Круглый стол:
«Безопасность в наше время — что необходимо для ее эффективного поддержания?»

Как мы и обещали, в этом номере мы открываем наш «КРУГЛЫЙ СТОЛ ПО ПРОБЛЕМАМ БЕЗОПАСНОСТИ». Мы хотим обсудить все, что связано с безопасностью – безопасность информации, безопасность личности, безопасность на работе, дома, на даче, в дороге и т.д . Что такое безопасность? Возможно ли добиться безопасности в нашем обществе и в наше время? Что для этого необходимо? И нужно ли это вообще?

Мы хотим, чтобы в разговоре приняло участие как можно больше заинтересованных лиц – и физических, и юридических. Не только тех, которые занимаются этими проблемами, но и тех, которые эти проблемы испытывают на себе. Пишите свои комментарии, пишите свои вопросы – мы постараемся ответить на все. Если Вам есть, что сказать – пишите. Круглый стол будет открыт столько времени, сколько потребуется.

И вот первая тема:
«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СЕГОДНЯ И ЗАВТРА»

Участники:
Валерий Андреев — *директор по науке и развитию компании ИВК*
Алексей Бугров — *главный специалист по информационной безопасности LETA IT-сотрапу*
Александр Колыбельников — *эксперт отдела внедрения систем информационной безопасности «Квазар-Микро»*
Сергей Мишенков — *технический директор компании АСВТ*
Дмитрий Огородников — *руководитель департамента информационной безопасности «Энвижн Груп»*
Дмитрий Попович – *глава российского представительства компании Eset Software*

Часть первая — проблема

Мы постарались сформулировать несколько, на наш взгляд наиболее интересных, вопросов и задать их первым участникам КРУГЛОГО СТОЛА.

Реальный масштаб и тенденции изменения информационных угроз, с которыми сталкиваются современные организации разного масштаба и разных направлений деятельности. Понимание этих проблем в самих организациях.

Сергей Мишенков. Информационные угрозы надо разделить на две группы. Первая – информационные угрозы, которые срывают работу внутри компании, в т.ч. биллинг. Вторая – доступ к передаваемой информации, задержки или перерывы в ее передаче.

Если говорить про масштаб и тенденции, то последнее время во всех странах появляются сообщения (публикации) о хакерских атаках. Угрозы есть, они заметны и зависят, конечно, от цены информации. Если информация чего-то стоит, ее кто-то продает.

Александр Колыбельников. Сегодня информация стала оружием, причем оружием повседневным и очень часто легко доступным. Для организаций разного уровня – в зависимости от размера, оборота, вида деятельности – угрозы разнятся. Но каждая организация обязательно имеет информацию, критичную для ее существования. К сожалению, понимание критичности, как правило, приходит вместе с инцидентами по утечке, утере и т.п. Но гром-то уже грянул…

Дмитрий Огородников. Что касается изменения информационных угроз, я бы отметил, что за последние два года угрозы и атаки стали более «адресными». Это связано, в первую очередь, с повышением организованности теневой стороны Интернет-сообщества и ориентированности создателей вредоносных программ не на «момент славы», а на получение прибыли.

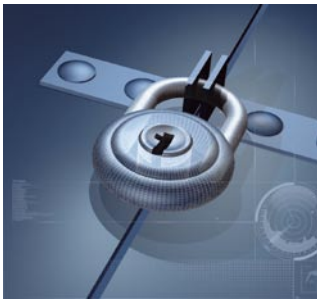
Если говорить о тенденциях, характерных для российских организаций, то можно

сказать, что отношение к информационной безопасности постепенно меняется. Раньше оно преимущественно заключалось в покупке какой-либо «железки» или программы, а сейчас значительно возросло число компаний, воспринимающих ИБ как одну из составляющих своего бизнеса. Т.е. как один из механизмов, помогающих успешнее вести дела и завоевывать доверие клиентов. В качестве другой тенденции можно назвать еще и то, что в России проблемы информационной безопасности по-прежнему волнуют главным образом крупный бизнес. Возможно, это связано с тем, что мелкие фирмы у нас имеют достаточно иных проблем, решение которых для них является более приоритетной задачей – проблема «выживания» не позволяет разбираться с вопросами информационной безопасности.

