ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ

ПИСЬМО
от 24 марта 2014 г. N 49-Т

О РЕКОМЕНДАЦИЯХ
ПО ОРГАНИЗАЦИИ ПРИМЕНЕНИЯ СРЕДСТВ ЗАЩИТЫ ОТ ВРЕДОНОСНОГО КОДА ПРИ ОСУЩЕСТВЛЕНИИ БАНКОВСКОЙ ДЕЯТЕЛЬНОСТИ

В связи с участившимися случаями воздействия на программное обеспечение компьютеров, банковских автоматизированных систем и информационно-телекоммуникационных сетей кредитных организаций, осуществляемого с применением вредоносного кода, следствием которого является нарушение их функционирования и финансовые потери кредитных организаций и их клиентов, в целях защиты интересов кредиторов и вкладчиков, а также повышения качества управления в кредитных организациях банковскими рисками (операционным, правовым, стратегическим, риском потери деловой репутации (репутационным риском) и риском ликвидности) Банк России направляет Рекомендации по организации применения средств защиты от вредоносного кода при осуществлении банковской деятельности.

Территориальным учреждениям Банка России довести настоящее письмо до сведения кредитных организаций.

Настоящее письмо подлежит опубликованию в "Вестнике Банка России".

Первый заместитель
Председателя Банка России
А.Ю.СИМАНОВСКИЙ

Приложение
к письму Банка России
от 24 марта 2014 г. N 49-Т
"О рекомендациях по организации
применения средств защиты
от вредоносного кода
при осуществлении
банковской деятельности"

РЕКОМЕНДАЦИИ
ПО ОРГАНИЗАЦИИ ПРИМЕНЕНИЯ СРЕДСТВ ЗАЩИТЫ ОТ ВРЕДОНОСНОГО КОДА ПРИ ОСУЩЕСТВЛЕНИИ БАНКОВСКОЙ ДЕЯТЕЛЬНОСТИ

Раздел 1. Общие положения

1.1. Настоящие Рекомендации по организации применения средств защиты от вредоносного кода при осуществлении банковской деятельности (далее - Рекомендации) подготовлены в целях противодействия распространению и воздействию вредоносного программного кода, нарушающего функционирование программного обеспечения (далее - ПО) автоматизированных систем, средств вычислительной техники и телекоммуникационного оборудования кредитных организаций, что может привести к невозможности выполнения кредитной организацией своих обязательств перед клиентами кредитной организации (далее - клиенты), контрагентами и Банком России. Рекомендации могут использоваться кредитными организациями при выборе и использовании организационных мер и технических средств защиты информации, обеспечивающих выполнение требований к обеспечению защиты информации при осуществлении переводов денежных средств, установленных Положением Банка России от 9 июня 2012 N 382-П "Положение о требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств", наряду с соответствующими разделами Стандарта Банка России "Обеспечение информационной безопасности организаций банковской

системы Российской Федерации. Общие положения" (СТО БР ИББС-1.0-2010).

1.2. В целях настоящих Рекомендаций используются следующие понятия:

вредоносный код (далее - ВК) - компьютерная программа, предназначенная для внедрения в автоматизированные системы, ПО, средства вычислительной техники, телекоммуникационное оборудование кредитной организации и ее клиентов - пользователей систем дистанционного банковского обслуживания (далее - ДБО), приводящего к уничтожению, созданию, копированию, блокированию, модификации и (или) передаче информации (в том числе защищаемой в соответствии с пунктом 2.1 Положения N 382-П), а также к созданию условий для такого уничтожения, создания, копирования, блокирования, модификации и (или) передачи;

автоматизированная система - совокупность функционально взаимосвязанных аппаратно-программных средств (компонентов), реализующих информационные технологии, используемые для осуществления банковской и иной деятельности;

атака ВК - воздействие ВК на автоматизированные системы, ПО, средства вычислительной техники, телекоммуникационное оборудование кредитной организации и ее клиентов - пользователей систем ДБО, осуществляемое локально или через информационно-телекоммуникационные сети, в том числе через информационно-телекоммуникационную сеть "Интернет" (далее - сеть Интернет);

