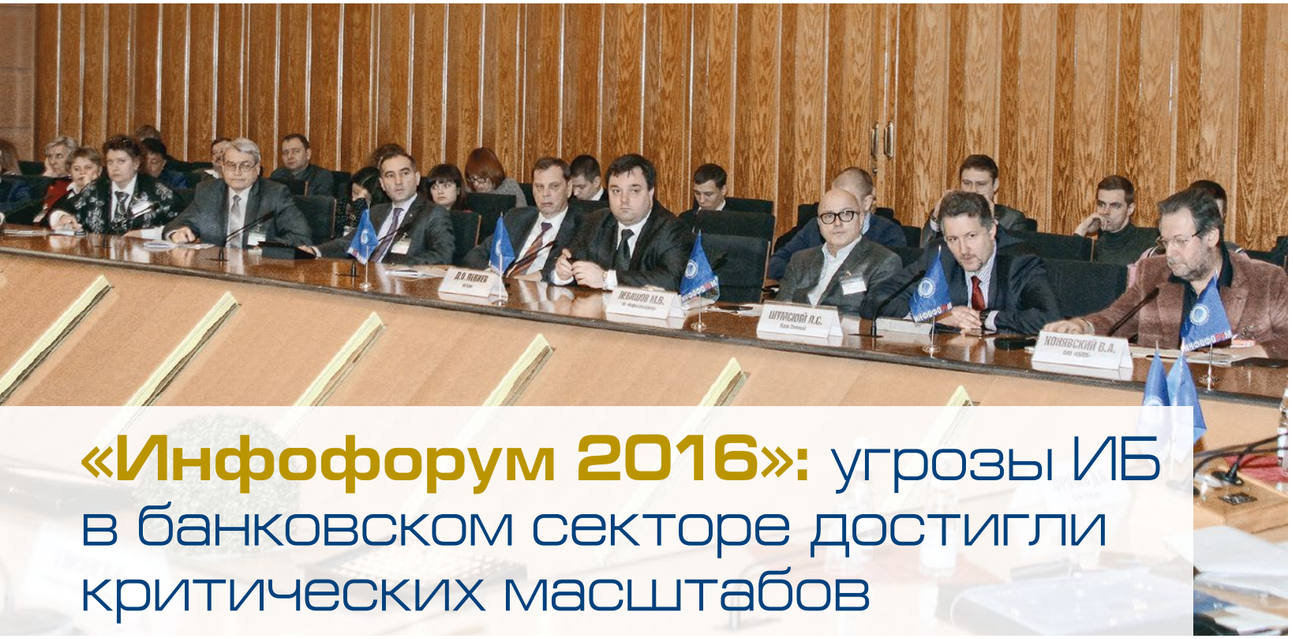


«Инфофорум 2016»: угрозы ИБ в банковском секторе достигли критических масштабов

Угрозы информационной безопасности бизнеса приближаются к критическому масштабу. К такому неутешительному выводу пришли участники панельной дискуссии «Мобильная безопасность и управление безопасностью ИТ-инфраструктуры», состоявшейся в рамках прошедшего в Москве 4–5 февраля «Инфофорума 2016».

В двухчасовой дискуссии, которую вели Дмитрий Фролов, глава Центра реагирования на компьютерные атаки Банка России, и Тимур Аитов, эксперт Ассоциации «Россия», приняли участие целый ряд экспертов в области безопасности, представляющих российские и международные ИТ-компании, банки, правоохранительные органы и иные властные структуры. Среди ключевых тем – противодействие новейшим типам кибератак на кредитно-финансовые организации России, развитие инновационных платежных инструментов и противодействие преступности в кредитно-финансовой сфере, безопасность в сфере мобильных платежей и систем ДБО, а также ряд других.

Обеспечение ИБ и запуск проектов: egg or chicken?

Как отметила **Мария Воронова**, ведущий эксперт по информационной безопасности компании InfoWatch, обсуждая вопрос совмещения интересов бизнеса, диктующих как можно более быстрый запуск на рынок нового сервиса, и необходимости обеспечить при этом максимально возможный уровень безопасности, «здесь правила игры диктует именно бизнес». По ее словам, зачастую бизнес изначально предпочитает брать на себя все потенциальные риски, лишь бы проект оперативно был запущен в коммерческую эксплуатацию, а вопросы безопасности решать задним числом, по мере выявления проблем. Как подчеркнула М. Воронова, во многом такая ситуация представляется ей оправданной, однако уже на этапе запуска сервисов необходимо инвестировать в некую ИТ-базу, которая впоследствии, по мере развития проекта, позволит обеспечивать безопасность на всех его этапах.

