Круглый стол

Кибервойна ближайшего будущего: ждем и готовимся?

В круглом столе принимают участие

Евгений ВИЛЬТОВСКИЙ,
руководитель компании ALPEIN Software в Швейцарии

Павел ВОЛЧКОВ,
заместитель начальника отдела консалтинга Центра информационной безопасности, компания «Инфосистемы Джет»

Михаил ВОРОБЬЕВ,
начальник аналитического отдела центра разработки технологий, АО «РНТ»

Алексей ЗЕНКЕВИЧ,
руководитель подразделения «Промышленная автоматизация», компания Honeywell в России, Белоруссии и Армении

Валерий КОНЯВСКИЙ,
д. т. н., заведующий кафедрой «Защита информации» ФРТК, МФТИ (ФизТех)

Игорь КОРЧАГИН,
руководитель группы обеспечения безопасности информации, компания ИВК

Алексей НОВИКОВ,
заместитель директора центра компетенций по экспертным сервисам, Positive Technologies

Виктор СЕРДЮК,
генеральный директор АО «ДиалогНаука»

Кирилл УГОЛЕВ,
руководитель направления инфраструктурных решений ИБ, компания «Астерос»

Кибервойны – уже реальность: применение кибероружия Stuxnet, саботаж производственных предприятий при помощи разработанных спецслужбами эксплойтов, слежка за высокопоставленными лицами других государств и пр. Атмосфера в киберпространстве накаляется, поэтому мы решили обсудить с российскими экспертами современную ситуацию в сфере защиты государственных ресурсов и информационных систем.

Насколько защищены, по вашему мнению, объекты критической информационной инфраструктуры РФ? Какие ключевые проблемы и риски кибербезопасности существуют в России и чем ситуация отличается от развитых стран Запада?

Евгений ВИЛЬТОВСКИЙ

На такой вопрос сложно ответить кратко, этому посвящены многие исследования и регулярно составляются подробные отчеты. Но год за годом эксперты и аналитические компании, специализирующиеся в области информационной безопасности, отмечают одну и ту же глобальную тенденцию: количество кибератак увеличивается, они становятся все изощреннее и приводят ко все более тяжелым последствиям.

Павел ВОЛЧКОВ

Понятие «объекты критической информационной инфраструктуры» – довольно размытое. Поэтому однозначно ответить на вопрос, насколько они защищены, невозможно – в зависимости от отрасли и организации

они защищены по-разному. В целом можно сказать, что, поскольку речь идет о критической инфраструктуре, защиты не может быть много, в любом случае хотелось бы более активных шагов со стороны регуляторов. Ключевые проблемы здесь такие же, как и в других отраслях: повсеместная нехватка кадров и отсутствие четкой, понятной нормативной базы. В подобных документах должно быть минимум вариативности и неоднозначных трактовок, только четкие предписания. Основным риском является нарушение технологических процессов, которое может повлечь за собой ощутимые последствия в реальном мире (техногенные катастрофы). Можно выделить два концептуальных отличия стран Запада: более зрелый подход, обусловленный длительным развитием нормативной базы, и менее острая проблема импортозамещения.

Михаил ВОРОБЬЕВ

Очевидно: давать общую оценку защищенности объектов критической информационной инфраструктуры РФ все равно, что измерять общую температуру по больнице. Какие-то объекты защищены лучше, какие-то хуже. Мы надеемся, что в связи с принимаемыми мерами на уровне законодательства ситуация изменится, уровень защиты будет повышаться.

К ключевым проблемам в кибербезопасности мы традиционно относим недостаточно высокую квалификацию персонала, обслуживающего автоматизированные системы. Кроме того, известные риски связаны с используемым на объектах критической инфраструктуры специализированным программным и аппаратным обеспечением зарубежного производства. Часто такие продукты отвечают за ключевые функции, обеспечивающие бесперебойную работу объекта. В случае необходимости их просто нечем будет заменить, и условия их эксплуатации нередко требуют выработки дополнительных мер обеспечения безопасности. Мы предполагаем, что западные страны имеют существенно больше возможностей диктовать производителям подобных продуктов свои условия и использовать программное обеспечение в качестве доверенного.