защита от ВК - организованная деятельность по защите автоматизированных систем, ПО, средств вычислительной техники, телекоммуникационного оборудования кредитной организации и ее клиентов - пользователей систем ДБО от атак ВК и устранению их последствий;

меры (мероприятия) защиты от ВК - организованные действия, имеющие целью осуществление защиты от ВК;

средства защиты от ВК - программные, программно-аппаратные средства, используемые для осуществления защиты от ВК;

защитное ПО - специализированное программное обеспечение, используемое для осуществления защиты от ВК;

контроль на наличие ВК - постоянная, периодическая или эпизодическая проверка автоматизированных систем, ПО, средств вычислительной техники, телекоммуникационного оборудования кредитной организации с целью выявления ВК;

база данных ВК - база данных, содержащая образцы известных сигнатур ВК;

фильтрация ВК - исключение из информационного потока сообщений, которые имеют признаки наличия ВК, или приостановление их обработки (помещение таких сообщений в карантин) с выдачей соответствующего уведомления.

Раздел 2. Организация применения средств защиты от ВК

2.1. Учитывая расширение применения систем ДБО, кредитным организациям рекомендуется обеспечивать надежное и эффективное противодействие атакам ВК, совершенствуемым по способам распространения и воздействия на автоматизированные системы, ПО, средства вычислительной техники, телекоммуникационное оборудование кредитной организации, на основе организации постоянного применения мер защиты от ВК, включающих нижеперечисленные.

2.1.1. Включение во внутренние документы по вопросам политики обеспечения информационной безопасности <1> положений, определяющих состав и содержание мер защиты от ВК средств вычислительной техники и следующих компонентов автоматизированных систем и телекоммуникационного оборудования кредитной организации (далее - объектов защиты):

<1> Принимаемые кредитной организацией в соответствии с пунктом 3.8, пунктом 14 приложения 2 к Положению Банка России от 16 декабря 2003 года N 242-П "Об организации внутреннего контроля в кредитных организациях и банковских группах" ("Вестник Банка России" от 4 февраля 2004 года N 7).

автоматизированных рабочих мест (далее - АРМ) системных и (или) сетевых администраторов, администраторов баз данных, администраторов информационной безопасности и тому подобное;

рабочих станций;

серверов, предназначенных для хранения информационных файлов (файловых серверов) и централизованного доступа к ним;

серверов баз данных;

серверов приложений;

почтовых серверов;

маршрутизаторов;

межсетевых экранов;

серверов, обеспечивающих представительство кредитной организации в сети Интернет (Web-, FTP-,

proxy-серверов, серверов доменных имен (DNS) и тому подобное);

банкоматов, платежных терминалов и тому подобное.

2.1.2. Закрепление функций по осуществлению защиты от ВК, а также по контролю над ее состоянием в положениях о структурных подразделениях кредитной организации, к компетенции которых отнесены: применение информационных технологий, обеспечение информационной безопасности и внутренний контроль, а также в должностных инструкциях работников кредитной организации, осуществляющих данные функции, и всех работников, имеющих доступ к компьютерам и объектам защиты.

2.1.3. Регулярное проведение обучающих мероприятий и контроля знаний работников кредитной организации по тематике защиты от ВК.

2.1.4. Регламентация и контроль выполнения порядка доведения до органов управления кредитной организации результатов осуществления мер защиты от ВК, сведений о предотвращенных и (или) состоявшихся атаках ВК, а также об их последствиях.

2.1.5. Регулярный сбор и анализ информации о распространении ВК с целью своевременной разработки и принятия необходимых мер защиты от ВК, в том числе рекомендуемых компаниями - разработчиками ПО.

2.1.6. Регламентация и контроль выполнения мер защиты от ВК в части обезвреживания выявленного ВК и устранения последствий его воздействия на деятельность кредитной организации.

2.1.7. Организация функционирования постоянной защиты от ВК в автоматическом режиме и использование средств централизованного контроля и управления средствами антивирусной защиты.