В свою очередь, **Михаил Левашов**, зам. генерального директора ГК «Инфосекьюрити», отметил, что на практике вопросы обеспечения безопасности в новых проектах решаются на стадии подготовки далеко не всегда. В результате известны примеры, когда буквально через несколько недель после запуска того или иного платежного сервиса компании сталкиваются с многомиллионными убытками, и только после этого обращаются за помощью к специализированным структурам, в том числе в рамках аутсорсинга, поскольку сами, как правило, не располагают ни штатом соответствующих специалистов, ни необходимыми компетенциями.

Лев Шумский, начальник управления информационной безопасности Связного Банка, подчеркнул, что в решении рассматриваемой дилеммы «интересы бизнеса – обеспечение безопасности» все зависит исключительно от зрелости бизнеса: «зрелый бизнес в обязательном порядке привлекает службу информационной безопасности во все свои процессы». Немаловажен, по его словам, и уровень зрелости самой службы ИБ – при этом развитому бизнесу вполне по силам решать эти задачи силами внутренних подразделений.

Со своей стороны, **Валерий Конявский**, заведующий кафедрой «Защита информации» МФТИ, научный руководитель ОАО «КБПМ», добавил, что в своей стратегии ИБ участникам рынка следует четко различать такие понятия, как угрозы и атаки. По его словам, именно угрозы, на которые своевременно не обратили внимания, очень быстро преобразуются в атаки. При этом он отметил, что самым слабым звеном в системах ДБО по-прежнему остается клиент, на которого нацелено большинство успешных атак преступников. На этом фоне, по мнению В. Конявского, клиента необходимо обеспечить средствами, которые позволят ему в случае мошенничества обезопасить себя от неправомерных претензий банка. В ходе своего выступления он продемонстрировал аудитории мини-компьютер российской разработки, который в первый день «Инфофорума 2016» вместе с другим решением – так называемым «Лучом Чемизова» – был показан президенту РФ Владимиру Путину. Главным достоинством представленной разработки В. Конявский назвал принципиальное отсутствие возможности заражения вирусами благодаря применению уникального типа аппаратной архитектуры, что позволяет эффективно использовать решение в системах ДБО на стороне клиента.

Зав. кафедрой «Защита информации» МФТИ отметил, что сегодня на запуск эффективного информационного сервиса может потребоваться не более нескольких недель, в то время как на то, чтобы сделать этот сервис действительно защищенным, действующие документы регуляторов заставляют тратить годы. Этот разрыв не зависит от разработчиков и целиком обусловлен текущей нормативной базой. На этом фоне нужно как можно скорее адаптировать требования регуляторов к реалиям современного рынка.

ЦБ РФ: ущерб от хакерских атак может быть сопоставим с последствиями применения ядерного оружия

Дмитрий Фролов, глава Центра реагирования на компьютерные атаки Банка России, отметил значительно возросшие за последнее время компетенции преступников, которые делают сегодня акцент на сканирование организационной и технологической составляющей ИБ-структуры банков, что позволяет им открывать все новые потенциальные уязвимости.

М. Воронова: «Уже на этапе запуска проекта необходимо инвестировать в ИТ-базу, которая позволит обеспечивать ИБ»

Последние давно уже стали предметом активной купли-продажи, в том числе на уровне государств, не говоря уже о преступных сообществах. При этом Дмитрий Фролов подчеркнул: «StaffNet использовал только 4 уязвимости и аналогичное количество эксплойтов, если же в сфере промышленного ПО будет задействовано 2000 эксплойтов, ущерб от такого рода атак будет сопоставим с применением ядерного оружия».

С 1 января 2016 г. в России выявлено уже не менее трех преступных атак на ИТ-системы банков, целью которых было хищение денежных средств на общую сумму 2 млрд рублей. Такие данные привел участвующий в дискуссии представитель Управления «К» МВД России **Евгений Михалев**. При этом он уточнил, что в результате мошенникам удалось похитить не более 300 млн рублей, в том числе благодаря четкой работе правоохранительных органов. В качестве примера он привел недавний инцидент, когда полицейские пресекли деятельность преступной организации, целью которой являлось масштабное хищение средств, находящихся на счетах целого ряда банков страны.

