softline direct

КАТАЛОГ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

1 (42)
2023 BY

Навстречу технологиям

Указ № 40
«О кибербезопасности».
Что нужно знать?
Стр. 36

SOC. В авангарде борьбы
с киберпреступниками
Стр. 44

PDM-системы. Зачем они нужны
промышленному предприятию
Стр. 48

+375 17 336 55 95

noventiq.by

5 причин выбрать Noventiq Belarus

20+
лет работы на ИТ-рынке Беларуси

25+
партнерских статусов и наград ведущих поставщиков hardware, software и cloud

550+
успешных реализованных проектов

50+
сертифицированных инженеров

6
офисов в каждом областном центре

Уважаемые коллеги, партнеры, друзья!

Представляем вашему вниманию
новый выпуск нашего журнала.

Рады сообщить, что после ребрендинга мы работаем под новым брендом Noventiq Belarus. Мы продолжаем выполнять нашу миссию, помогая организациям трансформироваться и работать эффективно и безопасно в условиях цифровой экономики. А в журнале будем и дальше делиться актуальной и важной информацией об ИТ-сфере, экспертными статьями и успешными кейсами по цифровизации бизнеса.

Сегодня на нашем рынке остается актуальной тема информационной безопасности. В феврале 2023 года в Беларуси вышел Указ № 40 «О кибербезопасности», который существенно меняет правила работы организаций в области информационной безопасности. В журнале мы кратко расскажем, о чем идет речь в данном Указе.

Еще одна актуальная тема, которая непосредственно связана с Указом № 40, — построение центров кибербезопасности, или SOC. В этом выпуске вы прочитаете, что из себя представляют эти структуры, на каких принципах они построены и зачем нужны компаниям.

Мы продолжаем рассказывать о доступных на белорусском рынке вендорах. В этом номере пишем о сетевых решениях, системе для резервного копирования «Кибер Бэкап», а также об экосистеме группы компаний «Астра».

Также вы узнаете про PDM-системы для промышленности, кибериммунные решения от «Лаборатории Касперского», бизнес-решения Directum, тренды информационной безопасности и многое другое.

Надеюсь, что эти и другие материалы будут полезны и помогут в цифровизации ваших компаний. Со своей стороны мы всегда готовы помочь в решении этой задачи. Вместе мы сможем создать действительно работающие ИТ-инструменты для вашего бизнеса.

С пожеланиями успеха и процветания,

Андрей Овсейко,

CEO Noventiq Belarus

Каталог программного обеспечения

Softline Direct

2023-1(42)-BY

Учредитель:
ООО «СофтЛайн Директ»

Главный редактор:
Андрей Андриевский

Дизайн и верстка:
Анастасия Зуркова

Адрес редакции:
220062, г. Минск,
пр-т Победителей, 108,
4 этаж, помещение 10

Распространяется бесплатно

Тираж:
2300 экз.

Подписано в печать
19.06.2023

Отпечатано
в типографии:
ОАО «ТРАНСТЭКС»,
220034, г. Минск,
ул. Чапаева, 5

Лицензия №02330/53
от 14.02.2014 г.
Выдана Министерством информации Республики Беларусь.
УНП 190147176

Заказ №

Зарегистрировано
в Министерстве
информации Республики
Беларусь.

Свидетельство
о регистрации № 2/87
от 19.07.2016

Перепечатка
и цитирование
материалов только
по согласованию
с редакцией журнала.

© Каталог
программного
обеспечения
Softline Direct

Контактная информация:
marketing.by@noventiq.com

СОДЕРЖАНИЕ

Как параллельный импорт повлиял на развитие ИТ-инфраструктуры бизнеса 4

Новости Noventiq Belarus 8

Noventiq Belarus закрывает все вопросы по построению ИТ-инфраструктуры бизнеса 13

Цифровизация

Как с помощью одного ИТ-решения экономить два часа работы сотрудника ежедневно 14

Внедрение решений Directum в ОАО «Белгорхимпром» 18

Инфраструктурные решения

На защите ваших данных. Обзор решения для резервного копирования «Кибер Бэкап» 20

Сетевое оборудование: новые решения, тестирование и реализованный проект 24

Решения ГК «Астра». Безопасность на всех уровнях 28

Безопасность

Кибериммунные решения от «Лаборатории Касперского» 32

Указ № 40 «О кибербезопасности». Что нужно знать? 36

Главные тренды кибербезопасности 38

SOC. В авангарде борьбы с киберпреступниками 44

САПР

PDM-системы. Что это и зачем они нужны промышленному предприятию 48

Обучение

Популярные и новые курсы 52

Расписание учебных курсов 53

Noventiq Belarus
в соцсетях

«Главная цель, которую сегодня преследует цифровизация и внедрение новых решений, — не замена человека, а помощь. Это касается в том числе и системы Directum, которая позволяет избавиться от рутинной работы и переключиться на более важные для бизнеса задачи. С ними может справиться лишь квалифицированный специалист, у которого обычно не хватает времени из-за высокой нагрузки».

Стр. 14

Наши специалисты лично тестируют все оборудование — как на соответствие заявленному производителями функционалу, так и на возможность совместимости с оборудованием других производителей. Также мы проверяем качество сборки изделия. Мы готовы лично проконсультировать вас практически по всем вендорам и рассказать об особенностях, преимуществах и недостатках их оборудования.

Стр. 24

Персональные данные — это ценный ресурс, который можно использовать разными способами: шантажировать организацию, из которой произошла утечка, для получения выкупа, продать информацию в даркнете, использовать данные для целевых атак или фишинговых рассылок. При этом до сих пор не все организации уделяют сохранности этой информации должное внимание.

Стр. 38

PDM-системы, несмотря на внешнюю масштабность, довольно легко осваиваются. И важнейшим препятствием на этом этапе служит внутреннее сопротивление самих сотрудников, которые хотят продолжать работать «по старинке». В свою очередь, руководство должно рассматривать системы класса PDM как необходимый бизнес-инструмент, способствующий повышению конкурентоспособности и дальнейшему развитию предприятия.

Стр. 48

Как параллельный импорт повлиял на развитие ИТ-инфраструктуры бизнеса

3 января 2023 года в Беларуси был принят закон № 241-З «Об ограничении исключительных прав на объекты интеллектуальной собственности». Директор по сервисам Noventiq Belarus **Антон Отчик** рассказал, как данный закон может отразиться на поставках программного и аппаратного обеспечения в нашу страну и стоит ли белорусским компаниям воспользоваться данной возможностью, либо лучше выбрать иные варианты.

Что изменилось с введением закона

После вступления закона в силу компании получили возможность приобретать и использовать критически важные для ИТ-инфраструктуры бизнеса решения. Ранее такие процессы тоже происходили, но находились в «серой зоне», то есть никак не регламентировались законодательно. Теперь эти процессы официально легализованы. Фактически «серый» импорт превратился в «параллельный».

Теперь компании имеют право покупать в других странах объекты интеллектуальной собственности и ввозить их в Беларусь без согласия правообладателей. В том числе речь идет о программном и аппаратном обеспечении.

Насколько сильно параллельный импорт повлиял на белорусский рынок?

Товар, ввезенный по параллельному импорту в Беларусь, имеет ряд особенностей:

- за счет дополнительного этапа купли/продажи, а также расходов на логистику его цена зачастую неконкурентоспособна при наличии на рынке аналогов;
- у такого товара нет гарантии производителя.

Поэтому если говорить о нашей сфере деятельности, компании пользуются возможностью параллельного импорта лишь для приобретения решений, у которых сегодня нет достойных альтернатив на белорусском рынке (по соотношению цена/качество). В то же время, если есть альтернативные решения либо компания может поддерживать в рабочем состоянии свою текущую ИТ-инфраструктуру, этот механизм не актуален.

Если говорить об аппаратных средствах (серверах, сетевом и прочем оборудовании), то эффект параллельного импорта можно заметить. Когда необходимое оборудование не поставляется по официальным каналам, то благодаря этому механизму субъекты хозяйствования находят возможности заказать и получить отдельные аппаратные средства с предустановленным набором лицензий. Это сразу решает несколько вопросов по работе ИТ-инфраструктуры бизнеса.

Что касается программных продуктов, то какого-то значительного эффекта мы не заметили. В этом плане корпоративные клиенты используют параллельный импорт только для решения специфических задач.

Параллельный импорт программного обеспечения

Когда мы говорим про параллельный импорт, то в первую очередь речь идет именно об аппаратном обеспечении, а не программном.

В ряде случаев компании, которые покупали ПО, имеют возможность продлить лицензию. Если говорить о покупке софта в другой стране, то в большинстве случаев это довольно сложная, в том числе в плане законодательства, процедура. К тому же, независимо от того, где и как такое ПО приобретено, если оно используется на территории Беларуси, то с точки зрения разработчика оно будет нелегальным.

Поэтому в долгосрочной перспективе большинство компаний будут рассматривать другие способы — поддерживать текущую ИТ-инфраструктуру в рабочем состоянии и параллельно планировать переход на доступные на рынке продукты там, где это возможно. Исключения составляют только сложные программные решения, которые невозможно получить другим способом и у которых нет альтернатив на белорусском рынке.

Риск параллельного импорта

Риск один, но очень существенный — отсутствие гарантийного обслуживания и технической поддержки от производителя. То есть если произошла поломка в оборудовании, завезенном по параллельному импорту, то единственная надежда бизнеса — это поставщик этого самого оборудования. В связи с этим могу дать два совета, которые позволят минимизировать этот риск.

- **Выбирайте надежного поставщика**

Сегодня параллельным импортом занимается большое количество компаний, в том числе небольших. Они выигрывают тендеры благодаря относительно низким для рынка ценам, привозят оговоренное количество оборудования и запасных частей, и на этом все. Обычно у таких мелких компаний нет квалифицирован-

ных специалистов, которые способны оказать консультационную или тем более техническую помощь клиенту. К тому же никто не даст гарантии, что год спустя данное юридическое лицо еще будет существовать.

Поэтому бизнес, приобретая товары по параллельному импорту, должен тщательно подбирать партнера. Это должна быть компания с собственным штатом квалифицированных специалистов, которые могут в том числе оценить качество покупаемого аппаратного обеспечения. Особенно если речь идет о приобретении оборудования, которое ранее использовалось.

И это касается не только крупных компаний. Скорее наоборот, для мелкого бизнеса выбор поставщика играет более существенную речь, потому что его финансовые возможности ограничены гораздо сильнее. И в случае возникновения проблем все затраты лягут на бюджет организации.

- **Наличие запасных частей и гарантийное обслуживание**

Еще один важный момент при параллельном импорте, который иногда значительно увеличивает финальную стоимость оборудования, — необходимость заказчика вместе с оборудованием приобретать на склад ЗИП. Особенно это касается критической инфраструктуры. Потому что в случае возникновения неисправностей быстро доставить запасные части не получится.

Тему гарантийного обслуживания я уже частично поднимал выше. Мелкие компании, без штата технических специалистов, не смогут помочь вам в обслуживании купленных решений. В лучшем случае они передадут данную работу на аутсорс сторонней организации, в худшем вы вообще останетесь без гарантии.

Еще один момент, на который хотелось бы обратить внимание, — высокие цены. Я бы рекомендовал компаниям тщательно подходить к выбору исполнителя и анализировать рынок. Решение здесь опять же одно — сотрудничать с надежными партнерами, которые не будут зарабатывать по 400–500% маржи с поставок оборудования.

Альтернативы параллельному импорту

Таких альтернатив у бизнеса три — либо продолжать поддерживать текущую ИТ-инфраструктуру в рабочем состоянии максимально долго, либо постепенно переходить на доступные на белорусском рынке решения, либо использовать облачные технологии.

Чтобы осуществлять техническую поддержку аппаратного обеспечения, решений по резервному копированию, виртуализации и другим, в компании должен быть штат квалифицированных специалистов. И речь здесь не об обычных системных администраторах, а именно об инженерах, которые прошли обучение у вендора, имеют опыт внедрения таких решений и работы с ними. Понимая эту потребность бизнеса, осенью 2022 года мы запустили собственную услугу по технической поддержке и уже заключили договоры с несколькими компаниями. Примечательно, что с каждым месяцем запросы на подобную услугу лишь возрастают.

Однако в долгосрочной перспективе и мы, и представители бизнеса понимаем, что вечно поддерживать устаревающие решения, особенно если речь идет об аппаратном обеспечении, не получится. Поэтому компании должны продумывать шаги по переходу на доступные на рынке ИТ-решения.

За последний год мы проделали большой объем работы в этом направлении — налажены контакты с десятками вендоров, уже есть успешные проекты, построенные на новых для рынка решениях. Фактически сегодня мы можем закрыть 95% потребностей бизнеса в этом направлении. На оставшиеся 5% приходятся решения, у которых в мире практически нет альтернатив. Но даже в таких ситуациях можно найти выход. Мы продолжаем работу по поиску новых партнеров, в том числе за счет расширения географии.

Наконец, последний выход — облачные решения. Сегодня эти технологии дают компаниям возможность использовать ИТ-решения в облаке: резервное копирование, виртуализация, информационная безопасность и многое другое. В ближайшее время мы запустим свой дата-центр с набором облачных услуг, которые смогут удовлетворить запросы большинства компаний без обращения к параллельному импорту. ■

Справка о законе

Закон от 03.01.2023 № 241-З «Об ограничении исключительных прав на объекты интеллектуальной собственности»

В Законе заложены следующие условия ввоза товаров по параллельному импорту:

1. Они должны быть включены в перечни товаров (групп товаров), являющихся существенно важными для внутреннего рынка.
2. Ранее товары (их группы) правомерно введены в гражданский оборот на территории любого государства непосредственно правообладателями ОИС, примененных (содержащихся) во ввозимых товарах, или иными лицами с их согласия (разрешения).

Основные положения Закона вступили в силу с 17 января 2023 года. При этом установлено, что нормы, предусматривающие возможность параллельного импорта действуют до 31 декабря 2024 года.

Если вам нужна консультация по технической поддержке инфраструктуры либо по выбору доступных на рынке ИТ-решений, свяжитесь с нами по телефону **+375 17 336 55 95** или электронной почте **belarus@noventiq.com**

Noventiq Belarus приняла участие в VIII IT-Security Conference

28–29 марта в Минске прошла VIII конференция «Технологии защиты информации и информационная безопасность организаций» (IT-Security Conference).

Мероприятие проходит уже в восьмой раз, в этом году участие в нем приняли около 400 руководителей и специалистов департаментов информационной безопасности и ИТ-департаментов.

Noventiq Belarus приняла участие в конференции совместно с партнером, компанией Security Vision. Также участники IT-Security Conference могли получить консультацию по решениям информационной безопасности на нашем стенде.

— IT-Security Conference — это площадка для общения и обмена опытом. Мы как поставщик и интегратор решений по информационной безопасности понимаем, чего не хватает бизнесу. А белорусские компании, в свою очередь, получают информацию из первых рук о новых потенциальных киберугрозах и способах противодействия им, — отметил руководитель отдела информационной безопасности Noventiq Belarus **Александр Дубина**.

Павел Любомский, который представлял на конференции компанию Security Vision с докладом «Реагирование на инциденты: автоматизация и оркестрация», рассказал о необходимости оптимизации человеческих ресурсов в сфере информационной безопасности:

— В текущих реалиях важно заниматься оптимизацией трудовых ресурсов, которые компании тратят на информационную безопасность. Высококлассных специалистов в этой области на рынке труда всегда был дефицит, поэтому важно, чтобы они занимались профильной работой — то есть созданием и внедрением новых систем защиты информации, расследованием инцидентов. Поэтому важно, чтобы в крупных компаниях были решения по автоматизации и оркестрации процессов ИБ, которые возьмут на себя все рутинные задачи по информационной безопасности. Так, наша платформа Security Vision способна роботизировать порядка 95% рутинного программно-технического функционала специалистов информационной безопасности.

Основные темы этой IT-Security Conference касались современных угроз кибербезопасности бизнеса и способов противостояния им в текущих условиях.

— Сегодня хакеры и преступные группировки буквально ежедневно проверяют информационные системы компаний на прочность. Регулярно появляется информация об очередной утечке данных или взломе. И в таких реалиях компании должны по-новому подходить к вопросу защищенности информационных систем, применяя не только технические, но и научные методы противостояния угрозам, — поделился с нами **Роман Мылицын**, руководитель отдела перспективных исследований российской группы компаний «Астра».

Роман выступил с докладом «Безопасность информационных систем в новых реалиях: угрозы и меры защиты». В нем он в том числе рассказал об операционной системе Astra Linux, которая позволяет обеспечить высокую защищенность и стабильность работы бизнес-процессов и ключевых сервисов организаций в текущих условиях.

— Сегодня операционная система Astra Linux благодаря встроенным средствам защиты информации собственной разработки не имеет аналогов ни в России, ни в Беларуси. Она единственная из российских ОС успешно прошла сертификацию ОАЦ и полностью удовлетворяет установленным нормативными документами требованиям безопасности. Система обеспечивает безопасность ИТ-инфраструктур любого масштаба и значительно упрощает эксплуатацию всех информационных систем корпоративной сети, а благодаря высокому уровню автоматизации позволяет направить усилия специалистов по информационной безопасности на другие задачи, — рассказал Роман Мылицын.

Также важное место в конференции заняло обсуждение изменений в законодательстве Беларуси, в частности Указа № 40 «О кибербезопасности».

— Белорусское законодательство направлено на создание новых эффективных инструментов для обеспечения высокого уровня безопасности критической инфраструктуры страны. Как раз на это нацелен Указ № 40, который регламентирует создание в белорусских компаниях Security Operations Center (SOC). Мы заранее готовились к выходу данного указа и уже готовы оказать помощь белорусским компаниям для выполнения его требований, — рассказал Александр Дубина.

Также на конференции наша компания получила диплом «За вклад в развитие технологий информационной безопасности в Беларуси и участие в IT-Security». ■

День технологий для Белорусской железной дороги

21 декабря специалисты Noventiq Belarus и «Лаборатории Касперского» провели в Могилеве День технологий для руководителей и ИТ-специалистов Белорусской железной дороги (БЖД).

В рамках мероприятия представители БЖД рассказали, с какими вопросами в сфере развития ИТ-инфраструктуры они столкнулись за последний год, в каких технических решениях нуждаются, а также поделились планами по цифровизации организации на ближайшее время.

Специалисты Noventiq Belarus рассказали о технической поддержке — новой услуге, которую компания запустила в этом году. Сегодня у нас имеется квалифицированный персонал, который может закрывать большинство вопросов поддержки работоспособности ИТ-инфраструктуры бизнеса, своевременного обновления компонентов и помощи при стрессовых нагрузках.

Также представители Noventiq Belarus рассказали о доступном на белорусском рынке программном и аппаратном обеспечении. Подробно были рассмотрены сетевые решения, средства виртуализации, системы хранения данных, операционные системы и иные решения.

Отдельные доклады были посвящены централизации доменной инфраструктуры Active Directory и инфраструктуре современного дата-центра, а также практическому опыту Noventiq Belarus в этих вопросах.

Представители «Лаборатории Касперского» рассказали участникам Дня технологий об общих принципах построения информационной безопасности и передовых решениях в этой сфере.

День технологий дал представителям Белорусской железной дороги отличную возможность рассказать о своих основных потребностях в плане цифровизации и модернизации ИТ-инфраструктуры. А специалисты Noventiq Belarus и «Лаборатории Касперского» смогли поделиться своими компетенциями, а также рассказали о решениях, которые сегодня доступны на рынке. ■

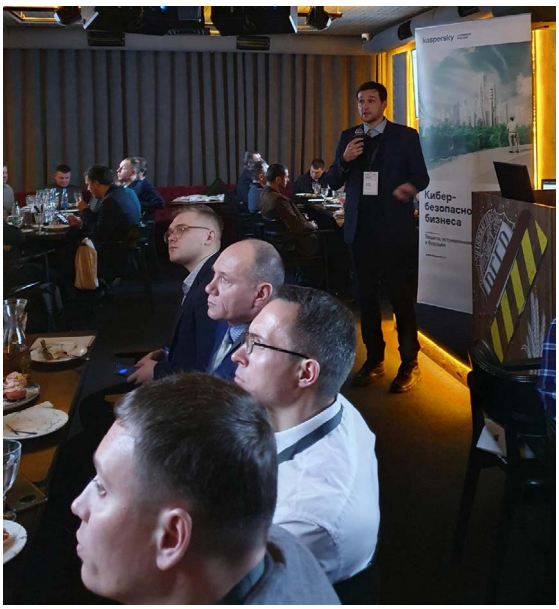
Вебинары от Noventiq Belarus

За последние 5 месяцев у нас прошли следующие вебинары:

- Инновационный подход к безопасности и удобству цифровых каналов обслуживания (решения SafeTech и Nopaper).
- Сетевые решения: обзор 2023.
- «Ныряем в контейнеризацию» и что нужно знать отделу безопасности.
- Платформа корпоративных коммуникаций и совместной работы. Миграция, практический опыт и планы развития (о решениях Communigate Pro).
- Инновационное решение для резервного копирования и аварийного восстановления (по решениям компании Vinchin).

Если вам интересны данные темы и вы хотите ознакомиться с записью встреч, пишите нам с указанием названия вебинара на почту marketing.by@noventiq.com. ■

Семинар «Системная безопасность промышленных предприятий»



16 февраля Noventiq Belarus совместно с «Лабораторией Касперского» провели обучающее мероприятие «Системная безопасность промышленных предприятий».

Устойчивое развитие промышленных предприятий и объектов критической инфраструктуры зависит от стабильности производственных и бизнес-процессов, надежной защиты важных активов и безопасности операционной (ОТ) и IT-инфраструктуры. Именно решение этих задач и стало основной темой прошедшей встречи.

На семинаре подробно обсудили вопросы кибербезопасности промышленных предприятий, обеспечение защиты АСУ ТП, были рассмотрены потенциальные угрозы и рекомендации по повышению уровня защищенности инфраструктуры.

Также было презентовано решение для защиты интернета вещей на уровне кибериммунных шлюзов для эффективной и безопасной трансформации АСУ ТП.

В конце мероприятия участники смогли задать интересующие их вопросы спикерам. ■

Семинар по решениям «Лаборатории Касперского»

27 апреля Noventiq Belarus совместно с «Лабораторией Касперского» провели семинар «Искусство комплексной безопасности». В мероприятии приняли участие практически полсотни представителей белорусского бизнеса и организаций — руководители ИТ-департаментов и специалисты по информационной безопасности.

Спикеры рассказали о последних тенденциях в обеспечении информационной безопасности компаний, а также о технологиях для системного подхода к защите бизнеса. Во время мероприятия представители вендора подробно остановились на решениях Kaspersky Thin Client, Kaspersky SD-WAN, Kaspersky Symphony.