Алексей ЗЕНКЕВИЧ

Существенное различие заключается в готовности инфраструктуры и объеме оказания услуг защиты. В России рынок оказания услуг защиты только формируется. На Западе он эволюционно складывался долгие годы в результате отношений между производителями средств автоматизации и их заказчиками, которые сначала создали рынок оказания услуг техподдержки, включая удаленную. В рамках этого рынка, в свою очередь, были созданы инфраструктура и целые системы техподдержки. Были построены глобальные центры оказания сервисов по всему миру, сформирована многочисленная клиентская база заказчиков, которые осознали эффективность перехода на сервисную модель. Сейчас продолжается развитие услуг, продуктов и инфраструктуры на существующей клиентской базе в сторону оказания услуг защиты производителями для своих заказчиков в соответствии с требованиями рынка. Возникают новые возможности для бизнеса: например, недавно Honeywell приобрела компанию Nextnine – ведущего поставщика решений для киберзащиты промышленных объектов, обладающего возможностями защищенной удаленной поддержки заказчиков. Nextnine имеет 10 тыс. активных пользователей на тысячах производственных площадок по всему миру в нефтегазовом, коммунальном, химическом, горнодобывающем и производственном секторах.

Валерий КОНЯВСКИЙ

Уязвимости современной аппаратной базы – это уязвимости, с которыми мы зачастую вынуждены мириться, хотя и знаем об их существовании. Конечно, все объекты критической инфраструктуры защищены с разными уровнями эффективности, какие-то лучше, какие-то не так хорошо. Но я считаю, что практически все информационные системы, основанные на использовании компьютеров на базе архитектуры x86, не защищены. Принципиальные уязвимости могут эффективно использовать те, кто их имплантирует в компьютеры. В этом и заключается принципиальное отличие от «развитых стран Запада», говоря языком вопроса.

Алексей НОВИКОВ

Сложно давать общую оценку защищенности всех объектов критической информационной инфраструктуры. Подобной открытой статистики для России сейчас нет. А с учетом изменений законодательства теперь

уже и не появится, так как сведения о защищенности объектов критической информационной инфраструктуры отнесены к государственной тайне. Как известно, во II квартале текущего года произошел ряд эпидемий вирусов-шифровальщиков, продемонстрировавших недостатки защищенности информационных систем. Необходимо отметить, что проблемы с защищенностью объектов критической информационной инфраструктуры есть не только в России – эта проблема характерна и для зарубежных компаний. Также идентичны и риски кибербезопасности (для России и для других стран мира). Ключевыми проблемами являются плохо выстроенные процессы обеспечения информационной безопасности и недостаточный уровень квалификации кадров: все организации в курсе, какие решения применять, как их внедрять, но с ежедневными задачами и операционной деятельностью в сфере ИБ мало кто в состоянии справиться на должном уровне.

Виктор СЕРДЮК

Было бы неправильно говорить об общем уровне защищенности объектов КИИ в России – все зависит от того, насколько правильно построен процесс обеспечения информационной безопасности на каждом конкретном предприятии. Однако можно с уверенностью сказать, что внимание к вопросам информационной безопасности со стороны организаций, которые с большой долей вероятности будут отнесены к КИИ, значительно усилилось за последние несколько лет.

Риски кибербезопасности определяются моделью угроз для каждой конкретной организации и зависят от множества факторов: наличия доступа к сети Интернет, степени территориальной распределенности, использования технологий удаленного доступа и т. д. Тем не менее в целом угрозы информационной безопасности как для российских, так и для западных компаний во многом идентичны.

Кирилл УГОЛЕВ

По моему мнению, о достаточной защищенности объектов критической информационной инфраструктуры говорить пока рано. Основная проблема – недостаточный уровень зрелости руководства, персонала и, как следствие, соответствующих ИБ-процессов, организованных в корпорациях.