Валерий Андреев. Новый уровень понимания важности ИБ насупил после 2003 года, считающегося провальным для рынка ИБ. Это привело к росту рынка ИБ, который развивается не только за счет новых решений, но и за счет использования старых наработок. Конкуренция на рынке серьезная, решения дорогостоящие, и отношение к ним соответствующее. Организации покрупнее прислушиваются к общим тенденциям на рынке ИБ и предпочитают сертифицированные по определенному классу решения в качестве средств защиты периметра, шифрования и разграничения доступа. Мелкие компании – из экономии – часто используют встроенные решения по ИБ из состава ОС. Практически у всех есть антивирусные средства и брандмауэры. Т.е., без информационной безопасности сегодня не обходится никто! И не потому, что угроз стало больше. Просто качество угроз сильно изменилось: они стали более изощренными и способными реально навредить репутации или бизнесу. Постепенно руководители предприятий приходят к пониманию необходимости выстраивания комплексной системы защиты – эффективной и сегодня, и в будущем. Это повсеместная тенденция.

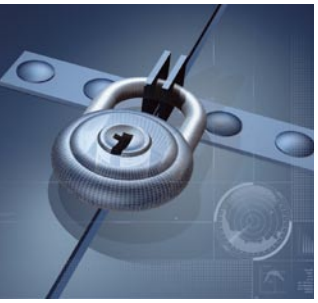
Алексей Бугров. В большинстве организаций прекрасно понимают, что ИТ-угрозы реальны, и что они постоянно изменяются. Но осознание этого факта, к сожалению, далеко не всегда влечет за собой целенаправленные действия. Заметные усилия по верификации и минимизации угроз предпринимаются только в тех организациях, где от ИТ зависит существование бизнеса. К сожалению, в остальной массе осознание серьезности проблемы приходит только после инцидента. Учтивая, что современному бизнесу все труднее обходиться без ИТ, инциденты будут приносить все большие потери. В результате, ИТ-безопасности в организациях будут уделять все больше внимания. И во многом именно налаженная ИТ-безопасность станет важным конкурентным преимуществом.

Дмитрий Попович. Общие проблемы, о которых мы говорим, полностью отражаются в сфере вредоносного ПО и киберпреступности. И здесь четко прослеживаются две тенденции. Первая – это использование атакующей стороной все более изощренных и совершенных технологий и инструментов. Например, современные вирусы способны за считанные минуты «размножиться» и заразить миллионы компьютеров, они способны замаскироваться в недрах ИС и стать практически незаметными. Способны самомодифицироваться, фактически обезоруживая традиционные сигнатурные методы защиты. Кроме того, постоянно сокращается время от выявления какой-либо бреши в системном или прикладном ПО до появления вирусов, которые используют. Более того, в конце 2005 года такие вирусы стали появляться еще до того, как о существовании бреши узнавали разработчики соответствующего ПО. Все это свидетельствует о том, что разработка вредоносного ПО вступила в новую фазу – энтузиасты-любители остались, но основная роль перешла к профессионалам. И с этим связана вторая тенденция. Все чаще вредоносное ПО используется как инструмент продуманного и спланированного компьютерного преступления.



Насколько острее стала проблема ИБ в связи с укрупнением информационных систем в государственном и корпоративном секторах?

Дмитрий Огородников. Естественно, что любое укрупнение системы в большинстве случаев связано с добавлением новых элементов и повышением ее сложности. С одной стороны, это делается для удобства и повышения оперативности деятельности, но с другой – ведет к увеличению количества «дыр» и уязвимостей, а также создает проблему эффективного управления всеми компонентами системы, в том числе и с точки зрения безопасности. Я хотел бы подчеркнуть, что организации, всерьез думающие о построении эффективной системы защиты информации, должны особое внимание уделять тому, как будет происходить управление системами защиты. Комплексность и «разветвленность» системы информационной безопасности имеет смысл только тогда, когда применяемые средства управления позволяют своевременно получать, анализировать и систематизировать полученную информацию о событиях безопасности.



Дмитрий Попович. Дело в том, что ИС не укрупняется сама по себе. Такое укрупнение – всегда следствие укрупнения бизнеса и увеличения масштабов деятельности организации. Естественно, у такой структуры появляются финансовые ресурсы, которые и привлекают кибермошенников или напрямую, в схемах информационного шантажа, или косвенно, в схемах хищения информации для перепродажи или информационных диверсий. Чтобы осуществить такие мошеннические схемы, преступники все чаще создают вредоносное ПО, специально ориентированное на определенную схему преступления в отношение конкретной организации. Причем важно учитывать, что организации постоянно обмениваются информацией. Поэтому сбор конфиденциальной информации крупной организации вполне можно наладить через ее партнеров, внедрив в их информационные системы соответствующее шпионское ПО. Надо сказать, что это – новая тенденция в среде киберпреступности. Тенденция, которую в полной мере еще не оценили не только руководители большинства организаций, но и многие участники рынка ИБ.

