безопасность

Самозащита для данных

– стратегия –

Количество кибератак на организации и частных пользователей растет с каждым годом. Наиболее уязвимыми отраслями являются финансовая и телеком-сфера, а также органы власти государственного управления. В связи с этим компании вынуждены постоянно совершенствовать технологии для отражения киберугроз. Специалисты утверждают, что ответственность за сохранение данных в цифровом пространстве несут и сами пользователи, которые должны стать более бдительными. Для этого необходимо развивать цифровую грамотность населения.

МАКСИМ КИМЕРЛИНГ

Специалисты обсудили вопросы цифровой безопасности

В современном мире все чаще встает вопрос об информационной безопасности. Проблемы защиты информации и способы защиты от кибератак специалисты обсудили в рамках бизнес-завтрака «Цифровая безопасность. Риски и возможности современной инфраструктуры», организованного газетой «Коммерсантъ Прикамье». В обсуждении приняли участие представители власти, бизнеса, банковского и IT-сообщества. Модератором встречи выступила Наталья Казаринова, профессор кафедры прикладной информатики, информационных систем и технологий ПГГПУ.

Дела государственные

И. о. начальника управления развития инфраструктуры министерства информационного развития и связи Пермского края Петр Шиловских отметил, что в связи с развитием цифровой экономики власти уделяют большое внимание защите информации. «Мы занимаемся цифровой экономикой, чтобы повысить качество жизни граждан, обеспечить должный уровень госуслуг»,— пояснил он. По его словам, ответственность за сохранность информации лежит не только на государственных органах, но и на самих пользователях. «Если люди владеют гаджетами, то нужно думать не только о том, как пользоваться их функционалом, но и об информационной безопасности. Необходимо прививать на уровне культуры закупку лицензированного программного обеспечения»,— подчеркнул господин Шиловских.

Замруководителя управления Роскомнадзора по Пермскому краю Алексей Юшков рассказал о законодательном регулировании информационной среды. Сегодня защита данных гарантируется несколькими федеральными законами: №149-ФЗ «Об информации, информационных технологиях и о защите информации», №126-ФЗ «О связи», №152-ФЗ «О персональных данных» и так далее. Все эти законы призваны гарантировать сохранность данных. «Решения цифровой экономики должны быть направлены на то, чтобы оптимизировать информационные процессы, с которыми человек справиться не готов»,— говорит специалист. Однако полностью взять под свой контроль вопрос защиты информации государство не в состоянии. Сейчас ответственность за сохранение данных лежит на обладателе созданных баз данных. Так, существуют государственные информационные системы, за которые полностью ответственны государственные органы, коммерческие же структуры осуществляют контроль за своими базами данных с привлечением лицензированных организаций.

«Зарегулировать все государством — не выход. Важно, чтобы коммерческие структуры подходили к этой процедуре не формально»,— отметил Алексей Юшков. По его словам, передавая свои данные, человек должен четко понимать, как эта информация будет в дальнейшем использована, то есть согласие на обработку данных должно быть информированным. «Но не каждый человек ответственно относится к этим вещам. Это вопрос нравственный, вопрос культуры. Персональные данные — это та информация, которую надо беречь и очень ответственно к ней относиться. Это вопрос двусторонний. Есть субъект персональных данных и оператор — тот, кто эти данные получил и обрабатывает в каких-то целях»,— считает специалист.

Вместе с тем участники встречи пришли к мнению, что государство, не отвечая полностью за цифровую безопасность различных систем, могло бы взять на себя ответственность за повышение цифровой грамотности населения. Илья Григоров, гендиректор ООО «Бион», подчеркнул, что Пермский край считается лидером по цифровизации, но есть необходимость создания единого окна информационной безопасности. «У нас много представителей малого бизнеса, которые часто работают сами по себе и не обязательно взаимодействуют с властью. У них возникают проблемы с информационной безопасностью. Кроме того, у жителей Пермского края растет количество гаджетов. К примеру, в семье из трех человек могут быть три смартфона, два планшета, другие устройства, и каждое из них находится под угрозой компьютерной атаки, поэтому необходимо, чтобы наша власть посмотрела не только в сторону развития своих информационных систем, но и позаботилась о том, чтобы люди понимали, как защитить себя в цифровом пространстве»,— отметил он.

Защита клиента

Свои меры защиты данных сегодня вынуждены разрабатывать коммерческие структуры, в первую очередь банки. Управляющий Пермским отделением ПАО Сбербанк Константин Подвальный сообщил, что информация, которая есть у банка, непосредственно связана с деньгами. «Одна из основных информационных систем, которыми клиенты пользуются сейчас — „Сбербанк-онлайн“. Это миллионы пользователей по стране и доступ к кошельку каждого. Поэтому основная задача — это защита пользователя»,— рассказал он. По его словам, 85% мошеннических атак, попыток хищений совершаются посредством обычных средств связи. «Это даже не хакерские атаки, а телефонный звонок»,— уточняет господин Подвальный. В связи с этим одним из основных моментов предотвращения хищений является работа с населением, обучение, качественная техподдержка. Вместе с тем сегодня технологии развиваются настолько быстро, что невозможно обучить всем тонкостям владения гаджетами всех пользователей, особенно людей старшего возраста. В этих условиях возрастает ответственность банка. Поэтому у Сбербанка есть собственное подразделение, разрабатывающее антивирусное программное обеспечение.

