Рекомендации по обеспечению информационной безопасности для Заказчиков услуг МТС Cloud

Глава 1. Общие рекомендации по обеспечению информационной безопасности*

*в документе использованы рекомендации Оперативно-аналитического центра при Президенте Республики Беларусь по обеспечению защиты общедоступной информации в информационных сетях.

Ссылка на ресурс: https://www.oac.gov.by/recommendations-for-government-agencies.

Используемые термины:

объекты информационной системы – средства вычислительной техники, сетевое оборудование, системное и прикладное программное обеспечение, средства технической и криптографической защиты информации (ОИС).

Рекомендуется реализовать следующие меры в информационных системах (ИС).

Защита ОИС

1. Обеспечить защиту средств вычислительной техники (СВТ) от вредоносного программного обеспечения.

2. Использовать криптографические алгоритмы защиты информации, интегрированные в программное обеспечение (ПО), в том числе самих носителей информации.

3. Отключить функции автозагрузки внешних машинных носителей информации при их подключении к СВТ.

4. Обеспечить контроль (автоматизированный) за составом ОИС.

5. Определить перечень разрешенного ПО, регламентировать и контролировать порядок его установки и использования.

6. Регламентировать порядок использования внешних машинных носителей информации, мобильных технических средств.

11. Обеспечить идентификацию и аутентификацию пользователей ИС.

12. Своевременно блокировать (уничтожать) неиспользуемые (временно неиспользуемые) учетные записи пользователей.

13. Обеспечить доступ пользователей к ОИС на основе ролей.

14. Блокировать доступ к ОИС после истечения установленного времени бездействия (неактивности) пользователя или по его запросу.

15. Обеспечить изменение атрибутов безопасности сетевого оборудования, ПО, установленных по умолчанию.

16. Ограничить количество неуспешных попыток доступа к ОИС.

17. Контролировать соблюдение правил генерации и смены паролей пользователей.

18. Обеспечить управление физическим доступом в помещения, а также к шкафам со СВТ, сетевым и другим оборудованием.

19. Предоставлять уникальные учетные записи привилегированных пользователей для авторизованного доступа к сетевому оборудованию.

20. Предоставлять временные учетные записи пользователей для авторизованного доступа в целях обслуживания ОИС неуполномоченными сотрудниками (сторонними организациями), обеспечить их контроль и отключение.

21. Предоставлять пользователям авторизованный доступ при подключении к ОИС из-за ее пределов.

Защита почтовых серверов

22. Использовать услуги хостинга уполномоченных поставщиков интернет-услуг.

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

24. Обеспечить спам-фильтрацию почтовых сообщений.

25. Использовать механизмы шифрования почтовых сообщений и (или) передачу почтовых сообщений с использованием криптографических протоколов передачи данных (SMTPS, STARTTLS).

26. Обеспечить фильтрацию почтовых сообщений с использованием списков нежелательных отправителей почтовых сообщений.

27. Использовать механизмы проверки PTR-записи почтовых сервисов.

28. Использовать механизмы проверки SPF-записи почтовых сервисов.

29. Использовать механизмы почтовой аутентификации отправителя почтовых сообщений (DKIM).

30. Блокировать массовую рассылку почтовых сообщений.

Менеджмент активов

31. Обеспечить централизованный учет информации об ОИС, разработать схемы физических и(или) логических соединений данных объектов с указанием активов с высоким уровнем важности.

32. Регламентировать порядок удаления информации с машинных носителей информации в случае вывода их из эксплуатации.

33. Регламентировать порядок хранения неиспользуемых машинных носителей информации.

Менеджмент сети

34. Обеспечить сегментацию (изоляцию) сети доступа в Интернет от сети передачи данных (СПД) ИС.

35. Обеспечить сегментацию (изоляцию) сети управления ОИС системами видеонаблюдения, СКУД и другими объектами от СПД ИС.

36. Обеспечить сегментацию (изоляцию) сети доступа в Интернет сторонних пользователей от СПД ИС.

37. Ограничить входящий и исходящий трафик (фильтрация) определенных приложений и сервисов (мессенджеры, социальные сети, онлайн-маркеты, анонимайзеры и др.).

38. Ограничить входящий и исходящий трафик (фильтрация) ИС только необходимыми соединениями (использование межсетевого экрана).

39. Отключить неиспользуемые порты сетевого оборудования.

40. Обнаруживать и предотвращать вторжения в ИС (IPS/IDS).

41. Обеспечить доступ пользователей в сеть Интернет с применением технологии проксирования сетевого трафика.

42. Использовать ОИС локальной системы доменных имен (DNS-сервер), в том числе для доступа в сеть Интернет, либо системы доменных имен, расположенной на территории Республики Беларусь.

Менеджмент уязвимостей

43. Периодически, но не менее одного раза в год осуществлять контроль отсутствия либо невозможности использования нарушителем свойств программных, программно-аппаратных средств, которые могут быть случайно инициированы (активированы) или умышленно использованы для нарушения информационной безопасности системы и сведения о которых подтверждены изготовителями (разработчиками) этих ОИС.

44. Обеспечить обновление ПО ОИС.

45. Обеспечить исправление выявленных уязвимостей ОИС.

Аудит безопасности

46. Разработать и внедрить план реагирования на инциденты информационной безопасности.

47. Организовать взаимодействие с подразделениями информационной безопасности (командами реагирования на компьютерные инциденты) по вопросам управления событиями (инцидентами) информационной безопасности.