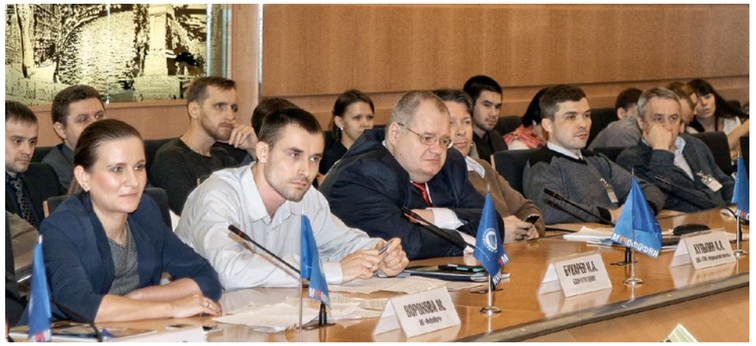
В свою очередь ведущий панельной дискуссии эксперт Ассоциации «Россия» Тимур Аитов отметил, что суммарные потери банков от действий преступников в 4-м квартале 2015 г. составили не менее 1,5 млрд рублей.

Microsoft: импортозамещение в сфере ПО не решит задачу обеспечения национальной безопасности?

Одной из ключевых тем двухчасовой дискуссии стали задачи импортозамещения и альтернативные сценарии, позволяющие обеспечить безопасность российской экономики, включая банковский бизнес, в сегодняшних геополитических условиях.

Отвечая на вопрос, заинтересованы ли отечественные ИТ-структуры в самостоятельной разработке безопасных

▸ **Панельная дискуссия «Мобильная безопасность и управление безопасностью ИТ-инфраструктуры» состоялась 5 февраля 2016 года в рамках прошедшего в Москве «Инфофорума 2016»**



Д. Репан: «Если каких-то пять лет назад было принято говорить о стороне банковского клиента как о недоверенной среде, то сегодня приходится говорить о среде тотально враждебной»

приложений для банков, **Дмитрий Репан**, председатель совета директоров компании «БИФИТ», отметил, что российские решения для обеспечения безопасности активно разрабатываются, постоянно совершенствуясь и усложняясь. По его словам, если каких-то пять лет назад было принято говорить о стороне банковского клиента как о недоверенной среде, то сегодня приходится говорить о «среде тотально враждебной». Ситуация чрезвычайно осложнилась – как на ПК, так и на мобильных платформах, поэтому защита от вредоносного ПО требует сегодня от разработчиков колоссальных усилий.

Со своей стороны **Андрей Иванов**, эксперт по информационной безопасности Microsoft, комментируя ситуацию с возможными сценариями импортозамещения в сегменте софтверных продуктов, подчеркнул, что сама по себе идея создания российских решений-аналогов может быть благоприятна для развития национальной экономики. При этом нельзя забывать, что полученные в результате отечественные решения должны быть по-настоящему конкурентоспособны, в том числе за пределами РФ, поскольку объемов коммерческой прибыли, полученной на рынке единственной страны, будет явно недостаточно для того, чтобы окупить инвестиции вендоров в разработку ПО.

Если же смотреть на импортозамещение с точки зрения обеспечения национальной безопасности, то в этом случае, по словам А. Иванова, открытыми остается целый ряд вопросов. Во-первых, нет никаких гарантий, что в той или иной российской компании не окажется инсайдеров, тайно обслуживающих интересы зарубежных правительств. Во-вторых, указал представитель Microsoft, сама компания-разработчик в лице своих владельцев и топ-менеджеров может быть спровоцирована заинтересованными

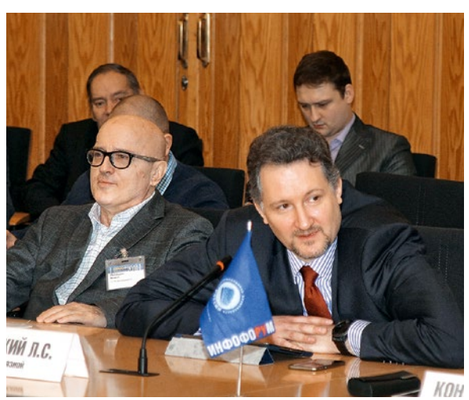
А. Иванов: «Импортозамещение – не панацея в плане обеспечения национальной безопасности»

структурами (например, зарубежными партнерами) на внесение тех или иных незадекларированных возможностей в свои софтверные продукты. Нельзя забывать, что любая российская ИТ-компания является прежде всего коммерческой структурой, закономерно ставящей интересы своего бизнеса превыше всего. Поэтому утверждения, что сам по себе переход на отечественный софт позволит обезопасить национальную экономику от попыток влияния извне, не имеют под собой объективных оснований.

