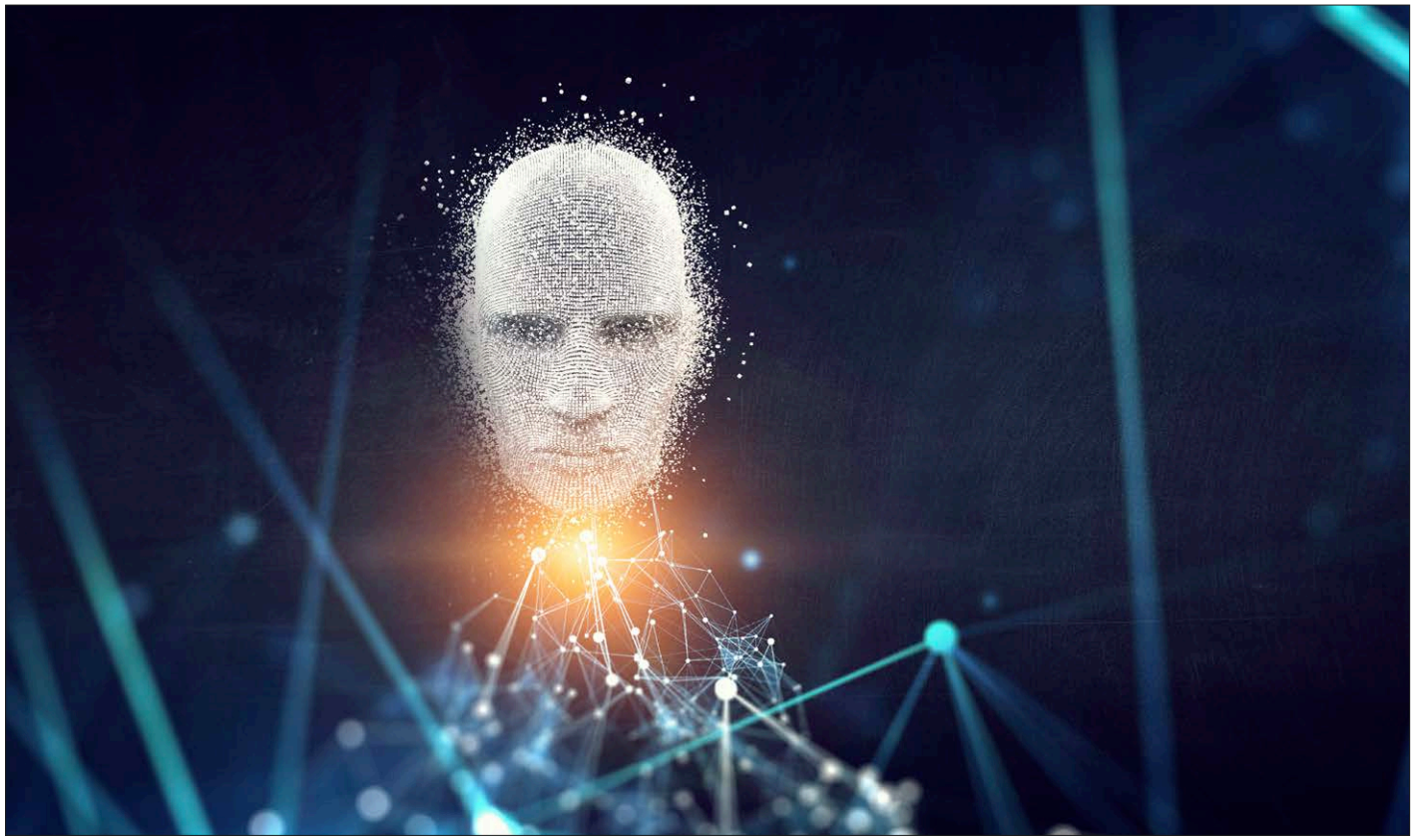
У нас в компании работает определённое количество студентов 3–4-го курса. Молодые люди начинают карьеру без отрыва от учёбы на 0,5 ставки, за год или два вырастая в высококлассных инженеров. В прошлом году мы наняли человека, который окончил первый курс, но он гений и уже работает на равных. Взять и выучить под себя — это очень логично, сегодня студенты технических вузов не борются за место на рынке труда, потому что это рынок борется за них. Глобально у этого тренда есть серьёзный минус: в долгосрочной перспективе такой быстрый взлёт может привести к просадке качества работы в ИБ.

Впрочем, мы находимся, на мой взгляд, на пороге очередной цифровой революции, которая всё изменит. Драматично рынок DevSecOps, да и ИТ в целом трансформирует массовое внедрение генеративного искусственного интеллекта, который возьмёт на себя простые задачи, которые можно чётко сформулировать. Это сильно скорректирует рынок труда в нашей сфере. Просто хороший код будет писать модель. Приведу простой практический пример: уже сейчас наши коллеги используют модель AppSec.CoPilot на основе ИИ, чтобы в автоматическом режиме анализировать и сортировать уязвимости, определять ложные срабатывания. Практика показала, что его точность 96%. Таким образом получается сэкономить рабочее время команды из 5 инженеров, которые потратили бы на этот процесс 8000 часов в год.

Человеческие ресурсы будут востребованы для более творческих задач. Чтобы оставаться ценным, ты должен уметь создавать. Техническую революцию успешно переживут талантливые инженеры, которые готовы развиваться, способные на глобальное мышление. Самым ценным станет то самое helicopter view, которое достаточно сложно в себе развить, не имея хорошего фундаментального образования. Которое, к моему сожалению, не успевают получить быстро развивающиеся в профессии молодые инженеры, а вузы не успевают трансформировать программы под современность.

Ещё один тренд: рынок соискателя, а в ИТ-отрасли сегодня именно он, предполагает, что выбор условий остаётся на стороне работника. Примером служит удалёнка, которая прочно вошла в нашу жизнь в пандемию и из жизни ИТ никуда больше не ушла. От 60 до 70% сотрудников, если мы говорим об инженерах, остаются на удалёнке. Это открывает возможности для подбора, потому что ты не привязан к поиску в Москве, талантливые инженеры могут работать с кодом в Красноярске, Калининграде и Мурманске. Мой личный топ (кроме очевидных МГТУ им. Баумана и МФТИ) возглавляет Сибирь, поскольку там есть вузы, которые дают качественное фундаментальное техническое образование. Это расширяет возможности для найма, поскольку удалёнка из тренда переросла в норму.

Ещё один тренд — более открытая индустриальная среда. Работодателю приходится учитывать личные планы на профессиональное развитие членов команд и давать им свободу



творчества. Сегодня одно из обязательных условий привлечения хороших ИБ-инженеров — команда экспертов, в которой есть у кого и чему научиться, готовая поддерживать инициативу и воплощать новые идеи. Руководить директивно «сверху» уже не получится. Чтобы успешно работать на рынке кибербезопасности, важно умение объединять профессионалов вокруг общей идеи и быть открытыми к тестированию гипотез. Бонус — мы получаем среду, которая непрерывно улучшает сама себя.

Чтобы эта система состояла из звеньев, каждое из которых достаточно автономно, чтобы привнести нечто новое и полезное, но при этом заряжено общей целью, стандартный цикл сотрудника начинается с анализа предыдущего опыта кандидата. Глядя на резюме кандидата, даже если в нём нет пометки «ищет работу», можно определить траекторию его развития и понять, какой проект можно было бы ему предложить, что могло бы стать логичным этапом его развития, и сопоставить это с актуальным запросом компании. Таким образом, мы не просто нанимаем в команду единицу, «винтики», а находим того, с кем совпадают наши цели и ценности. А дальше наша задача — создать условия, чтобы таланты могли проявиться в полной мере.

Когда речь идёт о сравнительно небольшой команде экспертов в узком сегменте РБПО, можно позволить себе роскошь выбирать и растить. Но рынок, где требуются специалисты по кибербезопасности, гораздо больше. Они востребованы на производстве, в финансовых и ТЭК-компаниях, в сервисах электронной торговли, да и вообще везде. Это сотни тысяч сотрудников, которых сложно найти, ещё труднее привлечь и удержать. Кадровый голод частично решается за счёт аутстаффинга и построения центров компетенций в DevSecOps для коммерческих компаний. За последние три года спрос на эту услугу вырос многократно. Если говорить о Swordfish Security, то в семь раз. Мы начинали этим заниматься в 2022 году в рамках «Академии кибербезопасности», и если в первый год работы на счету команды было три готовых центра компетенций на стороне клиента, то в 2024-м их более 20, а количество заявок на порядок выше. К нам регулярно обращаются наши партнёры с запросом о подготовке лидеров команд кибербезопасности внутри компаний. Мы видим, что не только отдельные компании-эксперты, но и рынок в целом готов вкладывать в людей, которые смогут делиться своими знаниями о разработке безопасного ПО со своими коллегами и вдохновлять их на развитие.

* * *

Технологии развиваются так быстро, что просто переждать кадровый голод в кибербезопасности, перекрывая его исключительно разовыми аутсорсинговыми услугами, уже не получится. Культуру кибербезопасности предстоит развивать во всех отраслях экономики, а значит, и кадры для неё выращивать. Дорогу осилит идущий, а в пункт назначения первыми доберутся те, кто делает серьёзные шаги уже сейчас.

«ГОРЕСТИ И РАДОСТИ» ПРАКТИЧЕСКОГО РБПО

ВЗГЛЯД РБПО-СООБЩЕСТВА ФСТЭК РОССИИ И ИСП РАН

Дмитрий ПОНОМАРЁВ
НТЦ «Фобос-НТ» / ИСП РАН / МГТУ им. Баумана
Интересы: аудит и консалтинг построения процессов безопасной и качественной разработки ПО, анализ поверхности атаки

В этой подборке опытом «удивительных открытий» и решений практических задач в области безопасной и качественной разработки поделятся коллеги — известные в сообществе инженеры — рангом от руководителя направления до владельца компании. Мы подобрали палитру рассказчиков так, чтобы охватить максимум различных технологических профилей — чтобы и сами истории, и стилистика их рассказа оказались интересны и полезны широкому кругу специалистов.

К числу моих любимых историй относится опыт разбора поверхности атаки с одним из заявителей на сертификацию. В ходе первичного анализа программно-аппаратного решения мы обнаружили там полноценный Jabber-сервер, написанный на C++. На вопрос «Зачем вам это в сертифицируемом продукте в 2022 году?» последовал ответ: «Да просто N лет назад какой-то один клиент попросил включить «за копеечку», ну, мы и включили, а в чём дело?» Далее последовала моя минилекция о стоимости и целесообразности фаззинг-тестирования сетевого Stateful-протокола в рамках и так горящей сертификации, в ходе которой верное решение — «Доктор сказал: резать» — было принято через 15 минут. Мораль истории проста: убирайте из состава вашего продукта весь непрофильный «для бизнеса» код, особенно код сетевых сервисов, формирующих поверхность атаки. Особенно в случае получения вашего первого сертификата соответствия. Пара недель на рефакторинг смогут сэкономить вам месяцы работы и миллионы рублей трудозатрат, не говоря уже о повышении защищённости продукта.

Ещё одна забавная (и типичная для отрасли) история, непосредственным участником которой являлись я сам и наши друзья из «Айдеко», опубликована ранее и доступна по ссылке (см. врезку в разделе «Выводы») [https://www.itsec.ru/articles/kak-pravilno-organizovat-process-bezopasnoj-razrabotki-po-sdl-6-shagov].

Желаю всем приятного и интересного «РБПО-шного чтива»!

Дмитрий СОРОКИН
технический директор компании «Базис»

На этапе внедрения безопасной разработки в наши продукты и проведения первичного аудита безопасности и качества кода наша команда инженеров столкнулась с неожиданной находкой: анализ выявил критические уязвимости в 150 библиотеках одного продукта. А до окончания спринта и выхода в релиз оставалось всего две недели. После проведённого анализа потребовалось выяснить, откуда взялось такое количество уязвимостей и как их исправить в такой короткий срок. На проведённом митинге с командой разработки после долгого разговора выяснилось, что все библиотеки относились к части неиспользуемого, устаревшего кода, о котором все, естественно, благополучно позабыли, пользуясь правилом «работает — не трогай».

Таким образом, просто избавившись от ненужного придатка в продукте, команда доблестно выявила критические уязвимости и также не менее доблестно их закрыла одним движением руки. С того момента команда разработки не оставляет устаревший код, но команда инженеров по безопасной разработке пристально за этим следит. А с появлением в нашем арсенале инструментов, созданных инженерами ИСП РАН и CodeScoring, мы повысили контроль за качеством и безопасностью нашего кода и выпускаемых нами продуктов. Это, в свою очередь, гарантирует надёжность и безопасность продуктов компании «БАЗИС».

https://corp.cnews.ru/news/top/2025-01-24_rossiyane_ispravili_pochti

Николай КОСТРИГИН
руководитель отдела БРПО, компания «Базальт СПО»

Интересы: развитие свободного ПО в целом и повышение доверия к нему в частности

Согласно укоренившемуся в сообществе РБПО тезису «Заимствованный код — твой код!», команда «Базальт СПО» постоянно проводит исследования программных пакетов, входящих в репозиторий свободного ПО «Сизиф» и его стабильные бранчи. Работа ведётся как самостоятельно, так и в кооперации с другими компаниями-разработчиками. Используется широкий арсенал свободных и проприетарных инструментов.

Не так давно сотрудничество в рамках Центра исследований безопасности системного программного обеспечения привело к интересному случаю, существование которого предполагалось, но на практике мало кто встречал. При исследованиях кода Qemu фаззингом было выявлено падение, получившее оценку серьёзности 6.6 по CVSS 3.1. Разработанный патч готовился к отправке в апстрим Qemu, когда выяснилось, что такое же исправление уже подготовлено другой компанией — участником консорциума, но как результат анализа срабатывания статического анализатора. Получился своего рода «выстрел Робин Гуда».

Интересные случаи, связанные с безопасностью свободного ПО, встречались в проекте «Сизиф» и раньше. К примеру, в отношении CVE-2017–1000408 и CVE-2017–1000409. При анализе кода библиотеки GNU libc, используемой в операционных системах «Альт», на подверженность этим уязвимостям выяснилось, что они были устранены в ней превентивно ещё в 2001 году.

Вообще говоря, принимая участие в разработке и доработке проектов СПО, мы относимся к РБПО-исследованиям не как к неизбежной, навязанной кем-то обузе, но как к возможности погрузиться в исходный код проекта, узнать его глубже изнутри.

Андрей КУЗНЕЦОВ
руководитель Центра внедрения и развития практик РБПО НТЦ «Фобос-НТ»

Интересы: построение комплексных РБПО-процессов и последующая сертификация СЗИ

Современные испытательные лаборатории, желающие соответствовать актуальным отраслевым стандартам, требованиям и стремительно меняющейся нормативной документации, неминуемо превращаются в «настоящие ИТ-компании» со спринтами, беклогами и пэйплайном. Эксперты лаборатории из классических «бумажных безопасников», всё больше становятся похожи на настоящих инженеров-исследователей, а сами лаборатории сталкиваются с суровой реальностью жизненного цикла разработки: если процесс не автоматизирован, его системно не существует. Автоматизация процессов тестирования ПО имеет первостепенное значение, поскольку обеспечивает, среди прочего, доступность информации о результатах тестирования для всех заинтересованных сторон, а так же воспроизводимость его результатов, не говоря о кратном ускорении процесса испытаний.

Комплексный подход к тестированию разрабатываемого ПО — это то, чего требует регулятор от компаний-разработчиков средств защиты информации именно сейчас. В частности, внедрения в жизненный цикл разработки программного обеспечения практик статического и динамического анализа (в том числе фаззинг-тестирования), что позволяет находить дефекты кода на ранних стадиях разработки. А это, в свою очередь, способствует повышению надёжности и стабильности работы ПО, многократному снижению затрат на экстренные исправления проблем «ушедших в прод».

Когда-нибудь эксперта лаборатории заменит бездушный и беспристрастный робот, но пока этого не случилось, экспертам необходимо автоматизировать свою деятельность и самостоятельно вживлять себе «кибернетические руки». Одним из процессов, который нам приходится автоматизировать, является фаззинг-тестирование — полезная, но нетривиальная практика, особенно если её выполняют разрозненные группы инженеров на своих ноутбуках. При такой организации деятельности даже простой сбор артефактов превращается в настоящее испытание.

Несколько раз обжёгшись, мы решили организовать собственный конвейер фаззинг-тестирования, автоматизирующий этапы: подготовки набора входных данных; запуска реализованных фазз-тестов; заведения задач по исправлению дефектов кода. Заручившись поддержкой и вычислительными мощностями коллег из ОрлГУ, начали изобретать свою «кибернетическую руку», использующую более 400 процессорных ядер и 500 Гб оперативной памяти. Как результат, уже за первый месяц пилотной работы конвейера многократно увеличилось количество обнаруженных дефектов кода, а число направленных в апстрим патчей (в т.ч. устраняющих уязвимости) исчисляется десятками: *https://fobos-nt.ru/novyie-dostizheniya-v-staticheskom-i-dinamicheskom-analize.html*

Антон ГАВРИЛОВ
владелец продукта Axel PRO

Интересы: безопасная разработка / разработка безопасного ПО и всё, что с ней связано

Многие в разговорах про безопасность видят только «лишения» и «ограничения». Однако зачастую практики РБПО могут помочь и разработчикам.

Знание объекта защиты — одна из самых базовых и важных вещей в информационной безопасности. Так же и с разработкой безопасного ПО. Важно понимать, из чего оно состоит, и по возможности минимизировать количество «лишних» компонентов. При этом важно не забывать, что «чужого кода» не существует: всё, что есть в ПО, оно «ваше».

Мне довелось участвовать в процессе сертификации достаточно «массивного» ПО, в котором присутствует очень много различных сервисов, работающих вместе, как единый организм.

В процессе изучения пакетов и образов контейнеров мы с разработчиками выяснили, что:

- для сборки многих образов используются похожие базовые образы; именно что похожие: golang:1.20.7, golang:1.20, golang:1.20.6, golang:1.20.14 и т.д.;
- в дистрибутиве содержатся образы, которые более не используются для корректной работы ПО;
- в дистрибутиве содержатся пакеты и образы разных версий, некоторые из которых не используются вовсе.

Почему это так? Ответ, как и всегда: «Исторически так сложилось». Да, где-то «недосмотрели», где-то «забыли», где-то «не знали».

В той выборке, о которой я говорил, суммарно получилось около 3000 разных пакетов в базовых образах контейнеров. Да, уникальных было в разы меньше, но как всё это поддерживать и анализировать, непонятно.

Было принято решение «всё почистить» — по возможности привести все базовые образы к единому «знаменателю», удалить ненужное и оставить только то, что реально используется.

В итоге осталось несколько базовых образов (ввиду специфики их «содержания»), а количество пакетов в них — не более 250 штук. Аналогичная ситуация (пусть и с меньшим «разбросом») получилась и с пакетами дистрибутива.

Да, классическая «инвентаризация», с которой начинается (практически) любая книга по информационной безопасности. Такой подход позволяет не только повысить уровень ИБ за счёт «отсечения лишнего», но и помогает разработке: вместо того чтобы поддерживать n базовых образов, можно поддерживать один и быть уверенным в том, что именно передаётся конечному пользователю и с какой версией.

Анатолий КАРПЕНКО
инженер по автоматизации, Luntry

Интересы: программная инженерия, безопасность ПО во всех её аспектах, надёжность ПО

В любой момент, всегда есть уязвимости, вероятность наличия НДВ, нежелательной функциональности. Этого не нужно бояться, нужно принять как факт и уметь работать в такой ситуации. Один из примеров — случай с CNI Calico. Проблема заключалась в том, что по умолчанию он отправлял телеметрию из инфраструктуры клиента своим разработчикам. Это было обнаружено совершенно случайно.

В этом и подобных случаях достаточно поправить флаги конфигурации запуска, но есть ещё куча других менее известных и документированных проектов, которые затаскивают разработчики к себе. Как они ведут себя, не очень очевидно, и это всё может привести к компрометации данных клиента. Поэтому к любому коду, как своему, так и стороннему, надо относиться с недоверием и выстраивать ZeroTrust-инфраструктуру.

Одним из подходов является уменьшение поверхности атаки и следование принципу наименьших привилегий, например, с помощью контейнеров. Оркестратор контейнеризированных приложений (например, Kubernetes) позволяет не только применить харденинг для самого контейнера (запретить запуск недоверенных файлов, сделать файловую систему доступной только на чтение и ограничить права пользователя), но и сделать ограничения на уровне самого оркестратора (настроить сетевые политики, мандатный доступ и т.д.). Экосистема вокруг контейнеризации позволяет организовать детектирование подозрительной активности, реакцию на неё, а в некоторых случаях вообще предотвратить её появление.

А как насчёт парадокса: безопасного ПО нет, а безопасная разработка есть? Тут все процессы надо внедрять, так как синергия безопасной разработки с безопасной эксплуатацией даёт максимальный успех, ведь всё это делается не ради процесса, а ради конечного результата.

Всем РБПО!

Алексей СМИРНОВ
основатель
CodeScoring

Интересы: полезные инструменты анализа ПО

100 УЯЗВИМОСТЕЙ В ГОД

Мы у себя в CodeScoring постоянно собираем и проверяем информацию про мировой Open Source. Эти данные нужны для защиты цепочки поставки и повышения точности композиционного анализа ПО. Собираем данные про сами компоненты (библиотеки) и их свойства, например: информация про уязвимости, патчи, эксплойты, а также данные о версиях, авторах компонентов, датах релизов и пр. Эти данные мы обрабатываем и зачастую узнаём много интересного, чем было бы полезно поделиться с сообществом.

В частности, мы постоянно строим и анализируем SBoM от множества открытых проектов. SBoM — перечень компонентов ПО, в котором указываются их версии и дополнительная информация об уязвимостях и условиях использования (лицензиях). В России он называется ППК — перечень программных компонентов.

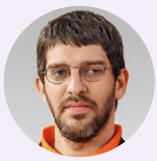
Однажды сформировав для своего ПО такой перечень, возможно проводить его актуализацию и следить за тем, какие уязвимости были обнаружены уже после того, как вы включили сторонний компонент к себе «под капот».

С одной стороны, формирование такого списка помогает более удобным образом следить за тем, сколько всего стороннего и с какими проблемами мы поставляем нашим заказчикам. С другой стороны, после выпуска даже самого «чистого» и безопасного продукта нет гарантии, что в сторонних компонентах со временем не обнаружатся новые проблемы. Поэтому ППК следует перестраивать (обогащать) и следить за новостями.

Наши последние расчёты показали, что в среднем ПО без обновлений за один год накапливает 100 (сто!) новых уязвимостей, из которых 10–15 являются эксплуатируемыми.

Отсюда следует логичный вывод, что, оценивая безопасность ПО, которое вы хотите использовать у себя, достаточно познакомиться с его динамикой релизного цикла. Если релизы раз в полгода, то есть над чем задуматься.

Следить за подобными проблемами помогает понятие композиционного анализа, которое было поставлено в один ряд со статикой и динамикой в обновлённом стандарте по безопасной разработке (ГОСТ Р 56939–2024). Верим, что осознанность использования сторонних компонентов и практики безопасной работы с ними будут только усиливаться.



Марк КОРЕНБЕРГ
технический директор
ООО «Айдеко»

Интересы: сноуборд, путешествия, инвестирование

В «Айдеко» мы ответственно подходим к кодовой базе, её минимизация и анализ занимают важную роль в процессах разработки безопасного ПО, и эта работа проводится нами самостоятельно, без давления со стороны регуляторов.

Так, во время сертификационных испытаний межсетевого экрана Ideco UTM специалисты «на спор» решили поискать интерпретируемый код и, что удивительно, нашли два избыточных интерпретатора, хотя главный архитектор был уверен, что ничего, кроме Python-кода, в составе дистрибутива нет. Ими оказались не используемый нигде Perl, который подтягивался из-за зависимостей, а ещё движок Mozjs из состава Firefox, который использовался для системы конфигурации очень популярного демона Policykit. В этом демоне конфигурация пишется на JS, а сам демон отвечает за систему раздачи прав пользователям и работает с root-привилегиями! В итоге Perl удалили из системы с помощью патчей компонентов, убирающих ненужную функциональность, и добавили проверку, чтобы он гарантированно не мог быть установлен. А PolicyKit переписали на Python, тем самым сократив кодовую базу. Такой подход позволил существенно упростить прохождение сертификационных испытаний.

Во время аудита и предварительной подготовки к сертификации процессов безопасной разработки мы нашли то, чего не должно быть в продукте (речь идёт о программе-агенте для рабочих станций), а именно библиотеки libGLX и libOpenGL. Это было похоже на настоящие археологические раскопки, и оказалось, что корень проблем — неверно собираемый фреймворк Qt, который по зависимостям притягивал много библиотек, без которых вполне можно обойтись.

Без использования OpenSource ПО написать современное решение невозможно. Но и с ними — опасно, поэтому регулярное устранение ненужной кодовой базы, обновление, различные виды анализа системы и кода, тщательный выбор компонентов и поставщиков ПО — это необходимость для безопасной разработки программного обеспечения в условиях увеличения функциональности продукта и роста команды разработки.

РБПО — МОДНЫЙ ТРЕНД ИЛИ НЕОБХОДИМОСТЬ?

ДИСКУССИИ НА ЭТУ ТЕМУ ПОДНИМАЮТ УРОВЕНЬ КУЛЬТУРЫ ИБ

Вячеслав ПОЛОВИНКО
руководитель направления собственных продуктов АМТ-ГРУП

В течение последних двух лет практически ни одно мероприятие или конференция по информационной безопасности не обходится без обсуждения вопросов разработки безопасного программного обеспечения. В профессиональном сообществе уже даже устоялся термин РБПО. Термин, во избежание множества толкований, был уточнён и зафиксирован в новом ГОСТ 56939–2024 как «содержание и порядок выполнения работ, связанных с созданием безопасного программного обеспечения и устранением выявленных недостатков, в том числе уязвимостей ПО».

Можно говорить, что РБПО — это процесс создания программного обеспечения, который включает в себя меры по обеспечению безопасности кода на всех этапах его жизненного цикла. Это актуально, несмотря на то что в вышеупомянутом ГОСТ 56939–2024 прямо отмечается, что *«поскольку модель жизненного цикла ПО зависит от специфики, масштаба, сложности ПО и условий, в которых ПО создаётся и функционирует, приведённые в ...стандарте процессы намеренно не связываются с конкретной моделью жизненного цикла ПО».*

Но, к сожалению, терминологические нюансы являются самой меньшей из проблем при внедрении РБПО.

Многие компании и отдельные команды разработки, даже те, которые напрямую не связаны с производством средств защиты, уже получили от своих заказчиков, внутреннего менеджмента и даже подразделений маркетинга требования к максимально оперативной организации РБПО. Причём часто срок реализации этих требований выходит за рамки разумного, вызывая только раздражение и негодование у исполнителей. С одной стороны, внедрение РБПО преподносится как очевидное и всеобщее благо. С другой стороны, процессы и процедуры его внедрения предлагаются настолько сжатыми по времени и ресурсам, что часто вызывают лишь удивление.

Попробуем разобраться, в чём же состоят сложности оперативного внедрения РБПО (далее «безопасная разработка») в жизнь обычного коллектива, команды или компании. Можно выделить несколько причин, почему компании не спешат внедрять безопасную разработку в свои процессы:

1. Сложность внедрения и отсутствие общедоступных полных и наглядных стандартов и рекомендаций. Внедрение безопасной разработки требует изменения существующих процессов разработки и эксплуатации, а также обучения сотрудников новым методам работы. Это может быть сложным и длительным процессом. Процесс требует квалифицированного менеджмента, инвестиций и должен опираться не просто на требования стандартов, а на примеры реализаций, референсные архитектуры и паттерны взаимодействия нескольких программных, а иногда и аппаратных решений. Не имея таких примеров, многие коллективы считают её чем-то слишком дорогим, организационно и технически сложным. Несмотря на появление очередного ГОСТ, конкретные практики внедрения безопасной разработки найти крайне сложно. Ещё сложнее собрать конвейер программных и технических средств, вычислительных мощностей, средств ИБ с учётом производства конкретного продукта. Отсутствие готовых решений затрудняет и замедляет процесс внедрения и вызывает справедливые опасения у тех команд, которые ещё только в начале пути.

2. Отсутствие понимания преимуществ и неопределённость результатов. Некоторые компании не понимают, какие конкретно преимущества на практике им даст внедрение безопасной разработки. Рассматривают культуру безопасной разработки просто как ещё один модный тренд, который не принесёт реальной пользы на практике. Особенно это актуально для компаний, чья технологическая экспертность сосредоточена в основном в отраслевых знаниях. Речь идёт о разработчиках АСУ

ТП систем, SCADA-систем, систем, применяемых в энергетике, продуктов в сфере консультационных услуг, программно-аппаратных решений «полевого уровня», IoT-решений. То есть таких решений, где надёжность функционирования и промышленная безопасность, точность получаемых данных ранее всегда превалировала над информационной безопасностью. Как и с процессами управления рисками, результаты внедрения безопасной разработки могут быть неопределёнными на старте, отложенными и часто неподтверждаемыми до тех пор, пока не наблюдаются конкретные инциденты безопасности в отношении разрабатываемого ПО. Часто компании опасаются, что они вообще не получат никаких результатов или что результаты будут достигнуты слишком медленно. Внедрение РБПО не воспринимается как что-то, что напрямую может увеличить прибыль, потому что в лучшем случае приводит к реализации нефункциональных требований продуктов, которые «продать рынку достаточно тяжело».

3. Сопротивление изменениям и страх перед ошибками. Любые изменения в процессах разработки и эксплуатации программного обеспечения могут вызвать сопротивление со стороны сотрудников. Специалисты могут опасаться, что внедрение новых методов работы приведёт к увеличению нагрузки или снижению их производительности. Более того, на первых этапах внедрения безопасной разработки именно так и происходит, что только подтверждает аргументы противников изменений. Несовершенство применяемых конвейеров сборки и систем тестирования, интеграционные проблемы на пути внедрения лишь добавляют в эту копилку свои аргументы против. Команды, менеджеры и отдельные специалисты могут бояться совершить ошибки при внедрении безопасной разработки. Ожидают, что новые процессы приведут к снижению безопасности их систем, навредят репутации, снизят прибыль. Эта проблема также актуальна в том случае, когда в уже существующие, хорошо отлаженные производственные конвейеры привносятся новые инструменты, решения, процессы.

4. Недостаток ресурсов. Внедрение безопасной разработки может потребовать дополнительных ресурсов, таких как время, деньги, квалифицированные специалисты, аппаратные мощности. Не все компании готовы выделить эти ресурсы. Чаще всего внедрение безопасной разработки воспринимается как ещё одна обязанность текущих команд. Делаются попытки автоматизировать дополнительно возникающие операции путём подбора «готового» программного обеспечения без какой-либо адаптации.

5. Необходимость пересмотра архитектуры системы. Часто архитектура разрабатываемых систем унаследована, закладывалась одним или несколькими ключевыми специалистами с учётом актуальных на момент проектирования задач (то есть «в прошлом»). Аспекты Security by Design могли откладываться на второй план или закрываться типовыми решениями: применением компонентов с открытым исходным кодом, базовыми фреймворками. В результате, когда для внедрения безопасной разработки необходимо пересмотреть архитектуру системы и внести в неё изменения, направленные на повышение уровня безопасности, это, с одной стороны, встречает сопротивление некоторых ключевых специалистов, а с другой — приводит к дополнительным затратам времени и денег. В ряде случаев внедрение РБПО вырождается в полный демонтаж старой архитектуры разрабатываемых систем.

6. Проблемы с интеграцией на организационном уровне и уровне корпоративной культуры. В основе идеи безопасной разработки лежит комплексная интеграция процессов разработки, эксплуатации и обеспечения безопасности в целом. Однако, как и в случае с унаследованной архитектурой систем, ряд новых процессов и систем не может быть внедрён в компании просто потому, что это может организационно, технологически и даже этически противоречить тем процессам, которые функционируют в организации сейчас. В разных компаниях могут существовать разные культурные нормы и ценности, правила, которые влияют на отношение к изменениям в целом и к вопросам защиты данных, применению средств защиты, разграничению доступа. В некоторых компаниях в принципе принят более консервативный подход к изменениям, что также замедляет внедрение безопасной разработки.

Однако вне зависимости от обозначенных ограничений, похоже, у внедрения процессов безопасной разработки в деятельность практически каждой организации-разработчика ПО нет альтернатив. С развитием технологий и увеличением количества киберугроз обеспечение безопасности разрабатываемого ПО становится всё более актуальной задачей. С внедрением процессов безопасной разработки компании смогут быстрее и эффективнее обнаруживать и устранять уязвимости в своих системах. Это позволит организациям снизить риски кибератак, защитить свои данные, системы и репутацию. Кроме того, уже очевидно, что безопасная разработка поможет компаниям соответствовать требованиям законодательства и стандартов безопасности, которые, как мы видим, ужесточаются с каждым днём.

* * *

Дискуссии по теме безопасной разработки, которые идут на рынке, уже сейчас способствуют развитию культуры безопасности в компаниях. Благодаря таким дискуссиям разработчики, менеджеры, заказчики, операторы систем и эксплуатирующие организации, да и сами специалисты ИБ лучше понимают важность обеспечения безопасности в своих продуктах.

ЗАВИСИТ ОТ ЦЕЛИ

ОЦЕНКА ПРОЦЕССОВ РАЗРАБОТКИ БЕЗОПАСНОГО ПО

Антон СВИНЦИЦКИЙ
директор по консалтингу
АО «ДиалогНаука»

Сергей КАНИВЕЦ
ведущий консультант отдела
консалтинга АО «ДиалогНаука»

Безопасность программного обеспечения (ПО) играет критически важную роль в условиях современной цифровой экономики. Регулярные кибератаки, утечки данных и нарушения конфиденциальности негативно влияют как на коммерческие организации, так и на государственные структуры. Одним из ключевых факторов повышения уровня защиты является корректная организация процессов разработки безопасного ПО. Однако разработка безопасного ПО — это не только внедрение технических мер защиты, но и организация процесса с акцентом на управление рисками, соответствие требованиям регуляторов и обучение специалистов. В данной статье рассмотрены основные методики и подходы к оценке процессов безопасной разработки.