Kaspersky Thin Client — это кибериммунная операционная система для тонких клиентов на базе KasperskyOS. Это решение позволяет бизнесу обеспечить максимальную защищенность рабочих станций при удаленном подключении сотрудников. Оно абсолютно новое для белорусского рынка, поэтому было важно ознакомить заказчиков с возможностями Kaspersky Thin Client.

Kaspersky SD-WAN — еще одно новое решение в линейке продуктов «Лаборатории Касперского». Оно актуально для организаций, которые обладают обширной филиальной сетью или планируют переместить часть ресурсов в облако.

SD-WAN — первый шаг на пути к архитектуре SASE. Она предполагает предоставление безопасного доступа к приложениям и корпоративным ресурсам безотносительно технологий подключения, географии, времени и устройств конечного пользователя. SASE подразумевает отказ от отдельных устройств безопасности и переход к единой концепции обеспечения сетевой безопасности в частных или публичных облаках.

Kaspersky Symphony — единая экосистема по информационной безопасности, в которую входят решения класса Security, EDR, MDR, XDR. Они обеспечивают передовую защиту рабочих мест, серверов, виртуальных машин, сетевого и почтового трафика, а также повышают осведомленность сотрудников. Все элементы платформы взаимосвязаны между собой, дополняют друг друга и входят в одну лицензию.

В ходе мероприятия участники активно обсуждали возможности новых решений с экспертами, а также анализировали перспективы развития сферы ИБ в Беларуси. ■

Специалисты Noventiq Belarus рассказали руководителям могилевских предприятий о цифровизации производства

23 марта представители Noventiq Belarus в режиме онлайн приняли участие в семинаре «Информационные технологии в системе управления современным предприятием», который был организован Могилевским агентством регионального развития. В мероприятии приняли участие руководители промышленных предприятий региона.

Руководитель направления САПР Олег Елистратов выступил с докладом «Автоматизация промышленных производств. Опыт на реальных кейсах». Он подробно рассказал о понятии «Индустрия 4.0», как промышленным предприятиям выйти на данный уровень. В рамках презентации спикер не только подробно описал возможности наших экспертов, но и привел в пример реальные кейсы, которые были реализованы на крупных белорусских предприятиях.

Дополнительно Олег Елистратов рассказал в целом про возможности Noventiq Belarus и подробнее остановился на вопросах информационной безопасности.

Также от нашей компании с докладом «Инвентарь руководителя: система управления процессами и документами Directum» выступила Ольга Шавлюк, pre-sale менеджер направления Directum Rx. Она рассказала, как с помощью инструментов системы Directum руководитель предприятия может закрыть большую часть вопросов по выстраиванию работы в компании — от документооборота до контроля за выполнением поручений и проведения совещаний. ■

Семинар о среде виртуализации zVirt

В конце прошлого года состоялся семинар «Российская среда виртуализации zVirt», на котором представители вендора «Орион софт» провели обзор платформы zVirt для запуска виртуализованных приложений, рассказали об архитектуре zVirt и рассмотрели основные возможности продукта.

Защищенная среда виртуализации zVirt обеспечивает управление серверами виртуализации, виртуальными машинами, хранилищами, кластерами и другими объектами среды виртуализации из единой консоли с русскоязычным интерфейсом.

В конце теоретической части участники и организаторы мероприятия смогли пообщаться друг с другом в неформальной обстановке, обсудить основные тенденции развития ИТ-отрасли и решение существующих проблем. ■

Серия мероприятий «Как решать ИТ-задачи в 2023 году?»

В первом полугодии 2023 года эксперты Noventiq Belarus провели семинары в Витебске и Гродно, а также вебинар под общей темой «Как решать ИТ-задачи в 2023 году?». Всего в них приняло участие около двухсот человек.

На этих мероприятиях сотрудники Noventiq Belarus рассказали о последних изменениях на рынке ИТ в Беларуси, сделали обзор доступных решений, поделились опытом — на что стоит обратить внимание при проведении цифровой модернизации.

Подобные мероприятия дают возможность белорусским организациям ознакомиться с доступными решениями и разработать план по модернизации своей ИТ-инфраструктуры. ■

Приняли участие в форуме Student's Digital Days

Student's Digital Days — это двухдневный научно-практический форум, который проводит кафедра маркетинга Института бизнеса БГУ. В этом году в нем приняли участие около 200 участников — студенты и магистранты из Беларуси и других государств. Они смогли из первых рук получить информацию от специалистов об использовании инструментов digital-маркетинга в управлении компанией.

HRD Noventiq Belarus Катарина Сильченко выступила с докладом «Сила мозга компетенций», в рамках которого рассказала о составляющих корпоративной культуры, жизненном цикле сотрудника в компании, необходимых компетенциях и как их прокачать. Также слушатели узнали, как определиться с выбором будущей работы и на что делать ставку в саморазвитии.

— Самое важное для студентов-маркетологов — понять, в какой сфере они хотят работать и какие продукты продвигать. Ведь зачастую из-за неудачного выбора первого места работы люди покидают профессию, — отметила Катарина Сильченко. — Поэтому финальная часть моего выступления была посвящена вопросу самоопределения, в том числе карьерного — на что стоит обратить внимание и какие вопросы задать самому себе, чтобы понять, чем ты действительно хочешь заниматься.

Также в рамках форума выступили представители Яндекса, Сбербанка, Relouis, GUSAROV и других компаний. ■

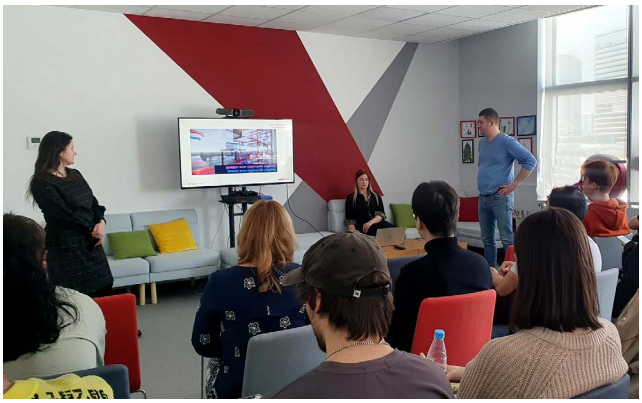
День открытых дверей в Noventiq Belarus

13 марта в рамках Дня открытых дверей офис компании Noventiq Belarus в Минске посетили студенты Института бизнеса БГУ.

В рамках визита студенты познакомились с карьерными возможностями и основными направлениями деятельности нашей компании — от совершенствования отдельных бизнес-процессов в компании до комплексных проектов по модернизации или созданию всей ИТ-инфраструктуры.

Сотрудники Noventiq Belarus рассказали о современных технологиях проектирования и их применении в реальной жизни, ИТ-системах по автоматизации бизнес-процессов в бизнесе, реализованных нашей компанией проектах.

Для студентов была проведена комплексная экскурсия по офису компании, они кратко познакомились с работой каждого отдела и его техническим оснащением. ■



Система виртуализации zVirt получила сертификат соответствия

В ходе испытаний, проведенных Научно-исследовательским институтом технической защиты информации, система виртуализации zVirt от компании Orion soft получила сертификат Технического регламента Республики Беларусь.

Сегодня zVirt занимает существенную долю рынка реестровой виртуализации в России. Платформой пользуется свыше 170 крупных российских компаний из нефтегазовой отрасли, атомной промышленности, финансовой сферы, госсектора — федеральных ведомств, госкомпаний и многих других. В совокупности ПО Orion soft установлено более чем на 3500 серверах виртуализации.

Система виртуализации zVirt подтвердила соответствие требованиям СТБ 34.101.1-2014, СТБ 34.101.2-2014, СТБ 34.101.3-2014. Получение сертификата Технического регламента Республики Беларусь ТР BY/112 02.02 ТР 027 036. 01 00773 гарантирует безопасность использования продукта в составе систем защиты информации:

- государственных информационных систем;
- критически важных объектов информатизации;
- информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено;
- информационных систем персональных данных, за исключением информационных систем класса 1 согласно СТБ 34.101.30-2017.

«Поскольку наличие сертификата соответствия является одним из ключевых требований подавляющего большинства заказчиков, процесс прохождения сертификации был нашей основной задачей сразу после запуска работы на территории Республики Беларусь. Я уверен, что наличие сертификата позволит как государственным органам, так и коммерческим компаниям перейти на безопасное и надежное решение по виртуализации, которым и является наш продукт zVirt», — подчеркнул директор по развитию бизнеса Orion soft **Максим Березин**.

Специалисты Noventiq Belarus готовы помочь белорусским заказчикам с внедрением системы виртуализации zVirt.

«zVirt — одна из самых перспективных систем виртуализации, которая сегодня представлена на белорусском рынке. Наши специалисты протестировали и по достоинству оценили ее функциональные возможности. Получение сертификата соответствия — дополнительное преимущество, которое гарантирует высокую надежность и безопасность zVirt. И сегодня специалисты Noventiq Belarus по запросу клиента могут провести презентацию решения, запустить пилот, а также внедрить данное решение», — отметил **Игорь Волокитин**, ведущий специалист по продажам Noventiq Belarus.

Также Orion soft подписала эксклюзивное дистрибьюторское соглашение с партнером Noventiq Belarus — компанией TenIT.

«Наша стратегическая задача — предоставлять белорусскому рынку инновационные технологии, которые будут способствовать дальнейшему безопасному развитию бизнеса клиентов, улучшению их инфраструктуры и автоматизации. Решение zVirt от Orion soft отвечает самым высоким требованиям заказчиков, и мы видим большую заинтересованность с их стороны в защищенных системах виртуализации, поэтому ожидаем хорошие перспективы технологического сотрудничества с российским разработчиком ПО», — прокомментировал **Алексей Новик**, директор компании TenIT.

О решении

zVirt — российская система безопасного управления средой виртуализации. Решение позволяет при помощи единой консоли управлять серверами виртуализации, виртуальными машинами, хранилищами, кластерами и другими объектами среды виртуализации. Платформа поддерживает онлайн-миграцию и балансировку виртуальных машин между хостами. zVirt работает как с классическими, так и с программно-определяемыми СХД, с сетями с использованием встроенных функций и интеграцией со сторонними Secure Digital (SD) решениями.

О компании Orion soft

Orion soft — российская ИТ-компания, разработчик программного обеспечения. Компания обеспечивает полный спектр услуг по поддержке работы с решением zVirt, а также предоставляет ряд сервисных услуг: аудит существующей платформы виртуализации; проектирование целевой платформы с учетом технологического стека и бизнес-задач; сайзинг платформы виртуализации на базе zVirt; разработка методики миграции и перевод информационных систем на новую платформу; обучение для ИТ-специалистов. ■

Следите за нами в соцсетях!

В наших группах в социальных сетях мы делимся современными тенденциями ИТ, анонсами наших мероприятий, последними новостями о законодательстве в сфере ИТ, а также интервью наших экспертов по разным направлениям.

Найти эту информацию вы сможете найти в Telegram-канале и группе Facebook. ■

Noventiq Belarus в Telegram

Noventiq Belarus в LinkedIN

Noventiq Belarus

решает все вопросы по построению ИТ-инфраструктуры бизнеса

Наша компания — ведущий глобальный поставщик решений и сервисов в области цифровой трансформации и информационной безопасности. Мы постоянно расширяем свои профессиональные компетенции и портфель решений для наших клиентов. Это дает бизнесу возможность выбора оптимального пути развития информационной инфраструктуры и проведения цифровой трансформации компании.

Если вам необходима помощь с выбором конкретного решения — можете обращаться к специалистам нашей компании.

Информационная безопасность	kaspersky, UserGate, Security Vision, КОМПАНИЯ ИНДИД, CTRLHACK
Операционные системы	ASTRA LINUX®, base alt, РЕДОС
Виртуализация	БРЕСТ РЕДСОФТ, base alt, ROS ПЛАТФОРМА, zVIRT
Системы управления базами данных	PostgresPro, РЕД БАЗА ДАННЫХ
Резервное копирование	КИБЕР ПРОТЕКТ, vinchin
Коммуникационное ПО	CommuniGate Pro UNIFIED COMMUNICATIONS PLATFORM, IVA TECHNOLOGIES, TrueConf, Vinteo VIDEO COMMUNICATION CORE
Сетевые решения	ELTEX SOLUTIONS, QTECH THE WORLD CLOSER, MAIPU MAKE IT INTELLIGENT, Ruijie, NSGate
САПР	АСКОН, ZWCAD, КБ ПАНОРАМА
Офисные приложения	Р7-ОФИС, МойОфис

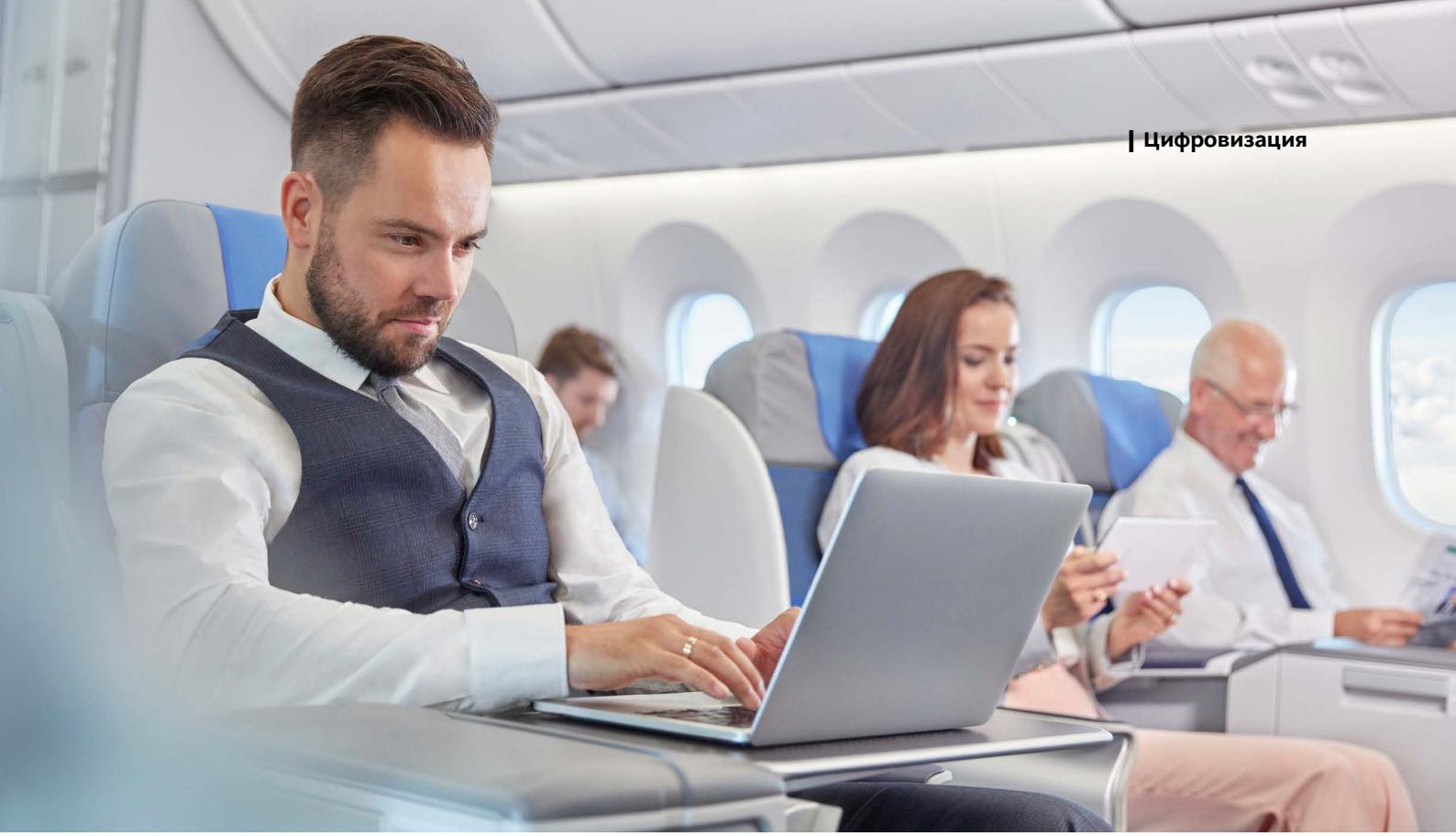
Как с помощью одного ИТ-решения экономить два часа работы сотрудника ежедневно

Из-за неопределенности на рынке белорусские компании и организации сегодня перешли на работу в режиме строгой экономии. Это касается даже традиционно успешных сфер бизнеса. В такой ситуации многие свернули программы по цифровизации и развитию, предпочитая тратить средства либо на создание «подушки безопасности», либо на развитие направлений, которые помогут увеличить прибыльность в короткой перспективе.

Чтобы выяснить, насколько белорусские компании готовы к цифровизации и как правильно рассчитать финансовые преимущества от этих изменений, мы обратились к руководителю направления Directum в компании Noventiq Belarus **Егору Ланкевичу**.

— Егор, насколько бизнес готов к внедрению новых решений в текущих условиях?

— Сегодня белорусские организации жестко подходят к формированию бюджетов. И мы как компания, которая занимается цифровизацией, понимаем это и улучшаем возможности взаимодействия. Так, совместно с Directum мы разработали акционную программу, благодаря которой белорусские клиенты могут получить скидку 25%.



Однако главная проблема не в этом. Я общаюсь с руководителями разных уровней, и, независимо от формы собственности, размахов или успешности бизнеса, большинство топ-менеджеров в начале разговора задают один и тот же вопрос: «Сколько это будет стоить?», хотя должны спрашивать другое: «Сколько денег мне это принесет?» То есть человек думает о затратах в текущий момент. Сиюминутная польза стоит на первом месте. Получается ситуация, когда лучше сэкономить рубль сегодня, чем получить сто рублей через год. В длительной перспективе такая политика ведет к постепенному увяданию бизнеса.

Так происходит независимо от состояния экономики или внешних обстоятельств. Есть компании, которые готовы меняться, а есть те, кто боится этого.

— Компании, которые готовы к изменениям уже сегодня, принадлежат к какой-то определенной сфере или у них просто все хорошо с финансами?

— По моим наблюдениям, на 90% все зависит от руководителя. Простой пример: у нас в проработке был клиент с хорошими финансовыми возможностями, который хотел перевести свой бизнес на нашу платформу. Мы начали переговоры, но вскоре они без причины сошли на нет. А потом я узнаю, что в компании работает большой штат специалистов, поддерживающих морально устаревшую систему, которую мы хотели заменить. И именно эти специалисты переубедили руководителя. Мол, и так все хорошо работает, зачем зря тратить деньги.

С другой стороны, у нас есть клиенты из разных отраслей, чье руководство смотрит на перспективу. Они и деньги могут найти, и изменений не боятся.

Приведу в пример компанию «Белгорхимпром», в которой мы пять месяцев назад внедрили решение Directum. Сегодня 85% договоров и документов там проводится в электронном виде, как итог — время согласования сократилось в 1,7 раза. При переводе в цифру сразу обнаружились процессы, которые можно улучшить, и сотрудники, которые большую часть времени заняты непонятно чем.

Также в «Белгорхимпроме» был проведен эксперимент. Одному и тому же сотруднику дали одинаковую задачу. В первый день он решал ее классическими методами, которые до этого были приняты в компании. Во второй раз задачу такого же типа он закрывал с подключением инструментов Directum. Оказалось, что с помощью нашего решения сотрудник сэкономил 2,5 часа своего рабочего времени.

Об эффективности внедренного ПО говорит и тот факт, что сейчас мы ведем с «Белгорхимпромом» переговоры по расширению функциональных возможностей решений Directum.

— В описанном кейсе речь идет об экономии времени. А как компания может просчитать финансовую результативность внедрения?

— «После установки Directum вы за год сможете сэкономить один миллион долларов», — хотелось бы мне так сказать. Но, как и с любым решением по цифровизации, к расчетам финансовой выгоды стоит подходить индивидуально.

Возьмем приведенный выше кейс и сотрудника, который ежедневно экономит 2,5 часа рабочего времени, то есть 50 часов в месяц при четырех рабочих неделях. Для удобства предположим, что сотрудник зарабатывает 1600 рублей и работает 160 часов. Получается, что ежемесячно только благодаря ему компания сможет сэкономить 500 рублей. Если у вас 10 таких сотрудников, то ежемесячная экономия составит уже 5000 рублей или 60 000 в год. А ведь мы говорим об одной конкретной задаче и одном сотруднике, в то время как Directum — это целая экосистема продуктов.

При этом все грамотные руководители понимают, что оптимизация процессов — это не только про экономию, но и про вклад в будущее бизнеса. Улучшая процессы, давая сотрудникам более удобные инструменты, мы в итоге получаем возможность больше зарабатывать.

— Вы говорили, что в 90% случаев внедрение новых решений в бизнесе зависит от руководителя. А что получает топ-менеджер от цифровой трансформации?

— Прозрачность бизнес-процессов и за счет этого возможность их контролировать. Казалось бы, это простые вещи. Но чем крупнее компания, тем больше темных пятен для руководителя. Поэтому он нуждается в инструменте, который дает возможность отслеживать эффективность работы своих департаментов, видеть проблемные места.

Еще один пример из нашей практики. Мы пришли в организацию и договорились о внедрении нашей системы за 60 дней. При заключении договора генеральный директор говорил, что у них «все в порядке, все налажено и работает как часы». Но уже на первом этапе наши специалисты утонули в хаосе, который там царил. Складывалось ощущение, что за документооборотом и соблюдением внутренних политик в компании вообще никогда не следили. Поэтому перед тем, как начать процесс цифровизации бизнес-процессов, нам пришлось наводить в них порядок, заново выстраивать связи, цепочки согласования. Как итог, сроки реализации увеличились в два раза. Уже потом, когда мы рассказывали руководителю, что творится у него в компании, он хватался за голову. Ведь до этого он думал, что «все четко».

Новые решения позволяют топ-менеджеру получить полное представление о текущих процессах и оперативно реагировать на возникающие проблемы. Это ведет к снижению затрат бизнеса и повышению его эффективности. А в текущей ситуации неопределенности на рынке крайне важно принимать быстрые, но в то же время обдуманные решения, которые имеют под собой аналитические данные.

— Новые технологии таят в себе еще одну угрозу — они могут лишить людей работы. А сегодня с развитием нейросетей эти страхи в обществе лишь усилились.

— Всегда при внедрении изменений сотрудники боятся лишиться работы. Так было при появлении первых калькуляторов, потом компьютеров, роботов на производстве. Однако с начала промышленной революции прошло более 100 лет, а с появления первого компьютера — 40 лет. Но сегодня при наличии нужных навыков любой человек по-прежнему может найти работу. А значит, дело здесь не в новых технологиях, а в нашем нежелании учиться чему-то и стремлении оставить все, как есть.

Главная цель, которую сегодня преследует цифровизация и внедрение новых решений, — не замена человека, а помощь. Это касается в том числе и системы Directum, которая позволяет избавиться от рутинной работы и переключиться на более важные для бизнеса задачи. С ними может справиться лишь квалифицированный специалист, у которого обычно не хватает времени из-за высокой нагрузки.