Продолжая дискуссию, **Лев Шумский**, начальник управления информационной безопасности Связного Банка, отметил, что оперативно создать российские разработки, которые позволят эффективно заместить решения международных вендоров, вряд ли удастся. Так, например, результаты недавнего тестирования зарубежных и российских платформ для обработки госданных, которое проводила Роснефть, по его словам, склонили эту компанию к выбору зарубежного решения.

В свою очередь, **Виталий Матвиенко**, начальник Центра разработок, производства и сертификации программно-технических средств и систем, Управление делами Президента РФ, подчеркнул, что задачи соблюдения национальной безопасности могут решаться не только переходом на отечественные программные решения, но и сертификацией продуктов зарубежных вендоров на отсутствие незадекларированных возможностей. По его словам, именно в этом направлении строится, начиная с 2003 года, сотрудничество с Microsoft. В настоящее время действуют 39 сертификатов в отношении продуктов этой компании, включая Windows 7, идут соответствующие переговоры в отношении Windows 10. Таким образом, все организационные вопросы

Л. Шумский: «Зрелый бизнес в обязательном порядке привлекает службу ИБ во все свои процессы»



Т. Аитов: «Суммарные потери банков от действий преступников в 4-м квартале 2015 г. составили не менее 1,5 млрд рублей»

с Microsoft уже давно решены, в том числе касающиеся системной поддержки сертифицированного регулярного обновления линейки ее продуктов с точки зрения обеспечения ИБ и устранения выявленных уязвимостей. Как отметил В. Матвиенко, к сожалению, кроме Microsoft, никто из международных вендоров не сотрудничает с Центром разработок системно, хотя интерес проявляют целый ряд зарубежных компаний – вопрос упирается в финансирование.

Киберпреступники подобрали идеальный ключ ко всем российским банкам?

В панельной дискуссии «Мобильная безопасность и управление безопасностью ИТ-инфраструктуры» также приняли участие целый ряд других экспертов, в том числе **Валерий Елизов**, специалист по информационной безопасности в госсекторе Hewlett Packard Enterprise, который рассказал о возможностях платформы коллективного взаимодействия для противостояния киберугрозам Threat Central, **Эльман Бейбутов**, руководитель направления аутсорсинга ИБ компании Solar Security, поднявший проблему взаимодействия коммерческих и государственных центров обнаружения и противодействия кибератакам, и **Игорь Бухарев**, начальник службы по созданию и технической эксплуатации БДПН ФГУП «Центральный научно-исследовательский институт связи», который коснулся новых угроз ИБ на фоне уже несколько лет широко практикуемой в России услуги переноса абонентских номеров (MNP – mobile number portability).

Одним из ключевых спикеров дискуссии был заявлен **Илья Медведовский**, генеральный директор компании Digital Security, специализирующейся на анализе защищенности систем и исследованиях в области ИБ. Поскольку обстоятельства не позволили этому признанному эксперту в сфере информационной безопасности лично присутствовать на мероприятии, журнал «ПЛАС» предложил ему прокомментировать текущую ситуацию в банковском секторе, резюмируя ключевые вопросы состоявшейся дискуссии.

По словам И. Медведовского, «ситуацию с безопасностью в банковской отрасли сегодня едва ли можно назвать даже напряженной – в ряде случаев она откровенно ужасает. Именно сейчас происходит то, о чем мы так много говорили на протяжении последних лет: вектор атак злоумышленников сместился с клиентов банков на сами банки. В результате деньги утекают уже не с клиентских счетов, а со «счетов» самого банка.

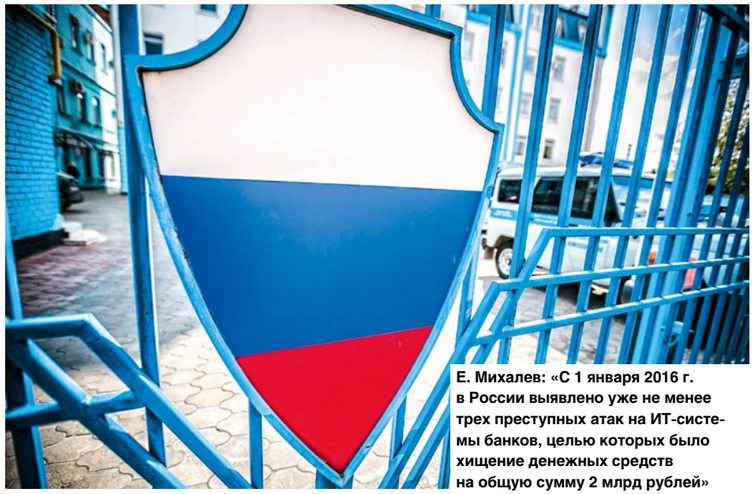
Откровенно говоря, злоумышленников и раньше привлекали внутренние ресурсы кредитных структур. Единственное, что сдерживало «плохих парней» – закрытость информации о том, как банк работает «внутри», где именно «лежат» деньги, а главное – как их оттуда вывести. Однако за последние несколько лет закрылось большое количество банков, их сотрудники потеряли работу, а их знания распространились и попали в распоряжение злоумышленников. И схемы захвата контроля над внутренними системами, которые последние пытались отработать ранее, вдруг «ожили», став реальностью.