2.1.8. Сочетание дистанционного (осуществляемого централизованно через информационно-телекоммуникационные сети кредитной организации со специально организованного управляющего АРМ) и локального контроля ВК (осуществляемого непосредственно на серверах различного назначения, рабочих станциях и АРМ администраторов банковских автоматизированных систем, информационной безопасности, баз данных, информационно-телекоммуникационных сетей кредитной организации, систем ДБО и тому подобное).

2.1.9. Организация функционирования рабочих станций автоматизированных систем с наделением пользователей этих рабочих станций минимально необходимыми для выполнения их функций правами и исключением их учетных записей из группы локальных администраторов.

2.1.10. Использование средств защиты от ВК различных организаций-производителей или поставщиков и их раздельная установка на следующих группах средств вычислительной техники и объектов защиты:

- рабочие станции;
- серверы;
- маршрутизаторы и межсетевые экраны.

2.1.11. Проведение испытаний приобретаемых средств защиты от ВК на совместимость со средствами вычислительной техники и объектами защиты, используемыми в кредитной организации, с другими средствами защиты от ВК, согласно разработанным и утвержденным регламентам. По результатам испытаний рекомендуется определять оптимальные настройки средств защиты от ВК для каждого средства вычислительной техники и объекта защиты с учетом особенностей технологии осуществляемого на нем процесса.

2.1.12. Регулярный контроль целостности и работоспособности защитного ПО (согласно разработанному и утвержденному регламенту).

2.1.13. Осуществление в автоматическом режиме обновления баз данных ВК средств защиты от ВК по мере их размещения (обновления) разработчиками средств защиты от ВК.

2.1.14. Осуществление фильтрации ВК во всех сообщениях электронной почты кредитной организации (применение защитных почтовых шлюзов).

2.1.15. Применение автоматизированных средств обобщения и анализа информации, фиксируемой в журналах протоколирования работы защитного ПО.

2.1.16. Заключение договоров (соглашений) с провайдерами <1> доступа к сети Интернет, предусматривающих осуществление ими фильтрации ВК в информационных потоках, поступающих от них в кредитную организацию.

<1> Понятие "провайдер" используется в значении, определенном в письме Банка России от 31 марта 2008 года N 36-Т "О рекомендациях по организации управления рисками, возникающими при осуществлении кредитными организациями операций с применением систем интернет-банкинга" ("Вестник Банка России" от 9 апреля 2008 года N 16).

2.1.17. Организация в кредитной организации специальных АРМ, обособленных от информационно-телекоммуникационных сетей, в том числе от сети Интернет, и оснащенных всеми используемыми в кредитной организации средствами защиты от ВК. Рекомендуется использовать указанные АРМ для

проведения дополнительного системно-независимого контроля на наличие ВК носителей информации, встроенных в средства вычислительной техники и в объекты защиты кредитной организации. Системно-независимому контролю на наличие ВК целесообразно подвергать носители информации, в отношении которых есть основания предполагать наличие ВК, не обнаруживаемого средствами защиты от ВК соответствующих средств вычислительной техники и объектов защиты кредитной организации. Также рекомендуется осуществлять системно-независимый контроль на наличие ВК съемных машинных носителей информации перед их использованием на средствах вычислительной техники и объектах защиты кредитной организации. Системно-независимый контроль на наличие ВК осуществляется под управлением операционной системы, загружаемой с носителя информации, заведомо не содержащего ВК.

2.1.18. Осуществление контроля использования съемных носителей информации с использованием организационных мер и специализированных средств, осуществляющих централизованный мониторинг подключаемых устройств, ограничение использования съемных носителей информации.

2.1.19. Регламентация состава и правил использования автоматизированных систем, ПО, средств вычислительной техники, телекоммуникационного оборудования кредитной организации на всех этапах их создания и эксплуатации в части обеспечения защиты от ВК в интересах выявления в составе ПО "посторонних" программных модулей, нерегламентированных процессов в оперативной памяти средств вычислительной техники и признаков некорректного функционирования ПО, что может свидетельствовать о воздействии ВК.

2.1.20. Регулярный контроль (предпочтительно не реже одного раза в месяц) состава и целостности ПО автоматизированных систем, средств вычислительной техники, телекоммуникационного оборудования кредитной организации, а также выполнения правил его использования в части обеспечения защиты от ВК (согласно разработанному и утвержденному регламенту).