МЕТОДИКИ ОЦЕНКИ ПРОЦЕССОВ РАЗРАБОТКИ БЕЗОПАСНОГО ПО

Оценка процессов разработки безопасного ПО является важным этапом для создания защищённых программных продуктов, направленным на проверку соответствия процессов современным стандартам, выявление слабых мест и разработку корректирующих мер. Сейчас уже существует множество подходов и инструментов для оценки зрелости процессов разработки, например OWASP SAMM, DevSecOps Maturity Model и Synopsys BSIMM, позволяющие не только оценить текущее состояние, но и наметить пути его улучшения. Рассмотрим особенности каждой из этих моделей.

OWASP Software Assurance Maturity Model (SAMM) — это нормативная или предписывающая модель, которая структурирует процессы разработки безопасного ПО. Она включает 15 практик, разделённых на пять бизнес-функций: Governance, Design, Implementation, Verification и Operation. Каждая практика состоит из двух потоков: A — «поверхностный» и B — «углублённый», что позволяет выбирать степень детализации. SAMM обеспечивает формализацию и измерение результатов, минимизируя затраты на оценку. Компания самостоятельно определяет целевой уровень зрелости в удобном для неё горизонте планирования: от одного до пяти лет. Для автоматизации оценки компания может использовать доступные инструменты, такие как SAMMwise или SAMMY.

OWASP DevSecOps Maturity Model (DSOMM) описывает практики, направленные на интеграцию безопасности в процессы разработки и CI/CD. Модель выделяет пять инструментов: Build and Deployment, Culture and Organization, Implementation, Information Gathering, Test and Verification, каждый из которых включает меры защиты, распределённые по пяти уровням зрелости.

Synopsys BSIMM — это описательная модель, базирующаяся на практике 130 организаций. Она состоит из четырёх доменов, каждый из которых включает три практики, разделённые на три уровня покрытия. BSIMM позволяет компаниям сравнивать свои достижения с общепринятыми в индустрии практиками, реализованными у лидеров рынка, а доступные инструменты облегчают процесс оценки.

КОНЦЕПЦИЯ ОЦЕНКИ ПРОЦЕССА РАЗРАБОТКИ БЕЗОПАСНОГО ПО

Центральное место в этой концепции занимает системный подход, который позволяет структурировать и интегрировать меры безопасности на всех уровнях. В основе такого подхода лежит идея цикличности и непрерывного совершенствования, что обеспечивает устойчивость к новым угрозам и адаптацию к меняющимся условиям.

Управление процессом безопасной разработки является основой для обеспечения системного подхода к защите программного обеспечения. Оно охватывает ключевые аспекты управления — от стратегического планирования до контроля и оценки соответствия, что обеспечивает комплексное внедрение мер безопасности на всех этапах разработки, в том числе позволяет оценить текущее состояние процессов по следующим направлениям:

- описание стратегии и планирование процесса разработки (так как эффективное управление начинается с формулирования стратегии, которая определяет долгосрочные цели

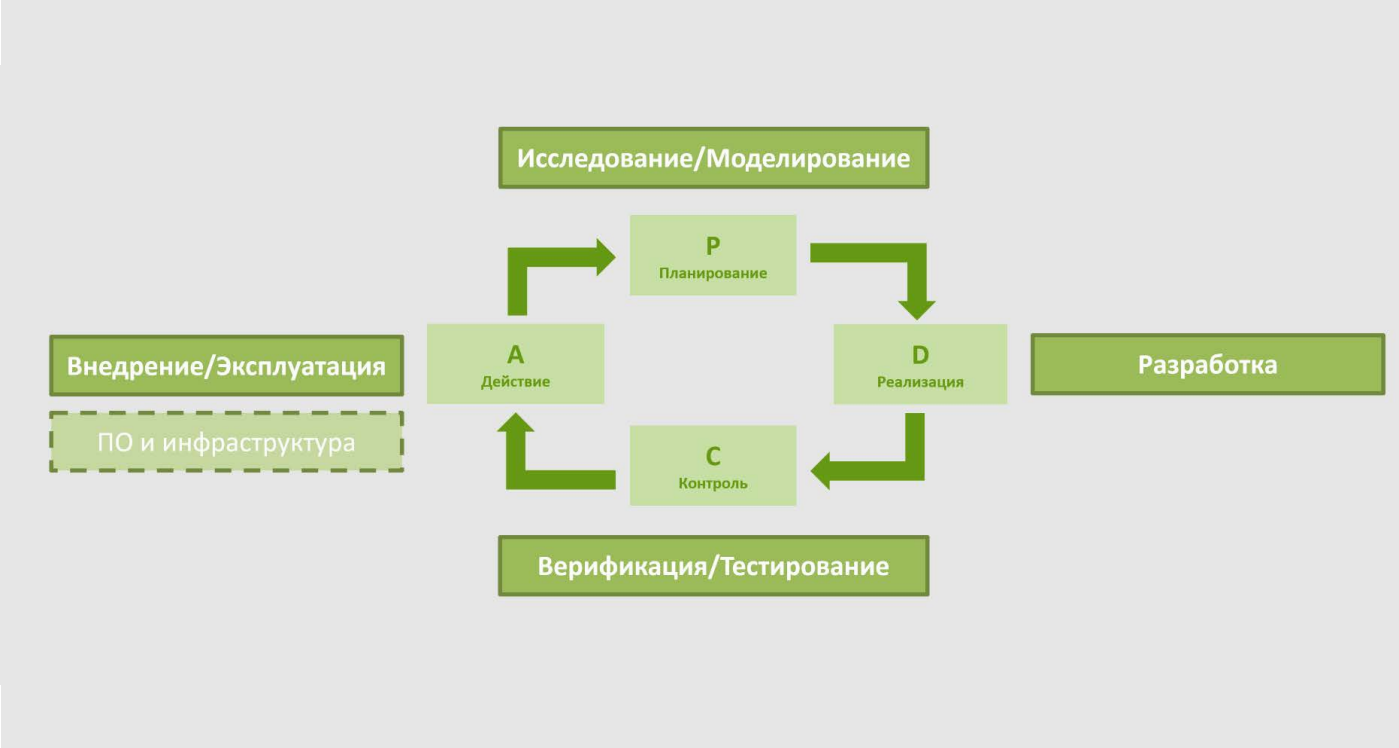


Рисунок 1. Соответствие элементов цикла PDCA мерам, относящимся к процессам безопасной разработки ПО

и задачи, в том числе в области разработки безопасного ПО);

- метрики эффективности (позволяют измерить и оценить текущий уровень безопасности разработки, а также отслеживать прогресс);
- повышение осведомлённости и квалификации (обучение персонала играет ключевую роль в предотвращении ошибок, связанных с безопасностью);
- контроль (контроль должен охватывать все аспекты процессов разработки и помогает обеспечить соблюдение установленных стандартов);
- оценка соответствия (эта часть включает проверку соответствия процессов безопасной разработки установленным стандартам и законодательным требованиям).

Цикл PDCA (планирование — реализация — контроль — действие) является универсальной моделью управления процессами, которая может быть применима и к процессам разработки безопасного ПО. В контексте обеспечения безопасности PDCA помогает систематизировать и интегрировать защитные меры на всех этапах жизненного цикла продукта (рис. 1).

Каждый элемент цикла включает набор ключевых мер и действий, по которым оцениваются процессы:

1. Планирование (PLAN) — этап исследования и моделирования:

- подготовка требований;
- моделирование угроз / оценка рисков;
- требования безопасности при использовании зависимостей;
- проектирование архитектуры.

2. Реализация (DO) — этап разработки ПО:

- управление конфигурацией ПО;
- требования к безопасности системы сборки и раскатки ПО;
- безопасность инфраструктуры разработки и тестирования;
- обеспечение целостности кода.

3. Контроль (CHECK) — этап верификации и тестирования:

- оценка архитектуры;
- анализ кода;
- тестирование защищённости.

4. Действие (ACT) — этап внедрения и эксплуатации:

- внедрение и эксплуатация (подготовка, доставка, вывод из эксплуатации);
- безопасность инфраструктуры (эксплуатация инфраструктуры ПО, тестирование на проникновение, управление уязвимостями, управление инцидентами).

ВЫВОДЫ

Выбор методики оценки зависит от целей организации: стремление достичь определённого уровня зрелости или соответствие международным стандартам. Использование моделей OWASP SAMM, DSOMM или BSIMM позволяет выявить слабые места в процессах и разработать долгосрочные стратегии совершенствования. Это обеспечивает соответствие требованиям безопасности, сокращает риски и укрепляет доверие пользователей. Представленная концепция возможна к применению и для новой редакции национального стандарта ГОСТ Р 56939–2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования».

Применение таких подходов делает процессы разработки ПО более надёжными и способствует достижению высокого уровня защищённости, соответствующего мировым стандартам.

ОБНОВЛЕНИЕ ОС «АЛЬТ СП» РЕЛИЗ 10

СЕРТИФИЦИРОВАННАЯ СУБД, ПОДДЕРЖКА СОВРЕМЕННЫХ ПРОЦЕССОРОВ «ЭЛЬБРУС»

Константин ГЕРАЩЕНКО
редактор «Базальт СПО»

«Базальт СПО» выпустила сертифицированное ФСТЭК России обновление операционной системы «Альт СП» релиз 10. В новую версию вошла сертифицированная СУБД PostgreSQL дополнительно к сертифицированным средствам виртуализации и контейнеризации. Появились сборки для процессоров «Эльбрус 2С3» и «Эльбрус 8СВ».

Согласно новым требованиям ФСТЭК России в состав операционной системы включены программные интерпретаторы (php, perl, lua, python, nodejs) и веб-сервер (nginx), прошедшие испытания по выявлению уязвимостей и недекларированных возможностей в ПО в соответствии с методикой ФСТЭК России.

Сертифицированная СУБД в составе ОС. В «Альт СП» включена система управления базами данных **PostgreSQL версии 16.6,** сертифицированная на соответствие приказу № 64 ФСТЭК России по 4 классу защиты. При этом защищенными являются не только одиночные установки СУБД, но и кластеры из нескольких баз данных.

Архитектуры, поддерживаемые «Альт СП». Сборки для архитектур x86_64 и aarch64 традиционно выпущены в исполнении «Рабочая станция» и «Сервер». В сборку для aarch64 добавлено ядро с поддержкой устройств на Rockchip 3588.

В обновленной версии появились сборки для рабочих станций для процессоров «Эльбрус 8СВ» и «Эльбрус 2С 3». Сборки для процессоров «Эльбрус 4С» и «Эльбрус 8С», созданные на основе 9-й платформы, входят в выпуск с ограниченной поддержкой (до августа 2026 года). Для тех, кто хочет перейти на релиз 10 для процессора «Эльбрус 8С», можно использовать образ для процессора «Эльбрус 8СВ».

Обновление установщика системы. В новой версии инсталлятор позволяет выбирать нужные приложения на этапе установки. Это упрощает первоначальную настройку системы, особенно для пользователей, которым нужна минимальная конфигурация для использования средств виртуализации или контейнеризации (рис. 1).

Добавлен режим OEM-установки, благодаря чему поставщики оборудования могут массово предустанавливать ОС на свои устройства.

Обновление средств управления контейнерами. По-прежнему используются инструменты **podman** (обновлен до 4.9.4) и **kubernetes** (обновлен до 1.31), доработан набор скриптов **podsec**: действия, которые раньше выполнялись вручную, теперь автоматизированы. В репозитории доступен набор пакетов kubernetes от версии 1.22 до 1.31, что позволяет пользователям плавно перейти к новому ПО.

Обновлены и входящие в состав «Альт СП» контейнеры. К набору контейнеров для разворачивания кластера kubernetes добавлены базовые контейнеры, в том числе и distroless-образы. Получить образы и их обновления также можно через сервис registry.altlinux.org (по тегу c10f2).

Обновление средств управления виртуальными машинами. Обновлена система виртуализации на основе Proxmox Virtual Environment (PVE). До 17 версии обновлена файловая система ceph — программная объектная сеть хранения, обеспечивающая как файловый, так и блочный интерфейсы доступа.

Добавлен модуль Linstor для управления блочными устройствами хранения данных. Linstor размещает тома для хранения данных и включает для них репликацию. Добавлена библиотека для программно-определяемой сети.

Для повышения отказоустойчивости кластера PVE добавлена служба Corosync Quroum, позволяющая кластеру выдержать большее количество отказов узлов, чем это позволяют стандартные правила кворума.

Программный комплекс «Альт Домен» в составе ОС. В состав исполнения Сервер входит программный комплекс для централизованного управления компьютерами и учетными записями пользователей «Альт Домен» (аналог Microsoft Active Directory), его можно выбрать на этапе установки как отдельную группу пакетов. В исполнении Рабочая станция есть группы «Клиент домена» и «Инструменты управления групповыми политиками», с их помощью развертывание программного комплекса «Альт Домена» упрощается.

Появилась система идентификации и управления доступом **Keycloak**. Она используется для аутентификации и авторизации как через локальные серверы, так и через соцсети и другие ресурсы, а также поддерживает двухфакторную аутентификацию и технологию единого входа SSO (Single Sign-On). Позволяет войти в несколько связанных сервисов с единым логином и паролем благодаря привязке к корпоративным системам хранения учётных записей.

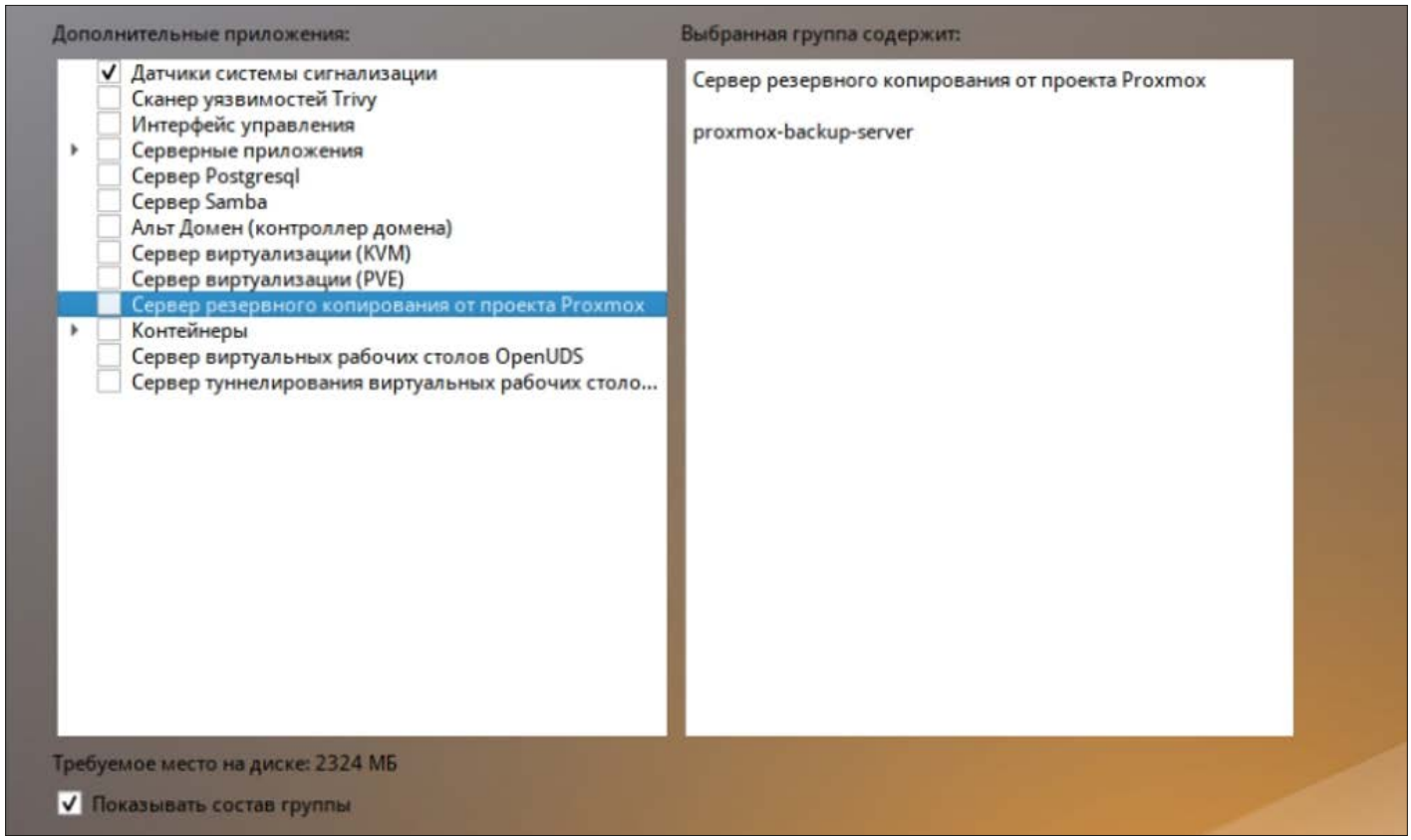


Рисунок 1. В новой версии инсталлятор позволяет выбирать нужные приложения на этапе установки

Новая система мониторинга событий безопасности. В состав инструментов мониторинга событий безопасности добавлено современное гибкое средство **icinga2**, которое можно использовать вместо **nagios**.

Безопасное использование USB-устройств. Основные функции по контролю и ограничению действий пользователя с USB-устройствами выполняют пакеты Alterator-usbguard и Alterator-usbmount, которые доступны через Вебверсию Центра управления системой.

Можно задавать правила для разрешения или блокировки устройств по их характеристикам, например, по идентификаторам или по интерфейсам. Администратор может управлять политиками через удобный интерфейс, импортировать настройки и аудит событий.

Добавлена возможность ограничивать доступ к файловой системе USB-устройств, можно настраивать права доступа для пользователей и групп и файловые системы для контроля доступа.

Добавлен новый механизм работы в режиме киоска. Он реализован в виде модуля Alterator, работает в графической среде рабочего стола и позволяет ограничивать возможности запуска программ по профилям, подготовленным администратором системы. В систему включены примеры таких профилей, которые можно использовать в качестве образцов.

Интерфейс пользователя. В «Альт СП» по умолчанию устанавливается тема «как windows», что делает внешний вид системы привычным пользователю.

Новый набор иконок поможет администратору сразу определить, обновлена ли система.

Преднастроена виртуальная клавиатура для окна входа и разблокировки хранителя экрана.

Появилось приложение, позволяющее администратору удаленно подключаться к рабочему столу пользователя при использовании графической оболочки MATE.

Новые функциональные возможности, обновление Java. Добавлено расширение к системному файловому менеджеру, которое позволяет высчитывать и сравнивать контрольные суммы файлов, в том числе и по алгоритму ГОСТ Р 34.11–2012.

В рабочую станцию включен **recoll** — инструмент для поиска информации в документах, архивах, и письмах по различным параметрам, в том числе по фрагменту текста.

Добавлена LTS-версия **Java 21**.

Совместимость. В ОС включен модуль **cryptopro-preinstall** (только для архитектуры x86_64), упрощающий установку официальных пакетов КриптоПро CSP (с поддержкой Rutoken S и ECP). Добавлены корневые сертификаты для сайтов от российского центра сертификации ООО «ТЦИ».

Обеспечена поддержка «Сигнатуры-L» — системы криптографической авторизации электронных документов, разработанной Банком России. Она предназначена для криптографической защиты электронных сообщений в среде операционных систем Linux.

Также реализована полноценная поддержка Медицинской Информационной Системы «САМСОН».

КВАРТАЛЬНЫЙ ОТЧЁТ

О НОРМАТИВНОМ РЕГУЛИРОВАНИИ В СФЕРЕ ИБ В IV КВАРТАЛЕ 2024 ГОДА

Екатерина РАЧКОВА
обозреватель BIS Journal

ПОДВЕДЕНИЕ ПРОМЕЖУТОЧНЫХ ИТОГОВ

11.12.2024 Банк России опубликовал обзор отчетности об инцидентах информационной безопасности при переводе денежных средств за III квартал 2024 года.

КРИТИЧЕСКАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА (КИИ)

28.12.2024 Правительство Российской Федерации опубликовало Постановление от 26.12.2024 № 1915 «О внесении изменений в постановление Правительства РФ от 14.11.2023 № 1912». Изменения внесены в части п. 3 Постановления.

ПЕРСОНАЛЬНЫЕ ДАННЫЕ (ПДН)

02.10.2024 Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации опубликовало проект приказа «О внесении изменения в перечень индикаторов риска нарушения обязательных требований при осуществлении федерального государственного контроля (надзора) за обработкой персональных данных, утвержденный приказом Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 15.11.2021 № 1187». Новым поводом для проведения проверки предлагалось сделать ситуацию, когда в контролирующий орган поступили сведения о двух и более случаях⁉ в течение календарного года трансграничной передачи персональных данных⁉ при помощи программных средств, владелец которых иностранные юридическое или физическое лицо, а их функционал предполагает передачу ПДн со стороны контролируемого лица, которое не подавало уведомления о намерении провести такую передачу.

03.10.2024 был утвержден ГОСТ Р 71414.1–2024 «Информационные технологии. Биометрия. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 1. Принципы и структура», устанавливающий требования к эксплуатационным испытаниям и протоколам испытаний в области биометрии. Стандарт введен взамен ГОСТ Р ИСО/МЭК 19795–1–2007 и начинает действовать с 01.01.2025.

10.10.2024 принят ГОСТ Р 71674–2024 «Системы искусственного интеллекта в клинической медицине. Набор данных в формате dicom для тестирования алгоритмов. Методы обезличивания набора данных и контроля набора данных на отсутствие персональных данных». Данный стандарт также будет действовать с 01.01.2025.

29.10.2024 Банком России опубликованы «Методические рекомендации Банка России по нейтрализации организациями финансового рынка угроз безопасности, актуальных при обработке биометрических персональных данных, векторов единой биометрической системы, проверке и передаче информации о степени соответствия векторов единой биометрической системы предоставленным биометрическим персональным данным физического лица при взаимодействии информационных систем организаций финансового рынка с единой биометрической системой» от 08.10.2024 № 18-МР, а также «Методические рекомендации Банка России по нейтрализации организациями финансового рынка угроз безопасности, актуальных при обработке биометрических персональных данных, векторов единой биометрической системы, проверке и передаче информации о степени соответствия векторов единой биометрической системы предоставленным биометрическим персональным данным физического лица в информационных системах организаций финансового рынка, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц, за исключением единой биометрической системы, а также актуальных при взаимодействии информационных систем организаций финансового рынка, иных организаций, индивидуальных предпринимателей с указанными информационными системами» от 09.10.2024 № 19-МР.

30.11.2024 опубликован комплекс Федеральных законов значительно увеличивающих суммы штрафов за утечку персональных данных в зависимости от числа субъектов, чьи персональные данные были скомпрометированы:

- Федеральный закон от 30.11.2024 № 420-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» (вступил в силу 11.12.2024).

◆ Федеральный закон от 30.11.2024 № 421-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» (вступает в силу по истечении 180 дней после дня его официального опубликования).

ПРЕЗИДЕНТ И ПРАВИТЕЛЬСТВО РФ

09.10.2024 было опубликовано постановление Правительства Российской Федерации от 09.10.2024 № 1350 «О внесении изменений в постановление Правительства Российской Федерации от 03.11.1994 № 1233». Данным Постановлением к служебной информации ограниченного распространения относят помимо прочего несекретную информацию, распространение которой может создать потенциальную угрозу интересам Российской Федерации, содержащуюся в документах Архивного фонда, хранящихся в государственных и муниципальных архивах, а также в архивах федеральных органов, уполномоченного органа управления использованием атомной энергии и уполномоченного органа по космической деятельности.

21.10.2024 опубликован Указ Президента Российской Федерации от 21.10.2024 № 901 «О внесении изменений в положения, утвержденные Указом Президента Российской Федерации от 10.09.2005 № 1062 «Вопросы военно-технического сотрудничества Российской Федерации с иностранными государствами». Изменения коснулись обеспечения защиты сведений, составляющих государственную тайну.

МИНЦИФРЫ РФ

22.10.2024 опубликован приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 16.09.2024 № 773 «Об утверждении перечня индикаторов риска нарушения обязательных требований при осуществлении федерального государственного контроля (надзора) в сфере идентификации и (или) аутентификации». Приказом установлен новый индикатор риска нарушения обязательных требований для федерального госконтроля (надзора) в сфере идентификации и аутентификации — поступление в Минцифры заявления об аккредитации организации для аутентификации на основе биометрии, содержащего информацию о работниках, непосредственно занимающихся такой аутентификацией, имеющих высшее образование в области информационных технологий или информационной безопасности, которые заявлены как работники аккредитованной организации, занимающейся такой аутентификацией.

05.12.2024 утвержден приказом № 1035 «Перечень нормативных правовых актов в сфере информационных технологий и распространения информации в социальных сетях, содержащих обязательные требования, подлежащих оценке применения в 2025 году».

09.12.2024 опубликован приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 26.08.2024 № 726 «О внесении изменения в приказ Мининформсвязи России от 9 января 2008 г. № 1 «Об утверждении требований по защите сетей связи от несанкционированного доступа к ним и передаваемой посредством их информации»». Приказ вступает в силу 01.09.2025.

ФСТЭК РОССИИ

20.12.2024 начал действовать ГОСТ Р 56939–2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования» (введен взамен ГОСТ Р 56939–2016). Стандарт устанавливает общие требования к содержанию и порядку выполнения работ, связанных с созданием безопасного программного обеспечения и устранением его выявленных недостатков, в том числе уязвимостей. ГОСТ Р 56939–2024 предназначен для разработчиков и производителей ПО, а также для организаций, выполняющих оценку соответствия процессов разработки ПО положениям настоящего стандарта.

ЦЕНТРАЛЬНЫЙ БАНК РФ

02.10.2024 Банком России опубликованы методические рекомендации от 30.09.2024 № 16-МР «Методические рекомендации Банка России по организации взаимодействия информационных систем организаций финансового рынка с инфраструктурой, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме». Новые рекомендации разработаны в целях обеспечения единства подходов кредитных организаций, некредитных финансовых организаций и организации взаимодействия их информационных систем с инфраструктурой электронного правительства.

03.10.2024 Банком России опубликован проект положения «Об обязательных для кредитных организаций, иностранных банков, осуществляющих деятельность на территории Российской Федерации через свои филиалы, требованиях к операционной надежности при осуществлении банковской деятельности в целях обеспечения непрерывности оказания банковских услуг».

Проект должен распространяться на кредитные организации, филиалы иностранных банков.

17.10.2024 Банком России было выпущено информационное сообщение «Противодействие кредитному мошенничеству: инициативы Банка России». Банк России предложил ввести обязательный период охлаждения по потребительским кредитам и займам между заключением договора и получением денег. Его длительность будет зависеть от суммы кредита (займа).

07.10.2024 приняты и введены в действие стандарты Банка России СТО БР ФАПИ.СЕК-1.6–2024 «Безопасность финансовых (банковских) операций. Прикладные программные интерфейсы обеспечения безопасности финансовых сервисов на основе протокола OpenID Connect. Требования» (взамен СТО БР ФАПИ.СЕК-1.6–2020) и СТО БР ФАПИ.ПАОК-1.0–2024 «Безопасность финансовых (банковских) операций. Прикладные программные интерфейсы. Обеспечение безопасности финансовых сер-

висов при инициации OpenID Connect клиентом потока аутентификации по отдельному каналу. Требования» (взамен СТО БР ФАПИ.ПАОК-1.0–2021).

ОТРАСЛЕВЫЕ ДОКУМЕНТЫ

06.11.2024 принят ГОСТ 19.101–2024 «Единая система программной документации. Виды программ и программных документов». Стандарт будет действовать с 30.01.2025.

06.12.2024 Приказом Федерального агентства по техническому регулированию и метрологии (Росстандарта) утверждены рекомендации по стандартизации № 1785-ст от 28.11.2024 Р 1323565.1.003–2024 «Информационная технология. Криптографическая защита информации. Криптографические алгоритмы выработки ключей шифрования информации и аутентификационных векторов, предназначенные для реализации в аппаратных модулях доверия для использования в подвижной радиотелефонной связи» (взамен Р.1323565.1.003–2017). Документ вступает в силу 01.01.2025.

18.12.2024 опубликованы ГОСТ Р 71840–2024 «Информационные технологии. Интернет вещей. Требования к платформе обмена данными для различных служб интернета вещей. Часть 1. Общие требования» и ГОСТ Р 71777–2024 «Информационные технологии. Интернет вещей. Термины и определения». Оба стандарта вступают в силу с 01.02.2025.

20.12.2024 начал действовать ГОСТ Р 71753–2024 «Защита информации. Системы автоматизированного управления учетными записями и правами доступа. Общие требования».

Также приняты и начинают действовать с 01.01.2025 следующие стандарты:

- ГОСТ Р 71174–2024 «Ноутбуки. Термины и определения» устанавливает термины и определения понятий в области портативных компьютеров со встроенным экраном и клавиатурой (ноутбуков). Предназначен для заказчиков, разработчиков, поставщиков и потребителей. Термины, установленные настоящим стандартом, рекомендуются для применения во всех видах документации и литературы, входящих в сферу действия работ по стандартизации и/или использующих результаты этих работ.
- ГОСТ Р 71202–2024 «Ноутбуки. Типы, основные параметры, общие технические требования» определяет типы, основные параметры, общие технические требования для ноутбуков. Настоящий стандарт предназначен для заказчиков, разработчиков, поставщиков и потре-

бителей, а также персонала сопровождения персональных электронно-вычислительных машин.

◆ ГОСТ Р 60.0.0.16–2024 «Роботы и робототехнические устройства. Жизненный цикл» устанавливает термины и определения понятий в области жизненного цикла роботов и робототехнических устройств, предназначенные для применения на всех стадиях жизненного цикла, определенных в ГОСТ Р 60.0.0.6 (должен применяться совместно с ГОСТ Р 60.0.0.4).

◆ ГОСТ Р 60.0.0.17–2024 «Роботы и робототехнические устройства. Управление жизненным циклом. Основные положения» устанавливает основные положения в области управления жизненным циклом роботов и робототехнических устройств (РРТУ) и предназначен для применения на всех стадиях жизненного цикла (ЖЦ) роботов, определенных в ГОСТ Р 60.0.0.6. На основе настоящего национального стандарта целесообразно, при необходимости, разрабатывать стандарты для отдельных видов роботов (групп объектов стандартизации), учитывающие их особенности на стадиях жизненного цикла, а также с учетом их специфики, объема, сложности и характера работ по назначению.

◆ ГОСТ Р 60.2.2.5–2024 «Роботы и робототехнические устройства. Сервисы, реализуемые сервисными роботами. Требования к системам обеспечения безопасности» определяет требования к системам обеспечения безопасности прикладных сервисов (далее — СОБПС), реализуемых сервисными роботами, которые поставщик прикладных сервисов может использовать для обеспечения безопасности пользователей и третьих лиц, когда он предоставляет прикладные сервисы в неструктурированных средах, в которых присутствуют как обученные, так и неподготовленные люди (например сервисы по указанию нужных направлений посетителям в аэропорту или торговом центре, по доставке лекарств пациентам в больнице, по подаче заказанных блюд клиентам в ресторане).

◆ ГОСТ Р 60.2.7.1–2024 «Роботы и робототехнические устройства. Модульный принцип построения сервисных роботов. Часть 201. Общая информационная модель модулей» определяет требования и руководящие указания к общей информационной модели (ОИМ) модулей сервисных роботов для обеспечения интероперабельности, возможности повторного использования и компонуемости. Настоящий стандарт определяет структуру ОИМ и детализирует ее использование по назначению, сущность атрибутов и подклассов. Требования настоящего стандарта применимы к сервисным роботам.

ПЕРЕЛОМНЫЕ РЕШЕНИЯ

ПОЧЕМУ ВЫПОЛНЕНИЕ РЕГУЛЯТОРНЫХ ТРЕБОВАНИЙ ЦБ ПОМОЖЕТ В БОРЬБЕ С КИБЕРМОШЕННИЧЕСТВОМ

Дарья ПЕНЗЕВА
корреспондент BIS Journal

В 2024 году Уральский форум «Кибербезопасность в финансах» был во многом посвящён борьбе с социальной инженерией, в 2025 году первая пленарка посвящена той же теме. И это не случайно: граждане теряют миллиарды рублей из-за «социальных инженеров.» Пока «перелома» в борьбе с кибермошенничеством добиться не удалось. В то же время выполнение кредитными организациями требований Банка России по подтверждению клиентских транзакций, выпущенных ещё в 2022 году, сможет если не решить проблему, то снизить количество мошеннических операций. И даже если суммы после выполнения всеми кредитными организациями снизятся всего на 20–30%, то это будут миллиарды рублей в год денег жителей страны, которые удастся спасти от мошенников. Тем более на рынке есть решения российских вендоров, которые как раз помогут выполнить регуляторные требования и в то же время защитить россиян.

НЕСОГЛАСОВАННЫЕ ОПЕРАЦИИ

Статистику ЦБ по хищениям у клиентов банков нельзя назвать позитивной. Количество банковских операций, совершённых без согласия (ОБС) клиентов, в России ежегодно превышает 1 млн штук. В 2023 году число зарегистрированных ЦБ таких операций суммарно составило 1,2 млн штук, за девять месяцев прошлого года — уже 0,9 млн штук. При этом объём похищенных в результате средств растёт: в позапрошлом году он составил 15,8 млрд рублей, с января по сентябрь 2024 года — уже 18,3 млрд рублей.

Жертвами чаще всего становятся физические лица: ОБС затрагивают сотни тысяч граждан каждый год. Неудивительно поэтому, что эта проблема стала одной из тем пристального внимания регулятора.

«Мы видим, что здесь перелома такого долгожданного, о котором мы говорили, конечно, не произошло... Конечно, для того, чтобы просто стоять на месте, чтобы не ухудшалась ситуация, надо бежать, и мы бежим. Но для того, чтобы двигаться вперёд, надо бежать в два раза быстрее», — говорила год назад председатель Банка России Эльвира Набиуллина (цитата по «Интерфакс»).

Одним из направлений такой борьбы с ОБС стало ужесточение требований ЦБ к защищённости транзакций клиентов банков. В начале 2022 году регулятор внёс в положение 683-П, по которому с октября того же года устанавливались более жёсткие, включая криптографическую защиту, требования по подписанию электронных сообщений для подтверждения операций по платежам и переводам, оформлению кредитов и т.п.

