МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ
по обеспечению информационной безопасности в российском государственном сегменте информационно-телекоммуникационной сети «Интернет» (RSNet)

г. Смоленск
2018 г.

Настоящие методические рекомендации разработаны во исполнение Указа Президента Российской Федерации от 22 мая 2015 г. № 260 «О некоторых вопросах информационной безопасности Российской Федерации» и разъясняют требования к подключению информационных систем и информационно-телекоммуникационных сетей к информационно-телекоммуникационной сети «Интернет» через российский государственный сегмент информационно-телекоммуникационной сети «Интернет» (далее - RSNet).

Методические рекомендации предназначены для пользователей персональных компьютерах, имеющих выход в сеть «Интернет», и ответственных за защиту информации в органах исполнительной власти Смооленской области и органов местного самоуправления муниципальных образований Смоленской области.

Методические рекомендации разработаны Департаментом Смоленской области по информационным технологиям в соответствии с Соглашением о подключении к информационно-телекоммуникационной сети «Интернет» и размещении (публикации) в ней информации через российский государственный сегмент информационно-телекоммуникационной сети «Интернет» (сеть RSNet) между Федеральной службой охраны Российской Федерации и Администрацией Смоленской области.

1. Общие положения

1.1. Во исполнение Указа Президента Российской Федерации от 22 мая 2015 г. № 260 «О некоторых вопросах информационной безопасности Российской Федерации» и в соответствии с Положением о распределенной мультисервисной сети связи и передачи данных органов исполнительной власти Смоленской области и органов местного самоуправления муниципальных образований Смоленской области (далее – РМС СО), утв. постановлением Администрации Смоленской области от 20 июля 2015 г. № 424 Департаментом Смоленской области по информационным технологиям организовано подключения РМС СО к информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет») и обеспечена возможность подключения государственных информационных систем Смоленской области, размещения (публикации) в сети «Интернет» информации органов исполнительной власти Смоленской области и органов местного самоуправления муниципальных образований Смоленской области через российский государственный сегмент сети «Интернет» (сеть RSNet).

1.2. Методические рекомендации предназначены для обеспечения информационной безопасности при работе в сети «Интернет» посредством RSNet и размещения информационных ресурсов органов исполнительной власти Смоленской области и органов местного самоуправления муниципальных образований Смоленской области в сети RSNet.

1.3. При подключении информационных систем и средства вычислительной техники органов исполнительной власти Смоленской области и органов местного самоуправления муниципальных образований Смоленской области (далее – органы власти Смоленской области) к сети «Интернет» посредством RSNet необходимо:

- руководствоваться требованиями указа Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена», приказа Федеральной службы безопасности Российской Федерации и Федеральной службы по техническому и экспортному контролю от 31 августа 2010 г. № 416/489 «Об утверждении Требований о защите информации, содержащейся в информационных системах общего пользования», приказа Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», приказа Федеральной службы охраны от 7 сентября 2016 г. № 443 «Об утверждении Положения о российском государственном сегменте информационно-телекоммуникационной сети «Интернет», постановления Администрации Смоленской области от 20 июля 2015 г. № 424 «О порядке использования распределенной мультисервисной сети связи и передачи данных органов исполнительной власти Смоленской области и органов

местного самоуправления муниципальных образований Смоленской области» и настоящих методических рекомендаций;

- пользоваться телематическими службами в сети «Интернет» при выполнении служебных задач с использованием электронных адресов в доменах, права на которые принадлежат органу власти Смоленской области или подведомственному ему учреждению, а сервисы электронной почты должны быть реализованы на программно-технических средствах, правом владения и (или) пользования которыми обладает орган власти Смоленской области или подведомственное органу власти Смоленской области государственное учреждение;

- осуществлять журналирование сетевых событий и действий пользователей в сети RSNet. Рекомендованный срок хранения информации – не менее трех месяцев;

- использовать только сертифицированные ФСБ России и (или) ФСТЭК России средства антивирусной защиты, межсетевого экранирования и систем обнаружения вторжений/компьютерных атак;

- определить ответственных за организацию рабочих станций (абонентских пунктов) сети «Интернет» (далее - АП) и подключению информационных ресурсов к сети RSNet из числа сотрудников органа власти Смоленской области (далее – администратор АП).

2. Правила пользования ресурсами сети «Интернет» посредством российского государственного сегмента сети «Интернет»

2.1. Рекомендуется осуществлять доступ к ресурсам сети «Интернет» с использованием только лицензионного программного обеспечения в соответствии с законодательством Российской Федерации.

