Приложение
к письму ОАЦ

Перечень первоочередных мер, необходимых для создания системы защиты информации в информационных сетях и системах

Для целей исполнения настоящих мер применяются термины в значениях, определенных в Положении о технической и криптографической защите информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, Положении о порядке аттестации систем защиты информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, утвержденных приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66 «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449» (далее – приказ ОАЦ № 66), Законе Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации» (за исключением термина «персональные данные»), Законе Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных», а также следующие термины и определения:

объекты информационных сетей (систем) – средства вычислительной техники, сетевое оборудование, системное и прикладное программное обеспечение, средства технической и криптографической защиты информации.

В целях исключения условий для компрометации информационных сетей и систем государственных органов и организаций, а также повышения их защищенности владельцам (собственникам) необходимо выполнить следующее.

В месячный срок:

1. Осуществить категорирование информации, обрабатываемой в информационных сетях (системах).

2. Провести анализ структуры информационных сетей и информационных потоков в целях определения состава (количества) и мест размещения объектов информационных сетей, их физических и логических границ.

3. Осуществить выбор и внедрение средств технической защиты информации с учетом рекомендаций изготовителя и ограничений, указанных в сертификатах соответствия, а также осуществить смену реквизитов доступа к функциям управления и настройкам, установленным

по умолчанию (в случае невозможности смены – осуществить блокировку данных учетных записей).

4. Определить состав информации о событиях информационной безопасности, подлежащих регистрации (идентификация и аутентификация пользователей, нарушения прав доступа пользователей, выявленные нарушения информационной безопасности и другое).

5. Обеспечить централизованный сбор и хранение информации о событиях информационной безопасности не менее года.

6. Обеспечить разграничение доступа пользователей к объектам информационной сети.

7. Обеспечить идентификацию и аутентификацию пользователей информационной сети.

8. Обеспечить изменение атрибутов безопасности сетевого оборудования, системного программного обеспечения и средств защиты информации, установленных по умолчанию.

9. Обеспечить контроль и управление физическим доступом в помещения, в которых постоянно размещаются объекты информационной сети.

10. Обеспечить синхронизацию временных меток и (или) системного времени в информационной сети и системе защиты информации.

11. Определить перечень разрешенного программного обеспечения и регламентировать порядок его установки и использования.

12. Обеспечить использование объектов информационной сети под пользовательскими учетными записями (использование административных учетных записей только в случае настройки объектов информационной сети или их особенностей функционирования).

13. Обеспечить обновление программного обеспечения объектов информационной сети из доверенных источников и контроль за своевременностью такого обновления.

14. Обеспечить сегментирование (изоляцию) сети управления объектами информационной сети от сети передачи данных.

15. Обеспечить защиту средств вычислительной техники от вредоносных программ.

16. Обеспечить управление внешними информационными потоками (маршрутизация) между информационными сетями. Использовать маршрутизатор либо коммутатор маршрутизирующий.

17. Обеспечить ограничение входящего и исходящего трафика (фильтрация) информационной сети только необходимыми соединениями. Использовать межсетевые экраны, функционирующие на канальном, и (или) сетевом, и (или) транспортном, и (или) сеансовом, и (или) прикладном уровнях.

18. Обеспечить контроль за внешними подключениями к информационным сетям.

В трехмесячный срок:

1. Разработать либо скорректировать политику информационной безопасности, в которой определить:

цели и принципы защиты информации;

перечень информационных систем, отнесенных к соответствующим классам типовых информационных систем, перечень средств вычислительной техники, а также сведения о подразделениях защиты информации или ином подразделении (должностном лице), ответственном за обеспечение защиты информации;

обязанности пользователей информационных систем;

порядок взаимодействия с иными информационными системами.

2. Разработать либо скорректировать (самостоятельно либо с привлечением специализированной организации) техническое(ие) задание(я) на информационные системы, в котором(ых) определить:

наименования информационных систем с указанием присвоенного им класса типовых информационных систем;

требования к системе защиты информации в зависимости от используемых технологий и класса типовых информационных систем в соответствии с приложением 3 к Положению о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, утвержденного приказом ОАЦ № 66 (далее – Положение);

сведения об организации взаимодействия с иными информационными системами (в случае предполагаемого взаимодействия) с учетом требований согласно приложению 4 Положения;

порядок обезличивания персональных данных (в случае их обработки в информационной системе) с применением методов согласно приложению 5 Положения;

требования к средствам криптографической защиты информации, включая требования к криптографическим алгоритмам в зависимости от задач безопасности (шифрование, выработка и проверка электронной цифровой подписи, хэширование, имитозащита), криптографическим протоколам, управлению криптографическими ключами (генерация, распределение, хранение, доступ, уничтожение), а также к функциональным возможностям безопасности и форматам данных. Профили требований, предъявляемых к средствам криптографической защиты информации, определяются Оперативно-аналитическим центром при Президенте Республики Беларусь (далее – ОАЦ);

перечень документации на систему защиты информации.