НОВЫЕ ТРЕБОВАНИЯ

В частности, наиболее распространённым способом подтверждения банковских транзакций являются коды из СМС и пуш-сообщений, которые, по сути, являются простой электронной подписью (ПЭП). Однако, по мнению регулятора, только кода стало недостаточно для защиты от мошенничества. Согласно новой редакции документа, теперь необходима усиленная квалифицированная электронная подпись (УКЭП), усиленная неквалифицированная электронная подпись (УНЭП) или же средство криптографической защиты информации (СКЗИ) с имитозащитой и аутентификацией отправителя сообщения.

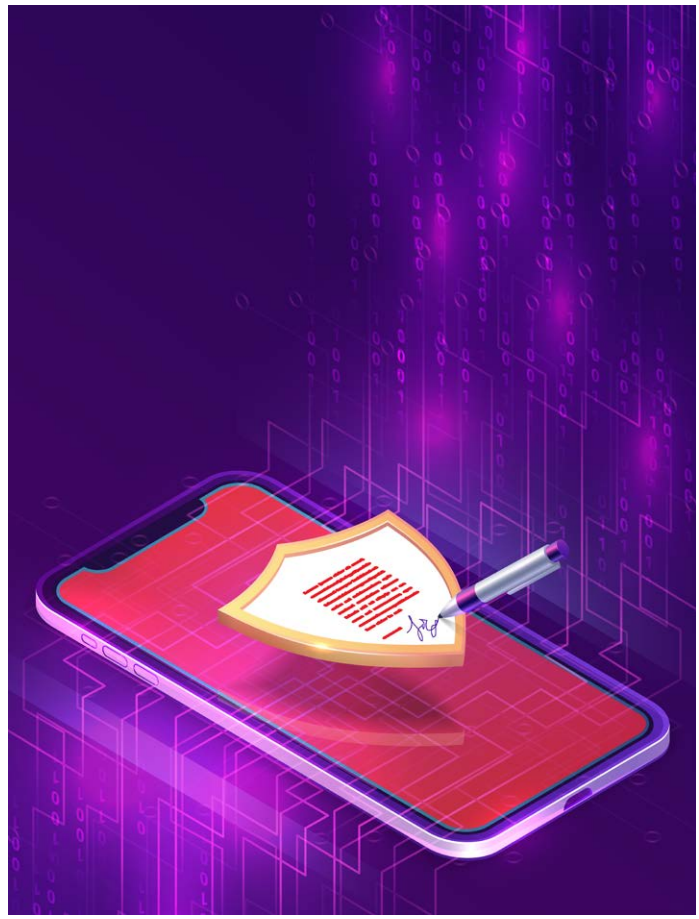
«Проблема кодов из СМС не только в том, что скрипты многих мошеннических звонков против граждан построены таким образом, чтобы выманить у клиента банка код из СМС или пуш и таким образом получить доступ к его личному кабинету, — поясняет генеральный директор SafeTech Денис Калемберг. — Использование одноразовых кодов, даже если они вычисляются с использованием данных операции, несёт в себе повышенные риски на пути всего своего жизненного цикла». Эксперт пояснил, что коды из пуш-уведомления или СМС-сообщения подвержены риску компрометации с момента генерации на стороне банка, в процессе передачи, как, например, из-за уязвимости протокола SS7, которую обнаружили более десятилетия назад. В частности, использовав эту уязвимость, хакеры впервые смогли похитить деньги клиентов немецких банков ещё в 2017 году, сообщало Süddeutsche Zeitung. Отдельно можно упомянуть массу способов украсть одноразовые коды при помощи фишинговых ресурсов и вредоносного ПО.

Криптографическая защита, требования о которой и ввёл регулятор в положение 683-П, как раз и должна защитить клиентов от мошенничеств, направленных на получение кода из СМС или пуш-сообщения, фрода внутри банка, технологических атак с перехватом сообщения. Безусловно, если ведомый «социальными инженерами» человек сам лично снимет деньги со своего счёта и передаст деньги в банк, то криптография тут

не поможет. «Но даже если удастся сделать невозможными хотя бы атаки с перехватом или сообщением третьим лицам кода из СМС и пуш-сообщений, сократив объём хищений на 20–30%, это в любом случае будет означать сэкономленные миллиарды россиян», — указал Денис Калемберг.

К сожалению, многие российские банки, занятые в 2022 году первоочередными проблемами, не спешили внедрять новые решения с криптографией. В марте 2023 года в информационном письме ЦБ ещё раз напомнил кредитным организациям о необходимости усиливать защиту подтверждения операций: использование ПЭП «возможно только совместно с СКЗИ, реализующими функцию имитозащиты информации с аутентификацией отправителя сообщения», настаивал регулятор.

Тем не менее штрафы, предусмотренные за нарушение нормативных требований ЦБ (до 0,1% от собственного капитала, но не менее 100 тысяч рублей), не очень пугали некоторые кредитные организации, которые продолжали использовать старые методы для подтверждения банковских операций. «Сумма возможного штрафа зачастую меньше, чем стоимость работ по внедрению или разработке новых технических средств для исполнения требований указания Банка России», указывали, в частности, в Совете Федерации (цитата по РБК). В результате в конце 2023 года сенаторы, например, даже решили значительно увеличить денежные взыскания с банков за неисполнение законов и нормативных актов регулятора. Впрочем, пока до поправок в закон дело так и не дошло.



РЕШЕНИЯ ЕСТЬ

В то же время ряд российских кредитных организаций всё же выполнил требования ЦБ, повысив защищённость своих клиентов от кибермошенничества. Технологические решения, которые позволяют обеспечить подтверждение транзакций в соответствии с требованиями ЦБ, существуют и активно используются кредитными организациями. Например, мобильная электронная подпись. Это специальное приложение для смартфона или SDK для интеграции в мобильное банковское приложение, построенное на основе асимметричной криптографии, то есть такого метода шифрования информации, который предполагает наличие сразу двух ключей — закрытого и открытого.

При этом закрытый ключ находится только у клиента, который видит все данные документа перед его подписанием, также здесь не существует кода, который можно было бы сообщить мошеннику или ввести на фишинговом сайте. Таким образом, при использовании мобильной электронной подписи просто исключена возможность операций без согласия клиента, когда сообщается код из СМС. При этом СМС банкам обходятся всё дороже, и отказ от них даёт немалую экономию расходов на связь.

То есть мобильная электронная подпись совмещает и низкую стоимость, и простоту распространения, и юридическую значимость, и высокую степень защиты транзакции.

В частности, именно такой функционал предоставляет PayControl ГОСТ — платформа, которая является средством для формирования УНЭП в смартфоне. Её разработчиком является российская компания SafeTech.

Мобильная электронная подпись в PayControl ГОСТ создаётся путём криптографических преобразований подписываемой информации в сочетании с уникальными характеристиками конкретного девайса. Клиент создаёт операцию в цифровом канале, информация о ней отображается в мобильном приложении на смартфоне, пользователь нажимает кнопку «Подтвердить», и транзакция подтверждается.

Процедура подтверждения операции занимает несколько секунд, для клиента подтверждение платежа происходит лишь одним тапом по экрану. Приложение доступно как на операционной системе Android, так и на IOS. Существует даже возможность работы со смарт-часов. Кроме того, существует версия для компьютеров и ноутбуков.

«Использование PayControl ГОСТ — это не только повышение безопасности и выполнение требований регулятора, но и улучшение клиентского опыта, — указывает Денис Калемберг. — Более того, согласно расчётам SafeTech, использование подобных решений даже несёт банкам финансовую выгоду: обычно на отправку СМС банки тратят порядка 500 рублей на одного клиента в год, а значит, экономия по итогам 12 месяцев может составить сотни миллионов рублей».

Всё заканчивается хорошо. Если всё закончилось плохо, значит, это ещё не конец.
Пауло Коэльо

ГДЕ ИЛЛЮЗИЯ, А ГДЕ РЕАЛЬНОСТЬ… — ВСЁ НЕ ТО, ЧЕМ КАЖЕТСЯ

РАЗМЫШЛЕНИЯ НАД ФЗ-233 ОТ 08.08.2024 «О ВНЕСЕНИИ ИЗМЕНЕНИЙ В ФЕДЕРАЛЬНЫЙ ЗАКОН „О ПЕРСОНАЛЬНЫХ ДАННЫХ“»

Сергей ВИХОРЕВ
советник генерального директора
ООО «Умные решения»

У нас считается, что любое изменение в области оборота персональных данных — это ужесточение требований. Поэтому с принятием Федерального закона № 233-ФЗ в очередной раз возобновилось брожение в среде причастных к обработке ПД, причём зачастую с пессимистическим уклоном: «Вот, скоро вообще нельзя будет обрабатывать персональные данные! Теперь будет тотальный контроль за действиями субъектов! Нам придётся теперь платить за возможность использования персональных данных из ГИС[1]!»

Всё это ещё и усугубляется комментариями вполне официальных лиц, которые хотят выдать имеющееся за желаемое: мол, закон о том, что надо защищать данные, полученные в результате обезличивания, и, вообще, такие данные — тоже персональные данные. В общем, караул, готовьтесь, грядёт апокалипсис!

НУ А ПЕСНЯ СОВСЕМ НЕ О ТОМ, КАК ПОССОРИЛИСЬ ЛЮДИ С КОТОМ

На самом деле закон не ужесточает, а определяет порядок обработки персональных данных в определённых условиях. И не всех, а только данных, полученных в результате обезличивания. И не всех данных, полученных после обезличивания, а только тех, которые используются для вполне определённой цели их обработки (раньше такого порядка не было!). Это коротко. А теперь с этого места поподробнее, попробуем перевести новеллы закона на обычный русский язык.

Прежде всего, выясним, что регулирует закон и для кого он имеет смысл. Закон определяет порядок оборота ПД, полученных в результате их обезличивания, которые используются для вполне определённых целей[2]: повышения эффективности государственного и муниципального управления, а также в целях, предусмотренных федеральными законами, определяющими случаи и особенности обработки персональных данных[3]. Как видно, список целей обработки, на которые распространяется закон, конечен и ограничен законодательством. Для остальных целей, которые в основном используются в обычных организациях, он не действует. Кстати, это подтверждается и дополнениями[4] к статье 23 ФЗ-152, которая подтверждает существующий на сегодня[5] порядок обезличивания ПД во всех остальных случаях. Соответственно, этот закон будет интересен только весьма ограниченному кругу пользователей, нуждающихся в обезличенной информации, получаемой из ГИС (количество операторов ПД в стране сопоставимо с числом юридических лиц, а вот с ГИС, по-моему, будут работать не более 5–10 %).

О СИЛЕ ЗАКОНА

Ну а теперь о том, какую силу имеет закон. Бесспорно, порядок обработки персональных данных в определённых условиях является императивной нормой. Но на самом

[1] ГИС — государственная информационная система.

[2] Изменения к части 1 ст. 13.1. ФЗ-152.

[3] Например, закон от 08.06.2020 № 168-ФЗ «О едином федеральном информационном регистре, содержащем сведения о населении Российской Федерации».

[4] Дополнение ст. 23 ФЗ-152 частью 12.

[5] Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных».

деле закон-то — бланкетный[6]. Почему? Да потому, что для того, чтобы закон заработал, правительству необходимо:

- определить цели, предусмотренные федеральными законами, при которых этот закон действует[7];
- определить государственную информационную систему для обработки составов таких данных[8];
- установить методы и порядок обезличивания персональных данных[9];
- установить порядок взаимодействия Минцифры и операторов персональных данных[10];
- установить порядок формирования составов данных[11];
- определить порядок доступа пользователей ГИС к составам данных[12];
- определить порядок проверки соответствия пользователей ГИС установленным требованиям[13].

При этом практически все пункты Правительство должно согласовать с ФСБ России. (Боюсь быть пророком, но что-то мне подсказывает, что не миновать нам криптографических методов обезличивания, может быть, на основе протокола Диффи-Хеллмана.)

Так что говорить о влиянии закона на бизнес пока ещё рано, надо дождаться издания перечисленных документов и тогда уж смотреть. Хотя, как мне кажется, существенных изменений для большинства операторов ПД ждать не следует.

ВОПРОСЫ БЕЗ ОТВЕТОВ

А теперь о том, кому это нужно. Говоря об обезличивании персональных данных, Роскомнадзор особо отмечает, что их обезличивание должно обеспечивать возможность их обработки, то есть такие данные должны сохранять основные характеристики обезличиваемых персональных данных[14]. То есть, говоря простым языком, обезличенные данные могут быть дополнены другими данными, полученными из других источников. В результате как раз и появятся те самые «составы данных», которые предусмотрены законом. Можно предположить, что такие данные будут обогащены дополнительной информацией. Наверное, это кому-то будет нужно и действительно сможет помочь в повышении эффективности государственного и муниципального управления.

Но вопрос вот в чём. Несколько раз перечитав текст закона, я так и не нашёл анонсированные некоторыми экспертами изменения в порядок защиты ПД после процедуры обезличивания. Как раньше было, так и осталось. Разве что Роскомнадзор обязан обеспечивать конфиденциальность поступивших от операторов данных, полученных в результате их обезличивания[15]. Роскомнадзор, конечно, сможет обеспечить конфиденциальность данных в ГИС. А какова ответственность операторов персональных данных? Ведь они остаются обладателями первичной не обезличенной информации и одновременно уже обезличенной информации, то есть, можно сказать, обладателями ключевой базы, которая позволит восстановить («деобезличить») данные, переданные в ГИС.

А с учётом того, что данные в ГИС будут обогащены, то позволят получить ещё и дополнительную информацию о субъекте ПД. На мой взгляд, такую ключевую базу данных надо бы защищать особо тщательно (тем более что все яйца сложены в одну корзину «составы данных»), и, наверное, это должно быть отражено в законе или хотя бы в тех подзаконных актах, которые планируются к разработке в развитие закона. Логичнее было бы защищать не уже обезличенные данные (там, если они правильно обезличены, кроме статистики вряд ли что возьмёшь), а ключевую базу данных, которая позволит расшифровать обезличенные данные и которая находится не под контролем Роскомнадзора, а у оператора персональных данных.

[6] Бланкетная норма — вид отсылочной нормы права, который содержит не само правило поведения, а отсылку к другим законам, подзаконным нормативным правовым актам, а также иным источникам (формам) права либо подразумевает такую отсылку.

[7] Изменения к части 1 ст. 13.1 ФЗ-152.

[8] Изменения к части 2 ст. 13.1 ФЗ-152.

[9] Изменения к части 3 ст. 13.1 ФЗ-152.

[10] Изменения к части 4 ст. 13.1 ФЗ-152.

[11] Изменения к части 5 ст. 13.1 ФЗ-152.

[12] Изменения к части 6 ст. 13.1 ФЗ-152.

[13] Изменения к части 8 ст. 13.1 ФЗ-152.

[14] «Требования и методы по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ», утверждены приказом Роскомнадзора от 05.09.2013 № 996, п. 3.

[15] Изменения к части 4 ст. 13.1 ФЗ-152.

БАНКИ СТРАНЫ «ПОД КОВРОМ»

ПОЧЕМУ ДЛЯ ЗАЩИТЫ ОТ DDOS-АТАК ВАЖНА ГИБКОСТЬ ПОДХОДА К ФИЛЬТРАЦИИ ТРАФИКА

Михаил ХЛЕБУНОВ
директор по продуктам Servicepipe

В 2024 году кредитные организации всего мира стали целью номер один по ковровым DDoS-атакам. Российские банки не исключение. Летом 2024 года из-за «ковра» наблюдалась недоступность сервисов у ведущих игроков финансовой отрасли. Почему именно крупные банки наиболее уязвимы перед такими атаками, а также почему гибкие правила фильтрации трафика наиболее эффективны для защиты от «ковра», рассказал BIS Journal директор по продуктам Servicepipe Михаил Хлебунов.

УГРОЗА ДЛЯ БАНКОВ ВСЕГО МИРА

Мощные DDoS-атаки уже давно являются общемировой проблемой. Так, в третьем квартале 2024 года, по данным Cloudflare (работает на глобальном уровне), количество DDoS-атак по сравнению с апрелем – июнем увеличилось на 49%, а по сравнению с аналогичным периодом прошлого года – на 55%. Всего американской компанией в июле – сентябре было зафиксировано 6 млн таких инцидентов, а с начала года – 14,5 млн. То есть в среднем каждый час в мире происходило приблизительно по 2200 DDoS-атак. При этом, согласно статистике Vercara (бывшая Neustar Security Services, также международный поставщик решений), более половины из таких инцидентов представляют собой так называемые ковровые атаки. Например, в первом полугодии доля «ковровых атак» достигла 75% от общего числа DDoS-нападений. «„Ковровые атаки“ – не новый метод атак, но взрывное увеличение их частотности – это новый тренд», – отмечала компания. На глобальном уровне чаще всего жертвами злоумышленников становятся банковский сектор и другие финансовые организации, указывает Cloudflare. На втором месте следуют ИТ- и сервисные компании, на третьем – телекоммуникационные предприятия и операторы связи.

Российский финансовый сектор также является целью номер 1 для ковровых атак. С начала 2024 года Servicepipe зафиксировал десятикратный кратный рост ковровых DDoS-атак. Согласно нашим данным, мощность таких нападений на российские банки во втором квартале выросла на четверть по сравнению с показателями первых трёх месяцев этого года. Особенность отечественного «ковра» – такие атаки проводят политически мотивированные хакеры.

В частности, в конце июля крупнейшим российским банком была зафиксирована одна из мощнейших в истории DDoS-атак. «Её длительность превысила 13 часов… одновременно использовалась как инфраструктура ИТ-армии Украины, так и несколько сторонних бот-сетей», – рассказывал «РИА Новостям» заместитель председателя правления Сбербанка Станислав Кузнецов (он назвал её сильнейшим нападением в истории группы). Кроме того, как сообщали СМИ, в этом году жертвами нападений уже стали Росбанк, Газпромбанк, Россельхозбанк, Райффайзенбанк и др. Для осознания масштабов угрозы можно перечислить лишь несколько кредитных организаций, которые признали DDoS-атаки, произошедшие в ноябре – декабре: банк «Санкт-Петербург», «Кредит Урал банк», Генбанк, Локо-банк и т.д.

Интересны злоумышленникам не только банки, но и другая критически важная финансовая инфраструктура. В июне в результате DDoS-атаки на Национальную систему платёжных карт (НСПК) – оператора карт «Мир» – произошли сбои в работе приложений сразу нескольких банков и компаний, писало Frank Media. По данным того же издания, «ковровая бомбардировка» ресурсов Московской биржи летом на время вывела из строя сайт торговой площадки и её финансового маркетплейса «Финуслуги». Наконец, в июле относительно успешной атаке подвергся даже Банк России. Сам ЦБ признавал, что отечественный финансовый сектор длительное время находится в условиях повышенных атак, периодически их интенсивность возрастает (цитата по «Коммерсантъ»).

БАНК – ИДЕАЛЬНАЯ ЖЕРТВА

Причин, по которым хактивисты используют против финансовых организаций тактику ковровых атак, три. Первая – злоумышленникам нужен общественный резонанс. А недоступность сервисов крупной финансовой организации не может остаться незамеченной. Вторая – ущерб российской экономике. Как отмечает Банк

России, в основных направлениях развития финансовых технологий до 2027 года кибератаки, в частности, несут риски для операционной деятельности финорганизаций и причинения им потенциального ущерба.

Третий фактор в специфике бизнеса кредитных организаций – в результате ковровых DDoS-атак вредоносный трафик идёт по всем или по большей части IP-адресов её цели, а чем крупнее организация, подвергшаяся такому нападению, тем больше у неё должно быть этих IP-адресов. Сама же специфика банковского бизнеса такова, что IP-адресов у банков много. Согласно нашей статистике, обычно «ковровая» DDoS-атака на российскую цель политически мотивированных злоумышленников длится приблизительно сутки, при этом атаковано может более чем 1000 IP-адресов, а затем хактивисты переключаются на другой объект. При этом зачастую нагрузка на один IP-адрес может быть совсем небольшой, на уровне мусорного трафика. А теперь представьте, что такая небольшая, казалось бы, нагрузка ложится на тысячи сервисов крупной финансовой организации, на десятки тысяч её IP-адресов. В случае если защитник попытается перенаправить весь поступающий вредоносный трафик по несуществующему маршруту (для этого используется механизм BGP Blackhole), как он мог бы вполне без проблем для работоспособности сделать при атаке лишь на несколько целей, то это, скорее всего, приведёт к недоступности всех сервисов, чего, собственно, и добиваются злоумышленники. Таким образом, чем крупнее ИТ-инфраструктура компании, тем больший ущерб может нанести ковровая атака и тем сложнее от неё защититься.

В третьем квартале 2024 года количество DDoS-атак увеличилось на 49%, а по сравнению с аналогичным периодом прошлого года – на 55%. Всего в июле – сентябре было зафиксировано 6 млн таких инцидентов, а с начала года – 14,5 млн

Кроме того, нередко защитники от DDoS-атак не оценивают вредоносный трафик в совокупности, а лишь нагрузку на каждый IP-адрес в отдельности. Этот подход оправдан при классической DDoS, но «при ковре» есть шанс распознать атаку лишь в момент деградации или даже полной недоступности сервисов защищаемой организации.

При этом необязательно ковровая атака будет осуществлена напрямую на банк. Она вполне может идти через сервис-провайдеров, мы уже видели такие примеры в 2024 году. Если такой провайдер доставляет трафик по каналу, где есть защита от DDoS-атак, то он будет обрабатываться различными сетевыми устройствами, но у каждого из них есть свой лимит мощности. И как раз цель такого нападения будет в том, чтобы этого ли-

После ухода из России глобальных вендоров решений по защите от DDoS-атак наша компания фактически осталась единственным игроком на отечественном рынке, в решениях которой вместо стандартных систем контрмер реализована гибкая настройка правил фильтрации

мита не хватило, чтобы эти устройства начали сбоить и, как результат, «легла» сама цель атаки. В таком случае могут оказаться затронутыми и другие клиенты атакованного сервис-провайдера.

БАНКИ ВСТАЮТ ПОД ЗАЩИТУ

Участники финансового рынка, уже столкнувшиеся с «ковром», пересмотрели подход к обеспечению защищённости сервисов. Многие банки также готовы работать на опережение. За последнее время Servicepipe со стороны финансового сектора зафиксировал трёхкратный рост спроса на услугу по аудиту устойчивости ИТ-систем к непрогнозируемым нагрузкам, то есть, собственно, на способность противостоять DDoS-атакам. Наших заказчиков – а это, прежде всего, крупные и средние банки – интересовала способность используемых ими решений выдержать ковровые атаки, похожие на те, которые случились летом этого года. Испытания проходят в специализированной лаборатории, которая была запущена в пилотном режиме в 2024 году, а в полном режиме будет работать в 2025 году.

Кроме того, летние атаки на финансовый сектор стали причиной возросшего спроса на решения по защите от DDoS-атак. Например, в июле он вырос втрое в сравнении с количеством обращений в компанию в среднем в месяц в первом полугодии 2024 года. При этом 65% банков, интересовавшихся решениями Servicepipe, говорили о необходимости новой защиты именно в связи с ковровыми атаками, ещё 20% пришли за защитой «под атакой» или сразу же после атаки.

Тот факт, что опасающиеся ковровых атак кредитные организации приходят именно в Servicepipe, неслучаен. Дело в том, что для эффективной защиты от «ковра» требуется высокая гибкость настройки правил фильтрации. После ухода из России глобальных вендоров решений по защите от DDoS-атак наша компания фактически осталась единственным игроком на отечественном рынке, в решениях которой вместо стандартных систем контрмер реализована гибкая настройка правил фильтрации.

Именно гибкие сетевые инструкции, лежащие в основе механизма XDP (eXpress Data Path), позволяют решениям Servicepipe оперативно отражать ковровые атаки. В них нет статичных правил, которые, как показали события лета 2024 года, явно не поспевают за всё более изобретательными методами хактивистов. В решениях Servicepipe реализована возможность динамически модифицировать фильтры и пороговые значения. Такой подход не только повышает устойчивость к атакам, но и обеспечивает удивительную гибкость: протоколы фильтрации адаптируются почти мгновенно, отбрасывая вредоносный трафик с минимальными задержками.

Что это означает для клиентов компании? Для многих из них летний «ковёр» не привёл даже к деградации, не то что недоступности сервисов. Они выстояли, хотя нагрузка порой была очень серьёзной. Также могу сказать, что среди столкнувшихся с летним «ковром» кредитных организаций немало тех, кто уже встал под защиту Servicepipe или пилотирует решение.

Если же переходить от технологии непосредственно к продуктам, мы предлагаем рынку систему интеллектуального анализа трафика FlowCollector и адаптивную систему очистки трафика DosGate.

FlowCollector позволяет детектировать ковровые атаки, что само по себе непростая задача. В систему входят отдельные умные счётчики, которые анализируют каждый IP-адрес, каждый сетевой префикс, а также суммарно все сетевые префиксы данной сети. Благодаря детальному подсчёту трафика можно не просто обнаружить аномалии, но и сегментировать конкретные блоки сети.

DosGate построен на основе сетевых инструкций. При фильтрации ковровых атак эти инструкции дают возможность отталкиваться не от позитивной, а только от негативной модели. То есть с помощью DosGate можно очень детально описать паттерны только вредоносного трафика для его блокировки или фильтрации. Кроме того, сетевые инструкции хранятся в гибких пакетах правил с уже готовыми паттернами самых распространённых ковровых атак. Интегрированное решение FlowCollector с DosGate позволяет обнаружить и отфильтровать ковровые DDoS-атаки любой сложности, а значит, обеспечить непрерывную доступность сетевых сервисов.

* * *

Подведём итог: глобальная статистика лидеров рынка по защите от DDoS-атак и данные Servicepipe – всё говорит о том, что «ковровые» атаки продолжатся. Злоумышленники могут временно сместить сферу своих интересов в сторону другой отрасли, но так или иначе атаки на банки вернутся. И уже от самих кредитных организаций зависит, смогут ли их решения противостоять «ковру» или у них будет шанс мелькнуть в новостях СМИ в качестве ещё одной кредитной организации, «лежавшей» несколько часов под атакой.

СЕМЬ ШАГОВ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

КАК ИЗ ПЕНТЕСТА ВЫЖАТЬ МАКСИМУМ

Максим ДЕЕВ
технический директор ARinteg

Новости о резонансных кибератаках убеждают в необходимости работать на предупреждение и усиливать информационную защищённость компаний. Вспомним хотя бы три из числа наиболее заметных кибератак 2024-го. Тогда NPD оказалась лёгкой добычей хакеров: из-за крайне низкой защищённости она поплатилась кражей 3 млрд строк персональных данных, содержащих имена, номера соцстрахования, адреса жителей разных стран. По словам РБК, эти данные стали золотой жилой для киберпреступников, они активно предлагали базу на теневых рынках для использования в мошеннических схемах. В другом случае хакерам удалось парализовать работу электронных систем 13 аэропортов Мексики, пригрозив утечкой трёх терабайт данных, если не будет выплачен выкуп. Наконец, атака вируса-вымогателя на корпорацию CDK Global сказалась на работе почти 15 тыс. компаний и обернулась совокупным убытком в $1 млрд.

Одной из действенных мер, позволяющих усилить информационную защищённость компаний, будет комплексный пентест. Он доступен и сравнительно небольшим организациям. На мой взгляд, главное, что требуется от пентеста, — быть эффективным. С акцентом на это и разберём: когда и зачем его проходить, какой отчёт получать по итогам, нюансы подготовки и выбора команды.

Напомню, что основная задача пентеста — смоделировать поведение злоумышленников и подтвердить возможность нанести финансовый, репутационный ущерб бизнесу во время реальной кибератаки. Он позволяет оценить защищённость информационной системы, проверить готовность специалистов к отражению атак, определить, насколько эффективны политики в области ИТ-безопасности, что можно усовершенствовать.

Как отмечает Help Net Security, в 2024 году средняя стоимость восстановления после атак шифровальщиков достигла $2,73 млн (+ $1 млн к 2023 г.). ExtraHop в своём отчёте, проанализировав долгосрочные финансовые последствия громких утечек публичных компаний, пришла к выводу, что организации сильно недооценивают последствия успешных кибератак, пока не окажутся в центре одной из них. По их расчётам, в среднем одна подобная утечка обходилась им в $677 млн.

Да, атаки на такие компании более заметны, но и небольшой бизнес хакеры не обходят стороной, сейчас все под угрозой. Согласно Help Net Security, в 2024 году более 50% жертв программ-вымогателей имели в штате менее 200 сотрудников, а 66% — менее пятисот.

Так что выбор для компаний невелик: либо проводить регулярные пентесты и повышать уровень защищённости, либо в какой-то момент стать объектом кибератаки с непредсказуемыми последствиями. По данным Positive Technologies, в 2024 году каждый второй киберинцидент в России нарушал бизнес-процессы компаний.

ИТАК, ВЫ НАЦЕЛЕНЫ ПРОЙТИ ПЕНТЕСТ

Во время подготовки к пентесту важно перепроверить ИТ-инфраструктуру, понять готовность к внешним ИБ-исследованиям. При необходимости — получить согласования от заинтересованных сторон (в том числе юридического отдела, владельца систем и т.д.). Правда, последнее не относится к тем случаям, когда пентест нацелен на проверку, к примеру, ИБ-персонала компании и призван показать, как специалисты будут реагировать на факт атаки. В этом случае тестирование для них оказывается «сюрпризом».

Для достижения цели в ходе пентеста используются разные сценарии хакерской атаки. Демонстрация того, как злоумышленник мог бы использовать ту или иную уязвимость и легко похитить данные или нарушить работу системы, зачастую производит большое впечатление и заставляет серьёзно задуматься о безопасности.

Порой такое сценарии бывают банальными, к примеру, по логину admin или взломав Wi-Fi, можно попасть во внутреннюю сеть, а там ничего не разграничено и есть доступ ко всему. Не стоит забывать, что некоторые принтеры раздают Wi-Fi. Достаточно к такому устройству подключиться, выполнить удалённое исполнение кода, и принтер становится мостом во внутреннюю сеть предприятия. Но любопытна скорее цепочка получения результата, и чем она длиннее, тем интереснее.

КОГДА И ЗАЧЕМ СТОИТ ПРОХОДИТЬ ПЕНТЕСТ?

Во всех случаях, если:

1. столкнулись с инцидентом или утечкой данных;
2. не проводили пентесты больше года;
3. внедрили новые сервисы или собираетесь это сделать;
4. предстоит развёртывание новой инфраструктуры (например, облачной платформы);
5. ожидается пик нагрузки (вследствие «чёрной пятницы» или «кибер-понедельника»);
6. перед крупным мероприятием, где используется онлайн-платформа;
7. вы стали отвечать за всё направление ИБ;
8. вам надо подтвердить соответствие нормативным требованиям (ряд законов и стандартов, к примеру PCI DSS, требуют проведения регулярных проверок безопасности);
9. отработали рекомендации предыдущего пентеста.

Тестирование на проникновение помогает своевременно выявить слабые места и подготовиться к потенциальным кибератакам в период проведения акций, распродаж, любых заметных мероприятий, поскольку такая активность со стороны компании обращает на себя внимание злоумышленников.

Выручит пентест и нового руководителя ИБ-направления. Да, ему не всегда всё расскажут, и нет гарантии того, что всё будет отражено в документации. Поэтому для него лучшая история, чтобы быстро понять, в каком состоянии находится ИТ-инфраструктура, — это провести полноценный пентест. Он покажет реальное положение дел с информационной безопасностью в компании, в том числе насколько качественно настроены имеющиеся СЗИ, позволит оценить их эффективность, поможет разработать стратегию развития ИБ.

КАКОЙ ОТЧЁТ ПОЛУЧАЕМ?

По итогам пентеста интересно получить подробный отчёт с глубоким анализом недопустимых событий, где указываются модель нарушителя, возможные векторы атак, приводятся оценки временных и материальных затрат на её проведение, прописываются найденные уязвимости, степень их критичности, к чему эксплуатация каждой из них может привести. А также даётся оценка их влияния на бизнес-процессы с рекомендациями по усилению средств защиты, оптимизации настроек, вплоть до того, какие СЗИ стоит приобрести с тем, чтобы закрыть обнаруженные уязвимости и повысить уровень защищённости. Мы такой отчёт предоставляем. В нём отмечаем, какие используем передовые технические решения и свои наработки. Пример такого всестороннего обезличенного отчёта можно запросить на сайте ARinteg в разделе «Тестирование на проникновение», оставив заявку.

Что из отчёта может узнать, каких рисков избежать, рассмотрим на одном из примеров.

Это был комплексный анализ защищённости: внешней и внутренней инфраструктуры, веб-ресурсов, мобильных приложений по модели «белого ящика». Атакующие добились полного контроля над системами заказчика, оценка уязвимостей проводилась по шкале OWASP и CVSS.

Тестирование внешней инфраструктуры выявило критическую уязвимость удалённого выполнения кода для хостов. В случае успешной эксплуатации она позволяла неавторизованному пользователю удалённо провоцировать сбои в работе устройств. Кроме этого, были выявлены уязвимости: переполнения буфера, удалённого кода, раскрытия чувствительной информации, в том числе и самая распространённая — устаревшее ПО.

При аудите защищённости веб-приложений обнаружилось, что учётные, чувствительные данные находятся в открытом доступе, то есть под угрозой в случае их утечки оказалась бы репутация компании.

Среди уязвимостей средней степени риска — раскрытие внутренней информации и о системе, вплоть до утечки данных служб DNS, то есть кто угодно мог видеть, какие сайты посещались и какими веб-приложениями пользовались. Причиной тому могла быть некорректно настроенная VPN-услуга, конфликт IPv6 или хакерская атака.

Внутренний пентест выявил использование ряда протоколов, паролей пользователей в открытом виде, открытые административные интерфейсы, пароли, заданные производителем, и т.п. Их эксплуатация позволяла атакующим реализовать все вероятные угрозы: нарушения целостности, доступности и конфиденциальности.

По результатам пентеста компании рекомендовалось провести обновление ПО до актуальных версий, ограничить публичный доступ по ряду адресов, убрать службу RTP с внешнего сетевого периметра, отключить вывод информации о точных версиях ПО и веб-серверов, не передавать пути к файлам и многое другое.