2.1.1. Рекомендуется осуществлять загрузку программного обеспечения на АП только с официальных сайтов разработчиков программного обеспечения.

2.1.2. Не допускается устанавливать программное обеспечение на АП без участия администратора АП.

2.2. Рекомендуется использовать информационные ресурсы сети «Интернет» исключительно в целях обеспечения деятельности органов власти Смоленской области в рамках решаемых ими задач. Не допускается посещать сайты, а также использовать специальное программное обеспечение, вовлекающие пользователей в пиринговые сети.

2.3. Не допускается использовать для доступа к сети «Интернет» средства анонимизации (виртуальные частные сети, прокси-сервера) в доменах, права на которые не принадлежат органу власти Смоленской области и правом владения или пользования, которыми не обладает орган власти Смоленской области или подведомственные органу власти Смоленской области государственные учреждения.

2.4. Рекомендуется использовать встроенные и/или лицензионные утилиты для web-браузеров, обеспечивающих вспомогательную фильтрацию трафика (отключения нежелательного контента, рекламы) и принудительное подключение к ресурсам сети «Интернет» с использованием защищенных протоколов обмена данными (при наличии данной возможности).

2.4.1. Рекомендуется контролировать подлинность сертификата сервера при использовании защищенного протокола обмена данными (цифровая подпись сертификата не должна быть просрочена, удостоверяющий центр должен быть известным и легальным).

2.5. Рекомендуется осуществлять доступ к ресурсам сети «Интернет» в непривилегированном режиме операционной системы АП. Вход в привилегированный режим должен осуществляться только администратором АП.

2.5.1. Использовать парольную защиту для доступа к привилегированному режиму операционной системы АП и к информационным ресурсам (сервисам) сети «Интернет» в соответствии с «Инструкцией по организации парольной защиты в органах исполнительной власти Смоленской области и подведомственных им учреждениях» (утв. приказом начальника Департамента Смоленской области по информационным технологиям от 10.09.2014 г. № 49). Не допускается использовать повторяющиеся пароли к различным ресурсам сети «Интернет».

2.5.2. Не рекомендуется хранить учетные данные для доступа к ресурсам сети «Интернет» в web-браузере или в отдельных файлах, хранящихся на АП.

2.6. Рекомендуется регулярно отслеживать работоспособность антивирусных средств и межсетевых экранов, конфигурацию их настройки, а также актуальность баз данных компьютерных вирусов.

2.6.1. Рекомендуется проверять антивирусными средствами защиты полученные файлы из сети «Интернет», в том числе по электронной почте. Не рекомендуется открывать электронные письма от неизвестных пользователей.

2.7. Рекомендуется использовать для работы с электронной почтой клиенты, работающие с использованием защищенного протокола обмена данными.

2.8. Рекомендуется осуществлять настройку web-браузеров для блокировки выполнения сценариев и другого потенциально опасного контента (Java-апплетов, Flash, ActiveX, Node.js и т.п.).

2.9. Рекомендуется своевременно обновлять операционные системы и программное обеспечение, установленные на АП, а также регулярно проводить резервное копирование информации, хранящейся на АП.

2.10. Допускается переносить информацию с АП на технические средства, на которых обрабатывается информация ограниченного распространения, только с использованием несекретных носителей информации, учтенных установленным порядком в делопроизводстве органа

власти Смоленской области. Несекретные носители, используемые для переноса информации, должны использоваться однократно и уничтожаться в порядке, предусмотренном для секретных носителей. После переноса информации до уничтожения указанные носители должны храниться в делопроизводстве органа власти Смоленской области. Перенос информации должен осуществляться с участием администратора АП.

2.10.1. Рекомендуется форматировать съемные носители информации, используемые для переноса файлов из сети «Интернет» на технические средства, не подключенные к сети «Интернет», в файловую систему NTFS и отключать возможность «записи» корневому каталогу (всем остальным каталогам: «полный доступ»).

2.11. Ответственным за защиту информации в органах власти Смоленской области, рекомендуется проводить на регулярной основе инструкторско-методические занятия с пользователями РМС СО, направленные на изучение и закрепление требований информационной безопасности при работе в сети «Интернет» на технических средствах, обрабатывающих информацию ограниченного распространения.

2.12. Ответственным за защиту информации в органах власти Смоленской области рекомендуется проводить периодический контроль выполнения требований по защите информации на средства вычислительной техники, имеющих подключение к сети «Интернет».