Если говорить о ключевых рисках, то в первую очередь это уязвимости в программных продуктах, которые иногда успевают закрываться производителями, а иногда нет. Вспомните недавних зловредов-шифровальщиков Petya и WannaCry. С другой стороны, мало выполнить все необходимые регламенты по обновлениям. К сожалению, к апдейтам тоже стоит относиться настороженно: существуют непреднамеренные вредоносные действия, когда установка обновлений может вывести из строя всю систему. Перед массовой установкой они должны проходить проверку в тестовых средах и уже потом имплементироваться в рабочую среду. Свежий пример – история с замками американской компании LockState: производитель допустил ошибку при обновлении ПО, в результате чего сотни его смарт-устройств перестали открываться.

Ситуация в России ничем не отличается от стран Запада: у нас такие же проблемы и абсолютно те же риски, поскольку используются одни и те же решения. Нужно понимать, что чем больше на рынке ПО, тем больше уязвимостей. Когда мы закрываем одну уязвимость, это не значит, что мы не открываем другую.

Какие отрасли, ведомства или организации наиболее привлекательны для атак хакеров? Какие критически важные с точки зрения безопасности сайты, сервисы и базы данных сегодня наиболее уязвимы?

Евгений ВИЛЬТОВСКИЙ

«Кто владеет информацией, тот владеет миром», – говорил Натан Ротшильд, основатель английской ветви Ротшильдов, который успешно торговал британским текстилем и через какое-то время основал собственный банк. С тех пор глобально ничего не изменилось.

Социальные сети, мессенджеры, интернет-провайдеры – все это места, где люди наиболее открыты, а значит, уязвимы. На сегодняшний день не обязательно взламывать банковский счет для получения выгоды, для злоумышленников гораздо привлекательнее базы данных и точки входа с большим количеством пользовательской информации. Тут ее можно не только получить, но и отслеживать изменения в реальном времени. Эта информация интересна многим структурам и может быть использована для очень широкого списка целей – от маркетинга до слежки и корпоративного шпионажа.

Именно по этим причинам мы создали свой продукт для корпоративных коммуникаций в Швейцарии, стране с самыми строгими законами по защите личного пространства человека.

Павел ВОЛЧКОВ

Смотря кого мы понимаем под хакерами, какой рассматриваем мотив. Если имеются в виду лица, действующие из хулиганских побуждений, то для них привлекательны любые, главное, чтобы самые публичные, организации. Если это лица, действующие из соображений наживы, то для них привлекательны организации банковского сектора. А если в качестве хакеров рассматривать спецслужбы иных государств, то здесь наиболее интересны органы власти, объекты ТЭК, а также военные структуры.

При этом не нужно забывать о таком явлении, как «разделение труда» в киберпреступности. Часто непосредственно взломами занимаются те, кто вообще никак не мотивирован в дальнейшем развитии атаки. Их задача – пробить периметр какой-либо организации и затем продать полученный доступ. Традиционно с технической точки зрения наиболее уязвимыми являются публично доступные веб-сервисы. С учетом того, что на текущий момент сайты органов власти зачастую не просто являются сайтами-визитками, а интегрированы с внутренними сервисами, можно считать их наиболее интересными целями атак для злоумышленников.

Валерий КОНЯВСКИЙ

На недавнем XI Форуме в Гармиш-Партенкирхене обсуждался, в частности, вопрос о допустимости того или иного уровня использования информации, полученной различными способами из иностранных информационных систем. Наиболее показательным, на мой взгляд, было выступление специалиста из США. Я процитирую его по памяти, но, надеюсь, не искажу смысла: «Представим, что в США близятся выборы президента. И представим, что кто-то, например Канада, захотела вмешаться в процесс выборов и с помощью хакеров получила интересующую ее информацию. Так вот, если Канада захочет опубликовать эти материалы – это ее дело. А вот если Канада будет использовать материалы для шантажа одного из кандидатов – это уже будет расценено как вмешательство во внутренние дела».