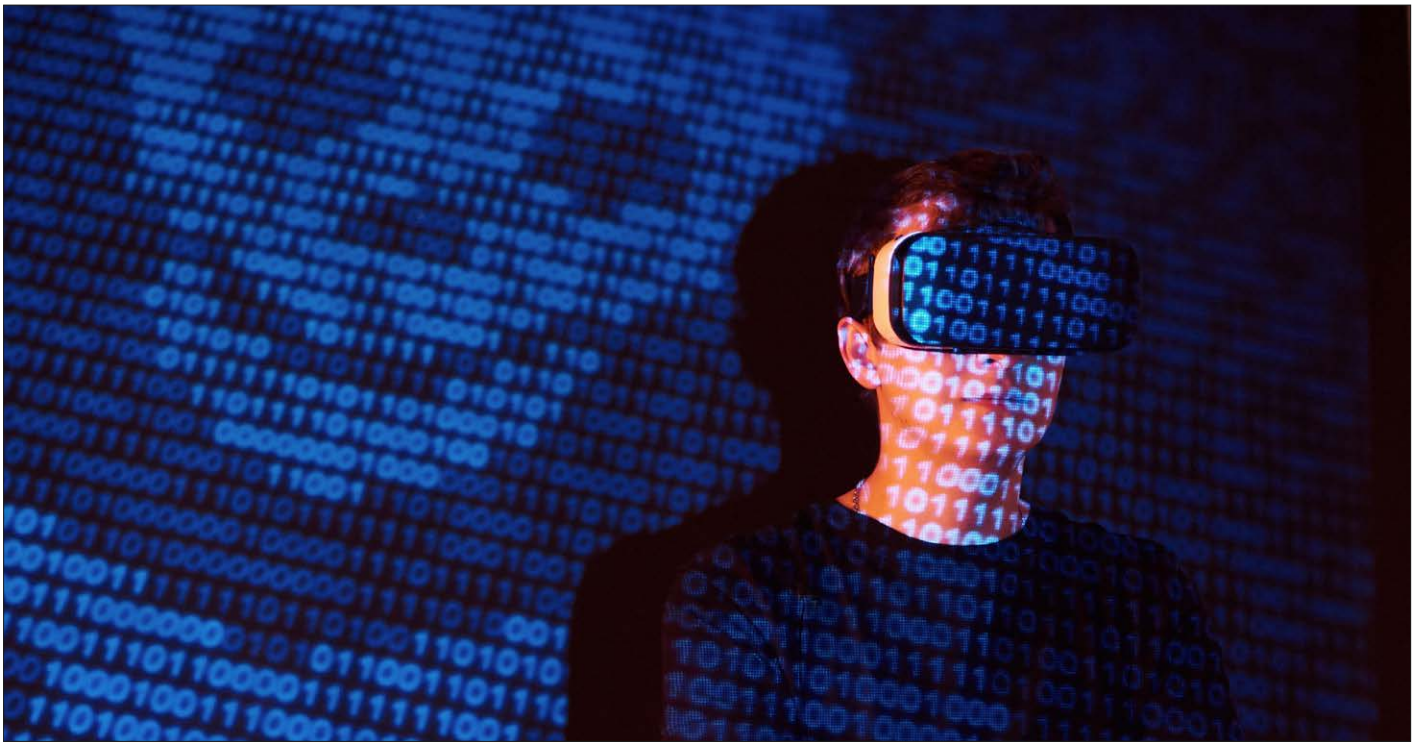
НА ЧТО СМОТРЕТЬ ПРИ ВЫБОРЕ ИСПОЛНИТЕЛЯ ПЕНТЕСТА?

На наличие сертификатов и лицензии ФСТЭК России, опыт работы в определённой отрасли, понимание её специфики. Полезно также запросить и изучить кейсы, отзывы, рекомендации заказчиков. Получить понимание уровня работы команды по тому, какое число пентестов и насколько успешно она провела.

ЧТО ЗНАЧИТ ХОРОШО ПРОПИСАННОЕ ТЗ?

Такое ТЗ максимально точно описывает, зачем проводится тестирование и какие задачи призвано решить, отражает все требования, исключает двусмысленные толкования и даёт чёткую картину того, что получаете на выходе.

В нём точно определены объекты тестирования (системы, приложения, сети), обозначены его границы, области и какие угрозы стоит учесть (утечка данных, фишинг, DDoS и прочее). Прописаны ограничения и исключения, ответственность сторон. Обозначены критерии успешности, какие этапы должны быть выполнены, учтены требования по неразглашению (NDA), сроки и время работ. Если быстрый пентест проводится за 1–7 дней и позволяет проверить отдельные компоненты (к примеру,



просканировать уязвимости веб-приложения) и оперативно выявить критические уязвимости, то глубокий пентест — это комплексное тестирование, которое занимает от 4 до 8 недель, он востребован и в том случае, когда требуется провести имитацию сложных и длительных атак.

УКРЕПЛЯЕМ СЛАБОЕ ЗВЕНО

При любой атаке самым уязвимым звеном будет человек, а потому атаки методом социальной инженерии будут в топе. Они настроены на то, чтобы любым способом заставить потенциальную жертву совершить нужное действие, а для этого её надо либо испугать (к примеру, сообщением: «ваш пароль успешно изменён» — и человек кликает по ссылке, не подумав), либо заинтересовать, либо пообещать выгоду.

В целях профилактики можно проводить учебные фишинговые атаки с максимально правдоподобными историями: под Новый год это письма от партнёров с подарками, путь к которым — переход по ссылке. С теми, кто на это попадается, проводить обучение.

В числе успешных недавних фишингов назову письма из псевдоРоскомнадзора о блокировках, письма о штрафах, также от псевдоhr может прийти письмо со списком сотрудников, подлежащих мобилизации, на это тоже нередко попадаются.

Не исключаются и «полевые занятия», допустим, с разбрасыванием флешек по офису. Обычно не более 20% сотрудников принесёт их в службу безопасности, остальные откроют их дома или на работе.

ПО ИТОГАМ ПЕНТЕСТА

Мы советуем максимально оперативно закрывать уязвимости, точно следовать рекомендациям отчёта и настраиваться на регулярные пентесты, это уже best practices, важный элемент ИБ-стратегии немалого числа компаний. Во время пентеста подсвечиваем заказчику уязвимости, чтобы по возможности он мог их сразу устранять или принимать компенсирующие меры. Если есть понимание критичности выявленной уязвимости, то такая работа выполняется максимально оперативно. Также рекомендуем быть готовыми миксовать экспертов для всестороннего исследования прочности киберграниц, хотя и здесь бывают исключения.

После того как компания отработает данные ей рекомендации, можно выходить на проверочный пентест, который покажет, как прошла работа над ошибками, удалось ли прийти в нужную точку или нет. Будет видна динамика, что станет весомым аргументом для руководства в проведении регулярных тестирований, которые позволят повысить текущий уровень ИБ компании и поддерживать её на высоком уровне.

* * *

ARinteg уже более десяти лет проводит пентесты для различных компаний, в том числе из финансовой сферы. Наши специалисты выступают спикерами ряда профильных мероприятий. Между проектами команда пентестеров проходит тренировки на различных площадках, например PortSwigger Academy, HackTheBox и многих других. Но чаще мы сами ставим уязвимые системы для отработки навыков. Так что постоянный мониторинг новых уязвимостей и мгновенная их отработка проходят на своих «грушах для битья». Всё это позволяет нам быстро выявлять уязвимости и предлагать эффективные решения по их устранению.

ALD PRO — ВОЛШЕБНАЯ КНОПКА ИМПОРТОЗАМЕЩЕНИЯ

ИЛИ ВЫЗОВЫ РОССИЙСКИХ РАЗРАБОТЧИКОВ

Евгений ПАУТОВ
директор по развитию серверного ПО, «Группа Астра»

Российские организации массово и активно переходят с зарубежных инфраструктурных программных продуктов на отечественные. Чаще всего — с разработок компании Microsoft, которая долго была лидером нашего ИТ-рынка, и мало кто мог предположить, что рано или поздно придётся искать замену её решениям. Само по себе импортозамещение — это серьёзный вызов как для ИТ-директоров, так и для администраторов ИТ-инфраструктур, объёмная задача, и она может занять несколько лет.

WINDOWS И LINUX

Если говорить о службах каталогов, то имеющийся на рынке софт для управления Linux-доменом не похож на тот, что привычен для администраторов MS Active Directory. Это относится не только к отечественному ПО, но и к Open Source. В службах каталогов для Linux другие терминология, интерфейс и подходы к работе. Почему так произошло?

FREEIPA

Windows и Linux существенно различаются архитектурой и идеологией построения. У разработчиков, которые создавали решения под Linux, например, FreeIPA, совершенно не было цели сделать что-то похожее на продукт для Windows. Они ориентировались именно на пользователей Linux с учётом специфики их ОС, и поэтому за основу службы каталогов ALD Pro мы взяли открытую FreeIPA. Но казалось бы, если есть готовое решение для администрирования Linux, зачем делать ещё и ALD Pro? К сожалению, у FreeIPA есть ограничения: нет возможности управлять параметрами компьютеров и пользователей, строить иерархии подразделений организации и т.д. Понимая всё это, мы добавили в ALD Pro эти функции, расширили возможности FreeIPA, и в итоге у нас получилось решение, которое позволяет закрыть задачи администраторов в части управления пользователями, компьютерами и серверами. Более того, мы не просто реализовали функционал, а ещё и разработали с нуля пользовательский графический интерфейс, который близок к MS Active Directory и по терминологии, и по методологии администрирования.

УЧЕБНЫЙ КУРС

Теперь перейдём непосредственно к пользователям. Как я говорил, импортозамещение — вещь достаточно длительная, но при этом все процессы и сервисы в ИТ-инфраструктуре должны работать бесперебойно, в том числе и служба каталогов. Несмотря на то что мы максимально постарались проработать интерфейс и функционал ALD Pro и сделать её похожей на Microsoft AD, всё же к ней требуется адаптироваться и приобрести определённые навыки. К тому же это Linux, значит, администраторам понадобится знание и самой ОС. Мы подумали об этом: разработали учебные курсы для тех, кто с Windows переходит на Linux. В программе два модуля: первый — это базовые принципы администрирования Linux, а второй — непосредственно управление доменом с помощью ALD Pro. Инженеры и разработчики продуктовой команды проработали курс достаточно глубоко, чтобы у администраторов сформировался надёжный фундамент знаний в новой для них области.

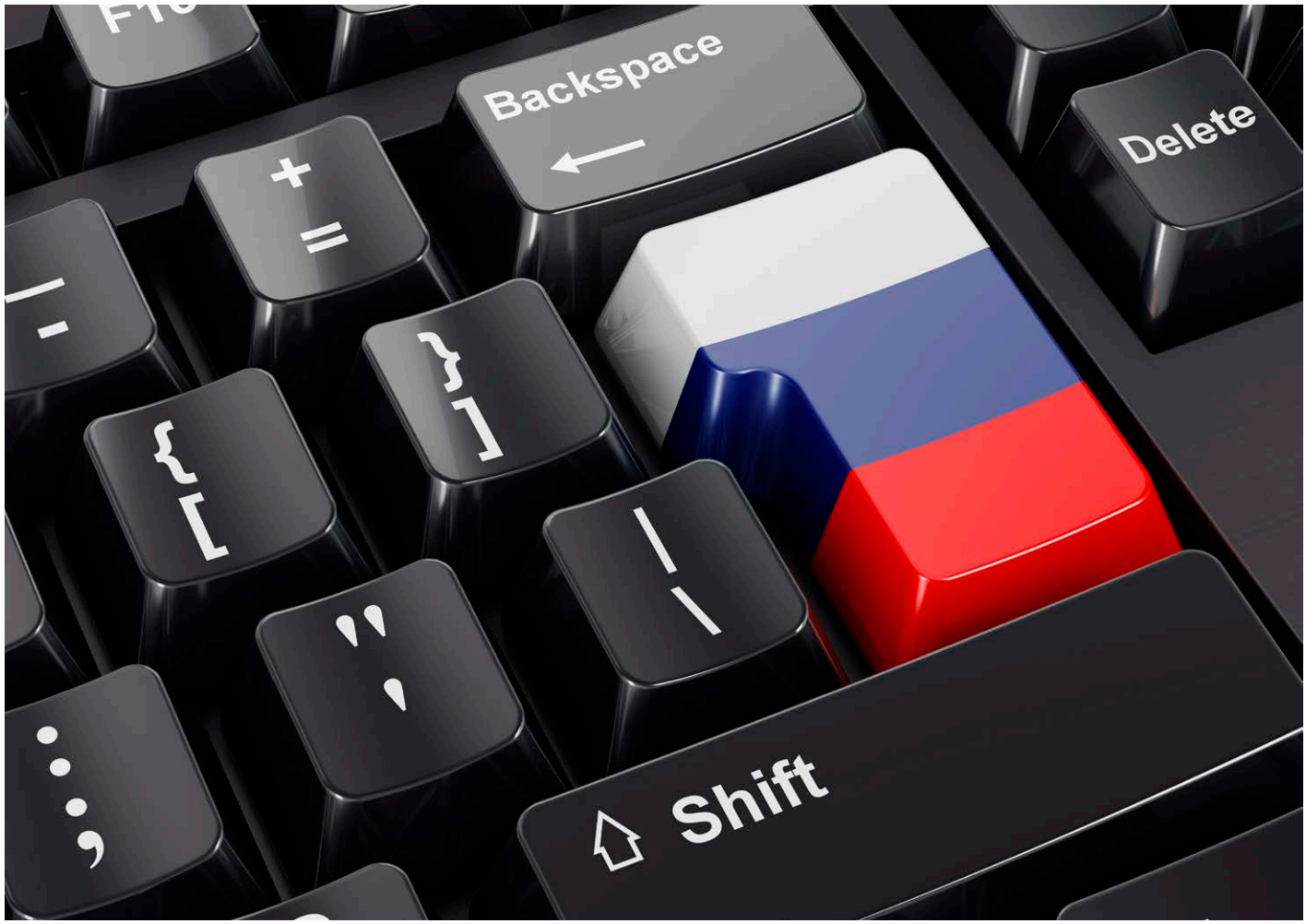
ГИБРИД

Есть ещё один немаловажный факт — миграция. Заказчикам какое-то время приходится пользоваться гибридной ИТ-инфраструктурой. Чтобы ALD Pro и MS AD успешно сосуществовали, мы выстроили между ними двусторонние доверительные отношения, сделали модуль синхронизации данных, глобальный каталог и многое другое, чего нет в конкурирующих продуктах.

Конечно, можно вспомнить и Samba — софт, который умеет работать с MS AD. Но он изначально создавался как доступная альтернатива MS AD, а не как полноценная служба каталогов для Linux. Поэтому если мы говорим о стратегическом выборе для построения именно Linux-инфраструктуры, то решения на основе FreeIPA более приоритетны.

БУКВА ЗАКОНА

При поиске альтернативы Microsoft Active Directory многие обращают внимание не только на функционал, но и на вопросы безопасности и соответствия требованиям законодательства. В ALD Pro мы учли эти аспекты и внедрили механизмы, которые обеспечивают высокий уровень защиты данных в соответствии с отечественными ИБ-стандартами.



БЕЗОПАСНАЯ РАЗРАБОТКА

Большинство российских разработчиков инфраструктурного ПО (в том числе и мы) сталкиваются с определёнными рисками при использовании зарубежных проектов. В случае с Open Source санкционные ограничения нивелируются тем, что Open Source — это мировое сообщество, и, если внезапно наши проекты отключат от «родительских», ситуацию можно решить созданием форков. Есть ещё один важный момент: исходный код открытого ПО может содержать уязвимости, и в нашей компании этот вопрос решается благодаря выстроенным процессам безопасной разработки, куда входят, помимо прочего, поиск и устранение уязвимостей.

ОРИЕНТАЦИЯ НА РЫНОК

Нередко можно услышать, что функционал отечественных продуктов недостаточно зрелый, широкий и в этом уступает аналогам от Microsoft. Но нужно помнить, что MS AD разрабатывали более двух десятилетий, так что рано или поздно мы её обязательно догоним и перегоним. Наша команда ориентируется в первую очередь на рынок и реализует то, что нужно клиентам сегодня. Мы учитываем специфику их инфраструктур, требования безопасности, особенности и пожелания.

Сейчас многие компании заинтересованы в развитии технологий SSO, IDM-решениях, мониторинге логов, построении отчётности, работе с облачными сервисами и т.д.

КООПЕРАЦИЯ И ИНТЕГРАЦИЯ

Любой рынок — это не только конкуренция, но и кооперация, совместная работа над продуктами и проектами. Мы активно прорабатываем интеграционные возможности, которые позволят создавать комплексные решения. ALD Pro уже успешно прошла тесты на совместимость с более чем 30 достаточно известными и популярными российскими приложениями и сервисами, и такая синергия помогает ускорить и расширить импортозамещение. Ведь очень часто препятствием в этом деле становится то, что выбранный продукт не умеет работать с приложениями и сервисами, которыми привык пользоваться клиент. Чем больше продуктов разработчик сможет охватить в вопросе интеграции, тем больше вероятность, что его ПО встроится в любую ИТ-инфраструктуру. Сотрудничество с вендорами других операционных систем тоже полезно: оно расширяет потенциал продукта в плане их поддержки. Эту совместимость надо развивать и поддерживать, чтобы очередное обновление ОС другой компании не «сломало» что-то в нашем ПО и не обернулось для заказчика неприятным сюрпризом. Поэтому желательно наладить взаимодействие и синхронизировать процесс разработки.

ЗАЩИТА УЧЁТНЫХ ЗАПИСЕЙ

КАК ОБЕСПЕЧИТЬ СООТВЕТСТВИЕ ТРЕБОВАНИЯМ РЕГУЛЯТОРОВ В ФИНАНСОВОЙ СФЕРЕ?

Михаил РОЖНОВ
технический директор MFASOFT

Защита учётных записей — одна из ключевых областей успешной практики информационной безопасности, а также предмет нормативных требований. Разберём требования PCI DSS4.0 и ГОСТ 57580 к защите учётных записей, а также то, как выполнить их с помощью российского программного комплекса Secure Authentication Server компании MFASOFT.

Большинство взломов происходят из-за компрометации пользовательских учётных записей, и именно поэтому к их защите подходят с большим вниманием. Однако при выборе комплексной стратегии ИБ в финансовых организациях возникает вопрос: на какой из стандартов стоит ориентироваться в первую очередь?

Чтобы ответить на него, нужно разобраться, чем отличаются требования самых важных стандартов информационной безопасности в финансовой сфере: отечественного ГОСТ 58570 и международного PCI DSS в редакции 4, которая пока не переведена официально на русский язык. Заметно, что при создании ГОСТ 57580 специалисты ориентировались на приказы ФСТЭК 17 и 21, а также явно повторили основные положения PCI DSS. Поэтому большинство решений, для которых выполняются требования PCI DSS, будут соответствовать ГОСТ 57580 и наоборот. Но есть и различия.

КАКОЙ СТАНДАРТ СТРОЖЕ?

Оба стандарта определяют одни и те же факторы доступа к учётным записям: знание (например, пароль), владение (например, токен) и биометрия. Однако PCI DSS разделяет многофакторную и многоэтапную аутентификацию. Для входа в систему пользователь должен предоставить два или более факторов, причём разной природы, но если пользователь видит результат проверки фактора после каждого этапа, то согласно PCI DSS это уже не многофакторная, а многоэтапная аутентификация.

Также оба норматива подразумевают наличие уникальных учётных записей, хотя использование общих аккаунтов PCI DSS в отдельных случаях допускает. Хранение и передача учётных данных в открытом виде запрещены по ГОСТ 57580, а PCI DSS требует надёжной криптографии, то есть использования принятых и проверенных отраслью алгоритмов с эффективной стойкостью ключа не менее 112 бит и надлежащими практиками управления ключами.

Кроме этого, в PCI DSS предусмотрено специальное требование для сервис-провайдеров, которые обслуживают сразу несколько систем: им необходимо вести уникальный фактор для каждой системы. Оба стандарта предписывают блокировать на 30 минут доступ в систему при неудачных попытках входа. В PCI DSS ограничение количества попыток — 10, тогда как ГОСТ 57580 оставляет этот параметр на усмотрение администратора. Стандарты также предписывают протоколирование процессов аутентификации и длительное хранение событий для возможного анализа.

Пересмотр прав пользователей по требованиям обоих стандартов должен производиться регулярно — в среднем не реже 1 раза в 6 месяцев. Но если PCI DSS призывает ориентироваться на активность учётных записей, то ГОСТ 57580 предписывает сопоставлять учётные записи с реальным персоналом и отключать аккаунты для уволенных сотрудников и подрядчиков, закончивших свою работу.

Однако, когда речь идёт о выборе пароля, более подробные и слож-

Чтобы соответствовать требованиям обоих стандартов, в большинстве аспектов можно полагаться на более строгие требования PCI DSS, а в вопросах выбора пароля лучше реализовать положения ГОСТ 57580

ные требования предъявляет именно ГОСТ 57580. В положениях PCI DSS указано, что пароль должен быть не менее 12 символов, тогда как ГОСТ требует 16 символов и задаёт разные параметры для разных групп, что реализовать сложнее. PCI DSS предписывает использовать буквы и цифры, ГОСТ 57580 — также символы и буквы разного регистра. Дополнительно по положениям ГОСТ 57580 пароль не должен быть легко вычисляемым и не должен повторять ни один из предыдущих.

Таким образом, чтобы соответствовать требованиям обоих стандартов, в большинстве аспектов можно полагаться на более строгие требования PCI DSS, а в вопросах выбора пароля лучше реализовать положения ГОСТ 57580.

КАК ВЫПОЛНИТЬ ТРЕБОВАНИЯ?

Сейчас одним из важнейших разделов требований к защите учётных записей является многофакторная аутентификация (multi-factor authentication, MFA). В PCI DSS версии 4 она обязательна для неконсольного доступа администраторов и для любого доступа к CDE (Cardholder Data Environment, среда данных держателей карт). Согласно ГОСТ 57580 она требуется для аутентификации эксплуатационного персонала, а также для всех пользователей, имеющих удалённый доступ.

Все эти требования можно реализовать при помощи доступных на российском рынке коробочных программных продуктов. Рассмотрим, как эту задачу решает программный комплекс Secure Authentication Server (SAS) компании MFASOFT. SAS — полностью российское решение, входит в реестр российского ПО. SAS имеет сертификат ФСТЭК по 4-му уровню доверия, что делает продукт одним из наиболее подходящих для реализации требований обоих стандартов.

СООТВЕТСТВИЕ ТРЕБОВАНИЯМ «ИЗ КОРОБКИ»

SAS уже сегодня используется в российских компаниях, обеспечивая соответствие самым строгим требованиям стандартов за счёт встроенных в него функций. Разберём его возможности на примерах конкретных положений PCI DSS.

Пункт 8.2.1. Все действия пользователей должны относиться к уникальному субъекту. Все субъекты доступа в SAS имеют уникальный идентификатор, поэтому любая операция однозначно определяет субъект доступа.

Пункт 8.2.2. Все действия, выполняемые пользователями с генерируемыми, системными или общими идентификаторами, должны однозначно определять субъект доступа. В качестве дополнительного фактора идентификации субъекта используется уникальный номер аутентификатора.

8.2.4. События жизненного цикла для идентификаторов пользователей и факторов аутентификации не должны происходить без соответствующего разрешения. SAS содержит встроенные механизмы аутентификации при доступе к консоли администрирования, ограничения для администраторов (IP-адреса, дни недели), разграничение доступа на уровне тенантов (виртуальных серверов) и разделов консоли администрирования.

Пункт 8.2.5. У пользователей, отношения с которыми прекращены, доступ должен быть немедленно отозван. SAS периодически выполняет синхронизацию по LDAP через специальный программный агент. Пользователи, которые заблокированы в каталоге LDAP или у которых истёк срок действия учётной записи, помечаются в системе как заблокированные. Также можно вручную или через правила ограничить срок действия учётной записи или группы.

Пункт 8.2.6. В случае неактивности субъекта доступа более 90 дней он должен быть удалён или заблокирован. В SAS можно установить автоматическую блокировку учётной записи, если она долго не используется. Дополнительно можно настроить автоматический отзыв токенов у заблокированных пользователей, что позволяет не только выполнять требования стандарта, но и экономить на стоимости лицензий, если выбрана модель оплаты по фактическому использованию.

Пункт 8.3.1. Доступ к объекту не должен быть предоставлен без указания пользовательского идентификатора и фактора аутентификации. SAS проверяет один или несколько факторов. Аутентификаторам можно назначать ПИН-код, и тогда при входе нужно вводить динамический пароль, состоящий из ПИН-кода и одноразового пароля, представляющих разные факторы.

Пункт 8.3.3. Неавторизованный пользователь не может получить доступ к системе, выдав себя за другого авторизованного субъекта доступа. SAS позволяет заново инициализировать факторы аутентификации, для которых нужно подтвердить личность пользователя, включая сброс ПИН-кода или перевыдачу токенов.

Пункт 8.3.4. Фактор аутентификации не может быть угадан атакой brute force. SAS позволяет временно блокировать учётную запись при попытках перебора и автоматически разблокировать её через определённый интервал времени.

Пункт 8.3.11. Фактор аутентификации не может быть использован кем-то ещё, кроме субъекта, которому он был назначен. Для этого в SAS для аутентификаторов отдельных типов можно задать ПИН-код, известный только владельцу токена.

Подробнее о компании MFASOFT и программном комплексе Secure Authentication Server:
https://mfasoft.ru

СООТВЕТСТВИЕ ТРЕБОВАНИЯМ В 2025-М

КОМПЛЕКСНЫЙ АУДИТ И КОНСАЛТИНГ ДЛЯ ИСПОЛНЕНИЯ НОРМ УКАЗА ПРЕЗИДЕНТА РФ № 250

Олег ИВАНОВ
генеральный директор ГК «ЦИБИТ»

Евгения КОЛОДИНА
первый заместитель генерального директора ГК «ЦИБИТ»

1 мая 2022 года Президент России Владимир Путин подписал Указ № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации». В целях повышения устойчивости и безопасности функционирования информационных ресурсов России документ ввёл целый ряд новых требований к обеспечению информационной безопасности на предприятиях страны.

Ключевые требования, введённые Указом № 250, коснулись:

- кадровых вопросов (создание на предприятиях, подпадающих под действие документа, структурных подразделений по информационной безопасности; возложение обязанностей руководителя такого подразделения на сотрудника в ранге заместителя руководителя организации; возложение на руководителя организации персональной ответственности за обеспечение информационной безопасности);
- вопросов импортозамещения (прекращение использования иностранного программного обеспечения и средств защиты информации с 1 января 2025 года).

У организаций, подпадающих под действие Указа, было два с половиной года на выполнение требований документа и внедрение необходимых новшеств и изменений в свою работу.

Олег Иванов:

— *Группа компаний «ЦИБИТ» работает 15 лет на рынке консалтинговых услуг в области информационной безопасности. Мы внимательно следим за развитием отрасли и, конечно, за изменениями, происходящими в законодательстве.*

Мы обратили пристальное внимание на введённые Указом Президента РФ № 250 требования, для выявления особенностей и потребностей рынка мы провели с нашими экспертами серию открытых вебинаров по ключевым нововведениям, после чего разработали комплексную консалтинговую услугу по приведению в соответствие требованиям Указа. Услуга включает несколько направлений – от консалтинга по лицензированию и аудита информационной безопасности для оценки уровня защищённости (в соответствии со ст. 4 Указа № 250) до кадрового подбора и непрерывного обучения специалистов по образовательным программам, согласованным с регулирующими организациями в области ИБ.

Таким образом, мы разработали универсальное решение, позволяющее обеспечить полное соответствие требованиям Указа в обозначенные сроки.

На момент публикации Указа, по нашим оценкам, в стране не хватало более 50 тысяч квалифицированных и соответствующих требованиям Указа специалистов

Одна из главных проблем, на которую обращает внимание Указ Президента России № 250, – острейший дефицит кадров в отрасли информационной безопасности России. На момент публикации Указа, по нашим оценкам, в стране не хватало более 50 тысяч квалифицированных и соответствующих требованиям Указа специалистов.

Евгения Колодина:

– *В состав ГК «ЦИБИТ» входит собственное кадровое агентство, которое помогает решать кадровые вопросы компаниям по всей стране уже больше 9 лет. И в рамках приведения в соответствие требованиям нового нормативного документа мы сразу же готовы были предложить нашим клиентам два решения – подбор сотрудников нашими профессиональными рекрутерами, которые знают всё об актуальных законодательных нормах, и обучение действующих работников, позволяющее получать необходимые компетенции.*

С уверенностью могу сказать, что, несмотря на продолжающийся кадровый голод в сфере кибербезопасности (в 2024 году количество вакансий в отрасли выросло на 18% по сравнению с

2023 годом), все клиенты нашего кадрового агентства сегодня выполняют требования Указа № 250.

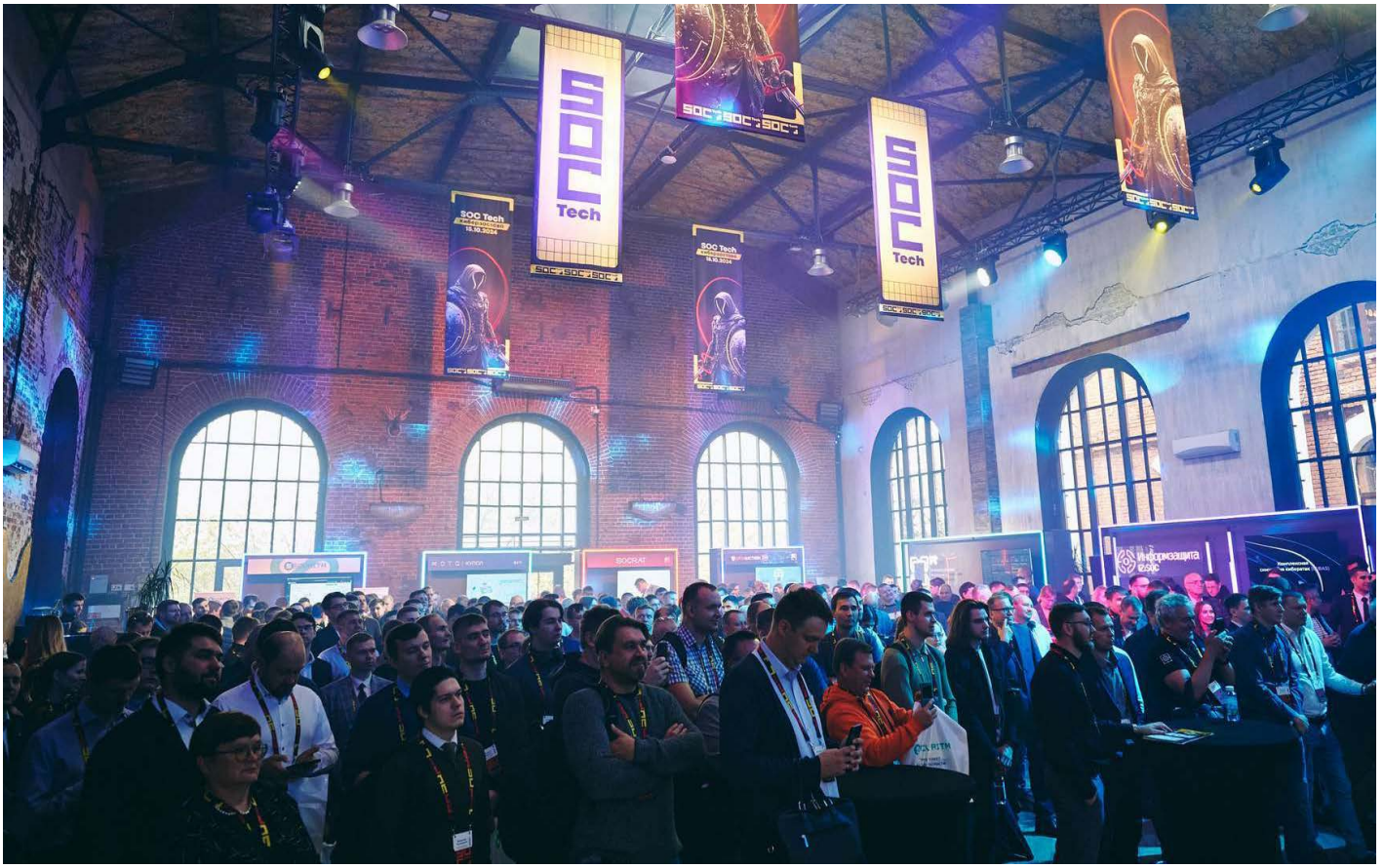
Кстати, судя по запросам работодателей в 2024 году, вопрос соответствия Указу № 250 по-прежнему актуален для очень большого количества компаний. Наш собственный рейтинг самых востребованных сотрудников возглавляет именно специалист по информационной безопасности. Отмечу, что также в списке самых нужных сейчас – архитекторы и инженеры по ИБ. А вот топ наиболее высокооплачиваемых специальностей в ИБ сегодня открывает именно руководитель службы кибербезопасности. И это неудивительно, учитывая высочайшую степень ответственности, возложенную на этих сотрудников, в том числе нормами Указа Президента № 250.

Отдельного внимания заслуживает проблема импортозамещения в сфере защиты информации, в том числе на объектах критической информационной инфраструктуры РФ (КИИ РФ). В соответствии с Указом Президента № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» и Указом Президента № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» полностью отказаться от зарубежного софта подпадающие под действие документов организации должны были до 1 января 2025 г. По информации экспертов ЦИБИТ на декабрь 2024 года, лишь около 20% таких компаний обеспечили полный переход на отечественные решения.

Олег Иванов:

— Конечно, достижение технологической независимости является одной из приоритетных целей для обеспечения киберустойчивости национальной экономики, при этом процесс требует времени и ресурсов. Иностранные производители разрабатывали и внедряли свои системы годами (если не десятилетиями), а нам предстоит реализовать переход в сжатые сроки. Но, несмотря на трудности, уже сейчас мы видим, что темпы импортозамещения довольно высокие: по оценкам Минцифры РФ, на конец 2023 года доля иностранных средств защиты информации составляла только 11%.