Например, строгая регламентация всех процессов, которая заложена в нашей системе, значительно упрощает жизнь сотрудников. Предположим, у каждого руководителя есть точно заданное время на согласование документов. То есть если я отправил на согласование договор, то я четко знаю, что в течение суток получу его либо согласованным, либо с правками. Больше не нужно будет 3–4 раза печатать одинаковые документы, ходить по кабинетам, класть бумаги в папки и ждать непонятно сколько.

И еще один неочевидный плюс, который мы заметили от использования нашего решения: в компании улучшается коммуникация между всеми отделами. Потому что когда все работают по одинаковым правилам и отслеживанием этого занимается электронная система, уменьшается количество взаимных претензий и обид.

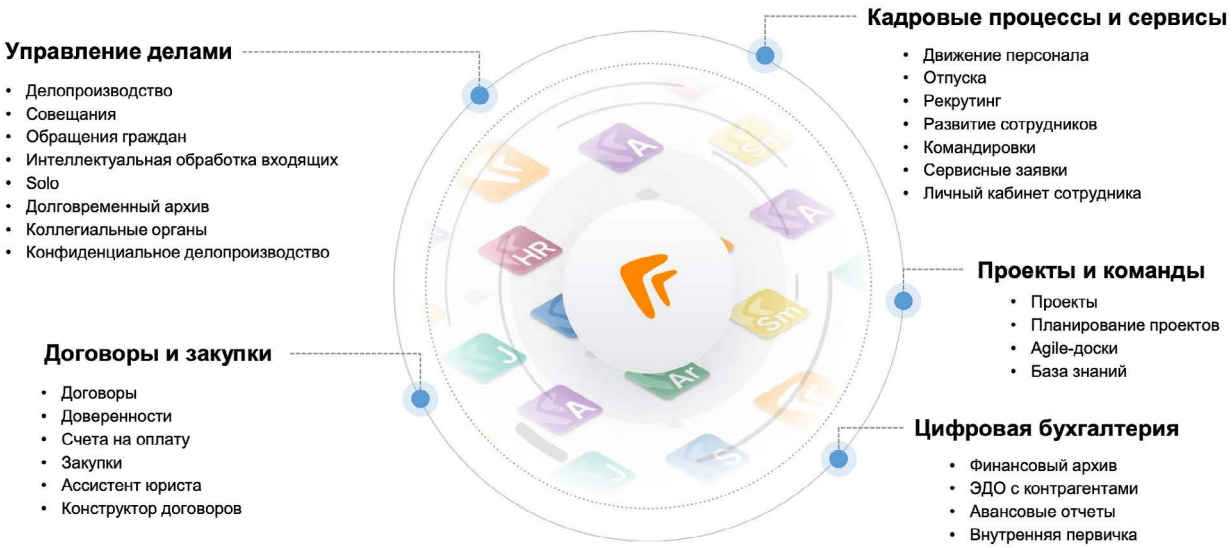
— С какими рисками сталкивается организация, которая внедряет изменения, и как вы с ними справляетесь?

— Три основных риска: несоответствие решения требованиям бизнеса, недостаточная поддержка со стороны разработчиков, недовольство сотрудников. В первом случае вы зря потратите деньги на неработающий инструмент, во втором — рискуете остаться без системы в случае технического сбоя. При недовольстве сотрудников купленное решение просто не будет применяться.

Если говорить про первый риск, то еще на этапе заключения договора мы проводим аудит бизнес-процессов клиента, изучаем выстроенные в компании коммуникации и в зависимости от этого предлагаем только те модули, которые будут у него работать. При необходимости можем запустить пилотный проект для нескольких пользователей, чтобы они смогли убедиться в эффективности системы.

Про недостаточную поддержку со стороны разработчиков решения: у нас налажены очень хорошие отношения с вендором, кроме того, в штате есть разработчики, которые могут устранить многие технические проблемы, а также при необходимости доработать внедренные улучшения под запросы клиента.

Что касается недовольства сотрудников, в любом случае требуется время, от одного месяца до полугода, чтобы они оценили преимущества новых решений. Мы стараемся упростить этот процесс. Так, у нас имеется система со встроенной инфографикой, благодаря которой сотрудники могут самостоятельно отслеживать свою эффективность. Это добавляет в процесс освоения элемент геймификации. ■



Если вам необходима консультация по внедрению решений Directum в компании либо вы хотите дополнительно узнать об акции, обращайтесь к специалистам Noventiq Belarus по телефону **+375 17 336 55 95** или электронной почте **belarus@noventiq.com**

Внедрение решений Directum в ОАО «Белгорхимпром»

О проекте

Заказчик: ОАО «Белгорхимпром»

Отрасль: добывающая промышленность

Численность сотрудников: более 800 человек

Задача: создание единой экосистемы электронного документооборота и интеграция с системой СМДО

Решение: поставка и внедрение решений Directum

Сроки внедрения проекта: 60 дней

О клиенте

«Белгорхимпром» работает с 1961 года. Сегодня это экспертный центр Беларуси по вопросам добычи и переработки калийных руд и другого минерального сырья, генеральный проектировщик ведущих предприятий горной и химической промышленности.

Организация занимается научными исследованиями и проектными разработками: от геологоразведки месторождения до технологии производства готовой продукции, технического сопровождения деятельности предприятия, осуществляет комплексное научное и проектное сопровождение действующих калийных производств.

Задача

Главная задача, которая стояла перед командой Noventiq Belarus, — создание собственной экосистемы электронного документооборота. При этом следовало интегрировать внедренные решения с Системой межведомственного электронного документооборота государственных органов Республики Беларусь (СМДО).

Решение

Для решения поставленных задач клиенту было предложено внедрить у себя систему Directum со следующими модулями:

- делопроизводство;
- договоры;
- обращения граждан;
- совещания.

Делопроизводство — модуль системы Directum, позволил в значительной степени автоматизировать работу с входящими, исходящими и внутренними документами. Входящие сообщения по электронной почте регистрируются в системе, бумажная корреспонденция попадает в нее после сканирования.

Эффект от внедрения модуля:

- время регистрации документов сократилось на 30%;
- повышена исполнительская дисциплина;
- сократилось время выполнения поручений.

Модуль Договоры позволил организовать договорную работу по внутренним правилам «Белгорхимпрома»: от генерации документов по шаблонам до согласования по настроенным маршрутам. Теперь проекты исходящих договоров и дополнительных соглашений создаются в системе Directum RX. Если документ поступил от контрагента, то он заносится в систему из файла или со сканера.

Эффект от внедрения модуля:

- договоры готовятся быстрее в три раза;
- ускорилось время согласования;
- появилась возможность быстрого поиска существующих договоров.

Обращения граждан — модуль для выстраивания комплексной работы с обращениями граждан без нарушения законодательства. Все обращения вносятся в систему, их удобно отслеживать и следить за соблюдением сроков.

Эффект от внедрения модуля:

- возможность автоматически сформировать отчетность по обращениям граждан;
- удобный способ отслеживать и отвечать на обращения граждан;
- сокращен риск нарушения законодательства.

Модуль Совещания — удобный инструмент для организации деловых встреч и заседаний: формирования повестки и ведения протоколов совещаний. Через данный модуль можно организовывать автоматическую рассылку поручений по принятым решениям и отслеживать их исполнение ответственными.

Эффект от внедрения модуля:

- повысилась эффективность совещаний;
- значительно ускорилось составление и согласование протокола совещания;
- усилился контроль за исполнением поручений.

Электронная цифровая подпись и интеграция с СМДО

В начале 2022 года была введена в эксплуатацию модернизированная Общегосударственная автоматизированная информационная система. В связи с этим был утвержден новый формат обмена данными между абонентами Системы межведомственного электронного документооборота (СМДО) государственных органов.

При внедрении электронного документооборота он был интегрирован с СМДО нового формата АИС МВ. Благодаря гибкости системы Directum и наличию в штате собственных разработчиков это удалось сделать в сжатые сроки.

Также в коробочную версию системы была интегрирована электронная цифровая подпись по стандартам Республики Беларусь.

Результат

Внедрение решений Directum в ОАО «Белгорхимпром» создало в организации экосистему электронного документооборота, которая состоит из четырех модулей — Делопроизводство, Договоры, Совещания, Обращения граждан. Реализована возможность более 100 одновременных подключений к системе.

«Отдельно хотелось бы отметить интеграцию решений Directum с Системой межведомственного электронного документооборота государственных органов Республики Беларусь (СМДО). Таким образом был удобно организован процесс обмена электронными документами с контрагентами посредством СМДО, включая отслеживание документа на каждом этапе пересылки», — отметил заместитель главного инженера — начальник отдела автоматизации бизнес-процессов ОАО «Белгорхимпром» В. П. Поручник.

В данный момент специалисты Noventiq Belarus продолжают сотрудничество с ОАО «Белгорхимпром» по расширению функционала систем Directum RX. ■

На защите ваших данных. Обзор решения для резервного копирования «Кибер Бэкап»

Резервное копирование данных — один из главных способов защиты бизнеса от вымогателей и киберугроз, которые уничтожают данные. Любой бизнес, который сегодня работает с большими объемами данных, должен озаботиться тем, чтобы они были не только надежно защищены, но и сохранены в разных источниках.

Еще одна проблема, с которой столкнулись белорусские компании в последний год, — это отсутствие на рынке привычных поставщиков решений данного класса. Сейчас есть возможность продлевать лицензии по действующим контрактам, но если речь идет о создании новой ИТ-инфраструктуры, приходится присматриваться к иным решениям.

Мы расскажем вам об одном из таких решений, которые сегодня активно внедряются белорусскими компаниями, — «Кибер Бэкап» от компании «Киберпротект».

Каким должно быть идеальное резервное копирование

Запросы бизнеса и организаций к решениям по резервному копированию стандартные: резервное копирование должно происходить стабильно и в четко запланированные сроки в автоматическом режиме, а в случае возникновения инцидента компания может в максимально сжатые сроки восстановить все данные и продолжить работу в прежнем режиме.

Основные проблемы, которые могут возникнуть при реализации этой задачи:

- слабая пропускная способность;
- некачественная настройка бэкапа;
- несовместимость (или плохая совместимость) решений разных вендоров.

Ключевые возможности решения «Кибер Бэкап»

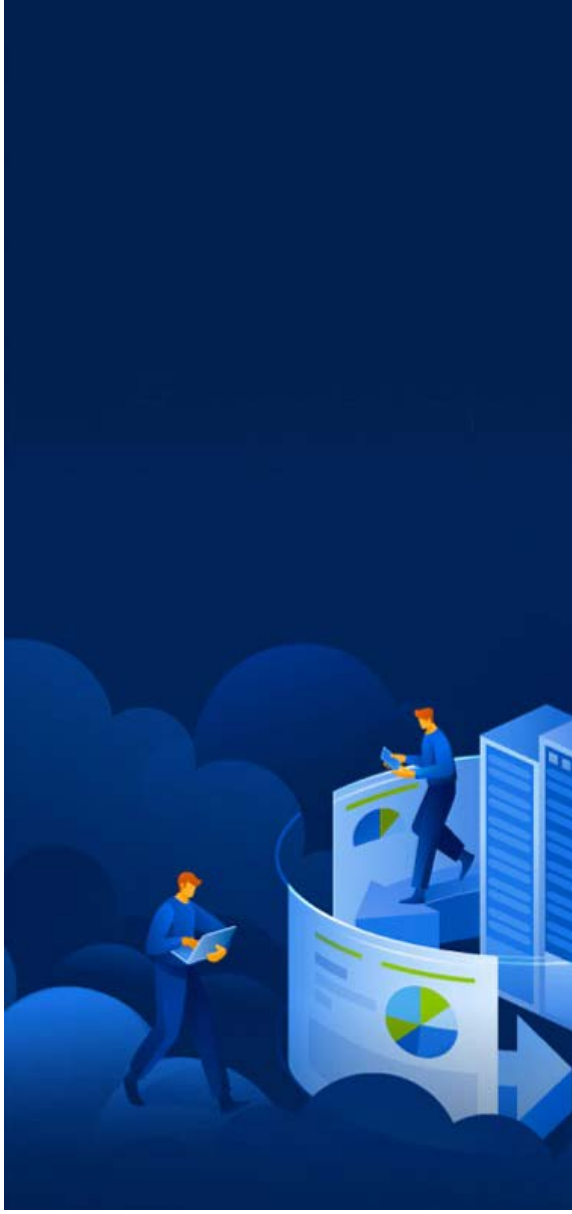
- **Управление.** Централизованное и интуитивно понятное управление резервным копированием и восстановлением данных через единую веб-консоль.
- **Мониторинг.** Визуализация состояния системы, инфраструктуры и процессов в реальном времени и за заданный период, оповещения о ключевых событиях.
- **Кроссплатформенность.** Поддержка отечественного и зарубежного, свободно распространяемого и проприетарного программного обеспечения.
- **Хранение.** Использование локальных, сетевых и облачных хранилищ, организация многоуровневого хранения резервных копий.
- **Масштабируемость.** Поддержка тысяч объектов резервного копирования, в том числе в географически распределенных инфраструктурах.
- **Оптимизация.** Управление нагрузкой на инфраструктуру: вычислительные ресурсы, сетевой канал и хранилище резервных копий.

Совместимость различных решений

Чем больше операционных систем, СУБД и виртуальных сред поддерживает решение по резервному копированию, тем лучше оно будет работать. В противном случае инженерам придется ставить «костыли» — то есть искусственно настраивать совместимость разных систем.

«Кибер Бэкап» не только поддерживает операционные системы Windows и macOS, но также работает с ядрами Linux вплоть до 5.0–5.15. Это позволяет поддерживать иные операционные системы, созданные на базе ОС Linux, в том числе российской разработки — Astra Linux, Альт Линукс, Ред ОС. Они пока плохо представлены на белорусском рынке, но в ближайшие годы их присутствие может значительно расшириться. Поэтому выгодно заранее иметь решение по резервному копированию, которое поддерживает представленные операционные системы.

Что касается работы с СУБД и различными корпоративными приложениями, то уже сегодня «Кибер Бэкап» отлично справляется с копированием и восстановлением MS SQL, MS Exchange, Postgresql, Postgres Pro, MS SharePoint, SAP HANA, CommuniGate Pro и других.



Особый подход к виртуальным средам

Большинство современных корпоративных инфраструктур работают в режиме виртуализации, в том числе и в качестве облачной среды. И, естественно, ответственным лицам хочется, чтобы весь кластер бэкапился понятным образом и мог восстановиться после любого сбоя из резервной копии.

Для этого, как правило, создается отдельное хранилище резервных копий виртуальных машин (ВМ), а сам механизм бэкапа запускается по безагентной схеме. Такой подход позволяет обеспечить защиту каждой ВМ без ручного вмешательства и установки дополнительных параметров, а также не снижать производительность пользовательских ВМ из-за резервного копирования.

В «Кибер Бэкап» безагентная схема работы реализована для систем виртуализации Microsoft Hyper-V, VMware vSphere ESX(i), oVirt, zVirt, Ред Виртуализация и других. Также многие платформы виртуализации можно бэкапить и методом установки агента внутрь гостевой виртуальной машины — это не противоречит политике лицензирования.

В расширенной версии «Кибер Бэкапа» доступен тиринг систем хранения. То есть вы можете распределить данные между накопителями разной скорости и надежности, чтобы обеспечить максимальную защиту наиболее важных данных. Для этого используется программно-определяемое хранение (на базе нашего собственного решения или внешнего продукта). Все емкости объединяются в один пул хранения резервных копий, а для размещения данных задаются общие правила.

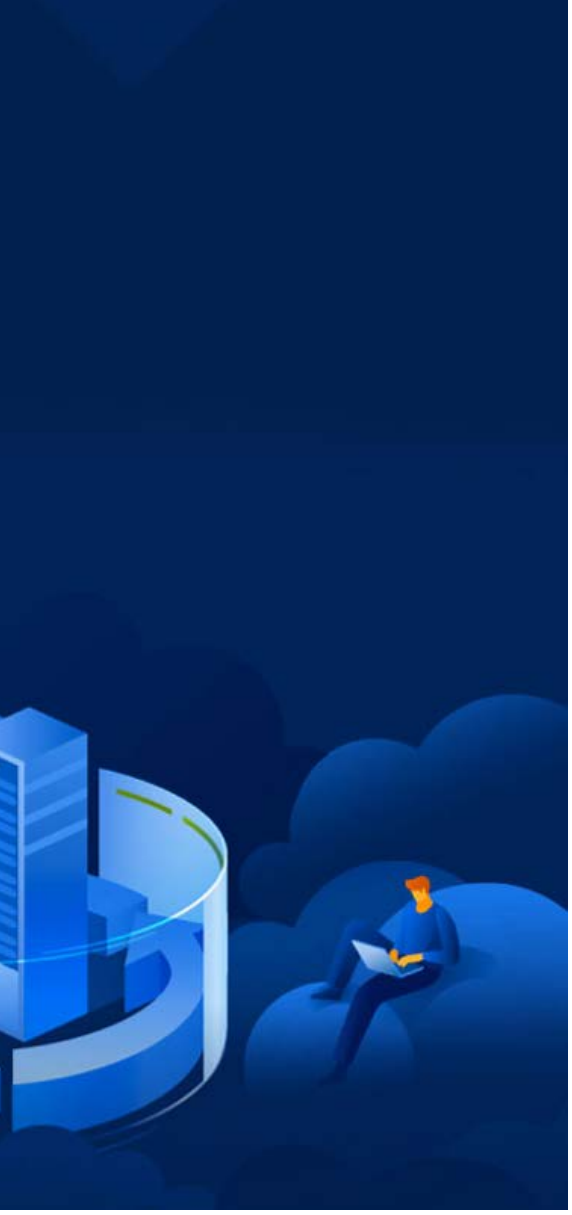
При создании резервной копии можно использовать дедупликацию. Причем в «Кибер Бэкап» реализован подход к дедупликации блоков переменного размера, что снижает нагрузку на сеть и позволяет сохранить полноценный подход к инкрементному бэкапу. Впрочем, это уже тема для отдельного технического поста.

Управление бэкапом

Управление резервным копированием в «Кибер Бэкап» оптимизировано для корпоративной среды. Через единую консоль можно управлять всем парком защищаемых ресурсов. Также модель доступа позволяет распределять обязанности между системными администраторами, чтобы они контролировали определенные участки инфраструктуры. Защита доступа поддерживает PAM-решения для повышения безопасности и лучшего контроля за действиями привилегированных пользователей.

Сервер управления, который представлен в виде веб-консоли, оптимизированный в том числе для работы с мобильных устройств, можно установить на отдельной машине x86-64, включая и виртуальную, которую также можно будет резервировать нашим же решением.

На рабочих станциях и серверах размещаются агенты, а для систем виртуализации агенты разворачиваются в виде апплайнса на том же гипервизоре. Их можно развертывать с применением групповых политик, а также автоматизировать процесс активации защиты за счет интеграции с Active Directory.



Восстановление системы

Восстановить данные, сохраненные «Кибер Бэкапом», можно различными способами, в том числе перенося рабочие образы между виртуальной средой и физической. Из наиболее интересных возможностей отметим:

- vmFlashback — быстрое восстановление образа на прежнем месте за счет возвращения только измененных файлов. Как инкрементальный бэкап, только наоборот.
- Универсальное восстановление — специальная технология развертывания образа на новом железе. Проблемы совместимости и наличия драйверов решаются автоматически.
- Мгновенный запуск ВМ — благодаря сохранению резервной копии виртуальной машины в виде единого файла запустить ВМ можно прямо из хранилища (конечно, если вы используете не самые медленные носители).
- Гранулярное восстановление — можно восстанавливать отдельные файлы, папки, письма или что-то еще. Поиск ведется непосредственно в самом архиве.

Регулярные обновления

«Кибер Бэкап» — решение, которое активно поддерживается вендором. Последнее масштабное обновление до версии 16 вышло в конце апреля прошлого года и добавило расширенные возможности по поддержке СУБД на основе PostgreSQL и систем виртуализации на основе OpenStack.

Теперь «Кибер Бэкап» может обеспечить полное и инкрементное резервное копирование PostgreSQL и СУБД на ее базе, включая работу с любыми хранилищами резервных копий: локальными и сетевыми папками, SFTP, ленточными библиотеками.

Также теперь «Кибер Бэкап» может защищать целые кластеры OpenStack без установки агентов на каждую виртуальную машину. Для OpenStack поддерживается полное, дифференциальное или инкрементное резервное копирование в любые типы хранилищ: локальные и сетевые папки, SFTP, ленточные библиотеки.

В данный момент решение «Кибер Бэкап» используется более чем 4000 клиентов. А общий объем защищенных данных приближается к 120 петабайтам. В том числе решение уже используют многие белорусские организации. ■

Правило «3-2-1»

Правило «3-2-1» изобрел фотограф Питер Крог, но со временем оно стало одним из базовых при резервном копировании данных. Крог боялся потерять свои снимки, поэтому изобрел способ, как максимально обезопасить их хранение, и описал его в книге «Управление цифровыми активами для фотографов». Звучит это правило следующим образом:

- необходимо иметь не менее 3 экземпляров данных;
- хранить копии не менее чем на 2 носителях;
- хранить не менее 1 копии данных за пределами офиса.

Если вы хотите узнать более подробную информацию о решении, получить конкурентное предложение о его внедрении в вашей организации, звоните **+375 17 336 55 95** или пишите **belarus@noventiq.com**

Сетевое оборудование: новые решения, тестирование и реализованный проект

За последний год рынок сетевого оборудования в Беларуси претерпел серьезные изменения. Появилось много новых производителей, которые пытаются заполнить нишу, образовавшуюся на месте компаний, ушедших с рынка Беларуси.

Мы кратко напишем об основных проблемах, с которыми сталкиваются организации при построении сетевой инфраструктуры, какие производители сегодня присутствуют на рынке, а также подробно расскажем о сетевом оборудовании Maipu и успешном проекте, который мы реализовали в Беларуси с использованием решений новых вендоров.

Проблемы при построении сетевой инфраструктуры:

- Большое количество компаний-производителей, малое количество компаний-вендоров. Разница между ними в том, что производитель, по сути, осуществляет сборку оборудования из чужих компонентов. От этого зачастую страдает как качество, так и последующее обслуживание аппаратного обеспечения.
- Отсутствие технической документации. Еще одна проблема, тесно связанная с предыдущей, — технической документации либо нет в принципе, либо она есть, например, на китайском языке. Это дает дополнительные сложности для установки и последующего обслуживания сетевого оборудования.