2.1.21. Регламентация правил создания, ведения и защиты от несанкционированного доступа резервных копий и архивов баз данных автоматизированных систем, телекоммуникационного оборудования кредитной организации, а также эталонных и рабочих копий системного и прикладного ПО автоматизированных систем.

2.1.22. Регулярный контроль (предпочтительно не реже одного раза в год) выполнения правил создания, ведения и защиты от несанкционированного доступа резервных копий и архивов баз данных автоматизированных систем, телекоммуникационного оборудования кредитной организации, а также эталонных и рабочих копий системного и прикладного ПО автоматизированных систем.

2.1.23. Разделение информационно-телекоммуникационных сетей кредитной организации на подсети (сегменты) по их функциональному назначению, по степени критичности влияния на выполнение бизнес-процессов и с учетом подверженности воздействию ВК с целью ограничения возможностей его распространения.

2.1.24. Использование средств анализа наличия на средствах вычислительной техники и объектах защиты неустраненных недостатков системного и прикладного ПО в части защиты от ВК.

2.1.25. Использование рабочих станций кредитной организации в терминальном режиме (с ограниченными функциональными возможностями) для обеспечения доступа к сети Интернет через специально выделенный сервер, целостность системного ПО которого регулярно контролируется согласно разработанному и утвержденному регламенту.

2.1.26. Разработка и тестирование планов по локализации средств вычислительной техники и объектов защиты кредитной организации, подвергшихся воздействию ВК, и последующему восстановлению работоспособности этих средств вычислительной техники и объектов защиты.

2.2. При выборе средств защиты от ВК рекомендуется отдавать предпочтение известным, хорошо зарекомендовавшим себя в течение продолжительного времени компаниям - разработчикам средств защиты от ВК, предлагающим продукты, использующие зарегистрированные товарные знаки, а также удовлетворяющие требованиям, которые рекомендуется изложить во внутреннем документе, подготовленном с участием структурных подразделений кредитной организации, к компетенции которых отнесено применение информационных технологий, обеспечение информационной безопасности, а также внутренний контроль, и утвержденном уполномоченным органом управления. Целесообразно предусматривать приобретение средств защиты от ВК у авторизованных партнеров компаний - разработчиков средств защиты от ВК.

Раздел 3. Функции органов управления кредитной организации в части организации защиты от ВК

3.1. В связи с возрастанием значимости противодействия в банковской деятельности угрозам, обусловленным распространением ВК, ориентированного на автоматизированные системы, ПО, средства вычислительной техники, телекоммуникационное оборудование кредитных организаций, органам управления кредитной организации целесообразно организовать:

3.1.1. Оценку защищенности от ВК автоматизированных систем, ПО, средств вычислительной техники, телекоммуникационного оборудования кредитной организации.

3.1.2. Оценку банковских рисков (операционного, правового, стратегического, потери деловой репутации (репутационного риска) и ликвидности), связанных с недостаточной защищенностью от ВК автоматизированных систем, ПО, средств вычислительной техники, телекоммуникационного оборудования кредитной организации, а также финансовых затрат на хеджирование указанных рисков и на необходимые организационно-технические мероприятия по защите от ВК.

3.1.3. Прогнозирование возможных неблагоприятных изменений ситуации с атаками ВК, вариантов реагирования кредитной организации на эти изменения и, при необходимости, оценку предполагаемых финансовых затрат для обеспечения мер защиты от ВК.

3.1.4. Определение лица, ответственного за организацию защиты от ВК (из числа заместителей единоличного исполнительного органа), а также структурных подразделений, участвующих в осуществлении защиты от ВК, к компетенции которых отнесены применение информационных технологий, обеспечение информационной безопасности и внутренний контроль (целесообразна подготовка плана организации защиты от ВК и возложение обязанностей по ее организации и осуществлению на ответственных лиц).

3.1.5. Определение подотчетности ответственных лиц и структурных подразделений, указанных в подпункте 3.1.4 пункта 3.1 настоящих Рекомендаций.

3.1.6. Определение порядка оперативного информирования органов управления кредитной организации о возможном возрастании угрозы атак ВК лицами, ответственными за осуществление мер защиты от ВК.