ЦИБИТ и в этом вопросе приходит на помощь. Мы оказываем комплексную услугу по проведению аудита применяемых средств и систем защиты информации в компании. Такая проверка позволяет обследовать организацию на наличие СЗИ с недействующими сертификатами, а также СЗИ, выпущенными в недружественных странах. Результатом работ является построение «с нуля» надёжной системы защиты информации или модернизация имеющейся системы.



КИБЕРЗАСТАВА SOCTECH

КРУГЛЫЙ СТОЛ О РАЗВИТИИ ПРОФЕССИОНАЛОВ В ИБ

В рамках конференции SOCTech состоялся круглый стол «Инструменты консолидации и систематизации работы бизнеса, образования и государства для развития профессионалов в сфере ИБ», организованный центром компетенций «Кибербезопасность» НТИ «Энерджинет»[1] (далее — группа «Кибербезопасность»), на котором были рассмотрены вопросы развития системы подготовки профессионалов для сферы информационной безопасности (ИБ).

РЯД ВОПРОСОВ

Повышенное внимание к данной теме обусловлено тем, что на текущий момент нет однозначного ответа по ряду вопросов:

- какова количественная и качественная оценка дефицита специалистов сферы ИБ, в том числе с учётом отраслевой и региональной специфики;
- какие компетенции специалистов сферы ИБ востребованы на текущий момент на рынке труда и в ближайшей перспективе;
- какова степень соответствия выпускников высшей школы и среднего специального образования (СПО) требованиям работодателей;
- какие подходы необходимы к независимой оценке квалификации специалистов.

Общая повестка по теме кадров гораздо шире, тем не менее дискуссия по вышеперечисленным вопросам носила наиболее острый характер.

ГРУППА «КИБЕРБЕЗОПАСНОСТЬ»

Эти вопросы затрагивались в рамках деятельности группы «Кибербезопасность», реализовавшей ряд проектов, в том числе и отчёты, затрагивающие подготовку кадров в области ИБ. При этом существенным моментом является статус и состав группы. Во-первых, она является общественным объединением специалистов, во-вторых, в её работе участвуют представители вузов, вендоров, интеграторов и иных компаний с равными правами голоса. Таким образом, вырабатываемые подходы носят независимый и объективный характер.

КАРТА И МАТРИЦА

Работа круглого стола началась с ключевого доклада лидера группы, руководителя отдела по развитию бизнеса InfoWatch ARMA Алексея Петухова. Он предложил скоординировать от имени группы усилия всех заинтересованных в области подготовки профессионалов.В качестве платформы для объединения предлагается открытая карта по развитию профессионалов ИБ (рис. 1), основ-

[1] Подробнее см. https://energynet.ru/people

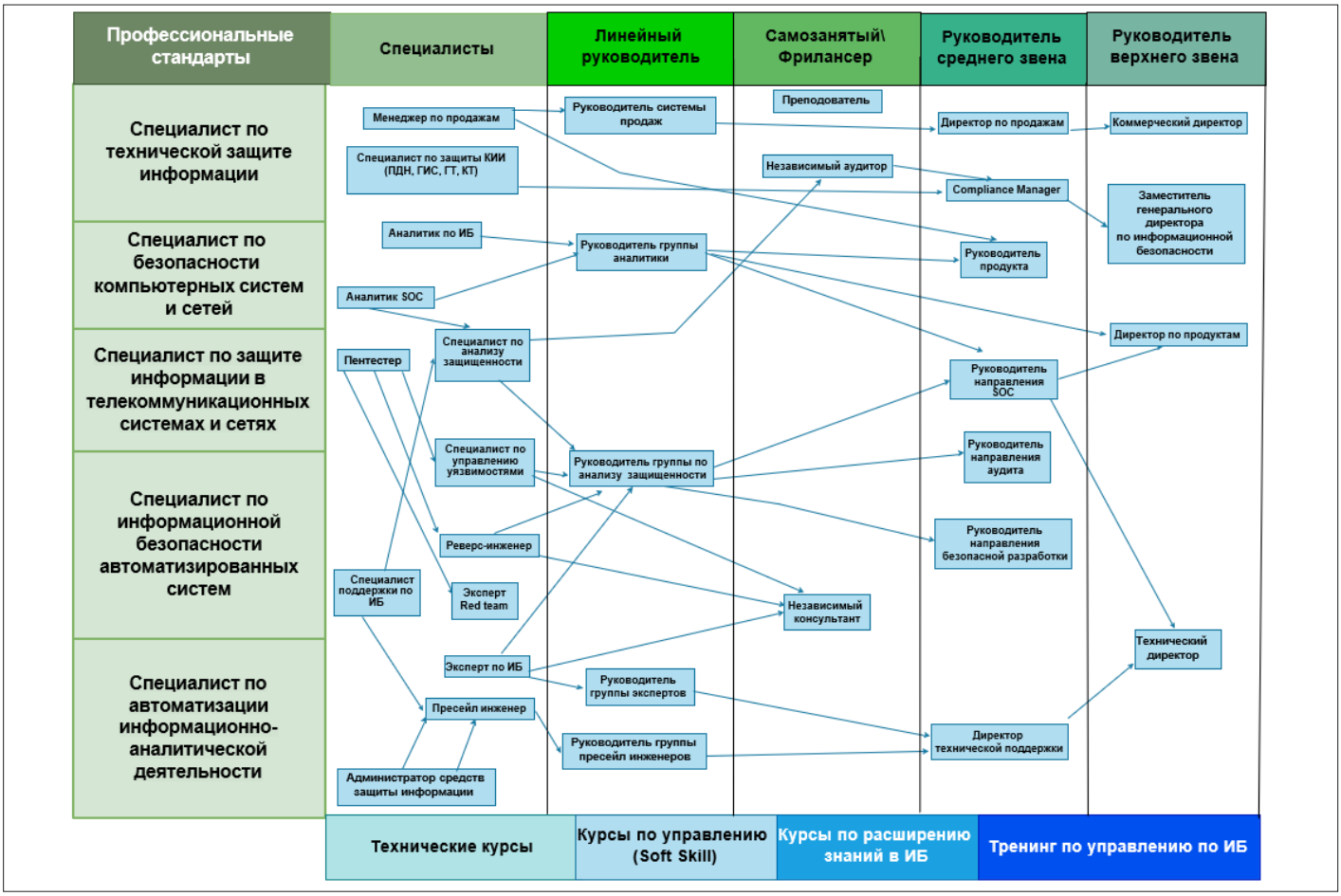


Рисунок 1. Карта развития профессионала

ными элементами которой являются роли специалистов по информационной безопасности, и описание каждой роли через матрицу компетенций (рис. 2), которое позволяет согласовать среди всех заинтересованных сторон фактические и нормативные требования.

Стоит отметить, что указанная карта составлена с учётом действующих профессиональных стандартов, фактического запроса работодателей и уровней иерархии, сложившихся в области обеспечения информационной безопасности. Как уже было отмечено, элементами карты являются роли (набор функциональных задач), реализуемые сотрудниками в зависимости от выбранного направления и уровня в иерархии. На этапе разработки карты было выявлено, что в настоящее время имеющийся набор принятых профессиональных стандартов описывает не все роли специалистов сферы ИБ, присутствующие на рынке труда. С другой стороны, часть работодателей ищет специалистов с набором компетенций, который однозначно можно трактовать как уникальный, что, как правило, приводит к увеличению сроков закрытия вакансий.

В ходе выступления также было отмечено, что, кроме карты развития профессионалов, требуется вести активное и обширное общение всех участников образовательной системы для создания единого информационного поля. С этой целью предлагается развивать открытый чат в «Телеграме» (*https://t.me/ProfessionalIB_Chat*), который позволяет не только координировать работу над картой и матрицей компетенций сотрудников сферы ИБ, но также обмениваться участникам тематическими новостями, информацией о планируемых мероприятиях и вести дискуссии.

НУЖНЫ НЕ СУПЕРМЕНЫ

В развернувшейся дискуссии по докладу в качестве экспертов приняли участие директор департамента цифровых технологий ТПП РФ В. А. Маслов, заведующий кафедрой комплексной безопасности критически важных объектов РГУ нефти и газа (НИУ) им. И. М. Губкина Д. И. Правиков, заместитель руководителя экспертной группы по кибербезопасности Ассоциации «Цифровая энергетика» А. В. Капустин и другие эксперты.

В. А. Маслов обратил внимание на активный поиск специалистов в области обеспечения ИБ со стороны государственных структур и предприятий, в том числе относящихся к объектам КИИ. Он высказал мнение о необходимости при поиске специалистов в области ИБ точно указывать требования к их квалификации, а не пытаться найти «сверхспециалистов», обладающих гиперкомпетенциями в ИБ, и решать вопросы обеспечения защиты информации за счёт одного специалиста.

Также В. А. Маслов поддержал идею взаимодействия представителей образовательной сферы с предприяти-

	Данные НН				
Вакансия	**Требования к опыту**	**Действие**	**Умения**	**Знания**	**Трудовые функции**
Инженер по информационной безопасности	1. Высшее образование в области информационных технологий, кибербезопасности или смежных областей	?	?	?	1. Анализировать существующую систему безопасности в компании и находить ошибки
	2. Опыт работы в сфере информационной безопасности от 2 до 5 лет	?	?	?	2. Участвовать в категорировании объектов информатизации, выявлении угроз безопасности информации и технических каналов утечки информации.
	3. Знание основных стандартов и методов обеспечения информационной безопасности, таких как ISO 27001, COBIT, ISA 62443	?	?	?	3. Проектировать комплексное решение по обеспечению безопасности информации, хранимой или обрабатываемой компанией
	4. Умение работать с различными технологиями и инструментами в области кибербезопасности, такими как файрволы, антивирусы, системы обнаружения вторжений и шифрования данных	?	?	?	4. Участвовать в определении потребности в средствах технической защиты информации, составлять заявки на их приобретение, контролировать поставку и использование
	5. Опыт участия в проектах по аудиту и оценке информационной безопасности, а также опыт разработки и внедрения политик и процедур безопасности	?	?	?	5. Составлять техническое задание по внедрению выбранных механизмов защиты данных

Рисунок 2. Матрица компетенций

ями, компаниями и организациями при формировании учебного плана подготовки специалистов в сфере ИБ, подчеркнув, что на выполнение Указов Президента России № 250 и 166 осталось не так много времени — до 1 января 2025 года.

Д. И. Правиков отметил, что одной из актуальных задач, которые сейчас стоят перед высшим образованием, является обеспечение и подтверждение качества подготовки выпускников высших учебных заведений, получивших подготовку по укрупнённой группе специальностей «информационная безопасность». Без формального определения компетенций нельзя организовать проверку на их соответствие для специалистов. Вместе с тем указанные компетенции должны быть актуальными по отношению к задачам, решаемым специалистами по информационной безопасности у основной массы работодателей. В этих условиях предлагаемая карта является удобным механизмом согласования компетенций и, как следствие, требований к специалистам.

ОБЪЕДИНЯТЬ УСИЛИЯ

Предложенный подход как одну из основ для развития взаимодействия для решения озвученных проблем также поддержал заместитель руководителя экспертной группы по кибербезопасности Ассоциации «Цифровая энергетика». «Мы должны объединять усилия компаний и экспертного сообщества, вузов, собирать полезную информацию совместно, обмениваться опытом, помогать развитию молодых специалистов, помогать им адаптироваться для наиболее эффективной работы с учётом актуальных потребностей и приоритетов ключевых отраслей экономики», — отметил А. В. Капустин.

В частности, он отметил, что повышение осведомлённости в области ИБ среди компаний отрасли электроэнергетики — одна из задач Центра экспертизы по вопросам информационной безопасности в электроэнергетике («Энерго ЦИБ»), работающего при Ассоциации «Цифровая энергетика». На основании опыта отрасли во взаимодействии с ведущими учебными центрами эксперты АЦЭ планируют разработать учебные курсы

Профессиональный стандарт			
Трудовые функции	**Действие**	**Умения**	**Знания**
Тестирование систем защиты информации автоматизированных систем	Проведение анализа структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем	Анализировать основные характеристики и возможности телекоммуникационных систем по передаче информации	Принципы построения и функционирования систем и сетей передачи информации
	Выявление уязвимости информационно-технологических ресурсов автоматизированных систем	Анализировать основные узлы и устройства современных автоматизированных систем	Эталонная модель взаимодействия открытых систем
	Выявление основных угроз безопасности информации в автоматизированных системах	Применять действующую нормативную базу в области обеспечения безопасности информации	Основные угрозы безопасности информации и модели нарушителя в автоматизированных системах
	Составление методик тестирования систем защиты информации автоматизированных систем	Контролировать функционирование технических средств защиты информации	Основные меры по защите информации в автоматизированных системах
	Подбор инструментальных средств тестирования систем защиты информации автоматизированных систем	Восстанавливать (заменять) отказавшие технические средства защиты информации	Особенности защиты информации в автоматизированных системах управления технологическими процессами

по основам ИБ для руководителей и специалистов компаний отрасли, с учётом необходимых потребностей и компетенций для области ИБ в электроэнергетике. Предложенная карта компетенций может стать дополнительным инструментом для консолидации усилий совместного формирования и актуализации необходимых компетенций специалистов ИБ.

ПОЛЕЗНАЯ КАРТА

Дискуссия, в которой, кроме заявленных спикеров, приняли участие присутствовавшие в зале специалисты, позволила отметить, что представленная карта может быть полезна в решении следующих задач:

- формирование организационной и ролевой моделей специалистов по информационной безопасности внутри компании;
- формирование требований при аттестации специалистов в компании;
- подбор программ дополнительного профессионального образования.

КЛЮЧЕВЫЕ РЕЗУЛЬТАТЫ ДИСКУССИИ:

1. Представленный прототип открытой карты по развитию профессионалов в целом положительно воспринимается заинтересованными экспертами и может быть использован для заявленных целей описания компетенций специалистов по информационной безопасности. Представляется целесообразным продолжить её развитие в части описания ролей и соответствующих им компетенций.

2. Представленный прототип карты по развитию профессионалов ИБ является открытой платформой, позволяющей учитывать мнение заинтересованных сторон при описании отдельных ролей сотрудников по информационной безопасности. Присоединиться к доработке прототипа открытой карты можно, например, через участие в телеграм-чате *https://t.me/ProfessionalIB_Chat.*

3. Группа «Кибербезопасность» берёт на себя роль технической поддержки данной платформы, координации работ по ее наполнению.

Свои предложения можно высылать на почту группы «Кибербезопасность Энерджинет» (*EnergyNetCS@yandex.ru*).

КОНФЕРЕНЦИЯ «СЕТЕВАЯ БЕЗОПАСНОСТЬ»

Анна КАТАНКИНА
корреспондент BIS Journal

В Москве прошла первая конференция «Сетевая безопасность», соорганизатором которой выступила АНО «НТЦ ЦК». Участники мероприятия обсудили требования к межсетевым экранам уровня сети, защиту веб-приложений и электронной почты, обеспечение безопасности удалённого доступа, VPN-шлюзы и проблемы инспекции SSL/TLS-трафика, использование криптографии в сетевой безопасности, а также задачи зеркалирования и анализа трафика и другие актуальные вопросы обеспечения сетевой безопасности.

В рамках конференции состоялась дискуссия «Вопросы информационной безопасности управления сетевым трафиком», модератором которой выступил Сергей Минаков, заместитель генерального директора по проектной деятельности АНО «НТЦ ЦК».

Открывая обсуждение, С. Минаков остановился на специфических вопросах ИБ управления сетевым трафиком, связанных как с сетевым оборудованием, так и с протоколами. В первую очередь это динамическая маршрутизация. Есть несколько специфических угроз, связанных с искажением маршрутной информации: когда активное сетевое оборудование занимается передачей трафика по чужим маршрутам либо меняет свои, и атаки с захватом блоков адресов маршрутизации систем коммутации пакетов. Если речь идёт об IP-маршрутизации, то идёт захват блоков IP-адресов.

Этой проблеме много лет: впервые с реализацией атак на протоколы внешней (пограничной) маршрутизации (англ. — External Gateway Protocol, Border Gateway Protocol) специалисты столкнулись в 1997 году. Впоследствии

число атак нарастало, это связано с тем, что при взаимодействии между операторами связи разных стран должны соблюдаться требования по транзитивности трафика между странами, обязательства при международной передаче трафика вне зависимости от конкретных политических вопросов.

Сегодня активно обсуждают вопросы искажения маршрутов и «угона» трафика из США в Китай, из Мексики и США в Беларусь и Россию. Но при этом на международном уровне в сервисах мониторинга крайне мало обсуждается увод сетевого трафика из Российской Федерации и других стран, недружественных для стран Запада.

Спикер обратил внимание на два инцидента. В первом случае «неправильная» настройка маршрутизаторов в нескольких странах, в том числе в России, привела к закольцовыванию трафика. Он поступал из США и Нидерландов, проходил через «Ростелеком», уходил в Узбекистан, возвращался в «Билайн» и уходил дальше, в частности в сервисы и хранилища данных компании Amazon. В тот же период в течение получаса аналогичная атака была произведена через операторов Швеции и Италии, только трафик уходил в США на систему фильтрации Cloudflare.

Остаётся только предполагать, зачем и кем это было сделано, отметил С. Минаков. Он также подчеркнул, что эти инциденты не нашли широкого освещения в мониторинговых агентствах. И задача участников дискуссии — обсудить вопросы, связанные с безопасностью российских операторов связи, безопасностью управления сетевым трафиком и механизмами, которые и способствуют, и препятствуют этому. Модератор также напомнил, что в декабре 2024 г. Роскомнадзор проводил киберучения по управлению сетями связи, в которых участвовали некоторые регионы России и ФГУП «ГРЧЦ».

Сергей Хуторцев (ФГУП «ГРЧЦ») заметил, что Роскомнадзор и Центр мониторинга и управления сетью связи общего пользования уделяют большое внимание устойчивости и безопасности работы сетей связи.

Сергей Минаков, заместитель генерального директора по проектной деятельности АНО «НТЦ ЦК»

Эксперт рассказал о мерах, которые принимаются совместно с федеральными органами исполнительной власти и другими регуляторами по созданию устойчивой работы российского сегмента сети Интернет. В частности, рассматриваются угрозы отказа работы глобальной системы DNS или некорректной работы иностранных интернет-регистратур, другой инфраструктуры управления сетями связи и сервисов, которые расположены за рубежом.

Для нивелирования угроз создана национальная система доменных имён (НСДИ), реестр адресно-номерных ресурсов (аналог RIPE NCC). НСДИ имеет собственную доверенную корневую зону системы DNS и систему резолвинга, которая позволяет подключиться и использовать национальную систему для своих целей. Все операторы связи уже подключены к ней. Ведутся работы по другим направлениям, проводятся ежегодные учения на сетях связи в рамках проверки созданных механизмов устойчивости их работы.

Останавливаясь на приведённых модератором кейсах по уводу трафика, представитель регулятора напомнил, что протокол маршрутизации BGP создан давно и не имеет встроенных механизмов валидации корректности анонсов маршрутов. Для борьбы с уводом трафика и сетевыми атаками строятся специализированные инфраструктуры открытых ключей для поддержки улучшенной безопасности инфраструктуры маршрутизации BGP в интернете (англ. — Resource Public Key Infrastructure, RPKI). Каждый оператор связи криптографически подписывает (заверяет) свои автономные системы. Для эффективной работы системы необходимо, чтобы подавляющее большинство операторов связи использовали механизмы валидации RPKI. Также должны создаваться некие централизованные элементы системы управления трафиком — технологические удостоверяющие центры или базы данных, которые в качестве доверенных сторон могут заверять данные и управлять жизненным циклом сертификатов безопасности для таких задач. В России уже создан и в пилотном режиме работает один из элементов RPKI в режиме совместимости с иностранными протоколами. Планируется, что до конца 2025 года механизм будет внедрён у операторов связи.

Тему перехода на отечественное оборудование и протоколы продолжил Сергей Калинин («С-Терра»). Он напомнил, что Указ Президента РФ № 334 «О мерах по соблюдению законности в области разработки производства, реализации и эксплуата-

ции шифровальных средств, а также предоставления услуг в области шифрования информации» был подписан в апреле 1995 года. Однако на тот момент компании не были готовы к переходу на отечественные программные и аппаратные средства, криптографические протоколы. С тех пор проделана большая работа. Российские компании переходят на отечественные криптографические алгоритмы, умеют управлять потоками данных. Криптографические шлюзы имеют право быть на узлах, умеют правильно и доверенно маршрутизировать, в том числе и применяя BGP, и инкапсулируя BGP в IPsec. Это хорошие технические решения, которые со временем придут на замену импортного оборудования, считает спикер.

Об особенности текущих проектов, которые ведутся под эгидой Минцифры и Национального технологического центра цифровой криптографии (АНО «НТЦ ЦК»), связанных с применением криптографических механизмов по управлению сетевым трафиком, динамической маршрутизации без образования средств криптозащиты информации (СКЗИ), рассказал Сергей Плотко («Цифровые решения»). Он отметил, что работы ведутся по защите протоколов динамической маршрутизации с использованием российских криптографических алгоритмов. При этом маршрутизатор или коммутатор — активное сетевое оборудование — не превращается в средство криптографической защиты, сохраняет свою основную функцию — высокоскоростную коммутацию сетевых пакетов, адресную маршрутизацию и приём-передачу информации. Для операторов связи и всех пользователей инфраструктуры важно, чтобы работа с сетевым оборудованием не усложнялась из-за использования российских криптографических алгоритмов. Поскольку перевод (превращение) сетевого оборудования в один из типов СКЗИ в правовом статусе приводит к возникновению ряда ограничений, эксплуатационных сложностей и проблем с разработкой и обновлением встроенного ПО.

С. Плотко подчеркнул, что исследователи провели работу и доказали возможность реализации отечественных криптоалгоритмов для защиты протоколов динамической маршрутизации, обеспечили подписи пакетов данных российскими криптоалгоритмами ГОСТ Р 34.10–2012, ГОСТ 34.10–2018, создали соответствующие программные библиотеки и реализовали это на оборудовании. При этом для защищаемых объектов КИИ, там, где используются внутренние протоколы динамической маршрутизации, такие криптографические механизмы можно расширить и реализовать и при помощи сертифицированных российских СКЗИ.

Решение было проверено на базе серийно выпускаемого маршрутизатора. При этом испытывался вариант полноценного Gateway: с одной стороны, иностранное оборудование поддерживало зарубежные протоколы стандарта OSPF, с другой — реализовывался модифицированный вариант протокола OSPF-GOST (условное наименование) с российскими стандартами криптографии, в частности, с хешированием и электронной подписью. При этом разработчики старались реализовать решение по модульному принципу, чтобы оно стало дополнением и чаще функционировало автономно, не вмешиваясь в большую часть основных функций маршрутизации.

По мнению спикера, технологический суверенитет во многом начинался с разработки ПО как более простой части. В рамках импортозамещения оборудования следующим шагом в обеспечении технологического суверенитета должны стать национальные стандарты, которые учитывают российские разработки и специфику их применения.

Дмитрий Задорожный («Код безопасности»), представитель Технического комитета ТК-26 «Криптографическая защита информации», сообщил, что в соответствии с rfc протоколы BGPsec и RPKI реализуют криптографическую функцию электронной подписи, которая неоднократно стандартизирована в Российской Федерации (1994 г., 2001 г., 2012 г.), поддержал идею российских разработчиков сделать спецификации по расширению протоколов OSPF, BGP и технологии RPKI и внедрять их в телекоммуникационное оборудование. Кроме того, эксперт обратил внимание участников на то, что большинство маршрутизаторов строятся на операционных системах с открытым программным кодом (сборки Linux, Free|NetBSD, OpenWRT), поэтому для реализации отечественных версий протоколов OSPF, BGPsec и RPKI разработчики маршрутизаторов легко смогут скооперироваться с разработчиками СКЗИ для портирования библиотек, уже реализующих криптографические алгоритмы. Вызывает опасение, что действующие маршрутизаторы поддерживают большое количество открытых протоколов, таких как IP Sec, OpenVPN, WireGuard и т.д., заявляемых в рекламных материалах, в результате возникают вопросы к их применению и позиционированию в случае защиты данных пользователей. Есть также вопросы к восстановлению эталонной прошивки маршрутизатора в случае его заражения, разработчики СКЗИ могут помочь производителям телеком-оборудования с внедрением технологии контроля целостности программного обеспечения. При этом организовать внедрение отечественных криптографических механизмов в маршрутизаторы неплохо было бы на базе АНО НТЦ ЦК, как тематической некоммерческой организации и для обеспечения совместной работы разных вендоров телеком-оборудования.

Сергей Болонистов (компания «Булат») заметил, что при выборе телеком-продукта необходимо ответить на вопросы: что защищает условное решение из коробки и какова стоимость защищаемой информации? Исходя из этого подбираются продукты и методы защиты. Спикер также напомнил, что в главную задачу оператора связи входит передача высоконагруженного трафика с минимальными задержками, поэтому, добавив в телеком-решение дополнительные криптоалгоритмы и обременив его нагрузкой, например, по полноценному шифрованию трафика, вендор получит низкопроизводительный криптошлюз, который ещё и требует сертификации как СКЗИ.

Необходимо чётко учитывать разницу между маршрутизаторами сетевого трафика и сетевыми шифраторами, помнить, что каждый тип оборудования должен заниматься своими задачами: есть существенная разница между функциональным назначением изделия — защита данных (шифратор) и отдельным механизмом (алгоритмом) защиты, реализованным в телеком-продукции, предназначенной для передачи данных и управления потоками данных (маршрутизатор, граничный шлюз).

С. Болонистов отметил, что шифрование сетевого трафика — ресурсоёмкая и не всегда востребованная у операторов связи задача. Необходимо внедрять криптографические механизмы, которые помогут навести порядок в управлении трафиком, сократить или существенно снизить ущерб от инцидентов ИБ, потребителю должны быть доступны дополнительные криптографические механизмы и средства, без которых резко падает производительность телеком-оборудования при реализации криптоалгоритмов. Но при необходимости повысить защищённость управления телеком-оборудованием потребитель может использовать доступный функционал, например встроенный протокол IP Sec совместно с BGP.

Также, обсуждая применение механизмов фильтрации, криптографического заверения маршрутов, доменных имён и других элементов технологии RPKI, все участники согласились, что нельзя приводить к единой точке отказа, когда простая авария может привести к невозможности проверить маршрут либо к перекоммутации трафика между узлами связи, и такой сценарий не будет заложен в систему. Также стоит учитывать, что для обеспечения тайны связи «чувствительный» клиентский трафик должен либо быть зашифрован и передан по определённым каналам, либо остаться внутри страны.

О необходимости передачи внутреннего трафика, не выходя за пределы России, напомнил и представитель регулятора. По всем фактам нарушения услуг связи или правил защиты информации операторы связи будут наказываться штрафами в соответствии с новой редакцией КоАП РФ.

Участники дискуссии отметили, что в настоящее время 90 % оборудования, которое есть на балансе операторов связи, — иностранного производства. При этом зарубежные процессоры, лежащие в основе телеком-решений, содержат аппаратную поддержку иностранных криптографических функций. Для противодействия угрозам компрометации механизмов управления активным сетевым оборудованием иностранных решений необходимо развивать российские криптомеханизмы и включить их в RPKI. Также в дискуссии были затронуты вопросы стабильности информационной инфраструктуры при одновременном наращивании и использовании активного сетевого оборудования и параллельно частичного закрытия его пограничными шлюзами.

Вместе с принимаемыми мерами по нивелированию угроз при использовании иностранных решений обсудили, как именно необходимо развивать отечественное оборудование, параллельно разрабатывая собственные криптографические алгоритмы, стандарты и протоколы, включая линейку для технологии RPKI и BRSKI (англ. — Bootstrapping Remote Secure Key Infrastructure).

В процессе дискуссии удалось поднять и вопросы доверенной разработки программных и аппаратных комплексов, доверенных решений, которые можно встраивать в раз-

личные продукты. Контролировать встраивание и целостность таких стандартных библиотек для различных операционных систем, а также оперативное восстановление повреждённых решений из репозитория можно на уровне унификации решений сообщества телеком-производителей или на базе Отраслевого центра ИБ в структуре АНО «НТЦ ЦК», который действует с 2023 г. и уже унифицировал ряд криптографических протоколов, отметили эксперты.

Была поднята проблема обновления и тестирования ПО сетевого оборудования. Важно, чтобы работающее устройство не стало «кирпичом» в процессе установки новой прошивки, и это задача любого вендора, который дорожит своей репутацией.

Участники обсудили проблемы оценки соответствия, технического регулирования, сертификации и использования оборудования со встроенными криптографическими механизмами в технологических сетях, сетях связи и на защищаемых объектах КИИ, указали особенности обеспечения высших органов государственной власти ИТ-решениями, для которых требуются сертификаты ФСБ России, необходимость дуального применения российских и зарубежных криптографических механизмов в средствах связи и передачи данных, в том числе на общедоступных магистральных каналах, которые маршрутизируют, в частности, и международный трафик.

Эксперты подчеркнули, что у нас уже есть российские решения, которые пропускают до 100 Гбит для сетевых шлюзов, и это неплохие показатели. При этом есть большие объёмы трафика и высокоскоростные нагруженные каналы, на них необходимо реализовывать механизмы RPKI, вместе с которыми возникает вопрос оценки соответствия в виде нотификации (уведомления), добровольной или обязательной сертификации. И для более системного разграничения и понимания у производителей, к какому типу относится коммутационное оборудование, что и как необходимо сертифицировать, нужна тесная работа операторов связи и регуляторов.

Призвали крайне внимательно отнестись к вопросам развития Национального УЦ Минцифры России, систем отраслевых технологических УЦ и внутренних корпоративных технологических УЦ, работающих с использованием сертификатов безопасности, и обратили внимание на проект поправок в Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи» в отношении Национального УЦ Минцифры России для задач обеспечения технологической независимости.

Совместная работа всех сторон по различным вопросам, поднятым в ходе панельной сессии, позволит начать решение задачи технологической независимости страны в российском телекоме, отметили участники обсуждения.

ОТКРЫТАЯ КОНФЕРЕНЦИЯ ИСП РАН

ИИ ВЗЯЛ КУРС НА «ИМПОРТООПЕРЕЖЕНИЕ»

Усам ОЗДЕМИРОВ
корреспондент BIS Journal

Одно из значимых мероприятий состоялось в декабре на территории кластера «Ломоносов» — Открытая конференция Института системного программирования им. В. П. Иванникова (ИСП РАН). «Хозяин» мероприятия, академик Арутюн Аветисян, принимал поздравления от известных государственных деятелей и спикеров пленарной сессии в связи с двойным юбилеем — 30-летием Института и 300-летием РАН.

Деловая часть мероприятия началась с выступления Александра Шойтова, заместителя министра цифрового развития, связи и массовых коммуникаций, президента Академии криптографии. Речь пошла о созданном в мае 2024 года Консорциуме для исследований безопасности технологий ИИ. Шойтов отметил, что на сегодняшний день к трём базовым организациям, подписавшим соглашение, присоединились ещё девять. Но уже в январе это число должно увеличиться на 16 значимых организаций, занятых в сфере ИИ и ИБ. Представитель Минцифры привёл слова президента Владимира Путина о том, что следует обеспечивать безопасность таким образом, чтобы не стоять на пути прогресса и не мешать ему своими действиями. Главное, по мнению Шойтова, это зрелый подход к ИБ. Необходимо на одной площадке находить технические решения для внедрения, которые являются удобными, унифицированными, достаточно простыми и по возможности недорогими.

В качестве спикеров в президиум были приглашены также заместитель министра энергетики Эдуард Шереметцев, заместитель директора Росфинмониторинга Антон Лисицын, начальник управления ФСТЭК России Дмитрий Шевцов и представители крупных государственных предприятий. Вице-президент ПАО «Транснефть» Андрей Бадалов заметил, что в компании очень взвешенно относятся к выбору технологий для внедрения, следуя принципу «не навреди». Шутка ли — «Транснефть» объединяет 67 тысяч километров магистральных трубопроводов. Регулярные обследования объектов проводятся в том числе с использованием беспилотных аппаратов на основе ИИ. Создана единая лабораторная информационная система, где также не обойтись без ИИ при обработке больших данных. В то же время, по мнению Бадалова, не следует впадать в эйфорию и думать, что ИИ решит все наши задачи. При наличии гигантского объёма данных очень важно их качество и грамотное выстраивание системной архитектуры.

Другим гигантом российской индустрии является «Росатом», объединяющий более 400 предприятий. Директор по информационной инфраструктуре госкорпорации Евгений Абакумов заострил внимание на том, что объекты с длинным жизненным циклом требуют дополнительных подходов к внедрению технологий и распознавания. «Например, как ИИ будет вести себя на протяжении 50 лет эксплуатации объектов атомной энергетики?» — задался вопросом Абакумов. Ответ неочевидный с учётом того, что сама эта область знаний сейчас получает большой импульс к развитию. Новые перспективы видятся в применении таких технологий, как ИИ математического моделирования и автоматизация творческого труда проектировщиков, технологов, конструкторов и инженеров-расчётчиков. По мнению Абакумова, на данном этапе развития рынка также требуется определённая стандартизация в отношении продуктов, которые разработчики предлагают для критической информационной инфраструктуры (КИИ).

Медицина также не чужда ИИ, и это одна из сфер, куда следует инвестировать, чтобы приносить пользу врачам и делать их труд продуктивнее. В выступлении генерального директора НМИЦ им. В. А. Алмазова Евгения Шляхто прозвучала явная неудовлетворённость существующим положением дел. К нему приходят представители компаний-разработчиков и предлагают брать их продукты, но будут ли они реально имплементированы, их мало волнует. Врачам от больших лингвистических моделей ИИ нужен не справочник — нужен член команды, полагает Шляхто. Отрасль достигла «плато продуктивности», и нужно создавать платформенные решения, целую экосистему, переходить, к примеру, от цифровой клиники к «умной» клинике.

* * *

Конференция под эгидой ИСП РАН, несомненно, вносит свой весомый вклад в развитие ИИ. Если в 2023 году в ней приняли участие чуть больше тысячи человек, то на этот раз зарегистрировалось 2200 человек. Как сказал один из выступавших, совместными усилиями мы должны добиваться того, чтобы результатом нашей работы было не импортозамещение, а «импортоопережение».