Алексей Бугров. Проблема ИБ – прежде всего проблема защиты информации, существовала она всегда. С появлением ИТ-технологий, с одной стороны, информацию стало проще хранить и защищать, с другой – появились и новые угрозы. Поэтому можно говорить об изменении характера угроз. Раньше секретные документы уносили в портфелях, теперь они «уходят» по ИТ-каналам. И если в организации система защиты информации не поставлена в принципе, то никакие действия с ИТ-технологиями не помогут информацию защитить. Если подняться с ИТ-уровня на уровень бизнеса, то укрупнение затрудняет выявление тех информационных ресурсов, защита которых необходима для надежного протекания ключевых бизнес-процессов. Крупной организации труднее оптимизировать затраты на ИБ – ведь ей необходимо в море информации выявить и защитить именно то, что важно, и не распылять средства на защиту второстепенного. Выстраивание такой системы – это новой виток развития ИБ, который только начинается.

Александр Колыбельников. На мой взгляд, проблема стала серьезней, возросла степень гетерогенности систем и степень охвата информационными системами деятельности государства на всех уровнях. Вместе с тем, растет и объем критически важной конфиденциальной информации, утечка которой может сказаться на каждом человеке. К сожалению, такие случаи происходят регулярно, и эта проблема должна стать предметом более пристального внимания со стороны ответственных государственных органов.

Валерий Андреев. Да, проблема стала острее. Переведя информацию в компьютерные системы и сделав эти системы глобальными, государство и крупные коммерческие организации, фактически, упростили дистанционный доступ к информации, в том числе и несанкционированный. Без системы ИБ чтение, копирование и пересылка происходят бесследно, и предприятие даже не знает, что в ее информационной системе уже орудует враг. Именно поэтому так важно надежно защитить крупные информационные системы.

Но для решения этой задачи стандартные механизмы идентификации и аутентификации недостаточны, кроме того, надо учитывать экстерриториальность пользователя. Вопросы ИБ глобального пользователя – актуальнейшая задача текущего дня. Здесь должны быть задействованы все известные механизмы доступа, в том числе СРД, ЭЦП, шифрование и прочие.

Сергей Мишенков. Чем больше информационная система, тем большая вероятность того, что на каком-то участке может произойти несанкционированный доступ. Проблемы ИБ пропорциональны укрупнению сети. В реальной жизни укрупнение информационных систем, как правило, связано с объединением всех территориальных площадок организации в единую территориально-распределенную сеть. При этом соединения на большие расстояния практически всегда проходят через операторские сети. Вероятность перехвата информации в различных участках различна. Обычно центральные офисы бывают защищены лучше и используют ВОЛС, в которой информацию перехватить сложнее. Уязвимость участков с медными линиями выше.

Почему происходят утечки конфиденциальной информации из защищенных организаций и неизбежны ли они?

Алексей Бугров. Утечки происходят, и они, к сожалению, неизбежны. Нельзя построить такую систему, которая бы полностью защитила от утечек. Но можно и нужно создавать защиту, затраты не преодоление которой на порядок ваше ценности информации. Только так можно защитить критически важные сведения. Хочу подчеркнуть, что эти затраты надо правильно распределить между организационными и техническими мероприятиями. Например, очень важно разработать регламенты работы с информацией, увязанные с целостной концепцией безопасности

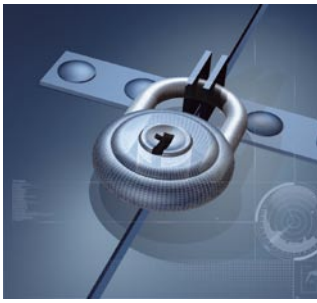
организации, и внятно объяснить сотрудникам, что можно делать, а что нельзя. Потому что нередко совершают то или иное действие с корпоративной информацией не из злого умысла, а по незнанию. Не менее важно направить усилия на защиту действительно важной информации, а не пытаться добиться единого уровня защиты для буквально всей информации в организации. Но выделить такую информацию организации самостоятельно очень непросто. И здесь могут помочь специализирующиеся на этом организации.