- Отсутствие или низкий уровень поддержки. К сожалению, многие компании, которые сегодня работают на белорусском рынке, обладают некачественной службой поддержки.
- Отсутствие специалистов. В компаниях нет сотрудников, которые имеют необходимые знания для работы с оборудованием новых вендоров.
- Качество. Учитывая, что многие вендоры массово пришли на белорусский рынок менее года назад, у наших компаний пока отсутствует опыт продолжительной эксплуатации их оборудования. Из-за этого не всегда есть уверенность не только в уровне качества, но также и в функционале, который заявляет производитель.
- Сроки поставок. Здесь все зависит от класса оборудования и вендора, но компаниям стоит приготовиться к тому, что сроки поставок заказанного оборудования могут составлять до полугода.

Как мы решаем эти проблемы

Noventiq Belarus работает лишь с проверенными вендорами на рынке, которые имеют подробную документацию к своим решениям.

Наши специалисты лично тестируют все оборудование — как на соответствие заявленному производителями функционалу, так и на возможность совместимости с оборудованием других производителей. Также мы проверяем качество сборки изделия.

Мы готовы лично проконсультировать вас практически по всем вендорам и рассказать об особенностях, преимуществах и недостатках их оборудования. К тому же у нас уже есть успешный опыт работы с решениями новых вендоров.

Какие вендоры сегодня работают на белорусском рынке

Самих вендоров немало — Eltex, Qtech, Zelax, Ruijie Networks, BDCOM, Maipu, Hengison, Edge-Core и другие. Но стоит помнить, что, во-первых, не все их оборудование доступно на нашем рынке и не каждый из вендоров может закрыть все потребности компании.

Поэтому перед разработкой проекта рекомендуем изначально проконсультироваться со специалистами по наличию оборудования на рынке, срокам его поставки и функциональным возможностям.

В целом, оборудование вендоров, которые в данный момент работают на рынке Беларуси, позволяет закрыть большинство задач организаций. Однако в отдельных случаях следует искать нестандартные подходы, например создавая один стек на разных вендорах. Не сказать, что такое решение недопустимо, скорее оно вызывает массу дополнительных сложностей, которые придется решать в процессе внедрения. В этом случае вам необходимо опираться на надежного партнера, у которого есть в штате специалисты с компетенциями по решению задач такого плана.

Сетевое оборудование Maipu

Компания создана в 1993 году, занимается исследованиями и разработками в области передачи данных. Имеет большой опыт, является основным поставщиком сетевых решений в Китае. В линейке продуктов вендора представлены маршрутизаторы, коммутаторы, беспроводные сети, SDN-решения, облачные сервисы для управления сетевым оборудованием. Maipu предлагает оборудование, необходимое для построения полноценной сетевой инфраструктуры и модернизации сетей. Компания имеет более 1500 патентов, около 50% ее сотрудников занимаются исследованиями и новыми разработками.

На решениях вендора можно строить 2- и 3-уровневые архитектуры. Единственная вещь, которая при этом лицензируется, — контроллер BD-LAN. В остальном вендор имеет четкое позиционирование — доступность всего функционала оборудования «из коробки».

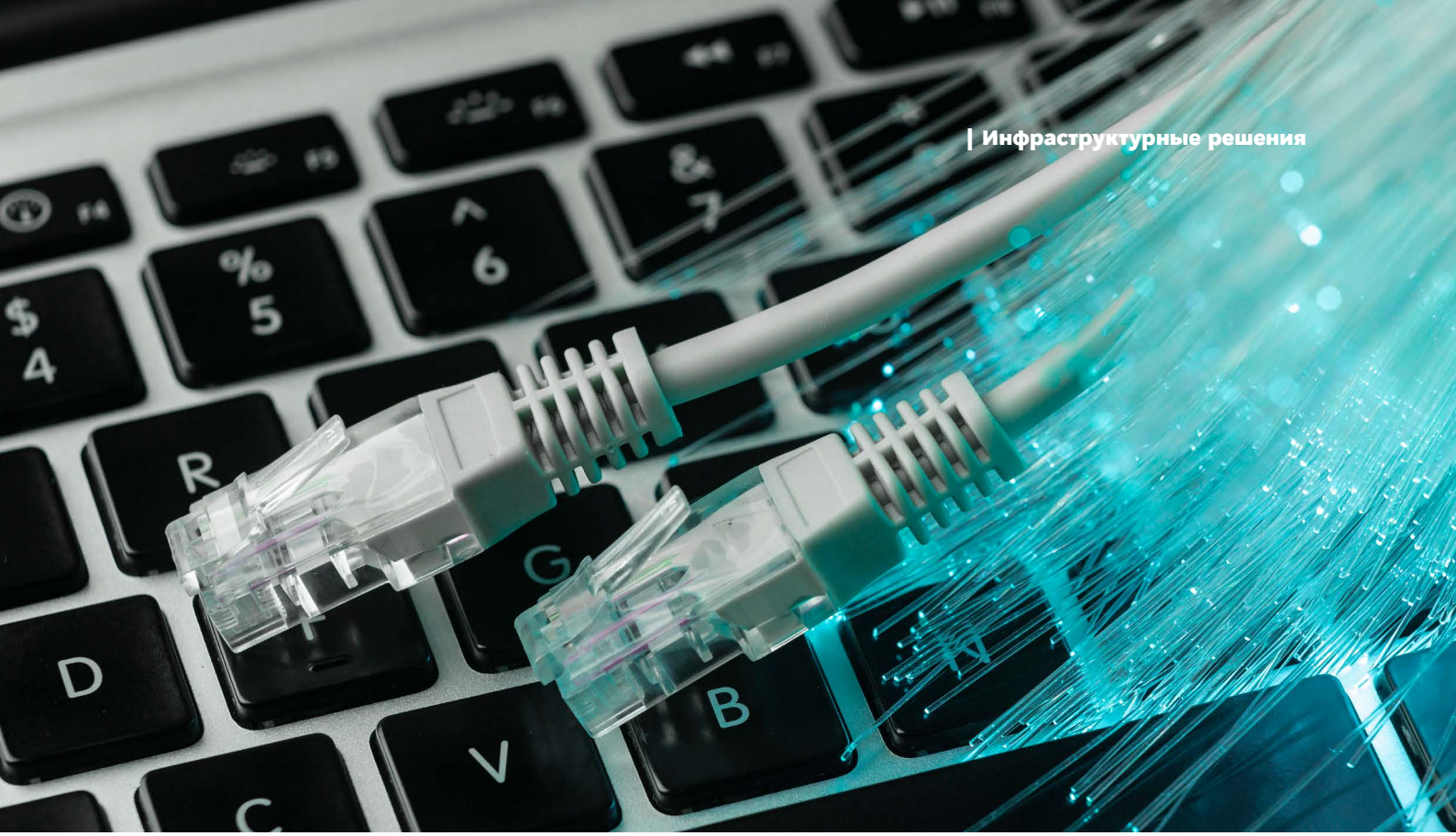
Оборудование Maipu использует унифицированное ПО. То есть нет разделения на коммутаторы Enterprise или для дата-центров. Все работает на одинаковом софте.

Тестирование оборудования Maipu

Наши специалисты провели тестирование практически всего оборудования Maipu, которое доступно сегодня на белорусском рынке. Мы проверяли как качество изделий, так и их заявленный функционал.

Если вы хотите подробно ознакомиться с результатами тестирования и узнать рекомендации по построению сетевой инфраструктуры — обращайтесь к нашим специалистам. Мы же кратко поделимся основными выводами.

- У Maipu доступен режим Rapid-VIST, который совместим с режимом Rapid-PVST у Cicso. Это позволяет встраивать коммутаторы Maipu в сеть Cicso без необходимости переводить всю инфраструктуру на какие-то открытые стандарты.
- Есть MSTP — открытый стандарт, который позволяет работать Maipu в одной сети с оборудованием других вендоров.
- Возможность стекирования доступна только через информационные аплинки.
- Апгрейд ПО проходит без перезагрузки всего стека, что есть далеко не у каждого вендора — некоторые производители требуют перезагрузки всего стека после обновления ПО на одном юните.
- Коммутаторы Maipu можно стекировать из разных моделей, построенных на одних чипах.
- Site-to-Site VPN. Подтвердили работоспособность режима как между оборудованием Maipu, так и с Cicso, Huawei и другими производителями. Нет VTI, и пока неизвестно о его реализации. Поддерживается только IKEv1, а IKEv2 — в разработке.
- Протокол динамической маршрутизации IRMP совместим с Cisco EIGRP и обладает теми же метриками. Практически ни у кого из других вендоров нет аналогов. И если сеть была построена на EIGRP, ничего нельзя было выбрать, кроме Cisco. Для многих это было критическим моментом.



Преимущества оборудования Maipu:

- Оборудование Maipu использует Command Line, практически аналогичный тому, что используется на оборудовании компании Cisco. Поэтому инженеры могут настраивать оборудование даже без дополнительного обучения.
- Маршрутизаторы и коммутаторы Maipu используют унифицированное программное обеспечение Unified IOS, поэтому нет необходимости платить за лицензии на дополнительный функционал (такой как: MPLS/L2TPv3/BFD/IPSLA и т. д.).
- Возможности интегрирования устройств Maipu с решениями Cisco (DMVPN, VXLAN-фабрика).
- Maipu предоставляет R&D-поддержку — разработку необходимого заказчику функционала.

Кейс, реализованный на новых решениях

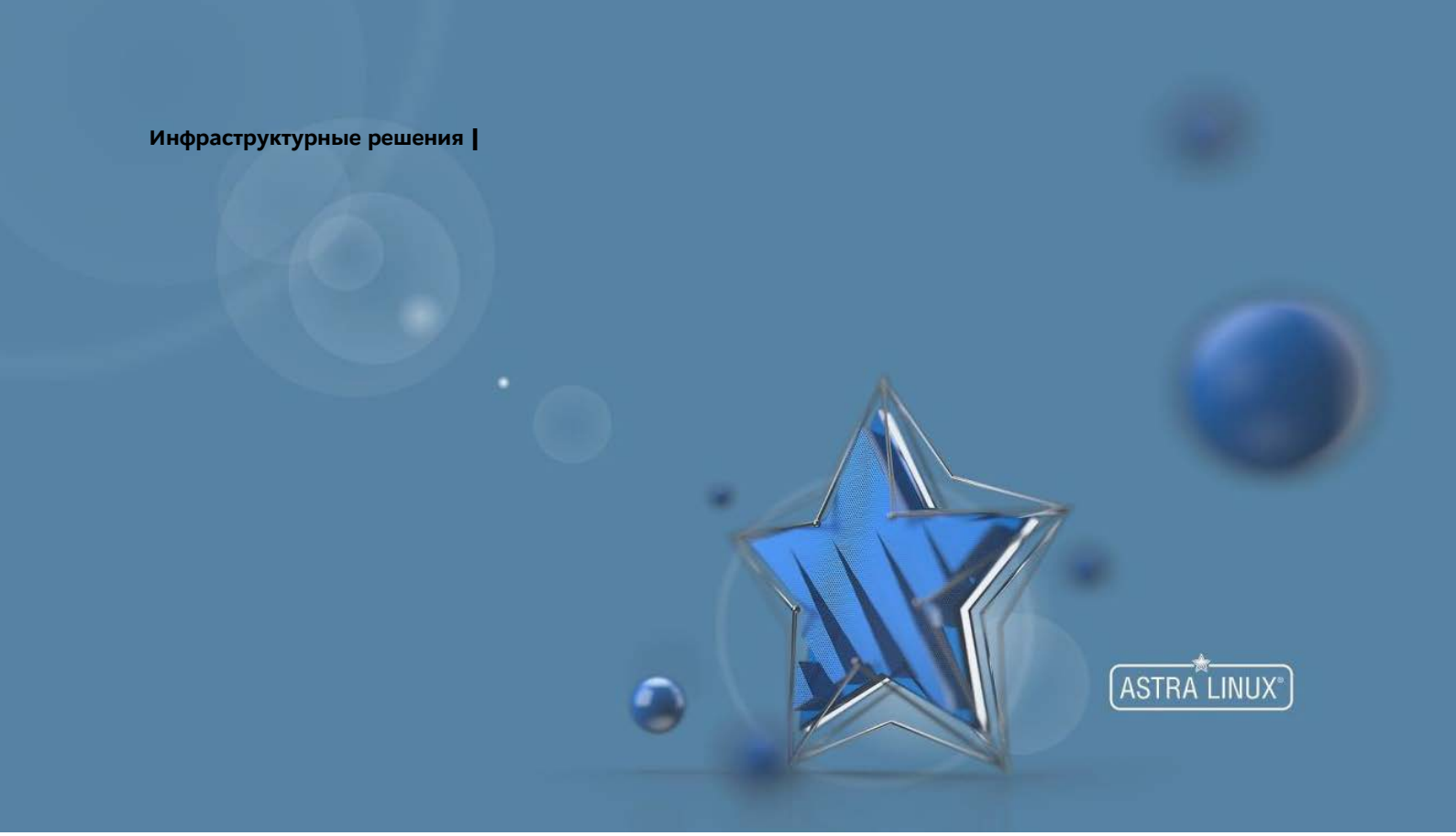
Этот проект был реализован в компании с сетью филиалов по всей стране. Стояла задача по модернизации сетевой инфраструктуры и ее унификации. По итогу весь проект был выполнен специалистами Noventiq Belarus с использованием доступных на рынке решений и без привлечения сторонних подрядчиков.

Учитывая, что в рабочие дни переключение сетевой инфраструктуры на новые компоненты было невозможно — филиалы постоянно должны были обмениваться информацией с головным офисом, — специалисты Noventiq Belarus провели монтаж нового сетевого оборудования параллельно с действующей системой. Таким образом удалось безболезненно для бизнес-процессов заказчика провести переход всей ИТ-инфраструктуры компании на новые решения. Сделано это было в максимально сжатые сроки в нерабочее время.

Также наша компания взяла на себя все работы по первоначальному администрированию работы нового оборудования. Была проведена настройка всех сервисов, которые до этого использовал заказчик, налажено подключение к внешним онлайн-сервисам.

После окончания работ по монтажу-наладке прошла опытная эксплуатация нового аппаратного обеспечения. На данном этапе специалисты Noventiq Belarus устраняли все возникающие сложности, а также оказывали ИТ-специалистам заказчика консультационную помощь. ■

Если вам требуется больше информации по выбору сетевого оборудования, обращайтесь **к специалистам Noventiq Belarus** по телефону **+375 17 336 55 95** или электронной почте **belarus@noventiq.com**



Решения ГК «Астра». Безопасность на всех уровнях

Последние несколько лет стали беспрецедентными по количеству хакерских атак на белорусские организации. И в данный момент тенденций на изменение ситуации в лучшую сторону нет. Поэтому построение безопасной ИТ-инфраструктуры сегодня является одним из ключевых направлений развития информационных технологий в компаниях.

Astra Linux — одна из лучших операционных систем в плане обеспечения безопасности, которая представлена на белорусском рынке. В этом году она получила сертификат соответствия от ОАЦ и является единственной ОС, доступной в Беларуси, обеспечивающей защиту как общедоступной, так и любой иной информации ограниченного распространения, включая информацию, затрагивающую интересы физических лиц, служебную информацию особой секретности и др. Она также может применяться в составе как негосударственных, так и государственных информационных систем, в том числе критически важных объектов информатизации.

О других преимуществах операционной системы Astra Linux и решениях ГК «Астра», о реализованных проектах, обучении сотрудников и планах открытия офиса в Беларуси мы поговорили с директором департамента по работе с региональными партнерами в России и ближнем зарубежье ГК «Астра» **Екатериной Хритоненковой**.

— Екатерина, начнем с самого важного — кому в первую очередь будут интересны решения ГК «Астра»?

— Сегодня наши решения будут интересны любой компании, которая хочет перейти на доступное и безопасное ПО с постоянными обновлениями и качественной техподдержкой.

Изначально у нас был один флагманский продукт — защищенная операционная система Astra Linux. Она создавалась с прицелом на организации, которые обладают критической инфраструктурой — государственные органы, финансовые организации, крупные промышленные предприятия и другие. Была цель создать продукт, обеспечивающий наибольшую защищенность, но при этом обладающий тем же функционалом, что и конкуренты.

Но мы всегда понимали, что одной операционной системы недостаточно для стабильной и безопасной работы организации. Поэтому постоянно работали над расширением своего портфеля решений. Часть из них разрабатывалась непосредственно нашими специалистами, в каких-то случаях мы приобретали компанию-разработчика и интегрировали готовое ПО в нашу экосистему.

Помимо операционной системы, в нашем портфеле решений есть система виртуализации «Брест», СУБД Tantor, VDI Termidesk, система резервного копирования RuBackup и другие. Всего 15 продуктов, которые закрывают большинство вопросов построения полноценной ИТ-инфраструктуры организации.

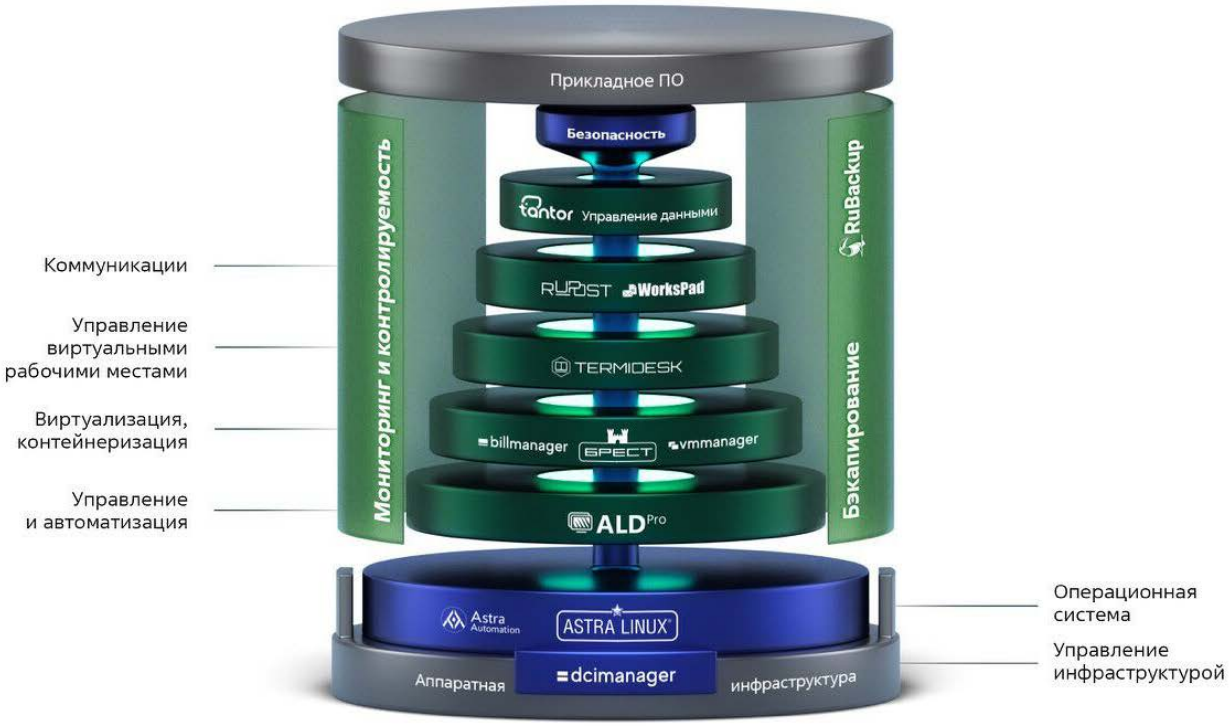
— ГК «Астра» работает с 2008 года, но на белорусском рынке вы активно стали продвигать свои решения лишь несколько лет назад. С чем это связано?

— В предыдущие годы нам не всегда хватало рабочих рук для удовлетворения потребностей даже российского рынка. Велась активная работа над выпуском обновлений к Astra Linux, разрабатывались новые решения.

В то же время нельзя сказать, что мы не обращали внимания на Беларусь — мы вели работы по получению сертификата соответствия. Специалисты из Беларуси приезжали в Россию, проверяли нашу разработку, тестировали нашу операционную систему, и мы вносили в нее изменения, предложенные белорусской стороной. Сегодня наша ОС может использоваться в любых информационных системах, в том числе в тех, которые связаны с государственными секретами.

Также мы видим, что у белорусских организаций появился серьезный запрос на наши решения. В первую очередь на операционную систему с высоким уровнем защиты, программный комплекс «Средства виртуализации «Брест», ПО для управления доменом ALD Pro и другие. Рост интереса связан в первую очередь с повышением рисков по информационной безопасности, а также с уходом с белорусского рынка других, в частности иностранных, вендоров. Однако у нас нет цели «почивать на лаврах» и просто занять освободившееся место. Мы хотим, чтобы заказчики переходили на решения ГК «Астра» осознанно, учитывая те преимущества, которые это им дает.

В ближайшие месяцы в Минске откроется наше официальное представительство. Это значительно упростит взаимодействие с заказчиками и партнерами в Беларуси, а также усилит конкурентное преимущество по оказанию консультационной помощи и техподдержки.



— Еще один важный момент, который будет интересен для белорусских компаний, — есть ли у вас реализованные проекты в Беларуси?

— Решения ГК «Астра» уже работают, например, на Белорусской атомной электростанции. Сегодня мы проводим успешное тестирование и пилотирование наших решений в организациях из разных отраслей экономики — банковская сфера, госорганы, медицина, образование. Это процесс не быстрый, зачастую связанный с определенными рисками, поэтому компании постепенно внедряют наши решения. У нас есть большой опыт по обеспечению даже достаточно сложных миграций. Сегодня любая организация может протестировать наши решения, подключившись к тестовому стенду. Для этого достаточно отправить запрос в Noventiq Belarus. При необходимости наши партнеры проанализируют инфраструктуру организации, проведут пилотирование, а затем и внедрение.

— Какие ключевые преимущества ваших решений можно выделить?

— Безопасность и надежность — наши главные козыри. ОС Astra Linux изначально создавалась с прицелом на обеспечение максимальной защиты ИТ-инфраструктуры. Этого же принципа мы придерживаемся и в других своих продуктах.

Второе преимущество, которое тесно связано с первым, — регулярные обновления. Сегодня новые типы атак и вирусы появляются ежедневно. Мы отслеживаем эти процессы и стараемся максимально быстро выпускать обновления своих решений, которые смогли бы им противостоять.

Третье — продуктово-сервисный подход. Мы и наши партнеры из Noventiq Belarus не только продаем программы, но также оказываем помощь по их внедрению и запуску, обучению специалистов, оказываем консультационную помощь и последующую техническую поддержку.

Еще одно наше важное преимущество — конкурентные цены по сравнению с аналогичными решениями у других вендоров.

— Внедрение новых решений — это всегда стресс для организации. Ведь идет перестройка не только ИТ-инфраструктуры, но также и персонала — как технических специалистов, так и остальных сотрудников. Есть ли у вас рекомендации, как сделать данный процесс более простым?

— На первом этапе мы рекомендуем компаниям внедрять наши решения параллельно с действующей инфраструктурой. Да, процесс займет больше времени, но зато не будет шокового эффекта. Параллельно с этим следует обучать технических специалистов, которые будут заниматься администрированием новых систем, а также тех сотрудников, которые первыми перейдут на новые решения.