КАК ВАЛЕРЬЯНКА ЗАЩИЩАЕТ КОМПАНИИ ОТ КИБЕРАТАК

НАДО РАЗВИВАТЬ КИБЕРКУЛЬТУРУ!

Андрей ЖАРКЕВИЧ
эксперт Start X,
ведущий рубрики

Свежие законы, ужесточившие наказание за утечки персональных данных, могут увеличить риск новых киберинцидентов. Причина такого парадоксального вывода в том, что главная причина утечек — небезопасные действия или бездействие сотрудников компаний. Людей. В том числе тех, кого оштрафуют на серьёзную сумму, если очередная кибератака окажется успешной. Угроза наказания создаёт мощную волну стресса, который крайне негативно влияет на способность сотрудников совершать правильные действия в критической ситуации.

Давайте внимательнее рассмотрим проблемы, цепочка которых привела к такому неожиданному результату, и выясним, как действовать, чтобы защитить компанию.

ПРОБЛЕМА №1

Киберинцидентов становится больше, несмотря на попытки их предотвратить

Не хочется создавать панические настроения, однако цифры говорят сами за себя. На конференции «Антифрод Россия 2024» представитель СК РФ сообщил, что за три квартала 2024 года совершено на 15,3% больше преступлений с использованием ИКТ, чем в 2023 году. Если брать ситуацию по отдельным отраслям, всё ещё печальнее. Например, по данным «Нейроинформ», число хакерских атак на логистические компании в 2024 году увеличилось на треть.

ПРОБЛЕМА №2

Последствия инцидентов становятся всё более масштабными

Операторы персональных данных обязаны выполнять требования закона, то есть защищать собранную информацию, однако у киберпреступников таких обязательств нет, поэтому сообщения о появлении в публичном доступе очередной базы утечек появляются с пугающей регулярностью. По словам главы «Ростелекома» Михаила Осеевского, персональные данные каждого россиянина уже опубликованы в сети. А эксперты InfoWatch выяснили, что «за первые шесть месяцев 2024 года в России зафиксирован антирекорд по утечкам персональных данных — скомпрометировано почти 1 млрд записей, на 33,8% больше, чем в первом полугодии 2023 года».

Самое неприятное, что данные из утечек не просто лежат в публичном доступе в ожидании, пока кто-нибудь их скачает. Хакеры и спецслужбы из недружественных стран агрегируют базы из различных утечек по номерам телефонов, ИНН, СНИЛС и другим ключевым полям, создавая сайты, где по номеру телефона можно выяснить всю подноготную любого жителя России от дня рождения, номера паспорта и накопленных бонусных баллов «спасибо» до банковских карт и даже остатков по счетам, пусть и не самых актуальных.

ПРОБЛЕМА №3

Ужесточение законодательства

Критическую ситуацию с утечками и другими киберинцидентами пытаются исправить на законодательном уровне. Например, 25 июля 2024 года вступил в силу закон 161-ФЗ, который обязывает банки приостанавливать подозрительные переводы и передавать в базу ЦБ данные скомпрометированных счетов.

Помогла ли эта мера сократить количество подозрительных переводов? Безусловно. Если говорить именно о краже денег с помощью банковских переводов.

Вот только мошенники, для защиты от которых и был принят закон, по-прежнему при деньгах. Они просто модифицировали схему, добавив в неё невольного «дропа» — случайного человека, которому «по ошибке» прислали деньги, собранные «маме на операцию». И ему просто нужно переслать их по правильному телефону, чтобы исправить досадную оплошность отправителя. Количество таких «ошибок» в 2024 году выросло на 20%.

Ещё один вариант обхода ограничений на переводы — переход на наличные. В этом случае деньги для перевода «на безопасный счёт»

передаются курьеру. Например, студентка РАНХиГС слетала из Москвы в Нижневартовск, чтобы забрать 950 тыс. рублей из сейфа и отдать «спасителям». А московская пенсионерка лишилась почти 150 млн рублей, причём часть она перевела на указанный счёт, а часть отдала наличными курьеру.

Получается, что новый закон всего лишь вынудил мошенников действовать иначе. Но при этом вместе с мошенниками под блокировку счетов попали добропорядочные граждане, не замешанные ни в каких кибераферах.

30 ноября 2024 года были подписаны ещё два закона, ужесточающие административную и уголовную ответственность за нарушение обработки и защиты ПДн. Теперь штрафы для граждан, должностных и юридических лиц, допустивших утечку, исчисляются сотнями тысяч или даже миллионами рублей в зависимости от количества попавших в публичный доступ записей данных. А за незаконное использование ПДн могут назначить как штраф, так и тюремное заключение.

ЧТО ПРОИСХОДИТ В КОМПАНИЯХ

Давайте взглянем на новую систему наказаний глазами руководителей компаний и ИБ-подразделений. Ведь это им грозят штрафы за киберинциденты с утечкой данных. Какие действия они должны предпринять?

Посмотрим правде в глаза. Запреты есть? Есть, да столько, что не сосчитать. Наказания есть? Ещё какие, с учётом свежих законов. А где рекомендации по организации защиты? Не абстрактные, а конкретные. Такие, которые реально сработают?

Компании остались один на один с киберпреступниками. Им приходится противостоять различным кибергруппировкам и даже целым киберармиям. Единого киберфронта нет. Есть островки благополучия, но в основном каждый за себя. Защищается как может, как умеет. Или покупает услугу по защите и надеется, что это сработает. Если бюджет позволяет.

А потом на очередной конференции CISO напоминают, что основная причина инцидентов — люди. Железки и услуги защищают лишь частично. Но люди спят и видят, как эту защиту нарушить или даже разрушить. С благими намерениями, если речь о «своих» сотрудниках.

Что остаётся делать CISO?

Поделиться своим стрессом с коллегами. То есть взять на вооружение методы законодателей и организовать жестокие наказания для всех нарушителей правил безопасности. Использовать управление через стресс для быстрого наведения порядка.

Обучение — это долго. Тренировки — ещё и дорого. А вот организовать для сотрудников пачку распоряжений с запретами и ознакомить под подпись — быстро и эффективно. С точки зрения поиска виновного. Но защитить от успешной кибератаки не только не поможет, а совсем наоборот. Следите за руками.

Сотрудник ознакомился со страшными карами за нарушения процедур безопасности. Теперь он боится сделать что-то не так. Вряд ли ему удалось запомнить все запреты, перечисленные в приложении к приказу. Из-за этого он боится ещё сильнее. И тут приходит письмо «от ИБ-руководителя» с указанием срочно скачать и установить обновление безопасности. Или проверить свой пароль на специальном ресурсе по ссылке. Или выполнить что-то ещё очень срочное и важное.

Что сделает сотрудник? Задаст вопрос в ответном письме? Вряд ли. Ведь он боится наказания. Поэтому он спешно скачивает и устанавливает «обновление», чтобы не лишиться премии. Потому что стресс. Критическое мышление отключено. Режим выживания подавил осознанность. Сотрудник совершил небезопасное действие.

В результате бэкдор открывает хакерам доступ в сеть. Бойцы очередной кибергруппировки крадут данные, шифруют документы и требуют выкуп. Или молча добавляют похищенную актуалочку на один из заблокированных Роскомнадзором агрегаторов утечек.

Об утечке становится известно регулятору. Организация и руководители получают штрафы. Угроза сурового наказания не помогла защитить компанию.

Кстати, это в РФ агрегаторы утечек заблокированы. А для телефонных мошенников с территории сопредельных государств всё в свободном доступе. И они пользуются этим, чтобы грабить всё ещё слишком доверчивых россиян. Несмотря на все блокировки, запреты подмены номеров и прочие не слишком эффективные попытки защитить людей.

СТРЕСС КАК БЫСТРОЕ РЕШЕНИЕ

Подведём промежуточный итог сказанному. Руководители компаний и ИБ-подразделений выбирают менеджмент через стресс не просто так. Высокие штрафы за утечки данных и несоблюдение нормативов создают стресс, ведь крупный штраф — это убытки для компании или даже угроза её существованию. Стремясь предотвратить финансовые потери, менеджеры усиливают контроль и давление на сотрудников.

Кроме финансовых последствий, существуют ещё и репутационные риски. Утечки

подрывают доверие клиентов и могут привести к их потере, а негативные публикации в СМИ и соцсетях снижают конкурентоспособность компании.

Даже незначительные ошибки могут иметь серьёзные последствия, и это усиливает напряжённость. Стремясь создать идеальную защиту, команда безопасности будет постоянно усиливать контроль над сотрудниками, увеличивая напряжённость.

ПОСЛЕДСТВИЯ СТРЕССА

Высокий уровень стресса ведёт к эмоциональному и физическому истощению сотрудников, к их профессиональному выгоранию. Их эффективность снижается, ведь постоянное напряжение снижает концентрацию и продуктивность. Ещё одно печальное последствие — самые квалифицированные кадры покидают компанию, не выдерживая давления.

В результате уровень безопасности организации снижается, поскольку переутомлённые сотрудники в состоянии стресса допускают больше ошибок. Растут затраты на поиск и обучение новых сотрудников, а также на ликвидацию последствий кибератак. Моральный дух в команде снижается, сотрудничество и коммуникации между подразделениями затруднены.

ЛЮДИ КАК ЛЮДИ

Стремление как можно больше запретить и жёстко наказывать за нарушение запретов характерно для компаний, в которых считают, что

- людей учить бесполезно;
- они всё знают, но не делают;
- лучше всего просто их уволить;
- а если не получается уволить, заблокировать техническими средствами всё, что они могут сделать опасного.

Если исходить из такой парадигмы, действительно, описанная выше система «издать приказ — ознакомить — наказать нарушителя» кажется единственным вариантом защиты. Поддерживать постоянный стресс, устраивать показательные порки, чтобы даже мысли не возникло сделать что-то не так. Но наш многолетний опыт работы в сфере ИБ говорит о другом.

Атмосфера нервозности и стресс значительно увеличивают вероятность ошибки. Конструктивная коммуникация в такой обстановке невозможна. Сотрудники боятся задавать вопросы, и это становится критической проблемой. Потому что все технические возможности совершить инцидент заблокировать невозможно. Всегда будут сотрудники с большими полномочиями, как бы команда безопасности ни боролась с этим. Люди всегда найдут способ передать свой пароль хакеру или сделать что-то ещё очень простое, нужное атакующему, так, что за этим не получится уследить. А всего один вовремя заданный вопрос предотвратил бы инцидент.

Люди будут действовать так, как им проще и понятнее. Так, как принято в их командах. Они будут пытаться выполнить свою работу, и если какие-то правила безопасности в этом мешают, будут их нарушать. Молча, не задавая вопросов.

Люди выбирают то, что соответствует их убеждениям. Если они во что-то не верят или не считают важным, они не будут это делать, даже если знают или умеют действовать иначе.

Любых, даже самых хороших курсов по повышению осведомлённости недостаточно, чтобы люди начали вести себя безопасно. Нужны навыки, которые человек умеет применять на практике, а ещё убеждения — вера в то, что будет способствовать правильному и безопасному поведению.

А ещё очень важно, чтобы команды безопасности понимали, как будут себя вести их коллеги, пытаясь выполнить свои служебные обязанности. И насколько им легко или сложно работать с учётом правил безопасности.

ЧТО ДЕЛАТЬ?

Развивать киберкультуру. То есть повышать осведомлённость людей в сфере информационной безопасности, тренировать навыки безопасного поведения и формировать правильные убеждения. Цель этих мероприятий — развитие коммуникаций между командой безопасности и остальными членами коллектива, выработка понимания, что безопасность — это не что-то абстрактное, чем занимаются за закрытой дверью специалисты по ИБ, а обязанность каждого сотрудника. И это важно не только потому, что могут наказать, но и потому, что от безопасности зависит благополучие компании и людей, которые в ней работают.

Крайне желательно, чтобы люди в компании видели в членах команды безопасности не надсмотрщиков, а коллег, которые готовы помочь в неясных ситуациях, объяснить сложные моменты, научить действовать правильно.

В этом случае не придётся рассматривать валерьянку или другие успокоительные в качестве обязательного компонента защитного комплекса. Потому что человеческий файрвол будет устойчиво работать вместе с аппаратными средствами безопасности, не давая сбоев в стрессовых ситуациях.

ИСПОЛЬЗОВАНИЕ СВОБОДНО РАСПРОСТРАНЯЕМОГО АНТИВИРУСНОГО ПО

ПРОВЕДЁМ РЕВИЗИЮ «АПТЕЧКИ»

Ярослав ПРОКУШЕВ
эксперт Управления по обеспечению информационной безопасности ДБ Банка ВТБ (ПАО)

Для защиты личных компьютеров во многих случаях достаточно использовать бесплатные антивирусные продукты. В России для компьютеров на базе операционных систем Windows 10/11 в качестве средства антивирусной защиты (САВЗ) в основном применяются Microsoft Defender[1] (антивирус, встроенный в ОС семейства Windows 10/11) или Kaspersky Free[2].

Доступ к загрузке дистрибутивов других бесплатных антивирусов, таких как Malwarebytes Free, Avast Free, AVG, Avira Free, для пользователей из России на данный момент заблокирован, а при эксплуатации или обновлении этих продуктов могут возникнуть проблемы. Также могут быть полезны антивирусные сканеры и программы для восстановления данных.

MICROSOFT DEFENDER ИЛИ KASPERSKY FREE

Отличительной чертой Microsoft Defender является то, что его работа малозаметна для защищаемого компьютера. Этот антивирус однозначно предпочтителен, если производительность вашего аппаратного обеспечения невысока. Нагрузка на систему может почувствоваться лишь при сканировании программной среды на обнаружение вредоносного кода, что характерно для всех антивирусов.

Однако у определённого процента домашних пользователей в силу ряда причин (лицензионная политика Microsoft, геополитические факторы, память об эпидемиях вирусов-шифровальщиков из-за уязвимостей нулевого дня) есть недоверие к защитным механизмам Windows, в том числе и к Microsoft Defender. В этом случае они могут установить на свой компьютер САВЗ Kaspersky Free.

Алгоритм работы антивирусного ядра Kaspersky Free схож со своими платными «старшими» собратьями. Надёжность работы Kaspersky Endpoint Security подтверждается исследованиями, проводимыми при сертификации данного продукта в испытательных лабораториях ФСТЭК и ФСБ России. Аналогичных тестов в отношении Microsoft Defender или других зарубежных антивирусов (кроме уже устаревших коммерческих версий Eset Nod32 и Symantec Endpoint Security) в России не проводились. А именно надёжность работы является важнейшим параметром при выборе САВЗ.

Сравним заявленные функциональные возможности антивирусов Kaspersky Free и Microsoft Defender (см. таблицу).

Как видно из таблицы, функциональные возможности двух антивирусов примерно одинаковы. Тесты, проводимые за последнее время различными зарубежными исследовательскими лабораториями (AV-TEST GmbH, AV–Comparatives), подтверждают достаточно высокую эффективность и надёжность работы этих двух решений[3] при незначительном преобладании в рейтинге у Kaspersky Free.

[1] Обзор антивирусной программы Microsoft Defender в Windows: *https://learn.microsoft.com/ru-ru/defender-endpoint/microsoft-defender-antivirus-windows*

[2] Возможности Kaspersky Free: *https://support.kaspersky.com/help/Kaspersky/Win21.19/ru-RU/101565.htm*

[3] Тестирование антивирусных систем: *https://www.comss.ru/page.php?id=12471*

Параметр сравнения	Kaspersky Free	Microsoft Defender
Самозащита	Имеется, включена по умолчанию	Защита от подделки
Контроль изменения настроек	Механизм парольной защиты, надо установить пароль	Изменение доступно администраторам
Интерфейс настройки параметров работы антивируса	Имеется собственный интуитивно понятный интерфейс настройки	Реализован с помощью политик безопасности или через прямую правку реестра. В оконном интерфейсе минимум параметров для настройки
Обновление антивирусных баз и антивирусного ядра программы	Имеется	Имеется
Периодическая полная или быстрая проверка	Требуется настройка	Требуется настройка
Выборочная проверка	Имеется	Имеется
Возможность проверки почтовых сообщений	Имеется, активировано по умолчанию	Имеется, требуется настройка через политики безопасности
Защита от эксплойтов	Имеется	Имеется
Защита от шифровальщиков	Имеется	Имеется
Защита от сетевых атак	Ограниченный функционал	Ограниченный функционал
Облачная защита	Имеется	Имеется
Контроль работы приложений (блокировка подозрительных и вредоносных действий)	Имеется	Имеется, Smart-Screen
Защита при работе в сети Интернет (контроль портов)	Ограниченный функционал	Ограниченный функционал
Эвристический механизм	Имеется	Имеется

Таблица. Сравнение некоторых заявленных возможностей антивирусов

Поэтому итоговый выбор будет зависеть от личных предпочтений пользователя и особенностей защищаемого компьютера.

НЕРЕЗИДЕНТНЫЕ СКАНЕРЫ

Вне зависимости от того, какое антивирусное средство вы используете для защиты компьютера, периодически для его проверки рекомендуется применять другое САВЗ. В качестве такого средства можно использовать антивирусные сканеры KVRT (Kaspersky virus removal tool) и Dr. Web CureIt. Это программы, которые запускаются пользователем с правами администратора и работают только во время выполнения проверки.

Во время работы оба сканера могут подключаться к облачным ресурсам своих организаций для повышения эффективности обнаружения ВПО. Важной особенностью этих двух программ является то, что они способны запуститься даже в серьёзно заражённой среде.

Если на защищаемом компьютере используются политики, ограничивающие запуск программного обеспечения, то следует разрешить исполнение программ из каталога *C:\Users\user_name\appdata\local\temp* на момент запуска антивирусных сканеров. В эту папку распаковываются их дистрибутивы. Если сначала выполняется быстрая проверка, то затем желательно дополнительно проверить каталоги: *C:\Program Files, C:\Program Files (x86), C:\System Volume Information, Корзины, C:\Program Data* и профиль пользователя.

Антивирусные сканеры других производителей могут позволить отыскать вредоносное ПО, которое не видно вашему штатному антивирусу. Такие случаи хотя и редко, но могут происходить. Если в качестве основного САВЗ используется Kaspersky Free, то для проверки предпочтительней применить Dr. Web CureIt. Если же постоянную защиту обеспечивает Microsoft Defender, то можно чередовать сканеры. Желательно выполнять такую проверку хотя бы один раз в две-три недели. Обязательно следует запускать сканирование, если было обнаружено вредоносное ПО.

Если же система настолько сильно заражена, что запустить ничего невозможно, то используют загрузочные диски этих же производителей — это Kaspersky Rescue Disk и Dr.Web LiveDisk. Они содержат антивирусные сканеры. С их помощью можно также спасти имеющуюся на компьютере пользовательскую информацию.

ИСПОЛЬЗОВАНИЕ ОНЛАЙН-РЕСУРСОВ ДЛЯ ПРОВЕРКИ СИСТЕМЫ

В том или ином виде взаимодействие с ресурсами разработчика предусмотрено во многих антивирусных системах, как свободно распространяемых, так и платных. В частности, использование облачных ресурсов предусмотрено в Microsoft Defender, Kaspersky Free (в случае активации опции подключения к Kaspersky Security Network). Также подключение к ресурсам облака возможно при использовании лечащих утилит. Доступ к антивирусному облаку повышает эффективность работы компонентов эвристического анализа, что уменьшает ложные срабатывания. Использование антивирусных облаков подразумевает отправку подозрительных файлов пользователей производителям. По этой причине некоторые пользователи отключают использование облачных ресурсов.

В случае если требуется проверить один или несколько файлов или ссылок, то можно использовать такие порталы, как *https://opentip.kaspersky.com/*, *https://www.virustotal.com/gui/home/upload*, *https://online.drweb.com/result2/*, *https://vms.drweb.ru/online/.*

КРАТКО О ШИФРОВАЛЬЩИКАХ

Если ваши пользовательские данные оказались всё-таки зашифрованы вымогателем, то можно попробовать их восстановить. Здесь важно определить разновидность шифровальщика, чтобы выбрать правильное «лекарство»[4]. На сайте Лаборатории Касперского приведён перечень утилит[5], восстанавливающих информацию после воздействия различного рода шифровальщиков. Можно также отправить заявку на расшифрование файлов на странице веб-портала другого известного российского разработчика САВЗ — ООО «Доктор Веб».

Тем не менее в ряде случаев данные восстановить всё-таки не удаётся. Поэтому в качестве самой действенной меры сохранения важной для пользователя информации рекомендуем её периодическое резервирование — копирование на съёмный носитель. Эта мера защитит вас не только от вредоносного ПО, но и от банальной поломки машинного носителя информации.

Также немаловажно соблюдать цифровую гигиену и ответственно подходить к выбору посещаемых в Сети интернет-ресурсов.

[4] Как удалить шифровальщик и восстановить данные: *https://www.comss.ru/page.php?id=4120*

[5] Бесплатная расшифровка файлов: *https://noransom.kaspersky.com/ru/*

«КИБЕРХАБ — ЖИВАЯ СТРУКТУРА, ЦИФРОВОЙ ЩИТ ДЛЯ РОССИЙСКИХ СТАРТАПОВ»

BIS JOURNAL И КИБЕРХАБ ФОНДА «СКОЛКОВО» ОТКРЫВАЮТ СЕРИЮ ПУБЛИКАЦИЙ, ПОСВЯЩЁННЫХ ПЕРСПЕКТИВНЫМ ИБ-СТАРТАПАМ

Игорь БИРЮКОВ
руководитель Киберхаба Фонда «Сколково» (Группа ВЭБ.РФ)

ЧТО ТАКОЕ КИБЕРХАБ

Время летит быстро, и сегодня многим кажется, что Инновационный центр «Сколково» был всегда. Однако это не так. Центр и его управляющая компания Фонд «Сколково» были созданы всего пятнадцать лет назад. За эти годы они объединили больше четырёх с половиной тысяч стартапов — резидентов «Сколково». Цель Фонда — поддержка технологического предпринимательства в России и коммерциализация результатов научно-исследовательской деятельности.

Об эффективности работы структуры говорят цифры. По словам Дмитрия Медведева, заместителя председателя Совета Безопасности РФ и главы Попечительского совета Фонда «Сколково», государство направило на развитие Инновационного центра Сколково порядка 197 млрд рублей, эти средства были полностью возвращены в бюджет, даже больше. Только с 2017 по 2023 г. сумма уплаченных налогов составила более 200 млрд рублей, что говорит о правильности принятого ранее решения.

В 2023 г. в рамках Центра развития цифровых технологий (ранее — ИТ-кластера) Фонда «Сколково» был создан Киберхаб, который объединил всех резидентов, работающих в сфере информационной безопасности. Хаб стал цифровым «щитом» для российских компаний. Он поддерживает новые прорывные решения в области кибербеза и помогает бизнесу в доступе к новейшим технологиям в сфере ИБ.

Киберхаб Фонда «Сколково» — это экосистема, на конец 2024 г. объединяющая порядка 70 стартапов. В ней есть как уникальные проекты, так и решения, конкурирующие между собой. Задача Киберхаба — объединить конкурентов и организовать взаимодействие трёх сторон: стартапов, вендоров/заказчиков и государства. Полученный в результате такого общения всех со всеми синергетический эффект ценен для сторон. Активный контакт резидентов между собой приводит к технологическому партнёрству и усиливает работу отдельных компаний.

РЕЗИДЕНТУРА КИБЕРХАБА

Чтобы стать участником Киберхаба, не существует отдельной процедуры. Есть стандартный порядок вступления в проект Сколково: надо пройти отбор, получить одобрение экспертного совета и стать резидентом Инновационного центра, выполнив регламентные юридические формальности. Резиденты получают налоговые послабления, которые повышают шанс выживания для маленьких компаний на начальных стадиях развития. Также существует поддержка в виде грантов, ей активно пользуются участники хаба. Особенно если им требуется довести свой продукт до финальной стадии, когда крупный вендор готов купить стартап для расширения своей продуктовой линейки.

Однако между идеей, с которой приходят в Сколково, и её воплощением в жизнь (с последующей продажей продукта или услуги) существуют многочисленные этапы, которые небольшому стартапу сложно пройти в одиночку. Киберхаб оказывает своим участникам менторскую поддержку, помогает компаниям развиваться по всем направлениям — от узконаправленных, связанных с развитием продуктов и технологий, до общих вопросов, касающихся HR, GR и PR, маркетинга и продаж, продвижения продуктов на рынке. Это важные моменты развития, на которые у небольших компаний, как правило, нет ни финансовых, ни кадровых ресурсов. Например, в прошлом

году мы провели продолжительный практикум по продажам и управлению персоналом для стартапов по ИБ. С резидентами Сколково и присоединившимися к ним желающими работали представители Фонда и вендоров, эксперты в своих областях.

Также резиденты Киберхаба выступают на многочисленных профильных мероприятиях и представляют свои решения как потенциальным заказчикам, так и потенциальным покупателям стартапов.

ПЕРСПЕКТИВЫ РАЗВИТИЯ

Киберхаб — живая структура. К концу 2024 года, вопреки ожиданиям экспертов и ситуации на рынке кибербезопасности, к нам присоединились 12 стартапов. Это рекордный прирост новых проектов по ИБ для Фонда «Сколково».

Многие новички приходят с решениями, у которых уже есть достаточное количество конкурентов. И молодые компании доказывают экспертам, что они имеют преимущество перед теми, кто давно зарекомендовал себя на российском рынке ИБ. Появляются стартапы, разрабатывающие облачные сервисы по информационной безопасности и решения MSSP, работающие с дипфейками их же средствами, предлагающие ИБ-продукты для предприятий малого и среднего бизнеса...

Наиболее «продвинутые» участники уже представили свои продукты на крупных мероприятиях. Не сомневаюсь, что вскоре они найдут своего покупателя. Поэтому в Киберхабе есть не только естественный приток, но и отток резидентов.

По данным за 2023 год, ставший рекордным по прибыли для российского кибербеза, выручка резидентов Киберхаба Фонда «Сколково» показала почти трёхкратный рост и составила 41 млрд рублей. В среднем рост ежегодной выручки резидентов Киберхаба составляет 20%

Компании растут и перестают быть участниками проекта Сколково, в том числе по финансовым причинам: годовой объём выручки превышает 1 млрд рублей. Но при этом у них открываются новые возможности, например, стать партнёрами Фонда «Сколково» и развивать вместе с ним новые технологии, вести научно-исследовательскую и просветительскую работу — заниматься глобальными вопросами информационной безопасности, а не просто создавать коммерчески успешные продукты и решения.

Прошедший год был очень успешным для Киберхаба. Я надеюсь, что в 2025 г. реализуются планы по развитию технологического партнёрства между резидентами, по созданию технологической экосистемы Сколково, объединяющей ИТ и ИБ-продукты.

* * *

Я уверен, что наш опыт чрезвычайно полезен для развития отрасли ИБ в целом, поэтому Киберхаб Фонда «Сколково» и BIS Journal открывают самостоятельный PR-проект — «Парад стартапов», который представит крупным планом перспективные и начинающие ИБ-компании, работающие на территории Инновационного центра.

СПРАВКА BIS JOURNAL

Игорь Бирюков, *руководитель Киберхаба Фонда «Сколково» (Группа ВЭБ.РФ).* Окончил Московский государственный университет приборостроения и информатики. Инженер-конструктор. Автор научных публикаций.

В 2006 году проходил службу в Федеральной таможенной службе, занимался аттестацией объектов информатизации. Многолетний опыт работы в сфере информационной безопасности. В 2009 г. возглавил направление по технической защите информации в ООО «Итеранет», дочерней компании НГК «Итера». С 2021 года развивал направление консалтинга по ИБ в АО «Энергоцентр», дочерней компании ПАО «Россети».

В 2023 году присоединился к команде Центра развития цифровых технологий Фонда «Сколково», руководит перспективными проектами в области информационной безопасности, развивает стартапы, формирует рынок новыми отечественными решениями по ИБ, доводя продукты резидентов от стадии идеи до тиражирования.

ЧТО НЕ ТАК С ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ?

КОМПАНИЯ PHISHMAN О ЛЮДЯХ И БЕЗОПАСНОСТИ

Алексей ГОРЕЛКИН
CEO Phishman

КЛАССИКА — НЕОБХОДИМАЯ, НО НЕДОСТАТОЧНАЯ

Классика информационной безопасности — внедрить как можно больше регламентов, закупить по максимуму технических решений и думать, что этого достаточно.

До 95% инцидентов происходит по вине пользователя — тоже классика информационной безопасности. Исследования и реальные кейсы показывают, что пользователи остаются самым слабым звеном в процессе ИБ. Незнание, неосторожность или элементарная невнимательность сотрудника может открыть двери для злоумышленников, сведя на нет все усилия технических систем.

ХОРОШАЯ НОВОСТЬ

Хорошая новость в том, что ИБ-комьюнити постепенно понимает: работа с пользователями — такой же приоритет. Всё чаще обращают внимание на концепцию People-Centric Security — подход, направленный на повышение уровня осведомлённости сотрудников об угрозах в области информационной безопасности, обучение их базовым принципам защиты информации и формирование навыков безопасного поведения в цифровой среде.

Несмотря на очевидные преимущества этого подхода, он остаётся недооценённым и редко интегрируется в ИБ-стратегии. И это проблематично.

РОЖДЕНИЕ PHISHMAN

Так родилась идея компании Phishman: не все понимали, что человек — самое слабое звено, хотя это было очевидно уже в начале 2010-х. В 2016-м появился Phishman и наш одноимённый продукт.

Начиная с 2020 года компания Phishman является резидентом Skolkovo, активно участвуя в государственных и образовательных проектах внутри страны и в международном направлении.

Всё началось с того, что людей надо было как-то обучать. Тогда решили стартовать с обучения защиты от фишинга. Это первое, что приходило на ум, и тогда фишинг был суперэффективным (сейчас это просто эффективный) вариантом атаки. Дальше мы начали развивать это, добавлять и другие темы ИБ.

ЧТО НЕ ТАК С ИБ?

Так что же не так с информационной безопасностью? Чем больше мы работали в этом направлении, тем больше понимали, что настоящая проблема ИБ кроется не в том, что индустрия не понимает важности обучения сотрудников (к этому рано или поздно придут), а в том, что делают это в корне неверно.

Есть два варианта: обучение через подписание регламентов и мнение «этого достаточно» либо бесконечные курсы — сложные и, по ощущениям сотрудников, бесполезные. Так или иначе — нет практики, нет вовлечения, нет коммуникации, нет киберкультуры.

Как итог: сотрудников вроде бы «обучили», а количество инцидентов не уменьшается. Почему? Потому что в обучении людей компании используют подход Data-Centric Security, сосредоточенный на защите данных. Данных, а не людей.

ДРУГОЙ ПОДХОД

В Phishman мы активно продвигаем подход People-Centric Security и формирование киберкультуры. Так пользователь становится частью безопасности компании, а не главной его проблемой, которую нужно по максимуму оградить, а не вовлечь.

Повышение уровня киберкультуры способствует созданию среды, где каждый сотрудник осознаёт свою ответственность за безопасность компании, а ИБ становится частью корпоративной культуры.

МИССИЯ

Миссия Phishman — показать, что информационная безопасность может быть с человеческим лицом. Сотрудник, понимающий важность ИБ и осознающий свою роль, становится не пассивным звеном, а активным участником процесса, способным эффективно противостоять угрозам.

* * *

Формирование киберкультуры — долгосрочная стратегия, которая работает. Это выгодно для бизнеса, это снижает издержки, связанные с инцидентами, и повышает вовлечённость сотрудников, что положительно сказывается на эффективности работы с безопасностью.

SECURITM: ПРОСТОЕ РЕШЕНИЕ ДЛЯ СЛОЖНЫХ ЗАДАЧ

Николай КАЗАНЦЕВ
CEO SECURITM

Информационная безопасность сегодня — это не только защита данных от внешних угроз, но и эффективное управление внутренними процессами службы информационной безопасности, которые сталкиваются с множеством задач: управление рисками, аудитами, соответствием стандартам, активами, техническими уязвимостями, а также планирование и автоматизация процессов. Традиционные инструменты, такие как Excel, часто оказываются неудобными. Они требуют ручной работы, которая отнимает время и отвлекает специалистов от стратегических задач. При этом бюджеты на увеличение штата ограничены, а дорогие и сложные Enterprise-решения подходят не всем.

Рассмотрим это на примере. Как часто технические системы безопасности создают ложное чувство защищённости, перегружая оператора информацией? Разрозненные системы, отчёты, не зависящие друг от друга. А сколько сил занимает ручной импорт информации в единые отчёты? SGRC устраняет этот барьер, помогая увидеть реальные риски и сфокусироваться на них. Это как новая пара очков для компании: теперь видны настоящие опасности, а не помехи.

Именно поэтому SECURITM поставил своей миссией создание инструмента, который упростит управление процессами и подойдёт любой компании, вне зависимости от её масштаба или бюджета. В мире, где требования к информационной безопасности постоянно растут, компании должны максимально эффективно использовать имеющиеся ресурсы. SECURITM помогает российским и СНГ-компаниям внедрять автоматизированные процессы управления информационной безопасностью.

ЧЕМ SECURITM ОТЛИЧАЕТСЯ ОТ ДРУГИХ РЕШЕНИЙ?

SECURITM — это система, которая объединяет все процессы информационной безопасности в одном окне. Мы предлагаем простой и доступный инструмент, позволяющий достичь быстрых результатов. Продукт можно настроить и запустить за пять минут, даже пользователи без опыта работы с подобными системами легко начнут работу в SECURITM.

Инструмент автоматизирует до 90% рутинных задач: больше не нужно вручную заполнять таблицы или собирать данные с сотрудников и контрагентов. Система легко интегрируется с корпоративными решениями, что делает её универсальной для любой инфраструктуры. Сегодня огромное количество времени сотрудников служб ИБ уходит на сбор и обработку данных. SECURITM освобождает ресурсы для стратегических задач, что позволяет специалистам сосредоточиться на развитии системы безопасности.

Отдельного внимания заслуживает созданная в продукте скоррелированная база регуляторных требований по информационной безопасности, где сейчас уже больше 100 документов, от приказов ФСТЭК и ГОСТов до лучших мировых практик и фреймворков, а также база готовых рисков и защитных мер. Это позволяет существенно сократить время на настройку и адаптацию системы под свои нужды.