Константин Подвальный отметил, что сегодня «Сбербанк» из собственно банка превращается в IT-компанию с банковской лицензией. Штат IT-специалистов в структуре банка превышает 10 тыс. человек. Банк намеренно оказался от аутсорсинговых услуг по этому направлению, чтобы самостоятельно контролировать все информационные процессы. «Мы сейчас своим клиентам, чьи устройства работают на Android, подключаем режим „антивирус“. На всех устройствах, где стоит „Сбербанк-онлайн“, автоматически обновляются антивирусные программы»,— подчеркнул банкир. Следующий шаг защиты данных — внедрение биометрии. Это позволит существенно повысить уровень защиты платежных средств, поскольку никто не сможет воспользоваться чужой банковской картой.

В условиях, когда большинство операций совершается в интернет-пространстве, новые IT-технологии появляются у каждого банка. Стоит отметить, что сбор биометрии банки начали еще летом прошлого года. Сейчас ее уже проводят 95 банков более чем в 4 тыс. отделений. По расчетам ЦБ, к июню 2019 года к процессу подключатся 60% банков, а к концу года — все 100%. Предполагается, что все данные будут собраны в единую систему (ЕБС). Гражданам нужно пройти первичную идентификацию в одном из уполномоченных банков, который снимет параметры и направит их в ЕБС. Если после этого клиент захочет получить в банке какую-либо услугу, ему достаточно пройти авторизацию в Единой системе идентификации и аутентификации.

Руководитель по развитию корпоративного бизнеса Пермского РО УФ ПАО «МегаФон» Илья Головнин заявил, что сотовые операторы также предлагают собственные системы защиты данных своим клиентам. «Все операторы столкнулись с тем, что общественный трафик в Wi-Fi-зонах, как правило, некачественный и в эти зоны могут врываться различные преступники, взломщики. Последствия бывают разные: вплоть до изменения той информации, которая идет от отправителя к получателю»,— пояснил специалист. Так, по статистике, две трети клиентов ежегодно подвергаются различным DDoS-атакам и другим киберугрозам. Поэтому все телеком-операторы и провайдеры ведут системную работу по защите информации.

Менеджер по продажам малотоннажных автомобилей «Телта-МБ» Артур Арутюнян отметил, что тема информационной безопасности актуальна и для автомобильной отрасли. «Раньше автомобиль воспринимался нами только как средство передвижения. На определенном этапе автомобиль стал мультимедийным комплексом, и все производители идут по пути усложнения электронных систем. Раньше мы не могли зимой автомобиль прогреть, а сейчас со смартфона можем проконтролировать его состояние. То есть автомобиль становится системой. А когда автомобиль становится системой, он становится уязвимым. Найдется много сомнительных личностей, хакеров, готовых воспользоваться через автомобиль информацией, которая находится в ваших компьютерах, смартфонах и других гаджетах»,— считает он. Господин Арутюнян сообщил, что каждый автопроизводитель разрабатывает собственные системы безопасности.

Страхование киберрисков

В условиях массированных атак актуальным становится вопрос страхования рисков информационной безопасности. На федеральном уровне уже обсуждается вопрос о внедрении обязательного киберстрахования, и сегодня ряд страховых компаний начали предлагать такие услуги. Директор департамента страхования финансовых рисков и ответственности ОАО «АльфаСтрахование» Денис Зенка рассказал, что такие страховые продукты направлены на защиту компаний от киберрисков. «Киберстрахование — новый продукт на российском рынке. Мы видим большое количество сообщений о взломах на сайтах, что приводит к перерывам в оказании услуг. Не все хакерские атаки приводят к каким-то убыткам. Но чаще всего компании все-таки сталкиваются с негативными последствиями атак. Например, был вирус „Петя“, который блокировал компьютеры, после этого вставала логистика, и конечно, это привело к перерывам в деятельности и существенным убыткам»,— рассказал господин Зенка.

Страховые продукты позволяют оцифровать последствия и возместить убытки. Помимо этого, существуют страховые продукты, связанные с ответственностью перед третьими лицами. «Это могут быть вещи, связанные с разглашением с персональных данных. Сегодня пока немного прецедентов, когда в связи с разглашением данных на компании в России были наложены большие штрафы. Но на Западе эта тема популярна. И когда российский бизнес взаимодействует с иностранными гражданами или контрагентами, нужно знать, что штрафы со стороны европейского регулятора существенны и исчисляются процентами от годового оборота»,— пояснил специалист.

Вместе с тем эксперт отметил, что процессы киберстрахования еще не отлажены. «Например, мы сталкиваемся с необходимостью проведения аудита, то есть некой страховой экспертизы, потому что довольно сложно получить необходимую информацию о безопасности компьютерных систем страхователя. Поэтому зачастую приходится прибегать к услугам подрядчиков, которые могут провести полноценный аудит и по его итогам вынести рекомендации страхователю по дополнительным мерам защиты и дать обратную связь по рискам»,— подчеркнул Денис Зенка. Учитывая это обстоятельство, пока преждевременно говорить об обязательном страховании киберрисков. «Обязательное страхование показывает себя эффективным, когда есть большое количество типовых вещей. Например, в автомобильной сфере это работает. Когда мы говорим о киберстраховании, предстоит еще проделать огромную работу и самим страховщикам, и их клиентам, которым придется стандартизировать многие вещи на предприятиях»,— подытожил он.

Ирина Пелявина