Именно для этого необходимы пилотные проекты. На протяжении определенного времени часть сотрудников компании либо определенное структурное подразделение переходит на наши решения. На этом этапе мы решаем возникающие сложности, оказываем консультационную помощь. А уже после успешного пилота можно говорить о полноценном внедрении наших решений.

— Расскажите подробнее про обучение специалистов. Для многих компаний это становится камнем преткновения. Как у вас обстоит с этим дело?

— Сейчас мы активно работаем над созданием нескольких образовательных центров, в которых будет проходить обучение по нашим продуктам. Их преподаватели прошли обучение в «Астра Академии» и получили статус сертифицированных преподавателей по операционной системе Asta Linux.

Уже сегодня в учебном центре Noventiq Belarus можно записаться на 14 курсов — Администрирование Astra Linux 1.7, Практический курс по работе с ПК СВ «Брест», Администрирование системы резервного копирования RuBackup и другие. Со временем их список будет расширяться, а программы актуализироваться. ■

ГК «Астра» — один из лидеров российского рынка информационных технологий в области разработки системного и инфраструктурного программного обеспечения. Работает с 2008 года. Первый флагманский продукт — операционная система Astra Linux с беспрецедентным уровнем защищенности. Сегодня ее используют более 15 тысяч организаций, в том числе государственные и коммерческие структуры, объекты критической информационной инфраструктуры, промышленные предприятия, банки, организации систем образования и здравоохранения.

Наряду с операционной системой ГК «Астра» предлагает решения для организации корпоративной почты, виртуализации, управления доменом, резервного копирования и другие. На данный момент у компании 15 продуктов.

Для получения консультации по решениям **ГК «Астра»** звоните по телефону **+375 17 336 55 95** или пишите на почту **belarus@noventiq.com**

АСТРА
группа компаний

Российский стек ПО для создания ИТ-инфраструктур любого масштаба

ASTRA LINUX®
Сервер. Десктоп. Мобайл. Защищенная ОС

ALD Pro
Система для управления службой каталогов

ASTRA AUTOMATION
Развертывание решений по клику

БРЕСТ
Облачная виртуализация

vmmanager
Серверная виртуализация

Astra Consulting
Всесторонняя помощь при проектах миграции

TERMIDESK
Инфраструктура виртуальных рабочих мест

billmanager
Платформа для биллинга облачных сервисов

tantor
СУБД и платформа для администрирования и мониторинга

RUBOST
Корпоративная почта

RuBackup
Средство резервного копирования

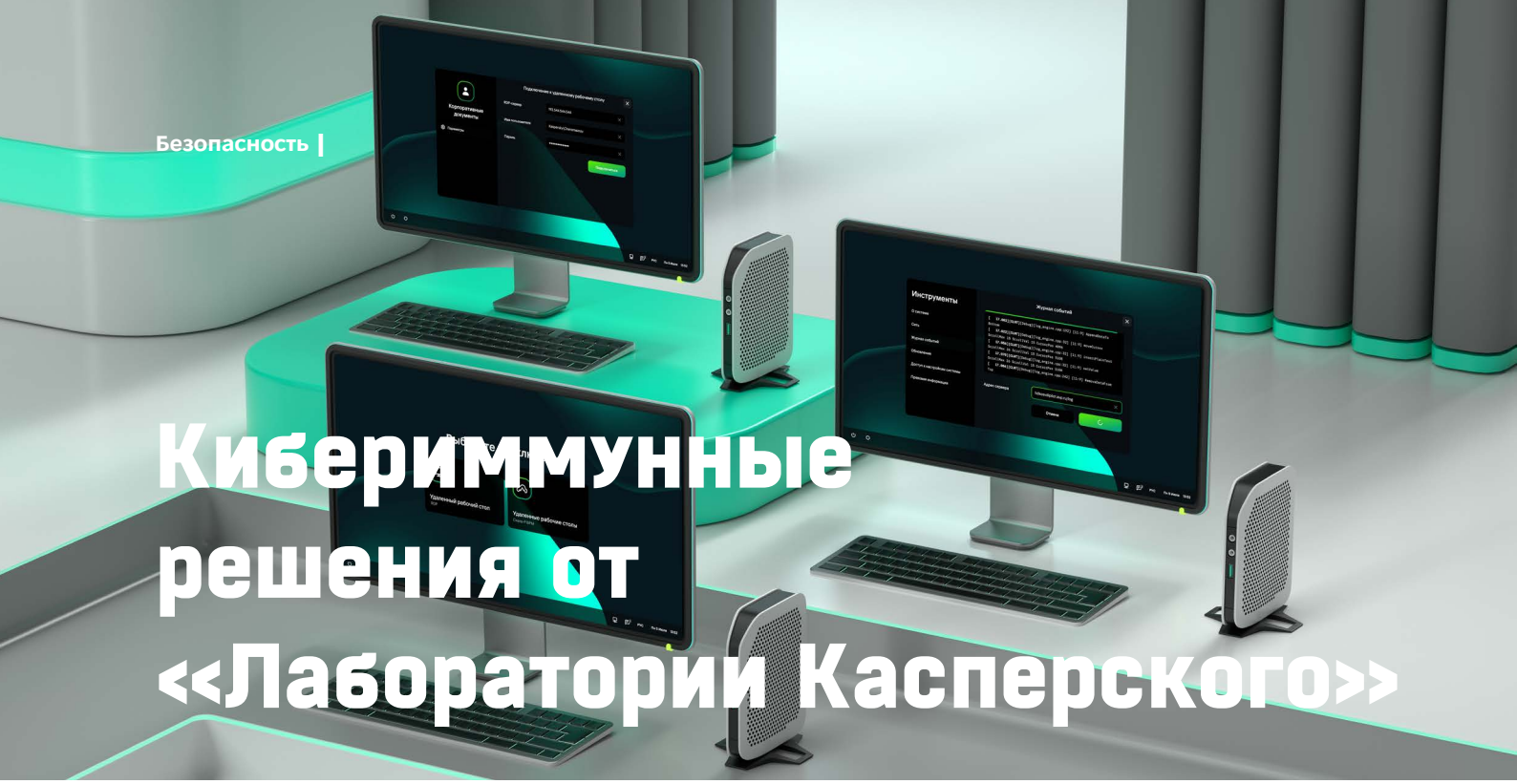
dcimanager
Платформа для управления физической инфраструктурой

WorksPad
Мобильное рабочее место

- Широкая экосистема совместимых программных и аппаратных решений
- Безопасная разработка
- Стабильность и защита ИТ-инфраструктур
- Инструменты автоматизации и механизмы миграции
- Быстрое и легкое развертывание ПО
- Комплексное сопровождение проектов внедрения
- Круглосуточная техническая поддержка

Более 2,5 млн инсталляций ОС Astra Linux

Российские ИТ-решения
https://astralinux.ru/
8(495) 369-48-16
info@astralinux.ru



Кибериммунные решения от «Лаборатории Касперского»

Современные угрозы в сфере информационной безопасности требуют от бизнеса внедрения новых продуктов, которые дают максимальную защиту ИТ-инфраструктуре бизнеса. Одно из инновационных решений в этой сфере — использование кибериммунных решений.

Кибериммунная система способна противостоять кибератакам без использования дополнительных (наложенных) средств безопасности. Подавляющее большинство типов атак на кибериммунную систему неэффективно и не может повлиять на выполнение ею критических функций.

«Лаборатория Касперского», один из мировых лидеров по обеспечению кибербезопасности, несколько лет назад представила микроядерную операционную систему собственной разработки — KasperskyOS. А сегодня в портфеле компании уже есть набор кибериммунных решений, которые гарантируют максимальную безопасность корпоративных пользователей.

Мы кратко расскажем о решениях этого класса.

KasperskyOS

KasperskyOS — это микроядерная операционная система для подключенных к интернету встраиваемых систем с повышенными требованиями к кибербезопасности. Она разработана в соответствии с архитектурами MILS и FLASK с добавлением собственных технологий безопасности «Лаборатории Касперского».

В основе KasperskyOS лежат три принципа:

- **Микроядерная архитектура.** Чем компактнее ядро ОС, тем проще его исследовать и тем меньше возможностей для возникновения уязвимостей. Ядро KasperskyOS — собственная разработка «Лаборатории Касперского», в нем нет заимствованного кода. В то же время, основная прикладная функциональность системы базируется на open source решениях.
- **Минимально возможная поверхность атаки на ядро ОС.** Поверхность атаки на ядро ОС определяется числом системных вызовов и других каналов внешних воздействий. Если архитектура микроядерная, то в ядре нет драйверов, оно не взаимодействует через оборудование с внешними источниками воздействий. В этом случае поверхность атаки зависит лишь от количества используемых системных вызовов. У KasperskyOS всего 3 вызова не контролируются монитором безопасности — это вызовы, отвечающие за IPC.

- **Гарантии изоляции.** Исключены любые возможности обмена данными между процессами в обход движка ОС Kaspersky Security System.

KasperskyOS позволяет гибко задавать политики безопасности — правила, которым будет следовать система весь свой жизненный цикл и которые не дадут ей выполнять потенциально опасные операции. Ее компоненты разделены на изолированные домены безопасности и не влияют друг на друга. Все их взаимодействия проходят через микроядро. Если что-то не соответствует заданным политикам, действие блокируется еще до его выполнения. А работоспособность обеспечивает строгая изоляция всех системных компонентов. Атака на иммунную систему не приводит к сбою — система продолжает выполнять критические функции, заложенные на этапе проектирования.

Где сегодня используется KasperskyOS:

- шлюзы для защиты интернета вещей, включая индустриальный;
- тонкие клиенты для подключения к удаленным рабочим столам;
- профессиональные мобильные устройства;
- электронные блоки в составе умных автомобилей.

Кибериммунный тонкий клиент

Тонкий клиент — это компактный компьютер, который подключается к удаленной среде для выполнения вычислений, работы с бизнес-приложениями и хранения данных. Тонкий клиент может быть частью терминальной, виртуальной или облачной инфраструктуры.

Ко всему прочему, тонкие клиенты имеют ряд преимуществ в сравнении с ноутбуками и персональными компьютерами — у них пассивная система охлаждения (а значит, минимальный уровень шума), низкий уровень энергопотребления, они компактные и занимают мало места. К тому же, они стоят меньше стандартных рабочих станций с установленными средствами безопасности.

Решение от «Лаборатории Касперского» представляет из себя аппаратно-программный комплекс, созданный при сотрудничестве с компанией ТОНК. На тонкий клиент установлена Kaspersky Thin Client — операционная система для тонких клиентов на базе микроядерной KasperskyOS. Она предназначена для предоставления пользователю доступа к удаленному рабочему столу и служит заменой локальной рабочей станции.

Первый тонкий клиент совместного производства TONK TN1200 был представлен 21 сентября 2022 года. Его технические характеристики — Intel Celeron 4125 Gemini Lake Refresh Quad-Core 2 ГГц, Intel® UHD Graphics 600, 4 ГБ ОЗУ, SSD-накопитель на 64 ГБ.

Kaspersky Thin Client значительно снижает риски безопасности за счет того, что информация не хранится на пользовательских терминалах, выгрузка данных на неавторизованные носители невозможна, а доступ к недоверенным ресурсам ограничен и контролируется ИТ-администратором.

Благодаря Kaspersky Thin Client обеспечивается целостность данных, передаваемых между пользователями, удаленным рабочим столом, сервером централизованного управления, серверами брокеров соединения и логирования. Также она позволяет управлять сертификатами и выполнять безопасное обновление.

Где используется Kaspersky Thin Client:

- государственные организации (рабочие места госслужащих, операторы МФЦ),
- финансы и страхование (локальные офисы, операторы колл-центров, службы поддержки пользователей);
- энергетика и производство (операторы SCADA/АСУ ТП систем, рабочие станции инженеров);
- логистика (доступ к системам учета);
- здравоохранение (приемные отделения, информационные табло, точки подключения рабочих мест специалистов);
- образование (учебные классы, лаборатории, олимпиады);
- ритейл (информационные табло, рабочие места кассиров, операторы колл-центров).

Kaspersky Secure Remote Workspace (KSRW)

В полной мере достоинства тонких клиентов раскрываются при наличии централизованной системы управления, позволяющей упростить процессы настройки, администрирования и поддержки. Оконечные устройства в составе инфраструктуры могут стать объектом для разного типа кибератак, таких как: перехват нажатий клавиш клавиатуры, заражение с неконтролируемых съемных носителей или использование уязвимостей вовремя не обновленной версии ПО, атаки на сетевой стек операционной системы, уязвимости в коде протоколов доставки удаленной среды. Поэтому необходимо обеспечить безопасное подключение к виртуальным рабочим столам.

Kaspersky Secure Remote Workspace — решение для построения управляемой и функциональной инфраструктуры тонких клиентов на базе KasperskyOS для защищенного подключения к виртуальным рабочим столам.

Кроме непосредственно тонких клиентов Kaspersky Thin Client, в состав KSRW входит единая консоль управления тонкими клиентами и другими продуктами «ЛК» Kaspersky Security Center (KSC) и плагин управления Kaspersky Security Management Suite.

Консоль Kaspersky Security Center, входящая в состав решения, позволяет управлять тонкими клиентами из единого центра, настраивать их, администрировать, доставлять обновления и собирать системные события. KSC активно используется другими продуктами «Лаборатории Касперского», и благодаря этому интеграция KSRW в существующую экосистему защиты корпоративных IT-систем может стать максимально бесшовной и не потребует найма дополнительных специалистов.

Врожденная безопасность решения Kaspersky Secure Remote Workspace обеспечивает выполнение следующих требований:

- целостность данных, полученных от пользователя, от сервера централизованного управления Kaspersky Security Center и от серверов брокеров соединения;
- безопасное обновление Kaspersky Thin Client;
- конфиденциальность данных, передаваемых между Kaspersky Thin Client, удаленным рабочим столом, сервером Kaspersky Security Center (KSC), сервером логирования и брокером соединения.

Где используется Kaspersky Security Center:

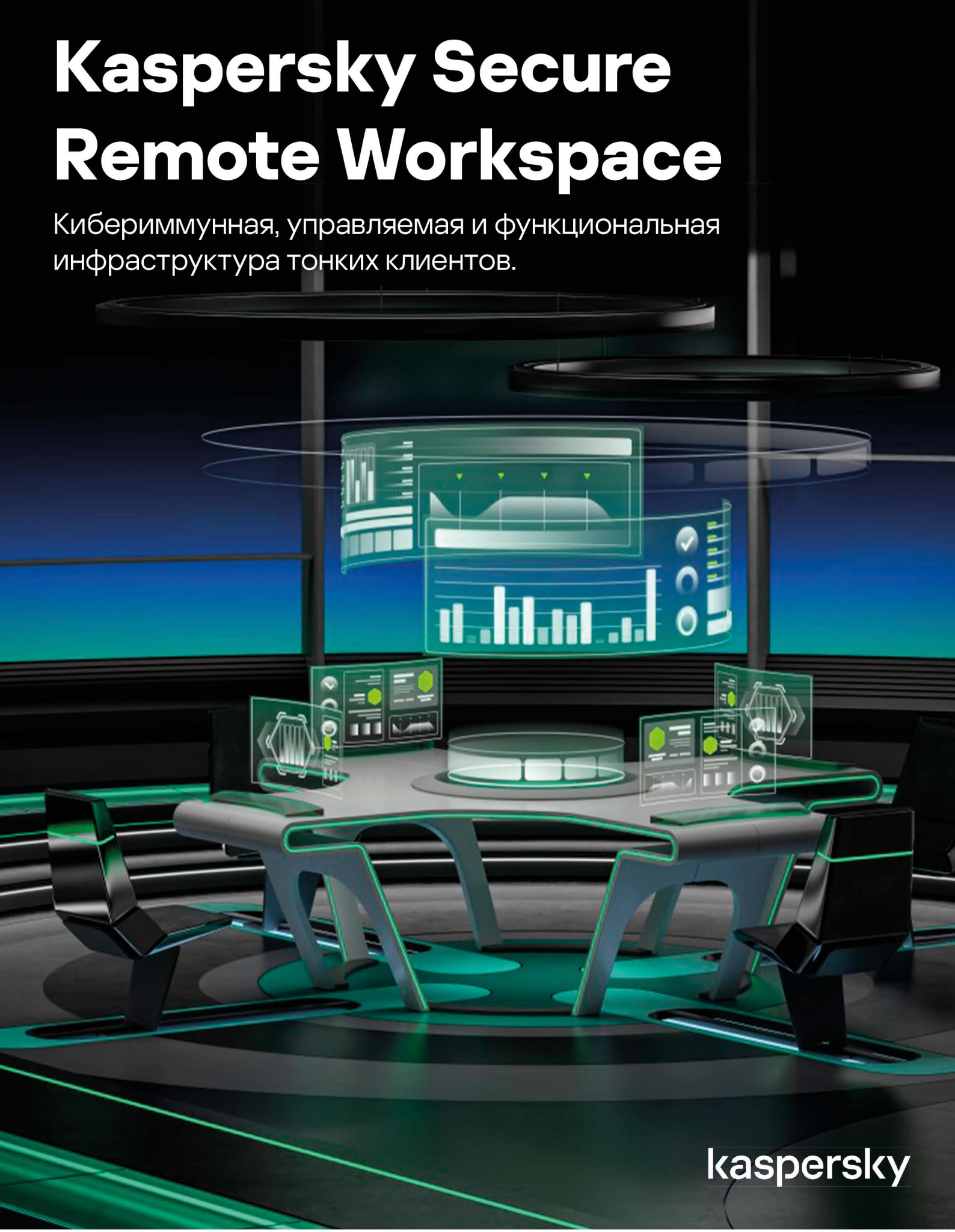
1. Головной офис и филиалы. KSRW эффективно для компаний с разветвленной филиальной сетью. В филиалы устанавливаются преднастроенные тонкие клиенты, которые безопасно подключаются к виртуальным рабочим местам и централизованно управляются консолью Kaspersky Security Center.
2. Учебные классы в образовательных учреждениях. Частая проблема в учебных классах — нецелевое использование десктопов и ноутбуков. Также высока вероятность взлома сети или заражения вредоносным ПО со съемных носителей. На тонких клиентах ученики и студенты могут подключаться только к необходимым сервисам, есть возможность ограничения использования съемных носителей.
3. Подключение к системам контроля привилегированного доступа. Системы контроля доступа привилегированных пользователей (Privileged Access Management, PAM) позволяют вести аудит действий специалистов (как внутренних, так и внешних) с расширенными правами, записывать сессии, управлять настройками парольной защиты и процессами авторизации и аутентификации. Применение решения Kaspersky Secure Remote Workspace совместно с системой PAM исключает использование сотрудниками собственных переносимых устройств, которые могут использоваться для атак на инфраструктуру. Также это позволяет контролировать подключение периферийных устройств.
4. Изоляция сегментов и предоставление заведомо безопасного доступа к КИИ. Безопасный и сегментированный доступ реализуется на базе системы СКДПУ НТ совместно с решением Kaspersky Secure Remote Workspace. Данная схема доступа позволяет ограничить доступ только необходимыми для работы устройствами с возможностью ограничения запуска произвольного ПО на целевом узле. Сбор и анализ событий в рамках сессий обеспечивается средствами системы СКДПУ НТ. При этом за счет расширенной интеграции с продуктами «Лаборатории Касперского», Kaspersky Industrial Cyber Security for Networks, реализуются дополнительные функции по контролю доступа напрямую к защищаемым ИС объекта КИИ. ■

В данный момент Noventiq Belarus совместно с «Лабораторией Касперского» реализует несколько проектов по кибериммунным решениям в белорусских компаниях. В будущем продукты такого класса станут одним из стандартов обеспечения безопасности. А вы уже сегодня можете получить консультацию специалистов по их поставкам и внедрению в вашей организации.

Обращайтесь по телефону **+375 17 336 55 95**
или пишите на почту **Vitaliy.Shavel@noventiq.com**

Kaspersky Secure Remote Workspace

Кибериммунная, управляемая и функциональная инфраструктура тонких клиентов.



kaspersky

NOVENTIQ
Global expertise, local outcomes

Получить консультацию по продуктам «Лаборатории Касперского» вы можете у эксперта Noventiq Belarus

Виталий Шавель
+375 17 336-55-95
Vitaliy.Shavel@noventiq.com

Указ № 40 «О кибербезопасности». Что нужно знать?

14 февраля 2023 года подписан Указ Президента Республики Беларусь № 40 «О кибербезопасности» (далее — Указ). Его цель — повышение уровня защиты национальной информационной инфраструктуры от внешних и внутренних угроз.

Указ направлен на дальнейшую реализацию положений Концепции национальной безопасности и взаимосвязан с Концепцией информационной безопасности. Реализация мер, предусмотренных в Указе, позволит консолидировать усилия по предотвращению, обнаружению и минимизации последствий кибератак на объекты информационной инфраструктуры, тем самым повысить безопасность и надежность информационных систем.

Вместе с юристами и специалистами по информационной безопасности Noventiq Belarus расскажем, какие изменения и в какие сроки нас ожидают в связи с принятием Указа.

Национальная система обеспечения кибербезопасности. Какие задачи выполняет и кто в нее входит

В Беларуси должна быть создана Национальная система обеспечения кибербезопасности, состоящая из:

- Оперативно-аналитического центра при президенте Республики Беларусь (ОАЦ);
- Национального центра обеспечения кибербезопасности;
- центров кибербезопасности инфраструктуры;
- авторизованного оператора электросвязи (ООО «Белорусские облачные технологии»);
- объектов информационной инфраструктуры и сетей передачи данных.

Координацию государственных органов и иных организаций по созданию и функционированию национальной системы обеспечения кибербезопасности будет осуществлять ОАЦ.

До 17 августа 2023 г. в структуре ОАЦ будет создан Национальный центр кибербезопасности, а для реагирования на киберинциденты в составе Национального центра кибербезопасности создается национальная команда реагирования на киберинциденты.

Национальная система обеспечения кибербезопасности будет выполнять следующие задачи:

- достижение максимальной скоординированности действий государственных органов и иных организаций по обнаружению, предотвращению и минимизации последствий кибератак на объекты информационной инфраструктуры;

- постоянный поиск потенциальных уязвимостей национального сегмента глобальной компьютерной сети Интернет;
- проведение анализа информации о кибератаках и вызванных ими киберинцидентах, установление причин киберинцидентов;
- оценка эффективности защищенности объектов информационной инфраструктуры от кибератак;
- прогнозирование ситуации в области обеспечения кибербезопасности.