Не знаю, как другие, я расценил смысл этих слов как предупреждение (или угрозу?), что по мере приближения выборов в информационное пространство будет выплеснуто очень много неожиданных для нас материалов. Вот поэтому, на мой взгляд, наиболее нуждающиеся в защите – это информационные системы органов государственной власти, госкорпораций, организаций кредитно-финансовой сферы.

Алексей НОВИКОВ

Наша статистика по киберугрозам за II квартал 2017 г. показывает, что две трети всех атак в этот период совершались в целях получения финансовой выгоды и еще 29% были нацелены на получение данных. Статистика говорит о том, что злоумышленники проявили повышенный интерес к частным лицам, на них (точнее, на их деньги и данные) было направлено 24% атак. До 10% атак пришлось на государственные организации, по 8% – на финансовый и образовательный секторы. К наиболее популярным методам атак относятся:

- использование вредоносного ПО – 38% (в этом случае наибольшее число атак приходится на инфраструктуру, мобильные устройства, а наибольшее количество пострадавших составляют частные лица);
- компрометация учетных данных – 16% (к числу наиболее атакуемых объектов относятся веб-ресурсы и пользователи, а наибольшее количество пострадавших приходится на долю частных лиц и государственных учреждений);
- социальная инженерия – 15% (объектами атаки чаще всего являются пользователи и инфраструктура компаний, практически половина всех пострадавших либо частные лица, либо образовательные учреждения);
- эксплуатация уязвимостей ПО – 14% (этот метод использовался чаще всего для атаки на инфраструктуру организаций, устройства Интернета вещей и мобильные устройства, около четверти всех пострадавших приходится на государственные и образовательные учреждения);
- эксплуатация веб-уязвимостей – 10% (в этих случаях объектами атаки оказывались только веб-ресурсы, более половины всех пострадавших составляют онлайн-сервисы, образовательные и финансовые организации).

При этом наиболее атакуемыми объектами являются инфраструктура и веб-ресурсы компаний (в совокупности более 60% всех атак были нацелены именно на них), продолжается рост числа атак на мобильные устройства, банкоматы и POS-терминалы (причем в большинстве случаев происходит заражение устройства вредоносным программным обеспечением).

Виктор СЕРДЮК

Выбор объекта для атаки зависит от целей, задач и мотивации конкретного злоумышленника. Например, с точки зрения извлечения прямой финансовой выгоды объектом нападения могут стать кредитно-финансовые учреждения, так как здесь злоумышленник может получить прямой доступ к денежным средствам банков и их клиентов. Если же целью злоумышленника является нарушение работоспособности объектов КИИ, то атаке могут подвергнуться АСУТП предприятий в различных секторах экономики.

Кирилл УГОЛЕВ

Да любые! Основной вопрос – в мотиве хакеров. Одно дело, когда это извлечение прибыли (WannaCry, Petya), и совсем другое, когда проводится таргетная атака, направленная, к примеру, на вывод из строя инфраструктуры завода и разрушение технологических процессов. Пример – вирус Stuxnet, который нанес серьезный урон иранской ядерной программе. Более того, существует вероятность, что некоторые вирусы оказывались причиной падения самолетов.

Мишенью для хакеров может быть все что угодно. В нашей практике был автосервис, у которого завелся вирус-шифровальщик, вымогающий деньги. Все, что разработано человеком, потенциально уязвимо.

Насколько эффективны, по вашему мнению, механизмы и технологии кибербезопасности, которые заложены/закладываются в систему ГосСОПКА? В какой мере принятый федеральный закон предоставит реальные рычаги борьбы с кибератаками?