Валерий Андреев. Сегодня такие утечки неизбежны, и я бы выделил две причины. Первая связана с принципиальным разрывом терминов и моделей, которыми пользуются специалисты по ИТ-безопасности и службы безопасности организационного уровня. В итоге возникает брешь, которая не позволяет правильно настраивать систему безопасности ИТ-уровня и эффективно использовать журналы событий безопасности в расследовании конкретных инцидентов. Вторая причина связана с гетерогенностью вычислительных систем, в которых сосуществуют различные вычислительные и телекоммуникационные платформы, а также разные поколения вычислительной техники и программного обеспечения. Большинство элементов инфокоммуникационной системы содержат те или иные средства, связанные с ИБ, но их разработчики порой придерживаются различных подходов и ориентируются на различные уровни требований. Соответственно, наладить правильное взаимодействие всех этих подсистем практически невозможно. Решить все эти вопросы сегодня можно. Но для этого надо использовать особые подходы к проектированию систем и использовать особый класс ПО. К сожалению, в России это еще не привилось.

Александр Колыбельников. Причин много, но я выделил бы две основные. Во-первых, отсутствие во многих компаниях процедуры независимого аудита адекватности применяемых мер защиты ИС. Во-вторых, это постоянное появление новых угроз, практически мгновенное использование в незаконных целях новых уязвимостей (так называемая «zero-day attack»), в то время как механизмы защиты от вновь появившейся уязвимости появляются с отставанием.

Дмитрий Огородников. К сожалению, полностью обезопасить себя от утечек конфиденциальной информации едва ли реально. Это связано с тем, что человеческий фактор может играть в утечках информации ведущую роль, и в ряде случаев бороться с этим просто невозможно. Человек может просто запомнить важную информацию, не используя при этом никакие средства и устройства. То, что организации действительно могут делать в рамках борьбы с утечками, это свести к минимуму риск «случайных» утечек, когда сотрудник-инсайдер не задумывается о том, какую ценность имеет передаваемая им информация, либо считает, что его деятельность никак не контролируется.

Сергей Мишенков. Как я уже говорил, главная причина в том, что за ценную информацию кто-то готов хорошо заплатить. Соответственно, и ресурсы, расходуемые на организацию утечки, могут быть сопоставимы с ценой информации. Важно понимать, что это серьезная организованная сила, талантливые специалисты, хорошая техническая база. А такое понимание у руководителей не всегда есть. В сознании людей все еще большое место занимают хакеры-хулиганы. Значит, и усилия по защите бывают недостаточными или неверно сфокусированными. Есть и другая причина, связанная с техническим прогрессом. Например, в отрасли связи происходит быстрый переход к сетям нового поколения NGN, к сетям широкополосного радио-доступа, системы защиты которых еще недостаточно отработаны.



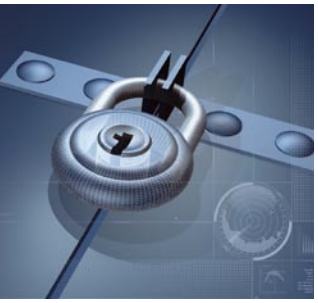
Дмитрий Попович. Давайте сначала посмотрим на само словосочетание «защищенная организация». На самом деле очень часто организация считает себя защищенной, а в действительности таковой не является. Например, слабая проактивная антивирусная защита делает структуру уязвимой для невыявленных вирусов. А задержки с обновлением сигнатурных баз – даже для известных. А использование на всех узлах сети одного и того же антивирусного ПО позволяет свободно распространяться в сети тем вирусам, которые преодолели защиту хотя бы в одном месте. И это только один пример. Поэтому на организационном уровне главная причина в том, что иллюзию защиты принимают за защиту. И пока это иллюзия сохранятся, утечки неизбежны.

Какой враг опаснее — внешний или внутренний?

Алексей Бугров. Опасны оба. Довольно часто при атаке на компанию одновременно действуют и снаружи, и изнутри. Поэтому разделять эти два понятия не совсем правильно. С обоими необходимо бороться с одинаковой строгостью.