Обращаем внимание:

Уполномоченные лица Национального центра кибербезопасности будут вправе требовать от государственных органов и иных организаций:

- представления документов (их копий) и (или) иной информации, в том числе технического характера, связанных с функционированием принадлежащих им объектов информационной инфраструктуры. Такие документы (их копии), иная информация должны быть представлены не позднее дня, следующего за днем предъявления требования об их представлении;
- обеспечения беспрепятственного доступа в помещения и иные объекты, в которых размещены объекты информационной инфраструктуры, а также к программно-техническим средствам (в том числе удаленно), с помощью которых обеспечивается их функционирование.

Уполномоченные лица организаций, которые оказывают услуги по обеспечению кибербезопасности объектов информационной инфраструктуры, обладают такими же правами лишь в том случае, если они определены в договоре на оказание услуг по обеспечению кибербезопасности.

Кто и в какие сроки должен создать центры кибербезопасности?

Согласно п. 3.5 Указа обеспечить создание своих центров кибербезопасности в срок не позднее 17 августа 2024 г. должны владельцы критически важных объектов информатизации, указанные в Приложении 1 к Указу, а также уполномоченные поставщики интернет-услуг, оказывающие услуги хостинга официальных интернет-сайтов и электронной почты.

Советом Министров Республики Беларусь не позднее 17 февраля 2024 г. будет определен перечень государственных органов и иных организаций, которые обязаны либо создать собственные центры кибербезопасности, либо приобрести услуги по обеспечению кибербезопасности у организаций, которые такие центры создали. Этот перечень будет пересматриваться и обновляться ежегодно.

Кроме того, до 17 февраля 2024 г. будут определены компании, у которых государственные органы и организации вправе закупать услуги по кибербезопасности, с применением процедуры закупки из одного источника.

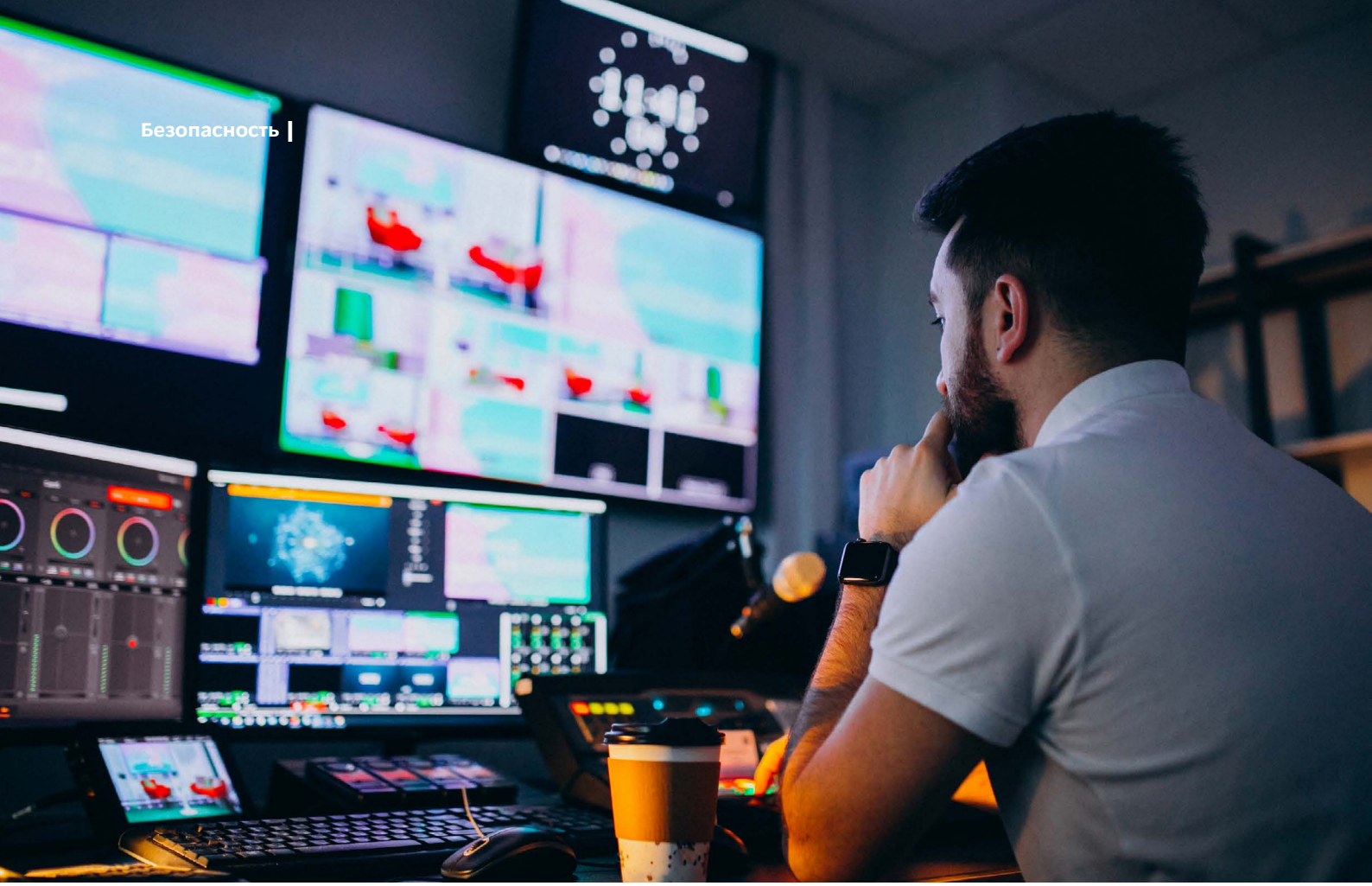
Что еще важно знать

Государственные органы и иные организации обеспечивают хранение информации о киберинцидентах, произошедших на принадлежащих им объектах информационной инфраструктуры, в течение не менее одного года.

Персональная ответственность за обеспечение кибербезопасности государственного органа и иной организации возложена Указом на руководителя этого органа (организации).

В данный момент мы ожидаем выхода дополнительных уточняющих законодательных актов по действию Указа № 40. Как только у нас появится подробная информация, мы проинформируем об этом на своем сайте и в социальных сетях. ■

Если вам необходима консультация по построению системы информационной безопасности в вашей компании, обращайтесь к нашим специалистам по телефону **+375 17 336 55 95** или электронной почте **belarus@noventiq.com**



Главные тренды кибербезопасности

Любые прогнозы, особенно в такой сфере, как информационная безопасность, воспринимают с недоверием. Сказать, как будут действовать киберпреступники через год или даже через месяц, крайне сложно, ведь их поведение связано в том числе с геополитической ситуацией, развитием новых технологий, обнаруженными уязвимостями.

Поэтому мы решили не гадать на кофейной гуще, а вместе с руководителем направления информационной безопасности Noventiq Belarus Александром Дубиной проанализировать основные тренды последнего года и рассказать, насколько высока вероятность их сохранения в будущем.

Экосистемный подход к информационной безопасности

Если раньше различные решения ИБ для бизнес-сегмента работали как самостоятельные решения, то сегодня есть тренд на создание единой экосистемы решений по информационной безопасности.

Произошло это из-за растущей сложности кибератак. Зачастую понять, что в систему произошло вторжение, можно, лишь проанализировав данные сразу из нескольких средств защиты. А сделать это можно только в том случае, если они настроены и работают как единая экосистема.

Наш прогноз. Решение, при котором все продукты по информационной безопасности объединены в одну экосистему, позволяет обеспечить наилучшую защищенность организации, поэтому тренд сохранится. Более того, уже в 2022 году поставщики решений по ИБ стали предлагать системы, которые позволяют объединять все системы защиты в одну экосистему.

Персональные данные

В 2021 г. в Беларуси вступил в силу закон «О защите персональных данных», который ужесточил требования по хранению и использованию персональных данных клиентов и сотрудников компаний. Это был важный законопроект, поскольку в последние годы кража персональных данных — одна из главных целей киберпреступников. Это очень ценный ресурс, который можно использовать разными способами: шантажировать организацию, из которой произошла утечка, для получения выкупа, продать информацию в даркнете, использовать полученные данные для целевых атак или фишинговых рассылок, мошенничества и кражи аккаунтов. Другими словами, преступники получают в свои руки настоящую золотую жилу.

В то же время не все организации уделяют должное внимание сохранности этой информации. К тому же с развитием цифровых взаимоотношений увеличивается риск утечки.

Наш прогноз. Охота за персональными данными будет продолжаться. Важно, чтобы организации в должной мере обеспечили их защиту.

Под ударом — госорганизации, промышленность, финансы

Если проанализировать отчеты компаний, которые специализируются на защите информации, в 2022 г. наибольшему количеству атак подвергались организации с государственной формой собственности, промышленные предприятия, финансовые структуры.

Наш прогноз. Данный тренд сохранится. Из других сфер, которые также находятся в зоне риска, — сфера услуг, медицинские учреждения, ритейл. То есть компании, которые хранят персональные данные своих клиентов, о чем мы писали выше.

Проще, но больше

Чаще всего в прошедшем году преступники использовали известные инструменты атак, но при этом их количество выросло в разы. Несколько раз были побиты рекорды по продолжительности и масштабам DDoS-атак, волны фишинговых писем и сайтов, популярными остаются программы-шифровальщики. Также стало известно о нескольких новых типах атак, которые произошли с использованием нейросетей.

Наш прогноз. Количество и уровень атак будут оставаться на высоком уровне. А появление новых «рекордов» во многом будет связано с внешними событиями.

Что касается использования новых технологий, то, учитывая уровень развития нейросетей, можно ожидать, что преступники активно начнут задействовать данный инструмент. В то же время разработчики нейросетей будут встраивать в них ограничения для запрета на противоправные действия.

Фишинг

Об этой угрозе стоит упомянуть отдельно. Фишинговые рассылки и сайты — легкий способ для мошенников получить доступ в корпоративную сеть. Преступнику не нужно задумываться о том, как обойти все защитные механизмы, достаточно сделать массовую или целевую рассылку на сотрудников компании, ожидая, пока кто-то из них «купится» на приманку. И, как показывает практика, в большинстве случаев данный метод срабатывает. То есть пользователи самостоятельно загружают зараженные файлы.

Наш прогноз. Фишинг — дешевый и эффективный способ атак, поэтому тренд на его популярность сохранится. В то же время белорусские компании будут активно повышать информационную грамотность сотрудников, чтобы все пользователи корпоративной сети научились отличать фишинговое письмо или сайт от настоящего.

Как оставаться в безопасности?

Как это ни банально, но, если не углубляться в технические детали, общие правила для информационной безопасности бизнеса остаются неизменными.

- Используйте только лицензионные версии решений по информационной безопасности с последними установленными обновлениями.
- Создайте, если еще нет, или постоянно держите в актуальном состоянии политику информационной безопасности в компании.
- Постоянно повышайте уровень информационной грамотности сотрудников: проводите обучения, информируйте о новых угрозах, следите за исполнением политики информационной безопасности.

Повторю известную фразу: информационная безопасность — это процесс. В первую очередь это должно инициироваться и поддерживаться бизнесом. Если важность информационной безопасности игнорируется, негативные последствия — лишь вопрос времени. ■

Тренды кибербезопасности от Gartner

Аналитическая компания Gartner выделила восемь ключевых трендов в сфере кибербезопасности, которые будут актуальны в ближайшие годы. Эти прогнозы помогут компаниям выработать наилучшую стратегию защиты своей ИТ-инфраструктуры.

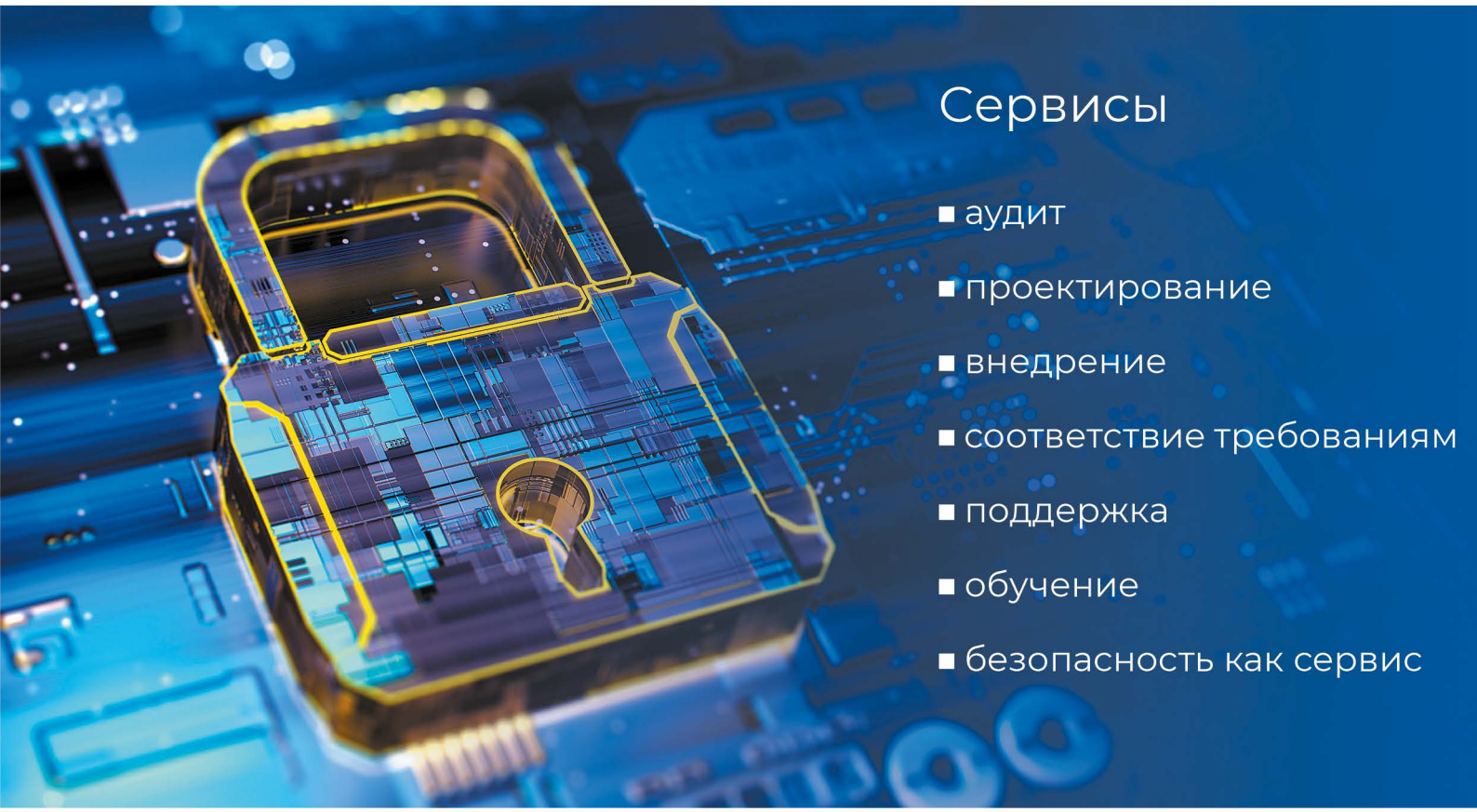
В докладе, который Gartner выпустила 28 марта 2023 года, анализируются главные тенденции рынка кибербезопасности, а также влияние на них макроэкономической ситуации и развития технологий.

Восемь прогнозов по кибербезопасности на ближайшие годы:

1. К 2027 году 50% директоров по информационной безопасности внедрят в свои программы киберзащиты методы, которые ориентированы на сотрудников. Согласно опросу Gartner более 90% работников, которые признались в совершении потенциально опасных для ИТ-инфраструктуры бизнеса операций, знали, что их действия повысят риск для организации. В связи с этим бизнесу понадобятся новые подходы к обеспечению информационной безопасности.
2. В 2024 году регулирование конфиденциальности будет охватывать основную часть данных о клиентах. Однако менее 10% организаций смогут успешно использовать средства обеспечения конфиденциальности в качестве конкурентного преимущества.
3. К 2026 году 10% крупных организаций будут иметь сформированную инфраструктуру нулевого доверия. Для сравнения, на начало 2023 года этот показатель составляет менее 1%.
4. В 2027 году примерно 75% сотрудников компаний будут приобретать, модифицировать или создавать различные технологии вне поля зрения ИТ-отдела. В 2022-м значение равнялось 41%, и, учитывая тенденцию к росту, бизнесу придется переоценить нынешнюю модель взаимодействия с сотрудниками в плане обеспечения их информационными технологиями.
5. К 2025-му 50% лидеров в сфере кибербезопасности безуспешно попытаются использовать количественную оценку киберрисков для принятия корпоративных решений.
6. В 2025 году почти половина руководителей в области кибербезопасности сменит место работы. 25% из них сменит работу из-за стресса, связанного с профессиональной деятельностью. Компании должны помнить о данном факторе, учитывая недостаток квалифицированных кадров в этой сфере на рынке труда.
7. К 2026 году в 70% компаний в состав совета директоров войдет один член с опытом работы в области кибербезопасности.
8. В 2026 году более 60% средств обнаружения, расследования и реагирования на инциденты будут использовать данные управления рисками для проверки и приоритизации обнаруженных угроз.

Если вам нужна профессиональная консультация по обеспечению информационной безопасности в вашей компании, можете обращаться **к специалистам Noventiq Belarus** по телефону **+375 17 336 55 95** или электронной почте **belarus@noventiq.com**

Компания Noventiq Belarus — лидер в сфере кибербезопасности Республики Беларусь!



Сервисы

- аудит
- проектирование
- внедрение
- соответствие требованиям
- поддержка
- обучение
- безопасность как сервис

- Защита онлайн-сервисов
- Защита инфраструктуры
- Защита веб и почты
- Защита от направленных атак
- Безопасность промышленных систем
- Обеспечение соответствия требованиям
- Защита данных
- Защита от мошенничества
- Защита сети
- Управление доступом

kaspersky

КОМПАНИЯ ИНДИД

INFOWATCH

UserGate

CTRLHACK

NOVENTIQ
Global expertise, local outcomes

КАРТА РЕШЕНИ
ИНФОРМАЦИОННО

Аудит — комплекс проверки компании на соответствие законодательству РБ, международным стандартам и внутренней политике компании.

Active Platform — платформа управления облачными сервисами.

AntiDDOS — обеспечение доступности веб-ресурсов, защита от атак типа DDOS.

Anti-Fraud — выявление и предотвращение мошеннических операций.

Awareness — повышение осведомленности сотрудников. компании в области ИБ.

Change Auditor — аудит изменений подсистем инфраструктуры.

DAG — контроль и управление доступом к неструктурированным данным.

DAM/DBF — защита баз данных.

DevSecOps — безопасная разработка. Разработка с учетом ИБ.

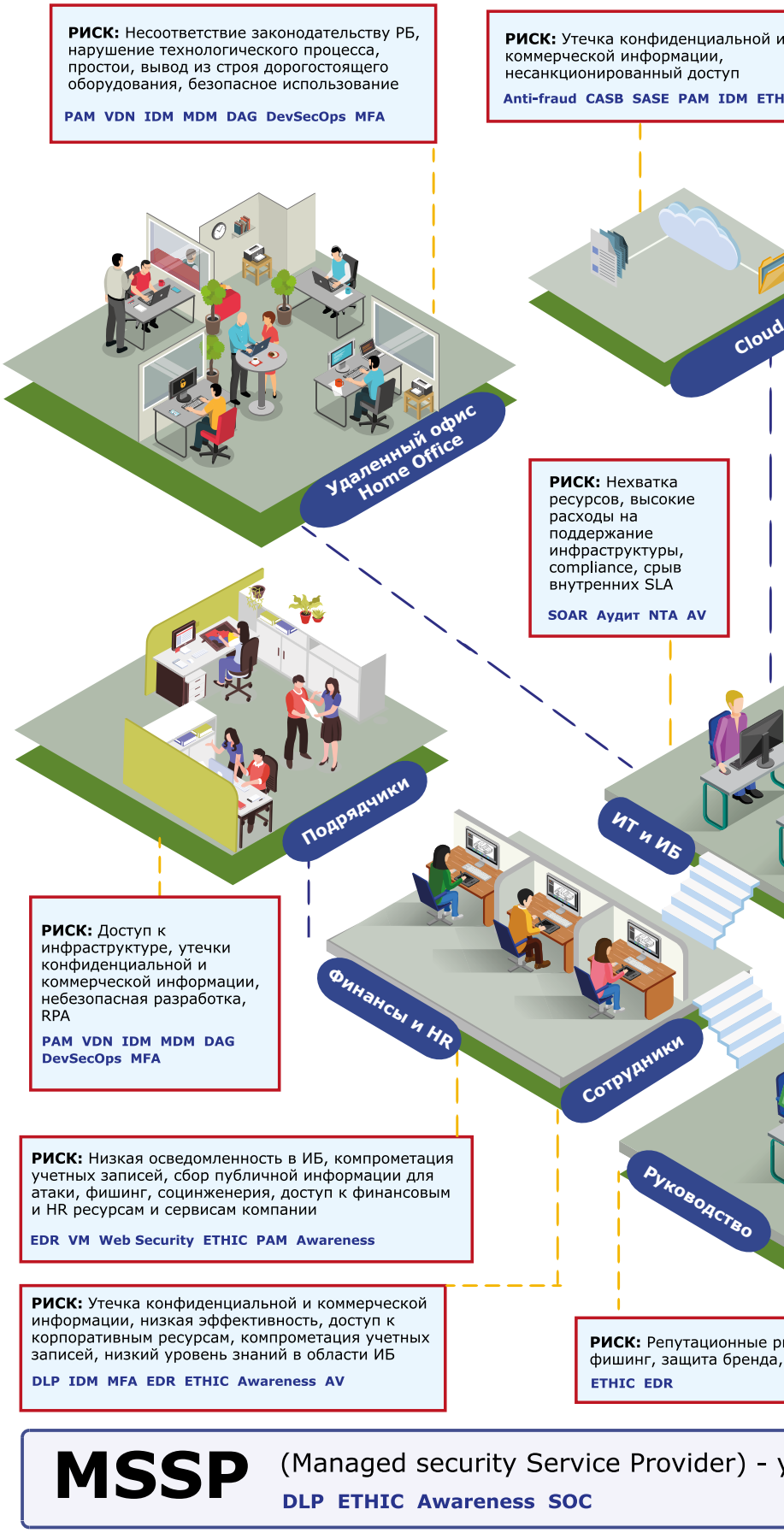
DLP — предотвращение утечек конфиденциальной информации.

EDR — обнаружение и расследование сложных угроз на конечных точках.