Внутри системы заложены основные процессы, с которыми сотрудник службы безопасности сталкивается каждый день:

- исполнение внешних и внутренних требований безопасности (модуль требований)
- снижение рисков информационной безопасности (модуль рисков);
- внедрение и поддержка различных организационных и технических мероприятий (модуль мер);
- оценка прогресса работы (модуль метрик);
- операционные процессы внутри отдела (модуль задач);
- автоматизация процессов (модуль RPA);
- сбор и анализ активов (модуль активов);
- модуль опросов, для взаимодействия с другими подразделениями.

Среди наших пользователей — предприятия из разных отраслей, от энергетики и банковского сектора до телекоммуникаций и госструктур. Универсальность системы позволяет адаптироваться к любым требованиям бизнеса.

Система активно используется не только в бизнесе, но и в образовательных учреждениях для обучения студентов информационной безопасности.

* * *

SECURITM меняет подход к управлению информационной безопасностью, делая сложное простым и доступным. Выбирая нас, компании получают не просто инструмент, а партнёра, который помогает справляться с любыми вызовами.

АЗЕРБАЙДЖАНСКАЯ РЕСПУБЛИКА

ОБЗОР ЗАКОНОДАТЕЛЬСТВА В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Александр ВИНОГРАДОВ
ФГУП «ЦНИИХМ»

Сергей МЕНЬШИКОВ
основатель Belarusian InfoSecurity Community

Андрей СИТНОВ
независимый эксперт

Валерий СОКОЛЕНКО
заместитель начальника службы информационной безопасности ICBC в г. Алматы

Следующее государство, для которого мы проведём анализ законодательства в области информационной безопасности (далее – ИБ), – Азербайджанская Республика.

БАЗОВЫЕ АКТЫ

Базовыми актами, закрепляющими общие положения о доступе к информации, конфиденциальности и защите информации, являются следующие законы:

Закон АР от 3 апреля 1998 г. № 460-IQ «Об информации, информатизации и защите информации»

Закон регулирует отношения, возникающие в связи с формированием информационных резервов на основе создания, сбора, переработки, хранения, поиска, распространения информации, с созданием и использованием информационных систем, технологий, средств их обеспечения, защитой информации, и определяет права субъектов, участвующих в информационных процессах.

Закон вводит основные понятия, связанные с информацией, её обработкой и защитой. В частности, закон вводит понятие «конфиденциальной информации» как «сведения, получение которых ограничено в целях защиты законных интересов граждан, созданных независимо от формы собственности учреждений, предприятий и организаций, других юридических лиц, а также профессиональная (врачебная, адвокатская, нотариальная), коммерческая, следственная и судебная тайна». В российском законодательстве понятие «конфиденциальная информация» определяется в Федеральном законе № 149-ФЗ «Об информации, информатизации и защите информации» более широко и включает в себя также государственную тайну.

Закон АР от 11 мая 2010 г. № 998-IIIQ «О персональных данных»

Закон регулирует отношения, связанные со сбором, обработкой и защитой персональных данных, формирование раздела персональных данных в национальном информационном пространстве, а также вопросы, связанные с трансграничной передачей персональных данных, устанавливает права и обязанности действующих в данной сфере государственных органов и органов местного самоуправления, физических и юридических лиц.

Закон определяет законодательные основы и общие принципы сбора, обработки и защиты персональных данных, правила и требования государственного регулирования в данной сфере, правила формирования персональных данных в информационных ресурсах, создания информационных систем, предоставления и передачи информации, права, обязанности и основы ответственности участвующих в данном процессе лиц, защите основных прав и свобод человека и гражданина, в том числе права на сохранение тайны личной и семейной жизни.

Специфичным для Закона о персональных данных АР является наличие понятия «информационные ресурсы персональных данных», определяемого как информационные ресурсы, накопленные в установленном законодательством порядке и объёме в информационных системах персональных данных, а также в отдельности. В российском законодательстве понятие «ресурс персональных данных» определено только в документах комплекса стандартов по обеспечению информационной безопасности организаций банковской системы Российской Федерации (СТО БР ИББС).

ОБЩИЕ СВЕДЕНИЯ

Официальное название государства — Азербайджанская Республика (далее — АР). Находится в восточной части Закавказья (Южного Кавказа) на побережье Каспийского моря, относится к Передней Азии, а также, по мнению некоторых источников, частично к Восточной Европе. Омывается водами Каспийского моря. Имеет сухопутную границу с Россией, Грузией, Арменией и Ираном. Нахичеванская Автономная Республика — эксклав Азербайджана — граничит с Арменией на северо-востоке, Ираном на юго-западе, Турцией на северо-западе.

Столица — город Баку. Государственный язык — азербайджанский.

Азербайджан является членом ООН, ОБСЕ, Совета Европы, СНГ, ГУАМ, ОЭС, Движения неприсоединения, Организации черноморского экономического сотрудничества, Организации исламского сотрудничества.

Органы, утверждающие и согласовывающие законы и подзаконные акты в области ИБ в стране: Президент Азербайджанской Республики, Центробанк Азербайджана.

Все рассмотренные в данной публикации документы имеют общереспубликанское значение и применяются для организации и обеспечения информационной и кибербезопасности.

Государственная политика АР в сфере информационной безопасности и кибербезопасности регулируется следующими нормативными актами и развивается по направлениям, представленным в статье.

Также специфичным для Закона АР является понятие «индивидуальный идентификационный номер» — единый неповторимый код, присваиваемый в установленном порядке лицу, персональные данные о котором вносятся в информационные системы персональных данных, и позволяющий однозначно установить соответствующие сведения о лице.

Законом вводится понятие «персональные данные особой категории» как сведения, относящиеся к расовой или национальной принадлежности, семейной жизни, религиозному вероисповеданию и убеждениям, здоровью или судимости. Что схоже с российским понятием «специальная категория персональных данных».

Кроме понятия «оператор персональных данных», имеются понятия «собственник персональных данных» и «пользователь персональных данных», что расширяет круг участников процессов обработки персональных данных.

Понятие «обезличивание персональных данных» в Законе АР отличается от российского, определено как «приведение персональных данных в состояние, при котором невозможно определить их принадлежность субъекту», и фактически включает в себя и российский вариант обезличивания (фактически обратимый процесс), и процедуры анонимизации персональных данных, которые де-юре пока не определены в российском законодательстве.

В зависимости от вида доступа (получения) персональные данные в АР делятся на несколько категорий и подлежат различной защите.

- Конфиденциальные персональные данные, за исключением установленных законом случаев, могут быть переданы третьим лицам только на основании согласия субъекта.
- Обеспечение конфиденциальности персональных данных общедоступной категории не требуется. Общедоступные персональные данные — данные о субъекте, обезличенные в установленном порядке, открытые им самим либо внесённые с его согласия в информационные системы, созданные для общего пользования. Фамилия, имя и отчество лица относятся к постоянно общедоступным персональным данным.
- Сведения специальной категории могут относиться как к категории конфиденциальных, так и к категории общедоступных персональных данных с учётом их особенностей и требований Закона о персональных данных.

Собственник или оператор должны осуществлять организационно-технические мероприятия, гарантирующие обеспечение защиты персональных данных (в том числе предотвращения их случайного и несанкционированного уничтожения, утраты, незаконного доступа, изменения и других случаев).

Биометрические персональные данные — это данные, характеризующие биологические особенности человеческого организма и позволяющие однозначно его определить: отпечатки пальцев и ладоней, изображение лица, сетчатка и радужная оболочка глаза, фрагменты голоса и его акустические параметры, результаты анализа дезоксирибонуклеиновой кислоты (ДНК), размеры тела, описание особых признаков и недостатков тела, почерк и подпись и другие.

Интересной является норма, определяющая право субъекта возражать против сбора и обработки персональных данных о нём, за исключением случаев, когда сбор и обработка данных носят принудительный характер в установленном законодательством порядке. Возражение субъекта должно быть представлено собственнику или оператору в письменном виде. Обоснование возражения субъекта не требуется. При получении данного возражения собственник или оператор должны незамедлительно прекратить сбор и обработку персональных данных. Как видим, Закон АР определяет также возможность принудительного сбора и обработки персональных данных в установленном законодательством Азербайджанской Республики порядке.

При сборе персональных данных собственник или оператор персональных данных обязан сообщить субъекту уровень защиты собираемых и обрабатываемых персональных данных в информационной системе, а также сведения о наличии сертификата соответствия на информационные системы и о прохождении ими государственной экспертизы. В российском законодательстве аналогичные нормы отсутствуют.

Президент АР 28 августа 2023 г. утвердил «Стратегии информационной и кибербезопасности Азербайджанской Республики на 2023–2027 годы». Документ является первой стратегией в Азербайджанской Республике в области информационной безопасности и кибербезопасности, стратегия в этой области определяет основные цели, принципы, направления и приоритетные задачи деятельности в стране, меры, свя-

занные с повышением уровня национальной информационной безопасности, обеспечению безопасности критической инфраструктуры государственных и частных секторов. Стратегия предполагает формирование и ведение реестра рисков информационной безопасности и кибербезопасности, мониторинг событий информационной безопасности, определение и применение критериев обнаружения инцидентов и критических ситуаций, расширение областей применения искусственного интеллекта, усиление персональной защиты.

ТАЙНЫ

Тайны, определённые законодательством РА:

Закон АР от 16 января 2004 г. № 590-IIQ «О банках» вводит «В соответствии с Гражданским кодексом Азербайджанской Республики банк обеспечивает тайну банковского счёта, операций и остатков по счетам, а также сведений о клиентах, в том числе сведений об именах клиентов, адресах, руководителях. Банк обеспечивает тайну сведений о наличии имущества клиентов в хранилище банка, сведений о владельцах такого имущества, характере и стоимости».

При анализе закона следует обратить внимание на ряд важных моментов. Из контекста данной статьи следует, что нормы Гражданского кодекса Азербайджана, регулирующие отношения в сфере банковской тайны, имеют приоритет над нормами Закона Азербайджанской Республики от 16 января 2004 г. № 590- IIQ «О банках», что делает последние вторичными по юридической силе.

Закон АР от 4 декабря 2001 г. № 224-IIГ «О коммерческой тайне» вводит, что «коммерческая тайна — это сведения, связанные с производственной, технологической, управленческой, финансовой и другой деятельностью юридических и физических лиц, разглашение которых без согласия владельца может причинить ущерб их законным интересам» и «ноу-хау — сведения, отнесённые как результат умственной деятельности к коммерческой тайне, не охраняемые патентом согласно законодательству или по соображениям владельца».

РАСПОРЯЖЕНИЯ И ПОСТАНОВЛЕНИЯ

Распоряжением Президента Азербайджанской Республики от 26 сентября 2018 года № 508 был разработан и утверждён «План действий по внедрению международного стандарта ISO20022 в инфраструктуру Национальной платёжной системы Азербайджанской Республики».

Постановление Правления Центрального банка Азербайджанской Республики от 14 июля 2021 года № 20/1 «Об утверждении «Порядка управления информационной безопасностью в банках»

Документ, устанавливающий минимальные требования по информационной безопасности в банках страны с учётом требований стандартов ISO/IEC2700X Международной организации по стандартизации, утверждён решением Правления Центрального банка и внесён в Государственный реестр правовых актов Азербайджана.

Новые правила содержат в себе механизмы безопасности человеческих ресурсов, управления активами, контроля доступа, криптографии, безопасности обмена информацией, обеспечения безопасности при приобретении, применении и поддержке информационных систем, защиты информационной безопасности в сервисных отношениях с внешними поставщиками, а также требования к управлению инцидентами информационной безопасности.

Постановление Правления Центрального Банка Азербайджанской Республики от 28 марта 2024 года № 14/2 «Об утверждении „Требований к обеспечению информационной безопасности субъектов, деятельность которых контролируется на финансовых рынках“». Данное постановление определяет минимальные требования к информационной безопасности в банках, небанковских кредитных организациях, за исключением кредитных союзов, страховщиках, лицензируемых лицах на рынке ценных бумаг, управляющих акционерными инвестиционными фондами и инвестиционными фондами, национальном операторе почтовой связи, платёжных организациях, организациях электронных денег, операторах платёжных систем, кредитных бюро, центральном депозитарии.

Надеемся, что данная статья поможет вам не заблудиться в Законодательстве АР. Мы постарались облегчить путь изучения и применения на практике нормативных законов и подзаконных актов в области ИБ.

* * *

В следующем номере журнала мы продолжим обзор законодательства в области информационной безопасности других стран.

ЗАКОН PIPL

«ЦИФРОВАЯ ДИКТАТУРА» ИЛИ ОБОРОНИТЕЛЬНАЯ КРЕПОСТЬ?

Мария КОЗЛОВА
корреспондент
BIS Journal, Пекин

Персональные данные — понятие новое и весьма нехарактерное для традиционного Китая. Индивидуализм всегда порицался в этике конфуцианства, которое как 2500 лет назад, так и сейчас доминирует в общественно-политической жизни Поднебесной. Да и само слово «конфиденциальность» (кит. «иньсы»), сложившееся из иероглифов «инь» (сокрытый, спрятанный) и «сы» (личный, корыстный, утаённый), вызывает явно не положительные ассоциации. Виновник такой тенденции — уклад жизни в Поднебесной, который оставил всё частное и личное в тени. В Китае, только объединив труд, а заодно и быт, можно было возводить стены и противостоять набегам кочевников, строить дамбы и спасаться от наводнений, работать в поле и собирать урожай.

С началом политики реформ и открытости в 1978 г. коллективизм начал уступать место личности. Так был запущен процесс включения права неприкосновенности личной жизни в китайское законодательство. Несмотря на то что Поднебесная отстала от стран-первопроходцев на несколько десятилетий, у неё перед глазами был пример титанов, на плечи которых оставалось только взобраться.

ДВА ЗАЙЦА И ТРЁХСТОРОННИЙ БАЛАНС

В западном мире существуют две точки зрения в отношении регулирования персональных данных. Они отличаются тем, чему отдаётся приоритет: Европейский союз пошёл по пути акцента на защите прав человека, а США поддерживали в первую очередь цифровую индустрию, которая развивается за счёт использования личной информации граждан.

Китай же погнался за двумя зайцами, и, надо сказать, оба были поданы к обеду: Поднебесная переняла и американский, и европейский опыт — последний в большей степени. В 2019 году ещё в проекте Закона о защите персональных данных (PIPL) была выдвинута концепция «двуглавого усиления и трёхстороннего баланса», то есть при балансе интересов личности, общества и ИТ-сектора необходимо усилить как охрану чувствительной части личной информации, так и законное применение её обычной доли.

ПО СРАВНЕНИЮ С GDPR

Несмотря на то что принятый в 2021 г. PIPL многое позаимствовал от европейского Генерального регламента защиты данных (GDPR), он не стал его копией. Во-первых, китайский закон вводит понятие «чувствительной персональной информации», которая защищается строже, чем иные личные сведения. Она трактуется достаточно широко: это любая «личная информация, которая после утечки или незаконного использования может легко нанести ущерб достоинству [или] причинить серьёзный вред личной или имущественной безопасности». В GDPR такого понятия нет, в законе ограничились лишь конечным перечнем видов информации, к которой применяются более строгие меры защиты. Как видим, государственные органы КНР, в отличие от ЕС, имеют широкие полномочия по трактовке положений закона.

Во-вторых, экстерриториальное применение китайского закона шире, чем у европейского аналога. Оба закона распространяют за рубеж своё действие:

- если физическим лицам на своей территории предоставляются товары и услуги извне;
- если поведение этих лиц анализируется за пределами своей территории.

Однако у PIPL на руках есть козырь: закон применяется и «в других случаях, определённых законами или законодательными актами». Эта оговорка позволяет органам власти трактовать требования PIPL так, как им удобно. Поэтому крупные международные компании, создавшие базы конфиденциальной информации жителей КНР, должны вести себя особенно осторожно. К примеру, им следует перенести сервера с данными китайских клиентов на территорию Поднебесной, чтобы не попасть под штрафы, которые составляют до 5% от общего годового дохода. Те, для кого обязанности, налагаемые PIPL, оказа-

лись непосильными, покидают китайский рынок. К примеру, социальная сеть LinkedIn и компания Yahoo заявили о завершении работы в КНР.

В-третьих, китайский закон, в отличие от GDPR, автоматически относит любую персональную информацию, касающуюся несовершеннолетних, к чувствительной.

Кроме того, при передаче персональной информации за пределы КНР PIPL требует проведения оценки безопасности. Вместе с тем в случае крупномасштабного мониторинга поведения людей в общественных местах оценка угроз не требуется, в отличие от предписаний европейского Регламента. Это объясняется особым вниманием, которое китайское правительство уделяет общественной безопасности.

Более того, PIPL совершил революционный рывок: теперь операторам персональной информации, владеющим интернет-платформами с большим количеством пользователей и сложной системой деятельности (например, Baidu, Sina), предписывается регулярно публиковать отчёты о защите личных сведений, а также создать независимый орган надзора. В него должны входить лица, преимущественно не связанные с платформой, которые будут следить за защитой частной информации.

И наконец, PIPL предполагает более суровые санкции за нарушение закона. Помимо штрафа, налагаемого на предприятия, ненамного большего, чем в ЕС, полагается конфискация незаконно полученных доходов, штрафы в отношении работников, допустивших нарушения, приостановка действия или отзыв лицензии.

ВЗГЛЯД ИЗ РОССИИ

В России, которая с интересом изучает опыт дружественных стран, PIPL воспринимается неоднозначно: для одних этот закон — символ «цифровой диктатуры», для других — крепость, которая защищает жителей Поднебесной.

Аргументы в защиту первой точки зрения нашли своё отражение в статье «Обзор закона КНР о защите персональной информации», размещённой на портале Закон.ру. Автор Д. В. Садовников, руководитель направления защиты персональных данных Департамента развития ИИ и МО «Сбербанка», считает, что PIPL вовсе не повышает уровень защищённости человека, ведь в нём не предусмотрены «ограничения в отношении state surveillance (государственного надзора)», например, на массовое биометрическое распознавание.

Кроме того, автор отмечает, что в приведённом в законе перечне чувствительных данных отсутствуют сведения о политических взглядах. Такое положение дел может вызывать опасения: в том случае, если КНР «объявит охоту» на противников линии партии, беззащитные китайцы, стоящие как на ладони у правительства, не смогут укрыться — их сожмут в кулак.

В этих рассуждениях упускается то, что массовое биометрическое распознавание в КНР используется для защиты мирных жителей: к примеру, оно позволяет быстро вычислить затесавшегося в толпе террориста-смертника. Общеизвестный приоритет социальной стабильности и благосостояния над политическими свободами не должен удивлять, ведь Запад не раз использовал продвижение «либеральных ценностей» для раскачивания ситуации внутри Китая. Так, в 1989 году это привело к крупным беспорядкам на площади Тяньаньмэнь. Однако Д. В. Садовников подводит читателя к заключению, что PIPL — это последний на данный момент шаг на пути установления «цифровой диктатуры» в Поднебесной.

Руководитель Роскомнадзора А. Ю. Липов сделал другой вывод. Он предложил позаимствовать китайскую законодательную новеллу, содержащуюся в PIPL. По его мнению, гражданам РФ тоже не помешало бы отказаться от «согласия на обработку персональных данных» и довериться государству, которое избавит человека от всех нежелательных последствий, вызванных необдуманным нажатием на кнопку «согласен».

Такой же точки зрения придерживается и доцент кафедры предпринимательского права и руководитель Центра азиатских правовых исследований Юридического факультета МГУ им. М. В. Ломоносова А. Е. Молотников. Действительно, человеку без соответствующего образования сложно прочитать многостраничный текст юридического согласия, не говоря уже о том, чтобы понять, в каких именно целях корпорации пытаются использовать его личную информацию. «Государство действует в интересах человека и может урегулировать спорные моменты», — утверждает А. Е. Молотников в защиту закона PIPL.

Несмотря на разное отношение наших соотечественников к PIPL, в Китае сходятся в том, что их закон — это самое подходящее решение вопроса по защите персональных данных, которое разработано с учётом особенностей исторического развития Поднебесной, менталитета её народа и государственной идеологии.

«ПРОФЕССИОНАЛИЗМ, УМЕНИЕ ДРУЖИТЬ И ПРЕДАННОСТЬ РОДИНЕ...»

ВЛАДИМИРУ ГЕОРГИЕВИЧУ МАТЮХИНУ — 80 ЛЕТ! ПО СЛУЧАЮ ЮБИЛЕЯ ВИНОВНИК ТОРЖЕСТВА ОТВЕЧАЕТ НА ВОПРОСЫ BIS JOURNAL

— Владимир Георгиевич, Ваше детство и юность пришлись на тяжёлые послевоенные годы. С какими трудностями приходилось в тот период сталкиваться, что особенно врезалось в память?

— В десять лет я потерял отца, остался с мамой и сестрой. И хотя отца уже не было, пример его служения Родине и профессии всегда показывал мне путь. Своим воспитанием я обязан маме, сестре и государству. А трудности были такие же, как у всей страны в послевоенный период. Я прошёл все нюансы дворового воспитания. Пришлось регулярно разгружать вагоны на железнодорожной станции, правда, за хорошие деньги.

— При изучении Вашей биографии создаётся впечатление, что Вы были целеустремлённым человеком и знали, чего хотите от жизни...

— Мне тоже кажется, что я был целеустремлённым в выборе профессии. Ребёнком я мечтал заниматься микроэлектроникой. Мне повезло, так сложились обстоятельства, что вначале я окончил МЭИ — факультет электронной техники, и меня взяли на военную службу в КГБ СССР. Я понял, что моего образования недостаточно, и, сдав экзамены, снова стал студентом, теперь уже мехмата МГУ... Учился вечерами, днём работал. Семья поддерживала! Всё нравилось! Коллеги были замечательные, умные образованные офицеры, они и помогали, и воспитывали. Многие стали друзьями на всю жизнь. Коричнев В. В., Башев В. А., Дудник С. Я., Кущ В. Л., Караваешников Е. К., Изотов Б. С., Бубеничик А. А., Прянишников К. В., Бекетов Е. Б., Лапшин А. В., Хрупов В. А., Кубаев В. И., Мосякин Ю. С., Чеченкин В. М., Гостев С. В., и многие другие. Школа жизни была превосходная, повезло!

Работа была очень интересная. Возглавлял Федеральное агентство правительственной связи и информации при Президенте РФ (ФАПСИ), был первым заместителем министра МО РФ, создавал и возглавлял Госкомоборонзаказ, Росинформтехнологии. Последние 14 лет работаю в АО «НИИАС» при ОАО «РЖД» — и везде по одной специальности.

— Что Вы думаете о современной системе образования в России? Способна ли она в существующем виде дать адекватный ответ запросам общества и государства?

— На мой взгляд, образование в России требует активной, срочной перестройки! Существующая система образования не отвечает современным

ВИЗИТНАЯ КАРТОЧКА

Владимир Георгиевич Матюхин родился 4 февраля 1945 года. В 1968 году окончил Московский энергетический институт по специальности «электронная техника», в 1973 году — механико-математический факультет МГУ имени М. В. Ломоносова по специальности «математика».

1969–2003 годы — военная служба в органах государственной безопасности. С 1991 до 1993 года возглавляет научно-исследовательский центр Федерального агентства правительственной связи и информации при Президенте РФ. С 1993 по 2003 год — заместитель, затем генеральный директор ФАПСИ. В 2003 году — Первый заместитель Министра обороны, исполняющий обязанности председателя Государственного комитета РФ по оборонному заказу. Воинское звание — генерал армии. В 2004–2010 годах возглавляет Федеральное агентство по информационным технологиям (Росинформтехнологии).

С 2010 года занимает должности в Научно-исследовательском и проектно-конструкторском институте информатизации, автоматизации и связи на железнодорожном транспорте (АО «НИИАС», дочернее общество ОАО «РЖД»): Первый заместитель генерального директора — научный руководитель; Председатель экспертного совета. Доктор технических наук, действительный член Академии криптографии РФ, Российской академии инженерных наук и Международной академии связи, дважды лауреат Государственной премии РФ.

запросам общества и государства! Данная система не учит мыслить, а является системой натаскивания!

— Занимая должность заместителя генерального директора ФАПСИ в 1990-е годы, Вы активно занимались работой над тематикой микропроцессорных пластиковых карт, внедрением электронных подписей в документооборот, включая их интероперабельное взаимодействие. Вы уже тогда понимали, какое значение они приобретут в будущем?

— Да, конечно. Я вплотную занимался этими вопросами, отчётливо понимая их важность для экономики России! Переход на микропроцессорную тематику был исключительно актуален в области информационной безопасности России. Но, к сожалению, это встречало большое сопротивление со стороны коммерческих структур. Бытовало мнение, что мы купим лучшие микропроцессоры за рубежом.

Производительность отечественных процессоров в то время не позволяла выполнять необходимые математические преобразования. Мы с группой единомышленников создали интеллектуальные карты на базе отечественного микропроцессора. Эти карты были полностью защищены по высоким криптографическим требованиям! Мы их применяли в качестве носителей ключей в шифраппаратуре. И это впервые позволило значительно повысить уровень защищённости передаваемой информации, а в дальнейшем — создать защищённую аппаратуру с российскими алгоритмами передачи речи на скоростях 2400–9600 бит/сек. Так была создана аппаратура «Разбег».

Чтобы взаимодействовать с заказчиками, мы проводили для коммерческих структур конференции «Российские интеллектуальные карты „РИК“», «PKI-Форум», который, кстати, проводится до сих пор. Но, к сожалению, рынок предпочёл карты «Виза» и «Мастеркард» на импортных микропроцессорах с импортным программным обеспечением. Сейчас в России срочно внедряется отечественная карта «МИР», прошло 25 лет!

Главные результаты были получены сотрудниками ФАПСИ. Необходимо отметить личный вклад Пярина В. А., Баранова А. П., Галдина А. А. и многих других. Недавно ОАО «РЖД» подписало соглашение о применении интероперабельного электронного взаимодействия с Китаем, и эти технологии внедрены в соответствующий документооборот.

— В своё время Вы сыграли важную роль в формировании в России информационной безопасности как отрасли. Как, на Ваш взгляд, со временем менялся характер рисков реализации угроз для информационной инфраструктуры и подходы к их преодолению?

— В СССР криптографической защитой занимались только в КГБ СССР и на специализированных предприятиях. После 1990 года началась

полная вакханалия. Сотни фирм стали разрабатывать и продавать собственные, зачастую непрофессиональные, разработки, что существенно снизило защищённость передаваемой информации. В большинстве случаев информация дешифровалась практически «вслед». Эту шифртехнику пытались внедрять в государственные экономические и финансовые структуры. В условиях рыночной экономики требовались правила регулирования процессов разработки и эксплуатации шифртехники. При моём личном участии были разработаны правила сертификации шифртехники и лицензирования предприятий-разработчиков. Необходимо было провести серьёзные работы, чтобы через короткое время государственные банковские и финансовые структуры признали разработанные принципы.

— Кибермошенничество и преступления в финансовой сфере в России приобрели пугающие масштабы, борьба с ними пока не приносит желаемых плодов. На Ваш взгляд, какие меры могли бы значительно повысить эффективность этой борьбы?

— В 90-е годы мы активно занимались внедрением так называемой электронной цифровой подписи (ЭЦП). Под моим руководством были разрабо-

таны процедуры электронного документооборота с широким применением ЭЦП. К сожалению, в ряде коммерческих приложений остались схемы доступа «логин – пароль», которые обладают простотой и дешевизной реализации, а реальной защитой не обладают. Более широкое внедрение ЭЦП позволит убрать большинство проблем, связанных с защитой информации, в том числе позволит эффективнее бороться с мошенниками.

– На рубеже XXI века и в нулевые годы под Вашим руководством были реализованы прорывные проекты, такие как защищённые системы видео-конференц-связи, предоставление государственных услуг в электронном виде, юридически значимый электронный документооборот, цифровая подпись и т.д. Как Вы считаете, в каком направлении должна двигаться цифровизация сегодня и каких опасностей следует избегать?

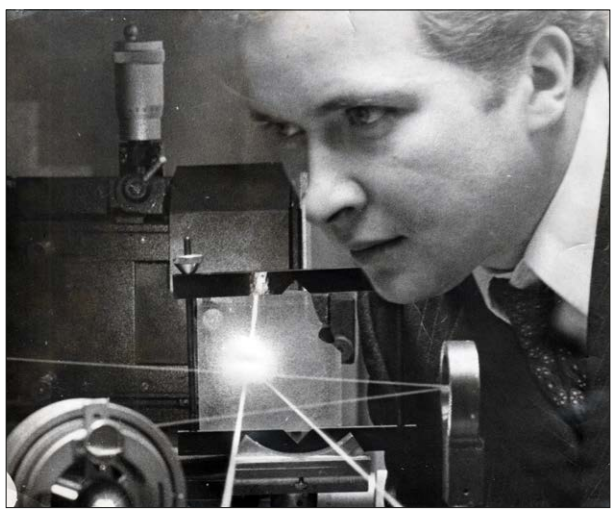
– Все перечисленные проекты на данном этапе выполняются и получили широкое внедрение. Опасения, как всегда, вызывает распылённость на разработки соответствующих систем для различных заказчиков этой продукции. Я считаю, потребностью чрезвычайной важности сегодня является разработка платформы стратегического планирования управления государством! Но у этой задачи нет госзаказчика.

– Следует ли нам опасаться активного развития искусственного интеллекта?

– Я за активное развитие искусственного интеллекта. Но только при жёстком соблюдении требований кибербезопасности. Считаю, что развитие самообучаемого искусственного интеллекта должно происходить под пристальным вниманием учёных.

– Долгие годы Вы вносите свой вклад в эффективную работу нашего железнодорожного транспорта как первый заместитель генерального директора – научный руководитель ОАО «НИИАС», председатель экспертного совета. Какую роль играют в наше напряжённое время транспорт и логистика, в каком направлении, по Вашему мнению, они должны развиваться?

– Мы создали интеллектуальную систему управления железнодорожным транспортом (ИСУЖТ) практически на всей сети железных дорог России в реальном времени. В начале разработки проблемным был главный вопрос: может ли современная вычислительная техника решать оптимизационные задачи с колоссальным числом параметров (стрелка, светофор, поездные бригады, локомотивы и др.)? Мы разработали быстрые алгоритмы, позволившие решать оптимизационные задачи в приемлемое время, создали программно-технические решения для всей сети с учётом обеспечения её информационной безопасности и внедрили их. По-моему, эти решения могут стать основой для совершен-



ствования системы управления всеми рабочими процессами на железной дороге.

— Вы — доктор технических наук, старший научный сотрудник, профессор, действительный член Академии криптографии Российской Федерации, Российской академии инженерных наук и Международной академии связи. Автор и соавтор более 170 научных работ, из них 1 монография и 2 учебных пособия, а также 34 патентов, авторских свидетельств на изобретения и свидетельств на государственную регистрацию программных продуктов. Лауреат Государственной премии Российской Федерации, лауреат Премии Правительства Российской Федерации. Что можете сказать про Вашу научную деятельность?

— В 1982 году я защитил кандидатскую диссертацию, в 2004 году — докторскую. Темой моих научных интересов всегда была информационная безопасность государства. Мне посчастливилось работать с такими учёными, как Котельников В. А., Прохоров А. М., Андреев Н. Н., Козлов В. Я., Фабрикант В. А., Лебедев С. А., Степанов В. Е., Велихов Е. П., Кузнецов Н. А., Красников Г. Я. и многими другими. Все мои научные коллективы состояли из творческих высокообразованных учёных. Я горжусь, что многие результаты научных разработок, в которых я принимал личное участие, реализованы в действующей аппаратуре. Многие наши разработки легли в основу проектов будущего. Научным сообществом высоко оценён мой вклад, я награжден Золотой медалью Академии криптографии РФ имени В. А. Котельникова за выдающиеся достижения в области криптографии, Золотой медалью А. С. Попова за значительный вклад в развитие отечественной науки и техники, дипломами многих научных конференций, являюсь лауреатом Премии В. М. Глушкова за разработку инновационных систем в сфере управления.

— В настоящее время конфронтация с Западом достигла небывалых масштабов.

Как быстро будет преодолено это противостояние и сможем ли мы выйти из него с выгодой для нашей страны?

— Конфронтация с Западом стимулировала нашу активность в вопросах защиты информации. Обновлены программно-технические средства защиты, повышена дисциплина выполнения регламентных работ.

Эффективность защиты будет зависеть от скорости реакции на обнаруживаемые уязвимости и совершенствование организационных мер. Считаю, что в перспективе конфронтация с Западом должна перейти в сотрудничество. Но концепция такого перехода должна быть поддержана и принята всеми ведущими государствами мира в рамках реализации многополярной системы миропорядка.

— Какие качества вы цените в людях и какие не приемлете?

— Профессионализм, умение дружить и преданность Родине. Не приемлю предательство в любом его проявлении, инфантилизм. Но мне повезло по жизни, я работал всегда среди достойнейших людей, беззаветно любящих свою Родину!

Вопросы задавал Усам Оздемиров

РОВЕСНИК АКАДЕМИИ

К 300-ЛЕТИЮ ФРАНЦА ЭПИНУСА

Борис СТОЛПАКОВ
историк криптографии

В прошедшем году вместе с юбилеем Российской академии наук отмечалось 300-летие со дня рождения академика Ф. Эпинуса, примечательного среди прочего тем, что он 33 года возглавлял криптографическую службу России в XVIII столетии.

МАТЕМАТИК СРЕДИ МАТЕМАТИКОВ, ВРАЧ СРЕДИ ВРАЧЕЙ

Фамилия Эпинус похожа на псевдоним с латинским звучанием. И это близко к истине. Согласно изысканиям биографов, одним из предков нашего академика 500 лет назад стал священник и богослов Иоганн Хох, активнейший деятель Реформации. И. Хох заменил свою фамилию её синонимом на греческом языке — Aipeinos (высокий), что постепенно и приобрело латинизированную форму — Эпинус.

Будущий академик Франц Эпинус появился на свет 13 декабря 1724 года (здесь и далее старый стиль) в г. Ростоке. Он был пятым ребёнком в семье профессора теологии Ростокского университета Франца Альберта Эпинуса.