Алексей ЗЕНКЕВИЧ

Создание системы ГосСОПКА – это необходимое условие дальнейшего развития России и ее партнеров. Создаваемая инфраструктура оказания услуг защиты (центры кибербезопасности, Security Operations Centers и другие центры) будут нуждаться в постоянном взаимодействии друг с другом, внешними партнерами и государством. Система ГосСОПКА должна взять на себя направляющие и координирующие функции для повышения эффективности всех участников в целом. При этом основную работу по защите критической информационной инфраструктуры будут выполнять центры ГосСОПКА, предоставляющие услуги операторам КИИ. Это, в свою очередь, должно помочь операторам КИИ снизить собственные риски/затраты, повысить эффективность своей защиты и в конечном счете увеличить стоимость имеющихся активов как менее рискованных и подверженных киберугрозам. Такой подход должен показать наибольшую эффективность для промышленных объектов топливно-энергетического комплекса, химической промышленности, транспортной и других отраслей, где доля частного инвестиционного капитала велика. В итоге привлекательность инвестиций в эти отрасли будет возрастать.

Алексей НОВИКОВ

Технологии, которыми оперирует ГосСОПКА, давно известны и уже много лет используются для защиты объектов критической информационной инфраструктуры. Качественный скачок, естественно, будет, так как ГосСОПКА (и все, что с ней связано) предъявляет требования не только к технологиям, но и к процессам. То есть теперь будут выдвигаться строгие требования не только к техническим средствам, но и к тому, как их эксплуатировать, какие процессы строить вокруг внедренных средств защиты. Принятие Федерального закона № 187-ФЗ «О безопасности критической информационной инфраструктуры РФ» и связанные с ним изменения в других законодательных актах станут мощным катализатором развития рынка информационной безопасности на территории РФ (а может быть, даже в ряде стран СНГ). Принятые изменения позволят комплексно подходить к вопросам защиты критической информационной инфраструктуры и ликвидировать существующие пробелы. Подписанный закон – пока лишь фундамент большой истории по качественному улучшению защиты критической информационной инфраструктуры Российской Федерации. Впереди еще несколько десятков подзаконных документов, которые детализируют права и обязанности всех участников рынка.

Виктор СЕРДЮК

С нашей точки зрения, ГосСОПКА является уникальным механизмом, который позволит, с одной стороны, обеспечить централизованный мониторинг событий, связанных с атаками злоумышленников, с другой – более эффективно реагировать на уже случившиеся инциденты безопасности. По сути, ГосСОПКА станет своего рода центром реагирования на инциденты CERT для тех организаций, которые будут к ней подключены. Кроме того, следует отметить, что последние эпидемии вирусов WannaCry и Petya продемонстрировали высокий уровень эффективности ГосСОПКА с точки зрения выработки оперативных рекомендаций по противодействию таким атакам.

Не секрет, что уровень проникновения глобальных коммуникационных сервисов (на базе социальных сетей, мессенджеров и т. д.) в бизнес-коммуникации отечественного корпоративного и особенно SMB-сегмента достаточно высок. Как вы оцениваете доверие к подобным (или конкретным) средам, как оно меняется в последнее время и как это скажется на рынке в целом?

Евгений ВИЛЬТОВСКИЙ

Как я уже говорил, мессенджеры и социальные сети – это самый лакомый кусок для взлома и шпионажа, в первую очередь для государственных структур, которые прикрываются борьбой с терроризмом. Уже не раз переписка в Skype или Facebook всплывала совсем по другим причинам. По моему мнению, речь идет о тотальной слежке за населением.

В наше время все больше мессенджеров и социальных сетей становятся «новым агентом» спецслужб, что дает толчок к созданию новых, защищенных средств общения, применяющих шифрование. Но и на них быстро «находят управу» или договариваются с производителем о внедрении бэкдоров.

Для этого мы и создали свою среду для корпоративной работы Swiss Securium в Швейцарии, которая на сегодняшний день является независимым политическим игроком в мире. Подобраться к личным данным в этой стране без веских на то оснований не так просто, а если они еще и зашифрованы и ключи для расшифровки находятся только у клиента, то это практически невозможно.

Валерий КОНЯВСКИЙ

Доверие близко к нулю, наверное, в этом никто не сомневается. Полагаю, что эти сервисы – в значительной степени средства накопления больших данных, на обработку которых мы, естественно, повлиять никак не можем.