И. Медведовский: «Ситуацию с безопасностью в банковской отрасли сегодня едва ли можно назвать даже напряженной – в ряде случаев она откровенно ужасает»

Очевидно, что, попав «внутрь» банковской ИТ-инфраструктуры, злоумышленник обретает широкий спектр возможностей по выводу денег. Здесь и центральная АБС банка, где фактически хранятся все данные о счетах клиентов, и АРМ КБР (автоматизированное рабочее место клиента Банка России), позволяющее перенаправлять деньги между банками, и интерфейс системы SWIFT для взаимодействия с иностранными банками.

Мы видим, что атакуют сегодня в основном именно АРМ КБР, что далеко не случайно, поскольку именно эта точка входа более универсальна по сравнению с другими банковскими системами. Так, например, если в той или иной кредитной структуре могут быть установлены различные виды АБС, не говоря уже о тонкостях бизнес-процессов, связанных с конкретным банком, то ПО для АРМ КБР везде одинаково, работа с ним регламентирована. Суть атаки на АРМ КБР достаточно проста: с корреспондентского счета атакуемого банка деньги пересылают на счета в других банках, откуда они впоследствии выводятся. По данным ЦБ РФ, за последний квартал 2015 года таким образом было похищено около 1,5 млрд рублей.

В целом та легкость, с которой реализуются сегодня подобные преступные схемы, мягко говоря, удивляет. Ведь у ЦБ РФ



Е. Михалев: «С 1 января 2016 г. в России выявлено уже не менее трех преступных атак на ИТ-системы банков, целью которых было хищение денежных средств на общую сумму 2 млрд рублей»

выработаны некие рекомендации по работе с АРМ КБР с точки зрения обеспечения безопасности. Если строго им следовать, можно значительно осложнить жизнь злоумышленникам. Это дает нам основание ожидать, что широкое информирование об угрозе позволит свести подобные инциденты к минимуму.

От себя можем посоветовать банкам три основных практических шага для защиты описанного выше слабого звена. Во-первых, выделите АРМ КБР в отдельный сетевой сегмент и максимально ограничьте к нему доступ на сетевом уровне (в идеале, соединения должны быть разрешены только «от АРМ КБР» и только в определенные места). Во-вторых, выведите хост из корпоративного домена (это крайне важно, так как безопасность домена поддерживать очень непросто). В-третьих, максимально ограничьте происходящее внутри ОС у хоста АРМ КБР: только разрешенное ПО, только разрешенные процессы (групповые политики вам в помощь).

Более того, возвращаясь к общей ситуации с обеспечением ИБ в банковском секторе, отмечу: вполне вероятно, что в ближайшее время какие-либо улучшения здесь могут наблюдаться только в контексте АРМ КБР, поскольку возможностей и каналов по преступному выводу денег остается все еще немало. Например, сценарий, аналогичный вышеописанному, возможно реализовать и в отношении SWIFT. Есть и еще один момент, который необходимо иметь в виду: данные из АБС непременно попадают в АРМ КБР. И злоумышленник, захватив контроль над АБС, может подделывать данные о платежных переводах в АБС, а оттуда они будут попадать в АРМ КБР (особенно опасно, когда АРМ КБР работает в автоматическом режиме).

Также полезно порассуждать о том, что есть различные «прямые связи» между банками, системы переводов и платежей, счета конечных клиентов банка, банкоматы и т. д. Поэтому вариаций атак множество, и оно слишком велико, чтобы сражаться с этими атаками на последнем, «денежном» этапе.

Решать проблему необходимо системно, концентрируясь на грамотном подходе к организации безопасности всей корпоративной сети и практической ИБ. Помните: вам не требуется идеальная защита. Вам необходимо построить такую систему, взлом которой атакующий сочтет слишком затратным предприятием».