Валерий Андреев. Всякий опасен! Но степень опасности того или иного нарушителя разнится. Это – предмет рассмотрения документа под общим названием «Концепция ИБ», который должен быть в любой структу-

ре. Там и объясняется, какой враг опаснее. Есть несколько тенденций. Часто внешний враг анонимен. Его желание сродни Герострату – разрушить информационный ресурс, нанести ему как можно больший ущерб, на как можно больший срок вывести его из строя. Такое глумливое желание чаще всего присуще «протестному электорату» с комплексом непризнанных гениев или борцов за идею. Внутренний враг всегда аутентичен. Его светлая мечта – чтобы функционирование инф-ресурса длилось как можно дольше во благо его узкокорыстных (или иных) целей. Стандартное инсайдерство с примесью шпионажа. Бывает и так, что внутренний враг становится внешним (см. выше) в момент принятия решения о его увольнении или служебном расследовании. Утечка информации об этом часто приводит его в «протестную зону». Самый опасный альянс – сращивание внешнего и внутреннего нарушителя для исполнения конкретной цели. Поведение пары как общего внутреннего нарушителя. Своеобразное on-line инсайдерство, когда актуальная информация должна в режиме реального времени уйти «на сторону», актуально для финансовых институтов.



Дмитрий Огородников. На этот вопрос не существует однозначного ответа – как внешние, так и внутренние угрозы могут нанести серьезный вред деятельности организации. Но, отвечая на данный вопрос, мне хотелось бы отметить, что, как правило, от внешних угроз (вирусных и хакерских атак и т.п.) инструменты защиты в подавляющем большинстве организаций уже используются, тогда как стратегия и тактика защиты от внутренних угроз далеко не всегда вообще существует в организации.

Если мерить «опасность» в денежном эквиваленте, то тут хочу отметить, что многие организации не подсчитывают полностью ущерб от утечки ценной информации, поскольку сделать это в абсолютных цифрах подчас просто не представляется возможным. Чаще всего подсчитывается прямой ущерб в виде штрафов, ответственности перед законом и срывов серьезных контрактов. Что же касается косвенных составляющих, таких как незаключенные контракты, подрыв доверия и аннулированные договоренности, то эти аспекты, как правило, не рассматриваются.

Особое внимание внутренним угрозам следует уделять еще и потому, что внутренний враг может быть гораздо лучше информирован о «слабых сторонах» в защите информационной системы. Кроме того, он просто может иметь открытый доступ к ресурсам, содержащим критически важную информацию, что избавляет его от необходимости применять особые навыки для доступа к данным и придумывать хитрые способы выноса полученной информации.

Александр Колыбельников. Опаснее тот, кто имеет больше возможностей доступа к критической информации. Часто внешний враг пытается найти «слабое звено» внутри компании и действует через него. При этом человек «изнутри» может действовать в интересах злоумышленников неосознанно, не подозревая, что он является невольным соучастником противоправных действий.

Дмитрий Попович. Опасно преступное сообщество, выбирающее способ атаки – снаружи или изнутри. При этом если используются технологии компьютерных вирусов, то программа-шпион, фактически, служит агентом внешнего врага в ИС организации. Ущерб, который этот агент нанесет, может быть разным – в зависимости от схемы преступления. Это могут быть случайно удаленные файлы или, например, нарушение работы компьютера. А может быть другая крайность – воровство или искажение ключевой информации. Внутренний враг в этой схеме также может участвовать, как правило, чтобы установить, где и как хранится действительно важная информация, и занести вредоносное ПО в систему. При таком участии действие внутреннего врага особенно трудно выявить. Но в международной практике уже есть прецеденты, когда были найдены и наказаны все участники компьютерных преступлений – и внешние, и внутренние. Но чтобы это стало повсеместным, необходимо совершенствовать законодательство и международное взаимодействие правоохранительных органов. Ведь компьютерные преступления, как правило, транснациональны.

Сергей Мишенков. Наиболее опасен внутренний враг в организации, где генерируется информация.

Внутренний враг в телекоммуникационных компаниях также опасен. Причем связанные с ним угрозы не ограничиваются упрощенным входом в ИС или доступом к системам управления критически важным оборудованием и ПО. Инсайдеру проще установить, например, несанкционированную точку доступа, через которую к сети можно будет подключиться извне. Против таких угроз защититься можно, но это требует системного подхода к проектированию ИБ и неукоснительного выполнения всех разработанных регламентов. Но стоит сказать, что, в принципе, любую информацию из любой информационной системы (как бы хорошо она ни была защищена) можно достать. В данном случае сопоставляются время и затраты на достижение цели и цена информации.