3.2. Проведение мероприятий защиты от ВК, указанных в подпунктах 3.1.1 - 3.1.6 пункта 3.1 настоящих Рекомендаций, целесообразно регламентировать соответствующим внутренним документом, утвержденным уполномоченным органом управления кредитной организации.

3.3. Органам управления кредитной организации рекомендуется организовать разработку внутреннего документа, регламентирующего регулярное (предпочтительно не реже одного раза в квартал) рассмотрение результатов осуществления мер защиты от ВК с выработкой необходимых организационных решений, в том числе по корректировке состава и содержания этих мер.

3.4. В целях обеспечения надежности и эффективности защиты от ВК органам управления кредитной организации рекомендуется определить обязанности, подотчетность и подконтрольность работников, ответственных за организацию постоянного применения мер защиты от ВК, предусмотренных подпунктами 2.1.3 - 2.1.26 пункта 2.1 настоящих Рекомендаций.

Раздел 4. Организация договорных отношений с клиентами - пользователями систем ДБО кредитной организации, в части обеспечения защиты от ВК

4.1. При организации защиты от ВК автоматизированных систем, ПО, средств вычислительной техники, телекоммуникационного оборудования кредитных организаций целесообразно учитывать, что АРМ клиентов кредитной организации, используемые ими для проведения сеансов ДБО (далее - клиентские АРМ систем ДБО), могут оказаться наиболее подверженными атакам ВК в силу возможных недостатков организации их защиты от ВК, а также ограниченных возможностей контроля состояния защиты от ВК со стороны кредитной организации.

4.2. Для снижения банковских рисков, которые связаны с недостаточной защитой от ВК клиентских АРМ систем ДБО (операционного, правового, стратегического, риска потери деловой репутации (репутационного риска) и риска ликвидности), кредитной организации рекомендуется:

4.2.1. Разработать, утвердить уполномоченным органом управления кредитной организации и при необходимости пересматривать требования по организации и осуществлению клиентами - пользователями систем ДБО защиты от ВК клиентских АРМ систем ДБО <1> (далее - требования по защите от ВК клиентских АРМ систем ДБО), а также порядок подтверждения выполнения клиентами - пользователями систем ДБО указанных требований по запросу кредитной организации <2>.

<1> Требования по защите от ВК клиентских АРМ систем ДБО могут касаться вопросов необходимости осуществления контроля на наличие ВК клиентских АРМ систем ДБО, настройки средств защиты от ВК, периодичности обновления баз данных ВК и других вопросов, относящихся к организации и осуществлению защиты от ВК.

<2> Порядок подтверждения выполнения клиентами - пользователями систем ДБО требований по защите от ВК клиентских АРМ систем ДБО по запросу кредитной организации определяется договором. Указанное подтверждение может осуществляться, например, путем запроса и получения подтверждения в интерактивном режиме в ходе сеансов ДБО с использованием специальной экранной формы, содержащей

выбираемые клиентами - пользователями систем ДБО варианты текста, подтверждающего (не подтверждающего) выполнение требований по защите от ВК клиентских АРМ систем ДБО.

4.2.2. Изложить требования по защите от ВК клиентских АРМ систем ДБО в договорах (соглашениях), предметом которых является предоставление клиентам услуг ДБО (далее - договоры), а также в эксплуатационной документации на системы ДБО и в памятках, передаваемых клиентам при заключении договоров.

4.2.3. При внесении кредитной организацией изменений в состав и содержание требований по защите от ВК клиентских АРМ систем ДБО информировать клиентов об этом и вносить соответствующие изменения в ранее заключенные договоры и эксплуатационную документацию на системы ДБО.

4.2.4. При изменении порядка подтверждения выполнения клиентами требований по защите от ВК клиентских АРМ систем ДБО вносить соответствующие изменения в ранее заключенные договоры.