Игорь КОРЧАГИН

В настоящее время использование глобальных коммуникационных сервисов стало не только одним из наиболее востребованных сервисов организации коммуникаций между собственными сотрудниками, но и ключевой площадкой обратной связи с клиентами и заказчиками, а также средой продвижения собственной продукции в глобальной сети.

Конечно, когда организация бизнеса построена с применением услуг и сервисов, предоставляемых третьей стороной и являющихся массовыми, в первую очередь возникают опасения в их безопасности и степени доверия поставщику данных услуг. Однако и отказаться от этих технологий нельзя. Так каков же выход?

Очевидным является классический подход с оценкой рисков применения технологий, четкое понимание и контроль целей их использования и уровня критичности информации, обрабатываемой таким способом, ибо уровень доверия к внешнему сервису мы изменить не можем. Второй важный аспект – обязательное повышение уровня осведомленности своих сотрудников в области информационной безопасности, в том числе о потенциальных угрозах, актуальных именно в связи с применением публичных коммуникационных сервисов, особенно социальной инженерии. Ну и последним этапом может являться внедрение специализированных средств защиты, например DLP-решений.

Виктор СЕРДЮК

На сегодняшний день коммуникационные сервисы на базе социальных сетей и мессенджеров являются очень удобным инструментов для обмена информацией, без которого уже сложно представить нашу повседневную жизнь. Тем не менее ни один из существующих сервисов, с нашей точки зрения, не может обеспечить 100%-ной гарантии конфиденциальности и целостности передаваемых данных. Для обеспечения защищенного обмена конфиденциальной информацией необходимо использовать специализированные средства защиты, предназначенные для решения такой задачи.

Кирилл УГОЛЕВ

Сложно выиграть в игре, правила которой устанавливаешь не ты, поэтому доверие к подобным средам крайне низкое. Здесь необходимо применять риск-ориентированный подход и четко осознавать последствия, которые могут возникнуть в результате утечки информации. В целом развитие коммуникационных сервисов – процесс неизбежный, к тому же многие из них применяются как стандарт, что произошло со Skype. Компании из SMB-сегмента чаще используют бесплатный сервис, а крупный бизнес обычно делает ставку на собственные ВКС – более дорогие, заточенные под нужды организации решения.

Насколько информационная безопасность связана с созданием собственной аппаратной базы и программного обеспечения? Не получится ли так, что полный переход на собственные продукты снизит уровень кибербезопасности?

Павел ВОЛЧКОВ

Безусловно связана. Но, во-первых, до полного перехода еще очень далеко. Во-вторых, не стоит забывать, что и в аппаратной базе, и в программном обеспечении главное – реализация и используемый стек технологий. В-третьих, аппаратная база и программное обеспечение не существуют в вакууме, в первую очередь с ними работают люди, которые, как известно, и являются самым слабым звеном. Практика показывает, что независимо от используемых технологий, уровня зрелости процессов разработки ПО и зрелости вендоров, его выпускающих, методы социальной инженерии позволяют обойти любые превентивные контроли. Кроме того, зарубежное программное обеспечение ничуть не безопаснее, любой широко распространенный продукт (и операционные системы, и СУБД, и прикладное ПО) содержит огромное количество постоянно обнаруживаемых уязвимостей, которые регулярно используются в громких атаках по всему миру. Так что опасения, приведенные в вопросе, напрасны.

Михаил ВОРОБЬЕВ

На этот вопрос нет однозначного ответа. Создание собственной аппаратной базы и программного обеспечения в перспективе расширит возможности испытательных лабораторий в части проводимых проверок, даст больше уверенности в отсутствии в исследуемых продуктах аппаратных и программных закладок. К минусам перехода на собственные продукты следует отнести вопросы, связанные с поиском уязвимостей в программном обеспечении. В продуктах зарубежного производства таким поиском занимается все мировое сообщество исследователей, что позволяет производителям оперативно получать информацию об уязвимостях и выпускать обновления безопасности, устраняющие такие уязвимости. Ситуация с отечественными продуктами, разработанными с нуля и не предназначенными на экспорт, может оказаться хуже – круг исследователей, выявляющих уязвимости в целях их устранения, сузится и защищенность продуктов снизится.