2.13. По всем фактам и инцидентам, связанным с обеспечением информационной безопасности при работе в сети «Интернет» необходимо обращаться в службу технической поддержки пользователей Service Desk по телефону 8 (4812) 29-22-22 («Мередиан» - 2-22-22).

Приложение
к методическим рекомендациям по обеспечению информационной безопасности в российском государственном сегменте сети «Интернет» (RSNet)

ПАМЯТКА
пользователю по правилам работы в сети «Интернет» и о возможных последствиях обращения к ресурсам сети «Интернет»

1. На персональных компьютерах, имеющих выход в сеть «Интернет», запрещается обработка сведений, составляющих государственную тайну, служебной информации ограниченного распространения, а также информации, для которой установлены особые правила доступа.

2. Для осуществления сеанса работы в сети «Интернет» необходимо использовать только лицензионное программное обеспечение программ-клиентов доступа к информационным ресурсам сети, установленное на персональном компьютере обслуживающим подразделением.

Изменение конфигурации программного обеспечения программ-клиентов доступа к информационным ресурсам сети должно проводиться только обслуживающим подразделением.

3. При получении файлов из сети «Интернет» их необходимо обработать антивирусными средствами, установленными на персональном компьютере обслуживающим подразделением.

При этом необходимо учитывать, что особую опасность представляют исполняемые файлы программ, доступные из конференций UseNet (особенно *.warez, *.cracks, *.hack) и на FTP-серверах, на которых распространяется нелицензионное («пиратское») программное обеспечение, а также программные средства «взлома» и нелегальной регистрации коммерческого программного обеспечения. В этих файлах могут содержаться программные закладки, программы типа «троянского коня» и другие программы скрытого негативного воздействия.

Во избежание утечки, искажения или разрушения обрабатываемой информации, а также повреждения операционной среды и прикладных программ, **не рекомендуется** получать из сети «Интернет» исполняемые файлы программ и осуществлять их запуск на персональном компьютере.

Группа администрирования РМС СО и подразделение обслуживания персонального компьютера **не несут ответственности** за последствия использования программных средств, полученных пользователями по сети «Интернет».

4. На некоторых WWW и FTP серверах для получения доступа к хранящейся на них информации будет предложено пройти регистрацию. При этом Вас попросят ответить на ряд вопросов, касающихся названия

организации, которую Вы представляете, рода деятельности, круга творческих и производственных интересов и т.д. В этом случае работу с таким сервером рекомендуется прекратить. В случае сохранения интереса к информации, хранящейся на данном сервере необходимо обратиться к руководителю или подразделению по обеспечению информационной безопасности организации для согласования варианта ответа на вопросы регистрации.

5. Во всех случаях, когда во время сеанса в сети «Интернет» что-либо покажется необычным в работе персонального компьютера или программного обеспечения, необходимо немедленно прекратить работу и вызвать представителя обслуживающего подразделения.

6. Запрещается устанавливать рабочую станцию сети «Интернет» в категорированных помещениях, кроме случаев, разрешенных законодательством Российской Федерации.

7. Необходимо ответственно относиться к хранению своей учетной информации (идентификатор пользователя, пароль) и не использовать электронную почту для пересылки подобной информации. В случае получения писем (даже от имени администратора сети) с требованием выслать подобную информацию, необходимо обратиться к ответственному за защиту информации.

В случае компрометации паролей Вы обязаны немедленно оповестить ответственного за защиту информации.

8. Несанкционированное использование компьютерных систем, неправомерный доступ к компьютерной информации, нарушение правил эксплуатации персонального компьютера, систем персональных компьютеров или их сетей, а также создание, использование и распространение вредоносных программ влечет уголовную и гражданскую ответственность, предусмотренную законодательством (статьи 272, 273, 274 Уголовного кодекса Российской Федерации).

9. Оператор РМС СО имеет право приостановить доступ пользователей к сети «Интернет» в следующих случаях:

- нарушение правил антивирусной защиты;
- распространения информации, оскорбляющей честь и достоинство других пользователей и персонала компьютерных сетей;
- попытки получить несанкционированный доступ к компьютерам сети «Интернет» с использованием собственных сетевых реквизитов;
- несанкционированного сканирования любого диапазона IP-адресов;
- нарушения авторских прав на информацию, представленную в сети;
- намеренного нанесения ущерба другим лицам;
- вмешательства в действия других пользователей или обслуживающего персонала (например, несанкционированный доступ к компьютерам и информационным источникам).