Когда в 1740 году Ф. Эпинус начал обучение в университете, он уже вполне владел латынью и имел некоторую математическую подготовку. В университете он посещал лекции одновременно на философском и медицинском факультетах. В 1744 г. Эпинус отправился на два года в Йенский университет, где занимался математикой и физикой, химией и медициной. Именно в Йене утвердились профессиональные навыки Эпинуса в самых разнообразных областях. Постоянное усвоение новых знаний в целях собственных исследований, умение использовать предшествующий опыт и аргументированно отстаивать своё мнение в научных дискуссиях сложились у него со студенчества.

Научные труды, диссертации не заставили себя ждать. В 1747 г. в родном университете Ф. Эпинус получил учёную степень доктора философии и начал читать лекции по математике, а в 1748 г. на медицинском факультете на публичном экзамене его удостоили степени доктора медицины. Одновременно Ф. Эпинус выпустил несколько самостоятельных математических работ. Но всё же Росток был научной периферией.

В БЕРЛИНСКОЙ АКАДЕМИИ ПО ПРИГЛАШЕНИЮ ЭЙЛЕРА

В середине XVIII столетия Берлин стал лидером среди столиц германских государств в плане развития научных исследований. Столица Пруссии обязана этим прежде всего своему королю Фридриху II. Как известно, его считают родоначальником германской государственности. Роста значимости Пруссии в европейских делах он добивался не только расширением её пределов, но и созданием условий для привлечения туда авторитетных специалистов. Так, в 1741 г. в Берлин переехал из Петербурга академик Л. Эйлер, правда, спустя 25 лет он вернулся в Россию. В 1754 г. в Берлинской академии наук временно утвердился в качестве астронома и Ф. Эпинус.

Сначала по рекомендациям своих учителей и по приглашению Л. Эйлера он приехал в Берлин для личной встречи. У Эйлера сложилось самое благоприятное впечатление о госте и его способностях, он представил Эпинуса Президенту академии П. Мопертюи. Так состоялось приобщение преподавателя провинциального университета к кругу ведущих учёных Европы.

Природный талант, воспитание, поддержка великого Эйлера, его пример, казалось бы, должны были прочно связать малоизвестного провинциала с Берлинской академией, но уже в начале 1756 года он стал искать пути перехода в Петербургскую академию наук.

ПЕРСПЕКТИВЫ В ПЕТЕРБУРГЕ

Перспективы материального достатка и независимости в научной деятельности в Петербургской академии рисовались более обещающими, а сведения о ней представлялись достоверными. Эти сведения приходили в Росток из петербургской общины церкви св. Екатерины. В небольшой по численности лютеранской общине пребывали вместе с семьями профессора Академии, в том числе Миллер и Рихман. Членами общины были академические руководители Шумахер и Тауберт. Видное положение в общине занимал брат жены старшего брата Ф. Эпинуса, купец, он сообщал родственникам о быте и нравах в академической среде и в начале 1756 года выступил посредником в контактах Эпинуса и Миллера.

В июле 1756 года Л. Эйлер получил от Г. Миллера письмо, где тот интересовался: «Что это за но-

вый астроном в Берлине, о котором пишут газеты? Может быть, г-н Эпинус больше подойдёт на должность профессора физики в нашей Академии?» Тогда в Петербурге искали физика на место Рихмана, погибшего от удара молнии в 1753 году. Эйлер ответил Миллеру, что «г-н Эпинус не только хороший астроном, но и хороший физик», и сообщил Эпинусу об этом запросе из Академии. Понятно, что предложение было лестно для Эпинуса, да и возможное жалованье утраивало его доходы. Он обменялся письмами с Миллером, и вскоре необходимые документы были отправлены в Петербург. Уже 26 октября их подписал президент. Правда, покинуть Берлин Эпинус не мог, не получив отставки и королевского разрешения на выезд. Л. Эйлер сам хлопотал за него перед королём, но желанное разрешение было получено лишь весной 1757 года. Начиналась Семилетняя война, в которой Пруссия и Россия состояли во враждебных коалициях.

СМЕНА ТЕМАТИКИ И НОВЫЕ ЗНАКОМСТВА

Осень 1756 г. стала знаменательной для Ф. Эпинуса и в плане существенной переориентации научных интересов: он начал исследования по электричеству. Сказался интерес к этой проблеме в семействе Эйлеров. Но всё же главным побудительным мотивом, вселившим уверенность Эпинуса в своём успехе, стал открытый им фундаментальный экспериментальный факт существования в природе естественных электрических диполей.

10 мая 1757 г. Эпинус прибыл из Любека морем в Петербург. Предваряя его приезд, Л. Эйлер в письме к Г. Миллеру от 5 апреля сообщал, что Эпинус уже в Ростоке. К письму были приложены образцы шифров, полученные Эйлером из Базеля. Да, и такое бывало.

Эпинус по приезде в Петербург посетил Х. Гольдбаха и передал ему рекомендательное письмо Эйлера, которое начиналось так: «Г-н профессор Эпинус, который имеет честь вручить это письмо, является не только моим очень хорошим другом, но имеет кроме своей основательной учёности такие заслуги, которые дают мне основание считать, что его знакомство с Вашим Высокоблагородием будет не неприятным, и поэтому я осмеливаюсь рекомендовать его Вашему Высокоблагородию».

Миллер был другом Гольдбаха, а тот, как известно, с 1742 г. возглавлял шифровальную службу России.

В ПЕТЕРБУРГСКОЙ АКАДЕМИИ НАУК

Ф. Эпинус быстро сходился с людьми. Поначалу и с М. В. Ломоносовым у него были дружеские отношения. Вместе с тем новый профессор физики буквально с первых же недель начал высказываться нередко критически по обсуждаемым проблемам. Он стал практиковать и изложение замечаний в письменной форме для передачи оппонентам.

Осенью 1758 года Эпинус начал писать фундаментальный труд «Опыт теории электричества и магнетизма». Уже в конце 1759 г. был напечатан весь тираж (650 экземпляров). Несмотря на малый тираж, эта книга приобрела широкую известность в мире. Известно, что труд Эпинуса высоко оценили современники: Франклин, Кавендиш, Вольта, Кулон, а впоследствии и Фарадей, Кельвин, Максвелл. Общее признание поставило Эпинуса в ряд «классиков науки».

Скоро его приближает к себе и двору великая княгиня Екатерина Алексеевна. Эпинус стал её учителем физики и математики. Затем 2 октября 1760 г. Главный директор Сухопутного шляхетского кадетского корпуса великий князь Пётр Фёдорович назначил учителя своей супруги Ф. Эпинуса главным инспектором классов Корпуса. Президент академии был вынужден согласиться с работой члена Академии в двух местах.

ГЛАВНЫЙ ИНСПЕКТОР КЛАССОВ

Заняв должность в Корпусе, Эпинус снял с себя массу житейских забот: он получил «государеву квартиру» с казёнными дровами и свечами. Эпинус работал в Корпусе до января 1765 года.

В русских официальных документах и письмах его обычно именовали Францем Ивановичем. В его обязанности входило составление программ учебных курсов, поиск преподавателей, «надзирание» за успеваемостью кадетов, организация и проведение экзаменов, в том числе в присутствии высочайших особ. Обучение кадет начиналось с шестилетнего возраста и продолжалось 15 лет. Корпус готовил не только военных, но и государственных чиновников. Сам Эпинус читал лекции по экспериментальной физике и принимал экзамены, причём был очень скуп на оценки.

Именно в эти годы, годы практической работы в значительном учебном заведении, ему и удалось найти методы обучения, эффективные в реальных условиях России той поры. Корпус имел крупнейший по тем временам контингент учащихся — 660 кадетов. Под руководством Эпинуса трудились около 80 человек — профессоров, адъюнктов, учителей, механиков, канцелярских служителей. Кадетом при Эпинусе был А. Храповицкий — будущий статс-секретарь Екатерины II и её референт по разведке и контрразведке. В обучении кадетов Эпинусу помогали поручик С. Порошин, ставший учителем и воспитателем Павла Петровича, поручик П. Пастухов — в будущем статс-секретарь Екатерины II в течение многих лет.

«Я ГОТОВ ПОСВЯТИТЬ СЕБЯ ТОЙ ДЕЯТЕЛЬНОСТИ...»

В конце мая 1764 г. Эпинусу было «повелено преподавать наставления в экспериментальной фи-

зике цесаревичу Павлу Петровичу». Окружающие отмечали, что «государыня особенно выделяет его своей благосклонностью». В судьбе Эпинуса зреет ещё один поворот, предопределённый близостью с Н. И. Паниным — воспитателем Павла Петровича и с 1763 г. канцлером России.

В письме к Панину на исходе 1764 г. Эпинус писал: «Я готов посвятить себя той деятельности, которую Е. И. В. мне предлагает, но я умолил её сохранить за мной место в Академии. Чтобы предотвратить море сплетен, в которое мне пришлось бы погрузиться, я умоляю направить Академии указ, который бы гласил: поскольку Е. В. доверила мне заниматься с великим князем, что не позволит мне регулярно работать в Академии, Е. В. освобождает меня от работы в Академии таким образом, чтобы Академия ничего не требовала бы от меня, исключая то, что я сам в состоянии делать по собственной воле, но что указом Е. В. я остаюсь ординарным членом Академии». Эти пожелания Эпинуса практически дословно перенесены в именной указ, подписанный Екатериной II 12 февраля 1765 г. Как ныне известно, этот указ маскировал другое секретное распоряжение, коим Эпинусу, зачисленному в Коллегию иностранных дел (КИД), устанавливалось жалование 3000 рублей в год с 1 января 1765 г. Начался длительный период общегосударственной деятельности Эпинуса.

33 ГОДА В ШИФРОВАЛЬНОЙ СЛУЖБЕ РОССИИ

Ф. Эпинус возглавил шифровальную службу России и оставался в ней 33 года. В обязанности Эпинуса и его подчинённых входило составление шифров и подбор ключей к перехваченной корреспонденции.

Потребителями шифров, создаваемых в КИД, были: императрица, её кабинет (общие и индивидуальные шифры для переписки с высшими чиновниками государства), коллегия иностранных дел (общие и индивидуальные шифры для переписки приблизительно с 70 дипломатическими представителями России за рубежом и между собой; для переписки с иностранными дворами; специальные шифры для переписки с секретными агентами русского правительства), армия и флот. Основные языки: русский, французский, немецкий. Реже использовались английский, испанский, итальянский. Особенно сложной задачей являлось для Эпинуса дешифрование перехваченных текстов. Этим он занимался лично.

УРОКИ ПАВЛУ ПЕТРОВИЧУ И ЗАДАНИЯ ЖИТЕЛЯМ

Наряду с работой в КИД Эпинус продолжал трудиться в Академии и давать уроки великому князю Павлу Петровичу. Эти уроки, а впоследствии лекции по физике, астрономии, анатомии с разной степенью углублённости в предмет, продолжались до 1779 г., как можно судить по фрагментам лекций, сохранившимся в Павловском Дворце — музее.

31 октября 1765 г. императрица «всемилостивейше апробовала» создание Вольного экономического общества. Эпинуса вскоре избрали в члены общества, а темой его вступительной речи стала актуальная проблема внедрения научных достижений в экономическую практику. Этой линии он придерживался и когда оценивал чужие работы, представленные на награждение медалями ВЭО, и когда обнародовал собственное предложение, обещая от себя награду за осушение болот на площади, достаточной для посева двух бочек ржи. Эффект превзошёл тогда ожидания. Воодушевлённые духовенством мужики под Выборгом осушили к осени 1772 г. болота площадью, пригодной для посева 83 бочек ржи. Эпинусу пришлось выдать пять наград.

Основное его местопребывание в 1770-х годах — это КИД и двор. После бракосочетания Павла, именным указом 20 октября 1773 г. Ф. Эпинус произведён в действительные статские советники, т.е. достиг генеральского положения.

РЕФОРМА НАРОДНОГО ПРОСВЕЩЕНИЯ: КАК ПОДСТУПИТЬСЯ?

Однако в перечне его достижений на первое место биографами ставится участие в создании российской системы народного образования.

В наследство от предшествующих царствований Екатерина II получила школу, которая нуждалась в реформировании. Элементарная подготовка учащихся по-прежнему основывалась на традиции чтения религиозных текстов и зубрёжке. Учебные заведения не были никак сопряжены друг с другом по программам, не обладали преемственностью. Отсутствовала профессиональная педагогическая подготовка учителей, не хватало учебников и пособий.

Накануне воцарения Екатерины II один из основателей Московского университета И. И. Шувалов вышел с представлением в Сенат об устройстве единой системы образования (школы грамотности в малых городах — гимназии в больших городах — университет или кадетский корпус в столицах), но предназначенной только для дворян. К обсуждению реформы подключили Академию наук. В предложениях её членов прозвучала мысль о допуске в школы и гимназии наряду с дворянами представителей «чиновных людей и знатнейшего купечества», а также зажиточных мещан или об устройстве, наряду с дворянскими, особых училищ для других сословий.

Ф. Эпинус присоединился к мнениям, предлагавшим систему построенных на преемственности обучения школ разного уровня или ступеней

Иллюстрация 1. Здание Сухопутного кадетского корпуса (Меньшиковский дворец)

единой школы. Однако, в отличие от большинства своих немецких и русских коллег по академии, не представлявших образование без изучения латыни, Эпинус полагал «в нижних школах латинский язык или совсем отставить, или оному только тех обучать, кои со временем учёными быть должны».

Практическим результатам обсуждения школьной реформы помешала смерть императрицы Елизаветы Петровны.

Служба Эпинуса в 1760–1765 гг. в Корпусе обогатила его педагогический опыт и помогла в дальнейшем при разработке основ русской общеобразовательной школы.

ВСТРЕЧА В МОГИЛЁВЕ

Ключевым документом в истории разработки проекта школьной реформы исследователями признаётся записка Эпинуса, подготовленная для Екатерины II в конце 1781 — начале 1782 г. Подлинник самой записки не найден, но детали разработки реформы стало возможным уточнить благодаря недавней находке историком Л. М. Артамоновой в архиве РАН русского текста записки Эпинуса, современного её составлению.

Первоначальным толчком к разработке этого проекта стала встреча австрийского императора Иосифа II с Екатериной II в Могилёве в 1780 г. Одной из главных тем их бесед стали австрийские «нормальные» школы.

Разговор об австрийских школах возник не случайно. Конечно, цель визита императора была далеко не просветительская. Но Иосиф II потребовал срочно прислать из Вены в Могилёв по два экземпляра всех книг, выпущенных для нормальных школ, в самых лучших переплётах. Подарок был принят Екатериной II с благодарностью. Экспертами австрийской системы образования стали Московский университет и Петербургская академия наук. Императрицу заинтересовала записка ректора гимназии при Московском университете Б. Б. Шадена, возглавлявшего её с основания до середины 1770-х годов, а затем организовавшего один из лучших частных пансионов Москвы. Видный учёный и педагог, среди учеников которого в разное время были Д. И. Фонвизин и Н. М. Карамзин, призвал перенять австрийские учебные методики и руководства. Самое же сильное влияние на разработку проекта школьной реформы оказала записка Эпинуса.

ЗАПИСКА ЭПИНУСА

«Записка не имеет подписи. Несомненно, что её не было и в немецком оригинале. Екатерине II был известен почерк Эпинуса настолько хорошо, что тот никогда не подписывал своих записок, подаваемых императрице, и лишь аккуратно ставил даты на них. Количество людей, позволявших себе такую вольность в переписке с Екатериной, было крайне ограниченным».

Сохранившийся в архиве перевод записки на русский язык оказал большое воздействие на дальнейшие формулировки документов по школьной реформе. Русскому выражению «народное училище», которым были названы общеобразовательные учебные заведения разного уровня, созданные при Екатерине II, соответствует немецкое

«Nationalschule». Видно, как вместо ещё не совсем привычной русскому уху «школы» употреблено общепонятное «училище», но ещё более примечательна трактовка этой школы как «национальной», т.е. «государственной» или «общенародной».

Австрийский школьный опыт являлся по существу удачным опытом усвоения греко-римской учебной традиции в условиях нового времени. Такой подход к обучению обеспечил успехи европейской науки. Эпинус предлагал максимально точно воспроизвести австрийскую модель реформы, поскольку не нашёл причин для её неуспеха в российских реалиях.

Началом всей реформы он полагал немедленное создание 3–4 образцовых училищ предположительно в Петербурге, Москве, Казани и Киеве. Такие училища не только давали бы общее образование, но также предназначались для подготовки педагогических кадров, которые, освоив школьные курсы, должны были дополнительно обучиться «наставлению для будущих учителей». Одновременно предполагался запрет заниматься учительской деятельностью всем, «кроме обучившихся и удостоившихся в нормальном училище».

Особое внимание к подготовке педагогов — краеугольный принцип «австрийского» проекта. Учитель должен был знать не только свой предмет, но и то, как учить ему детей по научно обоснованной методике — «способу учения».

«НАШЕМУ СОВРЕМЕННИКУ ТРУДНО ПРЕДСТАВИТЬ...»

«Нашему современнику трудно представить, что в число новейших методик, незнакомых даже образованным русским людям, входила задача учителя работать одновременно со всем классом, а не с каждым отдельным учеником по очереди, как это было в традиционной школе. Такой метод работы требовал снабдить учеников одинаковыми учебниками, а учителей — одинаковыми руководствами, научить тех и других пользоваться наглядным материалом в виде таблиц или других пособий, работать с классной доской и мелом. Соответственно, в классе должны были находиться дети одного уровня подготовки, вместе осваивающие одну и ту же программу и переходящие из класса в класс. Необходимо было создать школу нового времени, массовую не только по количеству учащихся, но и по характеру обучения. Принципиальным отличием нового „способа учения“ стало также требование „приучать их к собственному рассуждению“, а на опросах и экзаменах „узнавать их понятие о предлагаемых вещах“ вместо механического воспроизведения вызубренного».

Ещё одно важное положение, определённое Эпинусом, заключалось в том, что «способ учения» нельзя было перенять заочно, даже изучив выпущенные по нему руководства. Эта методика передавалась новым педагогам через практическое знакомство с ней в уже существующих училищах: «Сим образом получаются такие люди, кои знают совершенно все учреждения не только умозрительно, но и практически». Эпинус указывал, что в Австрийской империи среди перенявших эту методику есть люди, которые говорят на славянских языках и исповедуют православие. Их и надо попросить у императора для начала подготовки первых русских учителей: «И сие обстоятельство было бы весьма щастливо, дабы в противном случае народ, увидя первых учителей римско-католического вероисповедания, не получил бы отвращения к сим новоустановленным училищам».

«А ВОТ ТОЕ ВСЁ, ЧТО С ЭПИНУСОМ СЛОЖИЛИ»

Свой план Эпинус представил императрице в начале марта 1781 г. Для более широкого обсуждения он был переведён на французский и русский языки.

Записка Эпинуса стала предметом беседы между ним и Екатериной II, которая составила по результатам разговора «Черновые собственноручные замечания императрицы Екатерины II о средних и низших школах». Показательна последняя фраза этих записей: «А вот тое всё, что с Эпинусом сложили».

Основное место в записях императрицы занимают конкретные указания по реализации намеченных с Эпинусом мероприятий. В Петербурге должна быть учреждена в качестве образца одна «средняя» или «нормальная» школа, первоначальное содержание которой Екатерина брала на свой счёт. Для начала занятий в ней необходимо было перевести все книги, предназначенные для австрийских нормальных школ. Принято решение о создании специального органа по осуществлению образовательной реформы, который здесь назван «Школьной комиссиею». Ей предписывалось представить план для школ Петербургской губернии, ставшей экспериментальной площадкой реформы, рассмотреть и отредактировать переведённые с немецкого языка учебники, особенно по закону Божьему и родному языку, способствовать подготовке других необходимых переводов и сочинений методического назначения. «Императрица распорядилась, чтобы посол в Вене старался достать православных учителей для укомплектования хотя бы „одной нормальной школы“. В Россию с разрешения императора, правда, приехал только один педагог, но по знаниям и энергии он стоил многих. Это был выдающийся сербский просветитель Ф. И. Янкович де Мириево».

7 сентября 1781 г. последовал первый законодательный акт новой реформы о создании Комиссии об учреждении народных училищ, одним из членов

которой стал Эпинус. Её первое заседание прошло 13 сентября 1782 г. Тогда же состоялась и премьера «Недоросля», подчеркнувшая своевременность усилий императрицы. 22 ноября 1782 г. государыня пожаловала Эпинуса кавалером ордена Святой Анны с бриллиантами.

ПЕРВЫЙ ОБЩЕРОССИЙСКИЙ ЗАКОН О НАРОДНОМ ОБРАЗОВАНИИ — 1786 Г.

«Упорным рачением» Комиссии к 1791 году были созданы школы во всех губерниях — Россия стала державой с государственной системой просвещения. Эпинус пробыл в составе Комиссии до своего ухода с государственной службы в 1797 году. Отметим его ведущую роль в разработке первого общероссийского закона о народном образовании — «Устава народным училищам» (илл. 2).

Под докладом, при котором в 1786 г. был поднесён на утверждение императрице этот Устав, как и под другими важнейшими документами школьной реформы, стоит подпись Эпинуса. Трудами Комиссии были открыты во всех губерниях «главные» и «малые» народные училища, как тогда называли соответственно средние и начальные школы, подготовлены сотни педагогов и обучены тысячи детей. В 1797 г. в стране под ведением Комиссии действовала 281 школа, в них обучалось 17 598 детей и работал 721 учитель. Главное — система просвещения и образования устойчиво развивалась. Учреждённая в 1786 г. учительская семинария для подготовки учителей для народных училищ превратилась через 17 лет в Педагогический институт. На его основе в 1819 г. был открыт Санкт-Петербургский императорский университет. Первым его ректором стал М. А. Балугьянский, широкообразованный русин, приглашённый для преподавания в Россию из Австрийской империи в 1803 г.

«ЭТА РАБОТА ТРЕБУЕТ ОЧЕНЬ НАПРЯЖЁННОЙ РАБОТЫ МЫСЛИ»

В 1780-е годы Эпинусу уже тяжело давалось совмещение работы в КИД с ответственными поручениями императрицы, тому есть свидетельства. С 1781 г. Эпинус пересылал полученную при дешифровании информацию непосредственно императрице. И в одном из сообщений он высказался о собственном психическом состоянии при дешифровальной работе: «Эта работа требует очень напряжённой работы мысли. И если ты плодотворно, смотря по обстоятельствам, использовал два, три, максимум четыре часа из двадцати четырёх — остальная часть дня потеряна. Силы ума исчерпаны, его острота притупилась, и человек не способен ни к этой, ни к какой иной работе. Причины того, что я уже продолжительное время работаю не менее чем обычно, но имею небольшой успех, я позволю себе объяснить В. И. В. после того, как завершу работу, которая сейчас у меня под рукой. 11 декабря 1782 года». Вероятно, тогда Эпинус стал просить о своей замене, но ещё в 1788 г. такой человек не был найден. Эпинус постепенно отдаляется от «большого двора» и всё более пребывает в «малом» — при Павле Петровиче. По отзывам: «Эпинус исключительно привязан к великому князю, который, в свою очередь, полностью ему доверяет».


646 ЦАРСТВОВАНІЕ ГОСУДАРЫНИ
1786

ями, изволила мнѣ повелѣть сообщить вашему Превосходительству, о учиненіи подобныхъ предписаній и Земскимъ Исправникамъ пограничныхъ уѣздовъ Полоцкаго и Могилевскаго Намѣстничествъ, дабы приводимыхъ къ нимъ бѣглыхъ здѣшнихъ принимали безъ затрудненія, давая въ томъ росписки.

16.421. — Августа 5. — Высочайше утвержденный Уставъ народнымъ училищамъ въ Россійской Имперіи.

Воспитаніе юношества было у всѣхъ просвѣщенныхъ народовъ толико уважаемо, что почитали оное единымъ средствомъ утвердить благо общества гражданскаго; да сіе и неоспоримо, ибо предметы воспитанія, заключающіе въ себѣ чистое и разумное понятіе о Творцѣ и Его святомъ законѣ, и основательныя правила непоколебимой вѣрности къ Государю, и истинной любви къ отечеству и своимъ согражданамъ, суть главныя подпоры общаго Государственнаго благосостоянія. Воспитаніе, просвѣщая разумъ человѣка различными другими познаніями, украшаетъ его душу; склоняя же волю къ дѣланію добра, руководствуетъ въ жизни добродѣтельной и наполняетъ наконецъ человѣка такими понятіями, которыя ему въ общежитіи необходимо нужны. Изъ сего слѣдуетъ, что сѣмена таковыхъ нужныхъ и полезныхъ знаній сѣять еще должно съ малолѣтства въ сердцахъ отроческихъ, дабы они въ юношескихъ лѣтахъ возрастали, а въ мужескихъ созрѣвши, обществу плодъ приносили. Но какъ плоды сіи не иначе размножить можно, какъ распространеніемъ самаго наставленія: то для сего и учреждаются нынѣ такія заведенія, гдѣ на основаніи общихъ предписаній преподавать будутъ оное юношеству на языкѣ природномъ. Таковыя заведенія существовать должны во всѣхъ Губерніяхъ и Намѣстничествахъ Россійской Имперіи, подъ именемъ *Народныхъ Училищъ*, кои раздѣляются на *главныя* и на *малыя*.

Г.Л. I. — О Главныхъ народныхъ Училищахъ.

1. О классахъ Главныхъ народныхъ Училищъ.

§ 1. Въ каждомъ Губерискомъ городѣ быть одному Главному народному Училищу, состоящему изъ 4-хъ разрядовъ или классовъ, въ коихъ обучать юношество слѣдующимъ учебнымъ предметамъ и наукамъ на языкѣ природномъ, а именно:

§ 2. Въ 1 классѣ обучать чтенію, письму, первоначальнымъ основаніямъ Христіанскаго закона и добронравію. Начиная съ познанія буквъ, обучать складывать, и потомъ читать Букварь, Правила для учащихся, Сокращенный Катихизисъ и Священную Исторію. Обучающихся такимъ образомъ чтенію, заставлять при наступленіи второй половины перваго года писать съ прописей, выговаривать и писать цифры, церковныя и Римскія числа, и при томъ обучать ихъ первоначальнымъ правиламъ Грамматики, содержащимся въ таблицѣ о познаніи буквъ, которая находится въ книгѣ подъ заглавіемъ: *Руководство Учителямъ 1 и 2 класса.*

§ 3. Книги, по которымъ надлежитъ учить юношество вышесказаннымъ сего класса предметамъ, суть слѣдующія, изданныя по Высочайшему повелѣнію Ея Императорскаго Величества: 1. Таблица азбучная, 2. Таблица для складовъ, 3. Россійскій Букварь, 4. Правила для учащихся, 5. Сокращенный Катихизисъ, 6. Священная Исторія, 7. Прописи, и 8. Руководство къ чистописанію.

§ 4. Во 2 классѣ или разрядѣ, наблюдая тѣже предметы Христіанскаго закона и добронравія, начинать читать Пространный Катихизисъ безъ доказательствъ изъ Священнаго Писанія, книгу О должностяхъ человѣка и гражданина, и первую часть Ариѳметики; повторять Священную Исторію, продолжать

Иллюстрация 2. Начало текста «Устава народным училищам»

14 декабря 1797 г. статс-секретарь зачитал императору прошение: «Тайный советник Эпинус, в глубокой старости подвержен будучи многим болезненным припадкам, повергается к стопам монаршим и просит о всемилостивейшем увольнении его от всех дел. Себя и жребий свой предаёт беспредельному милосердию Вашего Величества». На документе карандашная помета «со всем содержимым», несомненно, передающая слова Павла I.

* * *

Эпинуса похоронили 16 августа 1802 года в Тарту, где он провёл последние годы. Могила сохранилась. Ни архива Эпинуса, ни его портрета до сих пор не найдено.

В МОРЕ БЕЗ КАРТЫ

ЗАМЕТКИ БЕЗОПАСНИКА

Александр ИГОНИН
эксперт BIS Journal,
ведущий рубрики

В прошлой заметке мы поговорили о пользователях. А сегодня предлагаю обсудить, пожалуй, самый животрепещущий вопрос в области инвентаризации: реестр хостов. По моим ощущениям, примерно в каждой первой компании полный и подробный реестр хостов сети отсутствует — а это чревато целой массой проблем: от невозможности проконтролировать степень покрытия сети СЗИ до огромных задержек в процессе расследования инцидента, пока выясняется, что же это за хост, кому он принадлежит и с чем его едят. «Бонусом» можно перечислить и многое другое: сложности с аудитами, благодатную почву для образования теневой инфраструктуры, проблемы с планированием закупок лицензий, бессмысленный расход вычислительных мощностей и многое другое.

Уже упоминавшийся нами ГОСТ Р ИСО/МЭК 27001–2021 содержит требование об инвентаризации активов. С практической точки зрения, конечным результатом инвентаризации я бы назвал собственно реестр хостов. Это может быть как обычная «экселька», так и какая-то мудрёная информационная система; главное здесь — содержание, а не форма. Из своего опыта я бы выделил следующие поля, которые неплохо иметь в реестре:

- IP-адрес (или адреса, если их несколько);
- имя хоста;
- владелец системы (с точки зрения бизнеса);
- администратор системы;
- операционная система (если она типовая);
- среда (тестовая/эксплуатационная и т.д.);
- описание (название ИС либо понятное краткое описание, например «пользователи», «межсетевой экран», «точка доступа Wi-Fi» и т.д.);
- комментарий.

При желании можно добавить и иные поля, например «хранимая информация», «степень критичности для бизнеса», различные теги («PCI DSS» или «бухгалтерия»). Но лучше всё-таки начать с базовых полей, а уже затем (возможно, никогда) добавлять новые. Вообще, автор является ярым приверженцем той идеи, что лучше сделать немного, но качественно, чем замахнуться на рубль, а ударить на копейку — как, к сожалению, зачастую и получается на практике.

Давайте быстро пробежимся по наиболее очевидным частям нашего реестра. Во-первых, там, разумеется, должны присутствовать все серверы и рабочие станции. Надо помнить, что не все они работают под управлением Windows, и заметная их часть может отсутствовать в Active Directory, поэтому ограничиваться простым экспортом данных из AD нельзя. Во-вторых, в реестре должно присутствовать сетевое оборудование — как минимум имеющее IP-адрес. В-третьих, не забудем специфические системы и сервисы, такие как IP-телефония, СКУД, гипервизоры, промышленные контроллеры, интернет вещей (IoT) и т.д.

Один из неочевидных моментов — это множественные адреса: если какой-то сервер имеет несколько сетевых интерфейсов (например, для доступа из других сетей), то все они тоже должны фигурировать в реестре. То же самое касается различных NAT-адресов, сконфигурированных на сетевом оборудовании: их тоже стоит внести в реестр, снабдив кратким описанием. И отдельно стоит отметить важность наличия в документе публичных IP-адресов организации, чтобы можно было легко найти, какой сервер/сервис обитает на том или ином IP-сокете, доступном из интернета.

Уделим короткий абзац решениям, которые предлагают «автоматически сгенерировать реестр хостов». Увы, но это так не работает — на выходе в лучшем случае получится просто список IP-адресов и имён без указания владельцев, администраторов и описания. Польза от такой информации есть, но заметно меньшая.

Вот вкратце и всё по теме инвентаризации хостов. К сожалению, организации не спешат выделять ресурсы на создание и поддержание актуальности такого реестра. В результате попытки разобраться в том, что происходит в корпоративной сети, напоминают путешествие в открытом море без карт: вокруг мелькают контуры неизведанных подсетей, рифы внезапных NAT, забытые сервера давно умерших приложений и сервисов... Надежда только на память старого лоцмана из IT-отдела да на обрывки старых списков хостов, составленных неизвестно кем в далёком прошлом. Звучит захватывающе, но на практике такая навигация крайне малоприятна. Лучше уж заранее позаботиться о карте и составить реестр хостов (ну или хотя бы подсетей для начала).

МЕДИА ГРУППА
АВАНГАРД

ПРИСОЕДИНЯЙСЯ К НАМ В 2025 ГОДУ!

Цифровая устойчивость промышленных систем — 2025 (ЦУПС-2025)
27–28 февраля,Москва, Центр событий РБК
Организаторы: Медиа Группа «Авангард», ИнфоТеКС, InfoWatch

Защита данных
7 апреля, Москва, Холидей Инн Сокольники
Организатор: Медиа Группа «Авангард»

Кадровое обеспечение информационной безопасности РФ
16–18 апреля, Москва, конгресс-центр МТУСИ
Организаторы: АНО «НТЦ ЦК», ФУМО по ИБ, Медиа Группа «Авангард», ИнфоТеКС

Технологии доверенного искусственного интеллекта
20 мая, Москва, кластер Ломоносов
Организаторы: АНО «НТЦ ЦК», Академия криптографии РФ, ИСП РАН, Медиа Группа «Авангард»
При поддержке: Минцифры России

Современные тенденции в криптографии (CTCrypt 2025)
3–6 июня, Великий Новгород
Организаторы: Академия криптографии РФ, Математический институт им. В. А. Стеклова РАН, АНО «НТЦ ЦК», ТК26

PKI-Форум Россия 2025
16–18 сентября, Санкт-Петербург
Организатор: Медиа Группа «Авангард»
При поддержке: ФСБ России, Минцифры России

Технологии SOC (Киберзастава SOC Tech 2025)
7 октября, Москва
Организатор: Медиа Группа «Авангард»

Конференция «Сетевая безопасность»
25 ноября, Москва, Холидей Инн Сокольники
Организатор: Медиа Группа «Авангард»

Открытая конференция ИСП РАН
9–10 декабря, Москва
Организатор: ИСП РАН

IB-BANK.RU

КОНСОРЦИУМ ИССЛЕДОВАНИЙ БЕЗОПАСНОСТИ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

20.05.2025
МОСКВА, КЛАСТЕР «ЛОМОНОСОВ»

III ФОРУМ

ТЕХНОЛОГИИ ДОВЕРЕННОГО ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

РЕГИСТРАЦИЯ
ib-bank.ru/trust-ai

ОРГАНИЗАТОРЫ

Национальный технологический центр цифровой криптографии

ИСП РАН
Институт системного программирования им. В.П. Иванникова РАН

Академия криптографии Российской Федерации

АВАНГАРД
Медиа Группа «Авангард»

ПРИ ПОДДЕРЖКЕ

минцифры
Министерство цифрового развития, связи и массовых коммуникаций РФ