Допускается не включать в техническое задание отдельные обязательные требования к системе защиты информации при отсутствии в информационной системе соответствующего объекта (технологии) либо при условии согласования с ОАЦ закрепления в таком техническом задании обоснованных компенсирующих мер.

3. Осуществить разработку общей схемы системы защиты информации, которая должна включать в себя:

наименование информационной системы;

класс типовых информационных систем;

места размещения объектов информационной системы;

физические границы информационной системы;

внешние и внутренние информационные потоки и протоколы обмена защищаемой информацией.

4. Разработать документацию на систему защиты информации в соответствии с техническим заданием, в которой описать порядок:

разграничения доступа пользователей к объектам информационной системы;

резервирования и уничтожения информации;

защиты от вредоносного программного обеспечения;

использования съемных носителей информации;

использования электронной почты;

обновления средств защиты информации;

осуществления контроля (мониторинга) за функционированием информационной систем и системы защиты информации;

реагирования на события информационной безопасности и ликвидации их последствий;

управления криптографическими ключами, в том числе требования по их генерации, распределению, хранению, доступу к ним и их уничтожению.

5. Осуществить выбор и внедрение средств криптографической защиты информации с учетом рекомендаций изготовителя и ограничений, указанных в сертификатах соответствия, а также осуществить смену реквизитов доступа к функциям управления и настройкам, установленным по умолчанию (в случае невозможности смены – осуществить блокировку данных учетных записей).

6. Определить способ и периодичность мониторинга (просмотра, анализа) событий информационной безопасности уполномоченными на это пользователями информационных сетей.

7. Регламентировать порядок использования в информационной сети мобильных технических средств и контроля за таким использованием.

8. Обеспечить контроль за работоспособностью, параметрами настройки и правильностью функционирования объектов информационной сети.

9. Обеспечить защиту обратной связи при вводе аутентификационной информации.

10. Обеспечить (централизованное) управление учетными записями пользователей информационной сети и контроль за соблюдением правил генерации и смены паролей пользователей.

11. Обеспечить блокировку доступа к объектам информационной сети после истечения установленного времени бездействия (неактивности) пользователя или по его запросу.

12. Обеспечить конфиденциальность и контроль целостности информации при ее передаче посредством сетей электросвязи общего пользования (использовать средства линейного или предварительного шифрования).

13. Обеспечить защиту от агрессивного использования ресурсов виртуальной инфраструктуры.

14. Обеспечить защиту виртуальной инфраструктуры от несанкционированного доступа и сетевых атак из виртуальной и физической сети, а также виртуальных машин.

15. Обеспечить безопасное перемещение виртуальных машин и обрабатываемых на них данных.

16. Обеспечить резервное копирование пользовательских виртуальных машин.

17. Обеспечить физическую изоляцию сегмента виртуальной инфраструктуры (системы хранения и обработки данных), предназначенного для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам.

18. Определить состав и содержание информации (в том числе конфигурационных файлов сетевого оборудования), подлежащей резервированию, и обеспечить ее резервирование.

19. Обеспечить защиту от несанкционированного доступа к резервным копиям, параметрам настройки сетевого оборудования, системного программного обеспечения, средств защиты информации и событиям безопасности.

20. Обеспечить в реальном масштабе времени автоматическую проверку файлов данных, передаваемых по почтовым протоколам, и обезвреживание обнаруженных вредоносных программ.

В шестимесячный срок:

1. Выполнить требования приказа ОАЦ № 66.

2. Обеспечить прохождение переподготовки или повышения квалификации по вопросам технической и криптографической защиты информации в порядке, установленном законодательством, работников подразделений, ответственных за защиту информации, в случае отсутствия у них высшего образования в области защиты информации.

В процессе эксплуатации информационных систем с применением аттестованных в установленном порядке систем защиты информации регулярно осуществлять:

контроль за соблюдением требований, установленных в нормативных правовых актах, документации на систему защиты информации информационных сетей (систем);

контроль за порядком использования объектов информационной системы (сети);

мониторинг функционирования системы защиты информации;

выявление угроз (анализ журналов аудита), которые могут привести к сбоям, нарушению функционирования информационной сети (системы);

резервное копирование информации, содержащееся в информационной сети (системе);

обучение (повышение квалификации) пользователей информационной сети (системы);

наладочные работы и сервисное обслуживание информационных сетей (систем) только с участием подразделения защиты информации или иного подразделения (должностного лица), ответственного за обеспечение защиты информации.