4.2.5. Предусматривать в договорах положения, в соответствии с которыми кредитная организация не несет ответственность в случаях финансовых потерь, понесенных клиентами в связи с нарушением и (или) ненадлежащим исполнением ими требований по защите от ВК клиентских АРМ систем ДБО, а также включать в договоры описание процедур разрешения споров, возникающих в связи с компрометацией аутентификационной и идентификационной информации, используемой клиентами для доступа к системам ДБО (логины, пароли, биометрическая информация и тому подобное) и (или) с нарушениями в работе клиентских АРМ систем ДБО, в том числе являющимися следствием воздействия на клиентские АРМ ВК.

4.2.6. Организовать консультирование клиентов - пользователей систем ДБО по вопросам защиты от ВК на постоянной основе с использованием телефонной связи, web-сайтов, электронной почты и тому подобное (прежде всего клиентов - пользователей систем ДБО, использующих сеть Интернет).

4.2.7. Организовать информирование клиентов - пользователей систем ДБО кредитной организации о новых разновидностях ВК, угрожающих безопасности клиентских АРМ систем ДБО, способах защиты от их воздействия и устранения последствий такого воздействия.

4.2.8. Организовать сбор информации о выявленных атаках ВК на системы ДБО и об обстоятельствах их обнаружения, систематизацию и анализ такой информации, ее доведение до сведения органов управления кредитной организации, а также информирование компаний - разработчиков средств защиты от ВК.

4.2.9. Организовать оперативное информирование клиентов - пользователей систем ДБО кредитной организации через каналы связи, отличные от используемых для ДБО (SMS-информирование, электронная почта и тому подобное), о поступлении от этих клиентов в кредитную организацию распоряжений о переводе денежных средств через системы ДБО и получение подтверждений клиентов о подлинности таких распоряжений.

4.3. При организации ДБО клиентов целесообразно организовать подготовку и переподготовку работников кредитной организации, ответственных за работу с клиентами - пользователями систем ДБО кредитной организации, обеспечивающие необходимый уровень знаний указанных работников кредитной организации о требованиях к защите от ВК (в том числе о требованиях по защите от ВК клиентских АРМ систем ДБО) и об изменениях в указанных требованиях по мере возникновения новых разновидностей ВК. Рекомендуется также оказывать содействие в устранении возможных недостатков в организации защиты от ВК у клиентов - пользователей систем ДБО.

Раздел 5. Организация договорных отношений с провайдерами, обеспечивающими функционирование систем ДБО кредитной организации, в части обеспечения защиты от ВК

5.1. Для снижения банковских рисков, которые зависят от состояния защиты от ВК у провайдеров, обеспечивающих функционирование систем ДБО кредитной организации <1>, рекомендуется включать в состав договоров на обслуживание и соглашения с ними об уровне обслуживания (Service Level Agreement) положения, предусматривающие обязательства этих провайдеров по осуществлению защиты от ВК в их автоматизированных системах и информационно-телекоммуникационных сетях, а также возможности кредитной организации по контролю выполнения этих обязательств.

<1> К числу таких рисков относятся операционный, правовой, стратегический, риск потери деловой репутации (репутационный риск) и риск ликвидности ввиду их причинно-следственных связей с возможными аварийными ситуациями у провайдеров.

5.2. Внутренние документы, регламентирующие осуществление кредитной организацией контроля выполнения обязательств по защите от ВК провайдерами, обеспечивающими функционирование систем ДБО кредитной организации и принявшими на себя обязательства по предоставлению кредитной

организации возможности осуществления такого контроля, рекомендуется согласовывать с этими провайдерами.

5.3. Для организации и осуществления контроля выполнения обязательств по защите от ВК провайдерами, обеспечивающими функционирование систем ДБО кредитной организации, предусмотренных договорами на обслуживание и Service Level Agreement, органам управления кредитной организации рекомендуется назначить ответственных исполнителей и определить их функциональные обязанности в должностных инструкциях.

5.4. В целях предотвращения распространения на автоматизированные системы, ПО, средства вычислительной техники, телекоммуникационное оборудования кредитной организации атак ВК, предпринимаемых в отношении провайдеров, обеспечивающих функционирование систем ДБО кредитной организации, рекомендуется предусматривать в договорах с этими провайдерами их обязательства по локализации воздействий ВК и их последствий в пределах автоматизированных систем и информационно-телекоммуникационных сетей провайдеров, а также ответственность за нарушение этих обязательств.