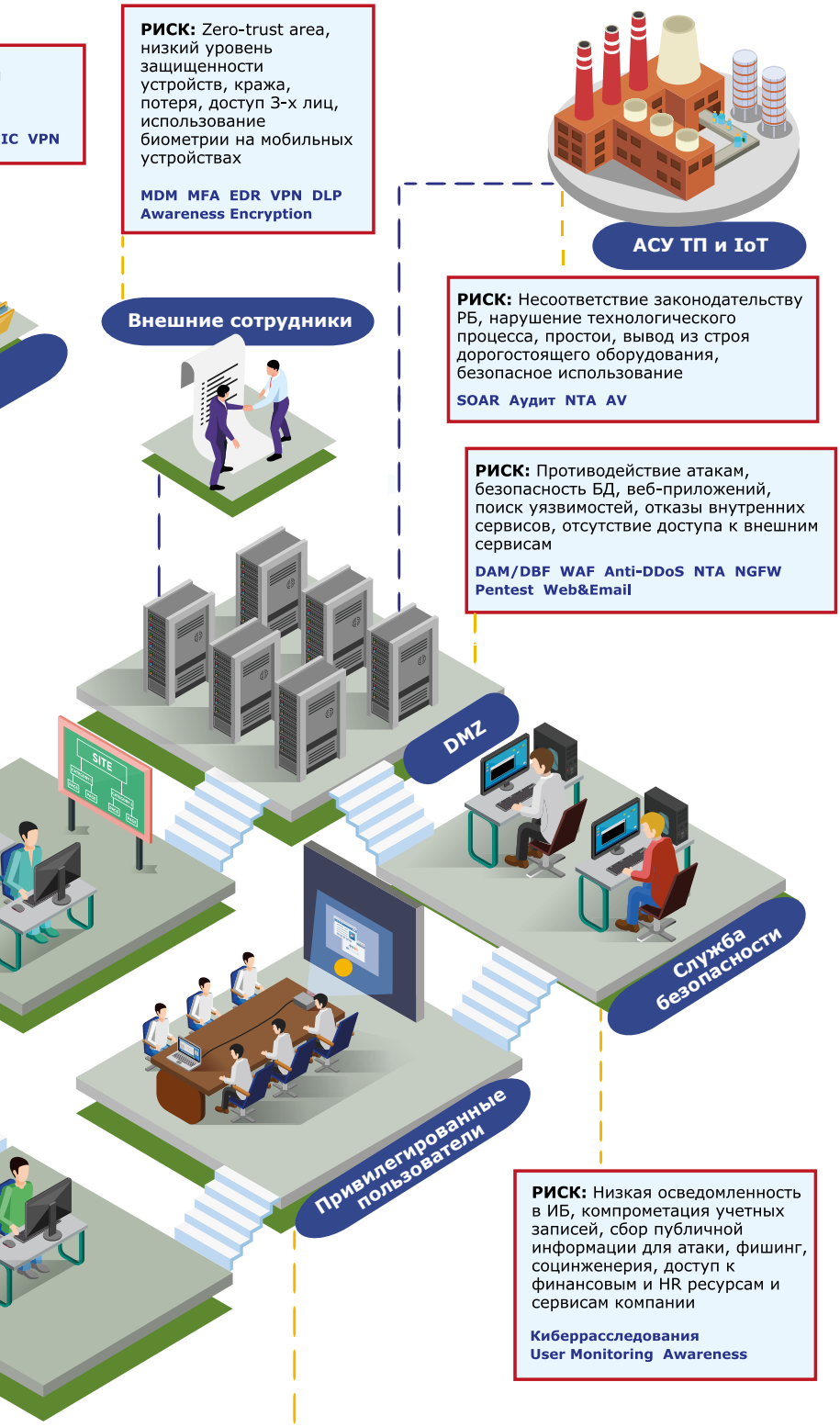
ETHIC — предотвращение нелегальных схем и махинаций с конфиденциальными данными.

IDM — управление доступом.

IRP — автоматизация процесса мониторинга, учета, реагирования на инциденты ИБ.



ЙИ И СЕРВИСОВ
ОЙ БЕЗОПАСНОСТИ



управляемые сервисы информационной безопасности.

MDM — управление безопасностью мобильных устройств.

MFA — многофакторная аутентификация.

NAC — контроль доступа к сети.

NGFW — межсетевые экраны, включающие в себя дополнительные функции — от IPS до NTA.

NTA — анализ сетевого трафика на периметре и внутри инфраструктуры.

PAM — контроль привилегированных пользователей.

Pentest — тест на проникновение в информационную систему.

SIEM — сбор и анализ событий информационной безопасности.

SL Finance — финансовый продукт Softline Belarus по рассрочке ИТ/ИБ услуг и сервисов.

SOAR — автоматизация, оркестрация и реагирование на инциденты ИБ.

SOC — центр мониторинга и реагирования на инциденты информационной безопасности.

VM — управление уязвимостями инфраструктуры.

VPN — построение защищенных каналов связи.

WAF — обнаружение и блокировка атак на веб-приложения.

Web&Email Security — мониторинг входящего трафика на наличие вредоносных вложений.

SOC. В авангарде борьбы с киберпреступниками

В данный момент Noventiq Belarus ведет работы по созданию и запуску собственного Security Operations Center. В нашем материале мы расскажем, что это за структура, какие функции выполняет и как может помочь в обеспечении безопасности бизнеса.

Что такое SOC

SOC — это аббревиатура от английского наименования Security Operations Center. В дословном переводе она обозначает «Центр операций по безопасности». Также в англоязычных источниках иногда используют другое название — CyberSecurity Operations Center (Центр операций по кибербезопасности).

На русском языке можно встретить другие названия SOC: Центр информационной безопасности, либо Ситуационный центр информационной безопасности, Центр мониторинга кибербезопасности, Центр обеспечения компьютерной безопасности. 14 февраля 2023 года был подписан Указ Президента Республики Беларусь № 40 «О кибербезопасности», в котором SOC получил определение как «Центр кибербезопасности».

В бытовом общении для простоты специалисты называют Security Operations Center еще проще — СОК (на русском языке).

Несмотря на разнообразие названий, они обозначают одно и то же: Security Operations Center — это структурное подразделение, которое непрерывно ведет мониторинг работы систем защиты информации и оперативно реагирует на все инциденты информационной безопасности. Занимаются этим специалисты по информационной безопасности. Основная задача Security Operations Center — быстрое реагирование на любые инциденты.

Кроме того, SOC — это не только технические системы, но и люди-эксперты, которые могут отличить ложное срабатывание защитного средства от настоящего и способны понять, являются ли несколько явно не связанных между собой сообщений от средств защиты звеньями одной цепи, означающей, являются ли инцидентом несколько явно не связанных между собой сообщений от источников событий.

Зачем нужен SOC?

Главный вопрос, который задают многие руководители организаций и ИТ-департаментов, — зачем нужен SOC, если в компании и так есть все средства для информационной защиты: антивирус, файервол, песочница и т. д. Мы выделили несколько основных причин.

- **Многие угрозы информационной безопасности нельзя обнаружить стандартными средствами**

Опытные хакеры никогда не пойдут на приступ защищенного периметра. Они всегда проводят разведку и ищут бреши в защите. Это могут быть уязвимости в операционной системе, в софте по информационной безопасности или в плохо обученных сотрудниках. И когда такая лазейка найдена, преступник проводит атаку. Тот же антивирус или файервол может не увидеть такую атаку или просто предупредить пользователя о подозрительных действиях. Как итог — хакер, воспользовавшись уязвимостью, получает доступ к корпоративной сети.

SOC в работе не опирается на показатели каких-то конкретных решений по ИБ, а нализирует всю ситуацию в целом. Специалисты по информационной безопасности фиксируют и отслеживают любые подозрительные действия или активности. Например, слишком большое количество измененных или удаленных файлов за короткий промежуток времени, нетипичный интернет-трафик, большое потребление ресурсов отдельными программами, отправка файлов больших объемов за пределы компании и прочие. Любой такой инцидент немедленно пресекается и проводится расследование его легитимности.

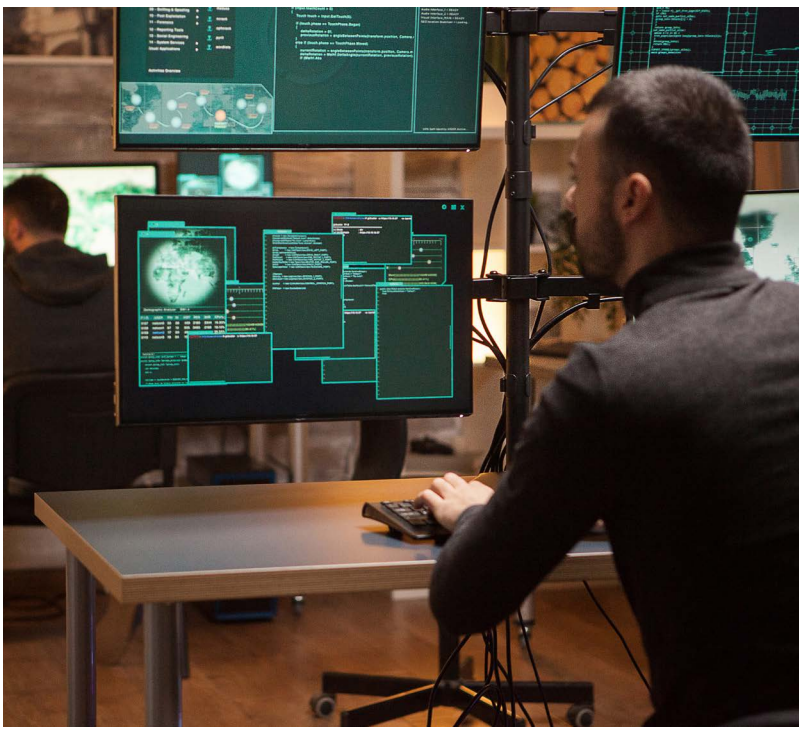
- **Скорость реакции**

При обнаружении и расследовании инцидентов ключевую роль играет скорость, с которой система отреагировала на атаку. Так, в первом примере пользователь может даже не заметить уведомления антивируса либо закроет его, не прочитав. Также специалист ограничен 8-часовым рабочим днем и может не увидеть инцидента, который произошел в его нерабочее время. А в это время вирус будет шифровать все новые файлы компании.

Специалисты SOC работают 24 часа 7 дней в неделю и на любую подозрительную активность реагируют практически мгновенно и пресекают любые подозрительные действия.

- **Слабая защита от атак изнутри**

Большинство средств по информационной безопасности, которые приобретают белорусские компании, защищают периметр от атак извне. В то же время, если в компании работает недобросовестный сотрудник, он может легко обойти эту защиту и совершить атаку изнутри компании — например, загрузить вредонос на рабочую станцию с правами администратора либо скачать и вынести из компании базу клиентов. И хотя для противодействия таким атакам есть DLP- и PAM-решения, они имеются и правильно настроены далеко не у всех клиентов.



В этом случае SOC анализирует любую подозрительную активность, вне зависимости от того, происходит она снаружи или внутри периметра.

- **Соответствие нормам законодательства**

Последняя в нашем списке, но точно не последняя по важности причина. Указ № 40 «О кибербезопасности» описывает ряд организаций, которые обязаны иметь Центр кибербезопасности.

Кто работает в SOC?

Сотрудники SOC находятся в авангарде борьбы с киберпреступниками. Для работы в таких центрах отбирают лишь самых опытных и лучших экспертов в своем деле. Многие из специальностей, о которых вы прочтете ниже, довольно экзотические для нашей страны, поэтому такие сотрудники высоко ценятся на рынке труда.

Отметим, что указанный здесь список специалистов примерный и может различаться в силу специфики задач Центра кибербезопасности. Также некоторые специалисты могут совмещать сразу несколько должностей.

Системный администратор (инженер) — специалист, который занимается настройкой систем SOC и отвечает за стабильность получения данных из систем компании-заказчика.

Специалист по настройке правил — сотрудник, который совместно с представителями заказчика составляет правила выявления и реагирования на инциденты (для SIEM, SOAR, IRP). Например, это правила корреляции в системах SIEM, правила автоматического реагирования, локализации и восстановления информационных систем при помощи SOAR- и IRP-решений. Также при необходимости данный специалист создает сигнатуры для антивирусов и систем обнаружения вторжений.

Аналитик — специалист, который осуществляет обработку инцидентов. Выделяют аналитиков 1-го и 2-го уровней. Аналитики 1-го уровня проводят «триаж» — распределение и отсев ложных срабатываний систем (False Positive срабатывания). В своих действиях аналитики 1-го уровня руководствуются прописанными сценариями реагирования. Если он не может самостоятельно справиться с инцидентом, тот переходит к аналитику 2-го уровня. Этот сотрудник не руководствуется сценариями, а анализирует ситуацию в целом, сопоставляя различные события в системе и факты, которые имеют отношение к инциденту. При этом он опирается на свой опыт. Если было использовано неизвестное вредоносное ПО или аналитик 2-го уровня не может установить причину инцидента, он отправляется еще дальше — к специалисту по реверс-инжинирингу либо форензик-эксперту.

Специалист по реверс-инжинирингу — эксперт высшей категории, как правило, профессиональный программист, который занимается изучением образцов вредоносного программного кода для противодействия кибератакам. Его задача — понять, что делает вирус, как он устроен и, как следствие, как можно ему противостоять. Для этого проводится тестовый запуск вируса в песочнице и анализируется его поведение, а также код.

Форензик-эксперт — специалист по компьютерной криминалистике. Он расследует атаку, прослеживает ее путь — с какого компьютера или узла она началась, как дальше продвигалась по ИТ-инфраструктуре, какие узлы были атакованы. Это позволяет четко понимать, какие файлы были заражены, повреждены или уничтожены в ходе атаки. Так можно легко оценить нанесенный ущерб, а если атака проводилась изнутри компании, форензик-эксперт сможет установить виновного.

Специалист по кибербразведке — эксперт, который работает на опережение. Он постоянно актуализирует информацию о новых угрозах на специализированных ресурсах, в том числе в даркнете, ищет информацию об уязвимостях заказчика или готовящихся на него атаках. Также он постоянно мониторит ИТ-инфраструктуру на наличие в ней скрытых угроз, незакрытых уязвимостей или затаившихся вирусах, которые могут быть активированы при определенном стечении обстоятельств (например, в определенную дату или при определенных действиях пользователей).

Менеджер SOC — сотрудник, который координирует работу Центра безопасности, а также взаимодействует с бизнес-представителями заказчика, выполняет организационную работу. Можно сказать, что он является лицом SOC.

Создать свой или воспользоваться чужим?

Центры информационной безопасности могут быть внутренними и внешними. То есть компания либо самостоятельно создает такой центр, либо отдает его задачи на аутсорсинг.

Внутренний SOC — это масштабный и дорогой проект, на проектирование, создание и аттестацию которого может уйти много месяцев. Кроме того, в компании всегда должны работать высококвалифицированные эксперты по информационной безопасности (примерный список мы перечислили выше), которые могут не только обнаруживать инциденты исходя из своего опыта, но и расследовать их. Заработная плата таких специалистов также составляет существенную сумму, которая ложится в бюджет бизнеса. И это не говоря уже о необходимости постоянной технической поддержки аппаратного обеспечения и его своевременной модернизации.

Учитывая вышесказанное, создание внутреннего SOC будет в первую очередь интересно высокобюджетным организациям с критически важной архитектурой, которые по тем или иным причинам не могут передать данную задачу на аутсорсинг.

Внешний SOC — это аутсорсинговая услуга, которую заказчику оказывает сторонняя компания, уже имеющая собственный SOC и штат необходимых специалистов. Они выполняют работу по реагированию на кибератаки, выявлению и расследованию инцидентов информационной безопасности в соответствии с оговоренными SLA. ■

Если вам необходима консультация по созданию SOC в вашей компании или вы ищете надежного партнера по информационной безопасности, обращайтесь к нашим специалистам по телефону **+375 17 336 55 95** или электронной почте **belarus@noventiq.com**

PDM-системы. Что это и зачем они нужны промышленному предприятию

PDM-система — это, по сути, автоматизированная база данных, в которой хранится информация обо всех изделиях, которые выпускает предприятие. Такие решения применяются в машиностроительной, авиационной, приборостроительной и других сферах промышленности — везде, где имеется большая номенклатура выпускаемых деталей и изделий. При этом, однако, в Беларуси PDM-системы до сих пор довольно слабо распространены. В основном это связано с тем, что многие руководители компаний предпочитают использовать более привычные системы хранения информации и не видят практической пользы во внедрении современных решений.

О том, что такое PDM-система, зачем она нужна предприятию и как проходит этап ее внедрения, рассказывает ведущий специалист по сопровождению программного обеспечения Noventiq Belarus **Виталий Каравай**.

Что такое PDM-системы и зачем они нужны

PDM (Product Data Management — управление данными об изделии) — это организационно-техническая система, которая позволяет управлять и хранить всю информацию об изделии. В частности — физические характеристики, материал изготовления и иные свойства. Ее внедрение позволяет:

- с высокой точностью определять объем работ и требуемое количество ресурсов;
- обеспечить параллельную работу сотрудников над одним проектом;

- использовать единое хранилище информации обо всех изделиях;
- увеличить эффективность планирования;
- уменьшить время на поиск информации;
- сократить время подготовки производства нового изделия;
- перейти на безбумажные технологии проектирования;
- повысить качество проектных работ и документации;
- унифицировать расчеты и документацию;
- упростить процесс сертификации качества изделий.

Конкретные показатели экономии времени/средств зависят от специфики производства. Мы готовы сделать для вас индивидуальную презентацию решения с его подробным анализом для вашего предприятия.

PDM-системы отлично интегрируются с решениями другого класса — ERP, CAD, CAE, Office и другими. Это значительно экономит время на разработку и проектирование новых изделий, а также на доработку существующих.

Основные функциональные возможности PDM-систем

- **Управление проектами**

Процессы согласования изделий, внесения правок и повторного согласования обычно отнимают много времени. В большинстве компаний они выстроены по устаревшей схеме, когда буквально каждое изделие согласуется с несколькими руководителями. Многие этапы проходят скорее формально.

PDM-системы позволяют выстроить процесс управления проектом, лишить его формализма и значительно ускорить все этапы согласования. Учитывая, что он проходит в электронном, а не бумажном виде, исполнитель получает уведомление о согласовании или внесении корректировок сразу.

- **Совместная работа**

На большинстве белорусских предприятий работает последовательная система внесения изменений. То есть вначале с изделием работает один отдел, затем он передает его следующему и т. д. Такая система досталась в наследство со времен бумажных чертежей, когда проект приходилось буквально переносить на ватмане в разные отделы.

Совместная работа значительно сокращает сроки проектирования. Хотя это и требует значительных изменений в организационной структуре компании, но есть одно условие: это работает при соблюдении правил «совместной игры» со всеми вытекающими требованиями к организации работы, дисциплине и уровню образования персонала.

- **Внесение изменений**

Актуальный состав изделия и данные о его параметрах — основа информационной системы предприятия. И пока в организации не научатся формировать и управлять составами изделий и документами в электронном виде, все другие задачи — технологической подготовки производства, планирования производства — эффективно решать нельзя.

На любом промышленном предприятии выпускается большое количество извещений об изменениях, а если организация существует давно, то вся деятельность конструктора сводится к изменению ранее разработанной документации. Для поддержания электронного архива в актуальном состоянии управлять изменениями необходимо, иначе электронный архив превратится в склад файлов с непонятным статусом.

- **Архив**

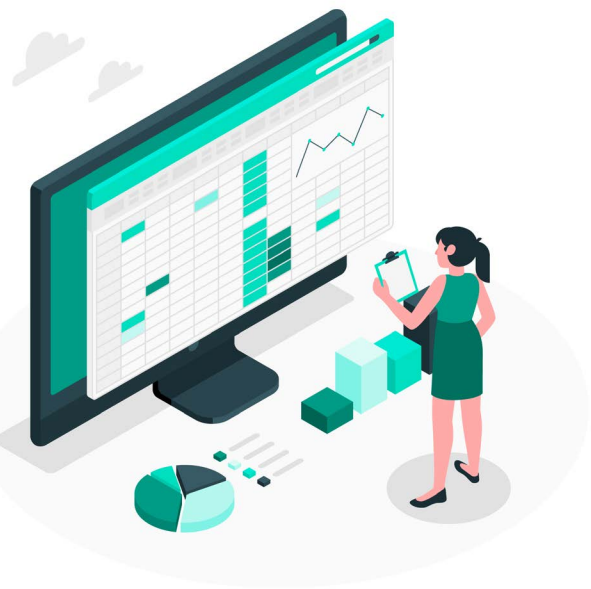
Любая PDM-система максимально эффективна при электронном документообороте, когда все документы в базе данных. Сегодня большинство промышленных предприятий работает с бумажным архивом, наработанным за предыдущие годы. При этом при проектировании новой продукции доля новых компонентов в его составе не превышает 30–35%. Остальные 65–70% — это узлы и детали, разработанные ранее.

PDM-система подразумевает постепенный перевод актуального бумажного архива в электронный вид. В будущем это позволит в разы сократить время на поиск и создание новой продукции.

- **Система поиска**

Конструкторы могут тратить до 10–15% рабочего времени на поиск предыдущих чертежей или их аналогов в системе. И чем больше номенклатура предприятия, тем больше на это уходит времени.

Причем зачастую конструктор не знает, что конкретно он ищет — у него может быть только косвенная информация. И PDM-системы в силу своей универсальности предлагают выход из такой ситуации: поскольку предметная область заранее неизвестна, в них есть возможность искать объекты по дополнительным параметрам.



Как выбрать PDM-систему

На первом этапе выбора конкретной PDM-системы и модулей, которые в нее входят, необходимо определиться с ее функциональными возможностями: расчет норм расходов материалов, расчет трудозатрат по изделию, выпуск документации на разработку, управление изменениями и другие. В этом вопросе следует исходить из целей предприятия и возможностей по внедрению технологий данного типа и их интеграции с системами, которые уже задействованы на производстве.

Для этого PDM-система должна обладать достаточной гибкостью. Функциональные возможности любой информационной системы ограничены, поэтому нужно определить бизнес-процессы, которые должны поддерживаться интеграцией, и уже на основе этого строить регламент взаимодействия систем в новых условиях с закреплением его в нормативных документах предприятия.

Еще один важный момент при выборе PDM — наличие детальной технической документации либо специалистов, которые помогут с ее освоением.