Валерий КОНЯВСКИЙ

Для целого ряда применений – это единственный путь. Вряд ли такой путь поджидает нас в области бытовой техники, но я бы не рекомендовал использовать бытовые средства, например, для управления своим счетом и т. д.

Если наши компьютеры и наши операционные системы будут сделаны плохо, то уровень кибербезопасности не повысится. Поэтому мы и делаем их хорошо.

Игорь КОРЧАГИН

Стоит отметить, что именно вопросы отсутствия собственной аппаратной базы и общесистемного программного обеспечения поднимаются как ключевые в тенденции реализации безопасности информационных систем, особенно в современных геополитических условиях. Большинство из нас давно понимает, что нельзя говорить о реальной защищенности информационных ресурсов в системах, функционирующих на базе импортного общесистемного ПО, даже с установленными наложенными СЗИ, а также на импортном современном аппаратном обеспечении, микрокод которого зачастую является для нас ящиком Пандоры.

Переход на отечественную аппаратную и программную платформы положительно скажется на уровне кибербезопасности отечественной ИТ-инфраструктуры. Работы над созданием собственных технологий связаны с повышением уровня компетенции в этой сфере. В частности, развитие собственных технологий позволит понять реальные принципы работы используемых технологий, а также оперативно реагировать на возникающие уязвимости и угрозы, связанные с их применением. Ну и, конечно же, не менее важным является вопрос цифрового суверенитета и выхода на мировой рынок отечественных ИТ-решений.

Виктор СЕРДЮК

Безусловно, импортозамещение в области аппаратного и программного обеспечения должно являться частью национальной стратегии обеспечения информационной безопасности. Эта задача особенно актуальна для военной отрасли России. С другой стороны, очевидно, что 100%-ное импортозамещение возможно только для решения узкоспециализированных задач, в остальном целесообразно применение компонентов и продуктов западных производителей в тех сферах, где они существенно превосходят российские аналоги.

Кирилл УГОЛЕВ

С одной стороны, переход на собственную аппаратную базу позволит повысить уровень ИБ. Так мы сразу закроемся от внешних угроз, намеренно заложенных производителем. Однако это не снижает вероятности возникновения других рисков для безопасности, например тех, которые могут быть созданы собственными сотрудниками. Все равно центром названной среды остается человек, а значит, гарантировать безопасность на 100% невозможно.

К тому же в нашей стране, к сожалению, пока мало компаний, которые могли бы показать серьезный уровень зрелости в обсуждаемом направлении. Использование устаревших технологий и отсутствие опыта могут сыграть злую шутку и снизить уровень кибербезопасности. И в областях, где требуются высокие технологии, быстрые вычисления, лучше обращаться к лидерам, которые производят более качественные решения и оборудование, а в некоторых случаях и более дешевые. ■

Состояние и перспективы радиотехнологий LPWAN по версии J'son & Partners Consulting

Компания J'son & Partners Consulting представила результаты исследования «Состояние и перспективы использования радиотехнологий LPWAN в различных сегментах рынка Интернета вещей (IoT)». Основные перспективы таких технологий связаны с удешевлением коммуникационных модулей и конечных устройств, интеграцией нескольких стандартов в одном чипсете и адаптацией регулирования. Появление гибридных чипсетов, поддерживающих различные стандарты в лицензируемом и нелицензируемом спектре, а также различные стандарты в лицензируемом спектре эксперты относят к существенным драйверам развития технологий LPWAN в России и в мире. По прогнозам J'son & Partners Consulting, к концу 2022 г. в России будет насчитываться не менее 10 млн подключений по технологиям LPWAN. Стандарты LPWAN будут использоваться в первую очередь в ЖКХ, «умных городах», в логистике, на транспорте и в сельском хозяйстве. В целом российский рынок будет развиваться в соответствии с общемировыми трендами, с задержкой на один-три года, если сравнивать с рынками развитых стран. Основные результаты исследования доступны на корпоративном видеопортале JSON.T