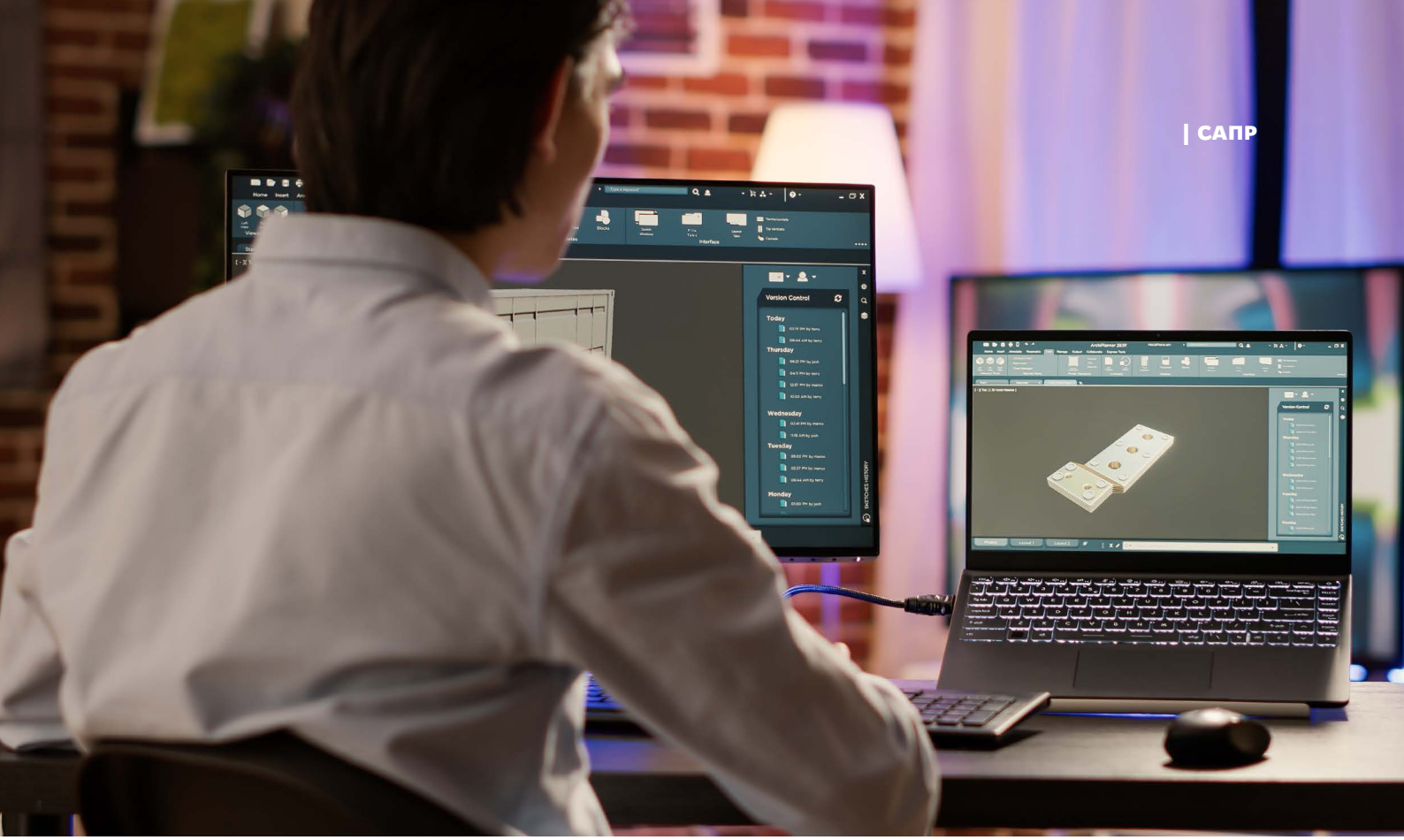
Внедрение PDM

Для внедрения PDM недостаточно просто приобрести и инсталлировать систему. Ее адаптация и интеграция затрагивает многие подразделения предприятия, меняются методы работы, возникают новые схемы взаимодействия специалистов. Фактически происходит полная трансформация всех процессов, которые завязаны на изготовлении продукции.

Для проведения всех этих работ самостоятельно предприятию необходимо нанять команду квалифицированных специалистов. Но в большинстве случаев гораздо выгоднее будет отдать эту работу своим партнерам — компании, которая будет поставлять решение, обучать сотрудников предприятия, запускать пилотные проекты и интегрировать PDM с остальными системами.

В общих чертах процесс внедрения PDM-систем нашей компанией происходит следующим образом:

- **Анализ и оценка систем предприятия.** Наши сотрудники анализируют решения, используемые в данный момент сотрудниками предприятия, а также информацию, которая в них хранится и которую необходимо перенести в PDM.
- **Составление графика внедрения с указанием всех этапов и необходимого для их завершения времени.** Итоговый график согласовывается с предприятием-заказчиком. Это необходимо, чтобы обе стороны понимали объем работ и сложности, которые могут возникнуть в процессе внедрения.
- **Обучение специалистов заказчика.** Это теоретические занятия, которые будут проходить на базе клиента. В этой части наши эксперты рассказывают в целом о PDM-системе, ее функциональных особенностях, показывают примеры работы с ней.
- **Внедрение и интеграция PDM.** Этот этап идет параллельно с обучением сотрудников. Сроки его исполнения зависят от номенклатуры предприятия, а также систем, с которыми работают сотрудники.



- **Запуск пилотного проекта.** К этому моменту сотрудники уже прошли обучение, а PDM-система внедрена на предприятии. Очень важный этап, который помогает определиться с проблемами, возникающими в системе, и вовремя их исправить.
- **Техническая поддержка.** После завершения всех этапов Noventiq Belarus продолжает оказывать заказчику консультационную помощь в работе с новыми решениями.

Интеграция CAD-, CAM- ERP и PDM-систем проводится на уровне управления всей содержательной и атрибутивной информацией и всеми связанными данными. Это позволяет создать на предприятии единую информационную базу по проектированию и подготовке производства. Когда эти работы будут завершены, любая информация по изделиям будет заводиться один раз, после чего станет доступна для всех информационных систем предприятия.

Важный этап запуска PDM — пилотные проекты. Они позволяют правильно выстроить все процессы, детально проработать функционал системы. Необходимо запустить пилот на реальном изделии, которое производится на предприятии, т. к. любые посторонние изделия не дадут полного представления обо всех особенностях работы в системе.

Второй важный момент при осуществлении пилота — сроки. Они не должны жестко ограничиваться планами производства. То есть в проработку необходимо брать изделия, которые уже изготавливаются на производстве по старым схемам. Таким образом, конструкторы и технологи, не ограниченные жесткими временными рамками, смогут детально изучить все особенности PDM, обратят внимание на все неточности и их можно будет своевременно исправить.

Что касается длительности проекта, то здесь опять же зависит от масштабов предприятия. Но в целом он рассчитан на 3–8 месяцев. Сюда входят закупка решения, обучение специалистов, пилотирование, запуск, поддержка.

Руководство должно рассматривать системы класса PDM как необходимый бизнес-инструмент, способствующий повышению конкурентоспособности и дальнейшему развитию предприятия. ■

Если вам необходима дополнительная консультация по PDM-системам и их внедрению на вашем предприятии, обращайтесь к Виталию Караваю по телефону **+375 29 808 76 76** или пишите на электронную почту **Vitaliy.Karavay@noventiq.com**

Популярные и новые курсы на русском языке

Учебный центр Noventiq Belarus анонсирует авторские программы обучения по популярным технологиям — теперь на русском языке!

Все чаще мы получаем запросы от наших клиентов по переводу учебных программ. «Почему программа обучения на английском, ведь инструктор ведет курс на русском?» — частый вопрос наших заказчиков. Отметим, что перевод авторизованных курсов просто невозможен — материалы разработаны непосредственно вендором и защищены авторским правом.

В части авторских программ обучения ответ прост: самая актуальная информация по новым технологиям от мировых компаний появляется в первую очередь на английском языке. Технологии же очень быстро меняются. Составление авторских программ обучения на русском языке — сложный и долгий процесс. Однако такие курсы пользуются неизменным спросом, и наш учебный центр стремится предоставлять услуги, максимально соответствующие потребностям наших клиентов. Разработка курсов на русском языке по самым популярным направлениям ведется постоянно.

Представляем **3 самых востребованных практических курса**, разработанных нашим инструктором Игорем Антоновичем, с материалами на русском языке!

Основы администрирования Linux

Самый базовый и фундаментальный курс, предназначенный для пользователей и начинающих администраторов, желающих научиться развертывать и обслуживать операционные системы Linux.

В курсе рассматриваются основные принципы работы системы, базовые команды и инструменты администрирования, а также ключевые понятия, которые должен знать системный администратор.

Данный курс содержит:

- 11 лабораторных работ.
- ★ 38 практических работ, закрепляющих знания и навыки работы с системой.
- Вся среда для практических заданий разворачивается на виртуальных машинах на сервере учебного центра. Вам не требуется дополнительно устанавливать Linux или другое ПО на свой компьютер.
- ★ Учебные пособия и лабораторные работы на русском языке.

Расширенное администрирование Linux

Данная программа является продолжением обучения по Linux и предназначена для ИТ-специалистов, прошедших курс по основам администрирования.

Курс углубляется в главные навыки системного администрирования Linux в области настройки и управления хранилищем, развертывания Linux и управления функциями безопасности.

Данный курс содержит:

- 15 тем для изучения.
- ★ 32 практические работы.
- Вся среда для лабораторных работ развернута на виртуальных машинах на сервере учебного центра.
- ★ Учебные пособия и лабораторные работы на русском языке!

Администрирование баз данных SQL Server

В июне 2023 года выходит обновленная версия курса по администрированию баз данных SQL с лабораторными работами и учебником на русском языке.

Курс построен на обновленной версии Microsoft SQL Server 2019.

Обучение предоставит знания и навыки, необходимые для администрирования и сопровождения Microsoft SQL Server. Курс рассказывает об инструментах и компонентах Microsoft SQL Server, предназначенных для поддержки базы данных.

Все программы доступны в каталоге и расписании на нашем сайте **edu.noventiq.by.**

Хотите записаться на курсы?

Заходите на наш сайт **edu.noventiq.by**, знакомьтесь с расписанием и программами обучения, нажимайте «Записаться» для оформления заявки — и наши специалисты свяжутся с вами для оформления документов.

Звоните или пишите нам:

☎ Тел.: **+375 17 336 88 31**

✉ E-mail: **edu.by@noventiq.com**

Код	Название курса	Дни/часы
Курсы Windows Server		
SL-WS	Администрирование и настройка Windows Server 2016 / 2019	5 /45
SL-WSAD	Установка и настройка Active Directory средствами Windows Server 2016	5 /40
SL-WSS	Обеспечение безопасности Windows Server 2016 / 2019	5 /40
SL-PS	Автоматизация администрирования с использованием Windows PowerShell	5 /40
55318	Расширенная автоматизация администрирования с Windows PowerShell	3 /24
MS-PKI	Установка и настройка центра сертификации в Windows Server 2016	3 /24
SL-RDS	Установка и конфигурирование служб удаленных рабочих столов	2 /16
SL-IIS	Администрирование роли Веб Сервер (IIS) в Windows Server	5 /40
Курсы SQL Server		
DP-080T00	Создание запросов при помощи Transact-SQL	2/16
SL-TSQL	Создание Transact-SQL-запросов	5 /40
SL-ASQL	Администрирование баз данных SQL Server	5 /40
SL-DSQL	Разработка баз данных SQL	5 /40
SL-PTSQL	Настройка производительности и оптимизация баз данных SQL	4 /32
55246	Настройка высокой доступности SQL Server 2016	3 /24
Курсы Power Platform		
PL-900T00	Основы Microsoft Power Platform	1 /8
PL-100T00	Конструктор приложений Microsoft Power Platform	3 /24
PL-300T00	Аналитик данных Microsoft Power BI	3 /24
PL-400T00	Разработчик Microsoft Power Platform	5 /40
PL-500T00	Microsoft Power Automate RPA Developer	4 /32
Курсы Microsoft 365		
SC-900T00	Основы безопасности, соответствия и идентификации Microsoft	1 /8
MD-102T00	Microsoft 365 Endpoint администратор	5 /40
MS-900T01	Основы Microsoft 365	1 /8
55354	Администратор Office 365	5 /40
MS-100T00	Службы идентификации и сервисы Microsoft 365	5 /40
MS-101T00	Мобильность и безопасность Microsoft 365	5 /40
MS-203T00	Обмен сообщениями Microsoft 365	5 /40
MS-500T00	Администратор безопасности Microsoft 365	4 /32
MS-700T00	Управление Microsoft Teams	4 /32
Курсы Exchange Server | Skype for business		
SL-EXCH1	Администрирование Microsoft Exchange Server 2016 / 2019	5 /40
SL-EXCH2	Проектирование и развертывание Microsoft Exchange Server 2016 / 2019	5 /40
Курсы Endpoint Configuration Manager (System Center)		
55348	Администрирование Microsoft Endpoint Configuration Manager	5 /40
Курсы Azure		
AZ-900T00	Основы Microsoft Azure	2 /16
AZ-104T00	Администратор Microsoft Azure	4 /32
AZ-120T00	Планирование и администрирование Microsoft Azure для рабочих нагрузок SAP	4 /32
AZ-140T00	Настройка и работа с виртуальным рабочим столом в Microsoft Azure	4 /32
AZ-204T00	Разработка решений для Microsoft Azure	5 /40
AZ-220T00	Microsoft Azure IoT Разработчик	4 /32
AZ-303T00	Microsoft Azure для архитекторов	5 /40
AZ-400T00	Планирование и внедрение решений Microsoft DevOps	5 /40
AZ-500T00	Технологии безопасности в Microsoft Azure	4 /32
DP-300T00	Администрирование реляционных баз данных в Microsoft Azure	4 /32
SC-200T00	Аналитик по безопасности Microsoft	4 /32
Курсы Microsoft Project		
Project	Управление проектами с помощью Microsoft Project	3 /24
Project Server	Бизнес-настройка Project Server 2013 / 2016	2 /16

Код	Название курса	Дни/часы
Project Server (рук)	Использование Microsoft Project Server руководителями проектов	1 /8
Project Server (исп)	Использование Microsoft Project Server исполнителями проектных задач	1 /4
Курсы Microsoft Office		
Excel-Base	Базовый курс по Microsoft Excel	2 /16
Excel-Adv	Углубленный курс по Microsoft Excel	3 /24
BI-Excel-Adv	Бизнес-аналитика средствами Microsoft Excel, Power BI и Power BI Desktop	4 /32
BI-MS	Бизнес-аналитика с помощью Power BI Desktop, сервиса Power BI, DAX и Power Query	6 /48
PowerQuery	Извлечение и трансформация данных с помощью Power Query / Get and Transform	2 /16
PowerBI-MD	Моделирование данных в Power BI	1 /8
VBA-Excel	Программирование на VBA для Microsoft Excel	4 /32
O365	Использование Office 365	3 /24
Access	Работа в СУБД Microsoft Access	3 /24
PowerPoint	Создание презентаций в Microsoft PowerPoint 2016	2 /16
Oracle		
12cSQL_PLSQL	Основы работы с Oracle SQL и PL/SQL	5 /40
19cPLSQL	Oracle Database 19c: PL/SQL Workshop	5 /40
19cTSQL	Oracle Database 19c: SQL Tuning for Developers	4 /32
12cDPU	Oracle Database 12c: Разработка программных модулей на PL/SQL	3 /24
PostgreSQL		
PostgreSQL-A	Администрирование сервера базы данных PostgreSQL, развертывание и использование приложений, трехзвенная архитектура	5 /40
PostgreSQL-D	Разработка и настройка SQL-запросов и приложений для сервера базы данных PostgreSQL	5 /40
PostgreSQL-M	Миграция базы данных Oracle в Postgresql для администраторов и разработчиков	5 /40
Курсы Linux | Unix		
SL-Linux	Основы администрирования Linux	5 /45
SL-Linux-Adv	Расширенное администрирование Linux	5 /40
LL-103	Сетевое администрирование Linux	4 /32
LL-104	Основы разработки shell-сценариев для командного интерпретатора BASH	3 /24
LL-105	Автоматизация администрирования Linux	4 /32
Zimbra	Администрирование Zimbra	4 /32
Solaris	Системное администрирование Solaris 11	5 /40
Курсы Astra Linux		
AL-1701	Astra Linux 1.7 для пользователей	2 /16
AL-1702	Администрирование Astra Linux 1.7	4 /32
AL-1703	Расширенное администрирование Astra Linux 1.7	5 /40
AL-1704	Сетевое администрирование ОС Astra Linux Special Edition 1.7	5 /40
AL-1705	Безопасность в ОС Astra Linux Special Edition 1.7	5 /40
BR-2901	Практический курс по работе с ПК СВ Брест	5 /40
Курсы РЕД ОС		
REDOS-101	Основы администрирования РЕД ОС	4 /32
REDOS-102	Системное администрирование РЕД ОС 7	4 /32
Курсы ALT Linux		
ALTADM1	Администрирование ОС Альт. Часть 1	5 /40
ALTADM2	Администрирование ОС Альт. Часть 2	3 /24
VMware		
SL-VSICM	Установка, настройка, управление vSphere V7.0	5 /40
SL-VSOS	Оптимизация и масштабирование vSphere V7.0	5 /40
SL-NSXT	Установка и администрирование NSX-T в центре обработки данных	5 /40
SL-VHDM	Развертывание и управление Horizon 8	5 /40
SL-vSAN	Планирование и развертывание, управление и эксплуатация, устранение неполадок vSAN	7 /56
SL-VROICM	Установка, настройка и использование vRealize Operations	5 /40
SL-VCDICM	Установка, настройка, управление vCloud Director	5 /40

Код	Название курса	Дни/часы
Лаборатория Касперского		
KL 002.11.6	Kaspersky Endpoint Security and Management. Базовый курс	3 /24
KL 302.11	Kaspersky Security Center. Масштабирование	3 /24
KL 009.12	Kaspersky Security Center. Управление системами	1 /10
KL 008.11.6	Kaspersky Endpoint Security. Шифрование	1 /8
KL 302.11K	Kaspersky Security Center. Масштабирование и управление системами (комплексный курс)	4 /32
KL 025.4	Kaspersky Anti Targeted Attack Platform, Kaspersky Endpoint Detection and Response	2 /16
KL 034.2.1	Kaspersky Unified Monitoring and Analysis Platform	3 /24
KL 005.11	Защита серверов Windows и встраиваемых систем	2 /16
KL 031.51	Kaspersky Security для виртуальных сред. Легкий агент	1 /8
KL 014.50	Kaspersky Security для виртуальных сред 5.0 Защита без агента	1 /8
Autodesk		
RevMep	Проектирование инженерных систем в Autodesk Revit	5 /40
RevDesign	Autodesk Revit для дизайнеров интерьеров	20 /40
RevArh	Базовый курс Autodesk Revit для архитектора	5 /40
RevStr	Проектирование строительных конструкций в Autodesk Revit	5 /40
Civ3d	Autodesk Civil 3D 2021	5 /40
Ainventor	Autodesk Inventor Professional 2021	5 /40
Anavisworks	Базовый курс Autodesk Navisworks	5 /40
AFusion360	Autodesk Fusion 360	5 /40
Check Point		
CCSA-R81.10	Управление безопасностью средствами Check Point R81.10	3 /24
CCSE-R81.10	Проектирование безопасности средствами Check Point R81.10	3 /24
CCTA-R81.10	Сертифицированный администратор по поиску и устранению неисправностей Check Point	2 /16
CCTE-R81.10	Сертифицированный эксперт по поиску и устранению неисправностей Check Point	2 /16
CCES	Специалист по обеспечению безопасности рабочих станций с помощью Check Point	2 /16
CommuniGate Pro		
CP-02	Администрирование платформы унифицированных коммуникаций CommuniGate Pro	3 /24
CP-03	Продвинутое администрирование CommuniGate Pro	5 /40
CP-04	Практические навыки по администрированию CommuniGate Pro. Этап 1: электронная почта, календари и файловое хранилище	5 /40
Управление проектами		
PM-in-IT	**NEW!** Курс «Менеджер IT-проектов» (управление проектами в сфере разработки ПО)	20 /52
PMIT	Управление проектами в области ИТ	5 /40
IT менеджмент		
ITIL 4	Основы ITIL 4	3 /24
COBIT 2019	Основы COBIT 2019	2 /20
SLIT-889	Управление процессами и структурой предприятия с помощью ИТ	2 /16
DevOps		
DevOps	Основы DevOps методологии, платформы и инструменты реализации	5 /40
DK-Base	Основы работы с Docker и Kubernates	4 /32
Информационная безопасность		
CyberSecurity-Online	CyberSecurity Online: обеспечение кибербезопасности и защита информации в организации	5 /20
ISRM-Online	Менеджмент рисков информационной безопасности	3 /12
НПА-ЗИ	Соответствие требованиям законодательства Республики Беларусь в области защиты информации	1 /6
ISA	Аудит информационной безопасности	4 /32
EH-1	Тестирование на проникновение и анализ безопасности. Базовый уровень	9 /72

Полный каталог курсов и подробные программы обучения вы можете найти
на нашем сайте **http://edu.noventiq.by**
Получить дополнительную информацию по курсам можно
по телефону **+375 17 336 55 41** или e-mail **edu.by@noventiq.com**

Уважаемые коллеги!

Предлагаем подписаться на наш журнал, а также подписать своих коллег и бизнес-партнеров.

В журнале мы всегда даем полезную и актуальную информацию об ИТ-решениях для бизнеса:

- Как оптимизировать бизнес-процессы с помощью доступных решений?
- Как выстроить систему информационной безопасности?
- Как подобрать правильное решение в зависимости от особенностей ведения бизнеса компании?

Вы также можете предложить тему для следующего выпуска нашего журнала по электронной почте **marketing.by@noventiq.com**

Наш журнал выходит с 2007 года два раза в год. Каждый выпуск призван дать экспертные ответы и продемонстрировать успешное внедрение технологических решений в белорусских компаниях.

ДЛЯ ПОДПИСКИ:

Перейдите по QR-коду, заполните анкету и выберите удобный способ получения журнала: электронную версию на email, печатную версию на почту, оба варианта.

ООО «СофтЛайнБел» гарантирует конфиденциальность и сохранность ваших персональных данных, которые будут использоваться исключительно для рассылки журнала.

Также вы можете подписаться на журнал, отправив письмо со своими данными (ФИО, почтовый или email-адрес, название организации) на почту marketing.by@noventiq.com.

УЧЕБНЫЙ ЦЕНТР

КУРСЫ

- Microsoft
- Kaspersky Lab
- Информационная безопасность
- 1С:Предприятие
- VMware
- Autodesk
- Solidworks
- Cisco
- Huawei
- Astra Linux
- BaseALT
- CheckPoint
- Fortinet
- Citrix
- Java
- JavaScript
- Python
- DevOps
- Oracle
- PostgreSQL
- Asterisk
- InfoWatch
- Управление проектами
- IT Management

kaspersky
Authorized Certification Center

NOVENTIQ
Global expertise, local outcomes

ЗНАНИЯ ДЛЯ РАЗВИТИЯ КАРЬЕРЫ

ИТ-КУРСЫ
ТЕСТИРОВАНИЕ
СЕРТИФИКАЦИЯ

КОНТАКТЫ

edu.by@noventiq.com
+375 17 336-88-31

edu.noventiq.by

Республика Беларусь, Минск, 220062,
пр. Победителей, 108, 4-й этаж

ГЛОБАЛЬНЫЙ ПОСТАВЩИК ИТ-РЕШЕНИЙ И СЕРВИСОВ

- Облачные решения
- Кибербезопасность
- Инфраструктура
- Бизнес-решения
- Техническая поддержка
- САПР и ГИС
- Учебный центр

+375 17 336 55 95 | noventiq.by