48. Сформировать подразделения либо назначить сотрудника(ов), ответственных за информационную безопасность.

49. Обеспечить централизованный сбор и хранение не менее одного года информации о функционировании СВТ, средств защиты информации, сетевого оборудования, систем, сервисов (netflow-трафик, лог-файлы запросов пользователей к локальным системам доменных имен, лог-файлы системы проксирования подключения к сети Интернет, лог-файлы предоставления пользователям динамических ip-адресов, лог-файлы работы серверов печати и др.), о действиях пользователей, а также о событиях информационной безопасности.

50. Периодически, но не менее одного раза в неделю осуществлять мониторинг (просмотр, анализ) событий информационной безопасности, функционирования ОИС.

51. Обеспечить защиту от несанкционированного доступа к резервным копиям, параметрам настройки сетевого оборудования и системного ПО, средствам защиты информации и событиям безопасности.

52. Осуществлять контроль за внешними подключениями к ИС.

Резервирование информации

53. Определить состав и содержание информации, подлежащей резервированию (в том числе конфигурационных файлов сетевого оборудования, лог-файлов служб и сервисов).

54. Обеспечить резервирование информации.

Дополнительные рекомендации

55. Осуществлять синхронизацию системного времени от единого источника.

Защита виртуальной инфраструктуры

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

Информирование и обучение персонала

57. Осуществлять обучение сотрудников правилам использования почтовых сервисов ИС, определения фишинговых сообщений и т.п.

58. Определять политики и процедуры информирования и обучения персонала, меры ответственности за нарушение требований по информационной безопасности.

59. Периодически, но не менее одного раза в квартал информировать персонал об угрозах информационной безопасности, правилах безопасной работы с ОИС.

60. Периодически, но не менее одного раза в год проводить с персоналом практические занятия по правилам безопасной работы с ОИС.

61. Периодически, но не менее одного раза в полугодие контролировать осведомленность персонала об угрозах информационной безопасности и о правилах безопасной работы с ОИС.

Глава 2. Рекомендации по первоначальной безопасной настройке подключения к ресурсам, размещенным в МТС Cloud

Для первого подключения к ресурсам, размещенным в МТС Cloud, клиенту передается по шифрованному каналу связи, например, средствами корпоративной почты ссылка для защищенного подключения к изолированной инфраструктуре клиента, либо данные для подключения к виртуальной машине клиента напрямую. Подключение к виртуальной машине ограниченно по портам доступа. Учетные данные для подключения передаются клиенту по шифрованным каналам связи разными способами: учетная запись, например, телефонной связью, в то время как пароль передается в зашифрованном архиве средствами корпоративной почты. Сам пароль к архиву сообщается клиенту средствами телефонной связи. После получения учетных данных и данных для подключения к инфраструктуре клиенту обязательно необходимо после первого подключения произвести смену пароля, либо создать новую учетную запись для подключения к инфраструктуре и отключить первоначальную учетную запись, использующуюся для первого подключения. После первоначальной настройки учетной записи, клиенту необходимо настроить права доступа к информационной системе – произвести настройку межсетевого экрана. Например, ограничить доступ к инфраструктуре с определенных IP адресов, либо разрешить доступ только с доверенных IP адресов, ограничить порты доступа, открыть только необходимый доступ к инфраструктуре, и другое. После настройки межсетевого экрана и смены учетных данных для подключения к инфраструктуре, первоначальная настройка инфраструктуры клиента может считаться безопасной.

Для усиления безопасности инфраструктуры клиентов, располагающих свои ресурсы на облачной платформе Huawei, доступен функционал антивирусной проверки (AV) сетевого трафика и проверки трафика системой обнаружения/предотвращения вторжений (IPS/IDS) на межсетевом экране. Так же доступен функционал логирования проходов трафика по правилам фаервола на межсетевом экране. Активация данного функционала доступна по запросу в службу технической поддержки МТС Cloud с указанием наименования клиента и правила фаервола, где данный функционал (AV, IPS/IDS, логирование) необходимо активировать. В случае добавления новых правил фаервола клиенту необходимо сформировать новый запрос в службу технической поддержки МТС Cloud с аналогичным описанием – наименование клиента, название правила фаервола, тип функционала. Обращаем ваше внимание, что данный функционал значительно усилит вашу информационную безопасность на межсетевом экране и будет блокировать вредоносную активность.

Глава 3. Рекомендации по организации удаленного доступа к информационной системе

В целях обслуживания ОИС возможно предоставление временного удаленного доступа для сотрудников сторонней организации. Данный доступ должен предоставляться путем создания временной учетной записи, с правами доступа только к необходимому сегменту ОИС. Учетная запись должна содержать персональное уникальное имя. Категорически не рекомендуется использовать чужую учетную запись и (или) передавать кому-либо данные своей учетной записи (логин, пароль и (или) иные средства аутентификации в ОИС), использовать одну учетную запись для нескольких пользователей.

Для передачи пользовательских данных необходимо пользоваться несколькими различными защищенными каналами связи для разных типов передаваемых данных. Например, передача пароля возможна средствами защищенной корпоративной почты, передача логина - телефонной связью.

Пароль к учетной записи должен соответствовать следующим требованиям:

1. длина пароля должна быть не менее 8 символов;
2. в числе символов пароля должны присутствовать символы трех категорий из числа следующих четырех:
- прописные буквы английского алфавита от A до Z;
- строчные буквы английского алфавита от a до z;
- десятичные цифры (от 0 до 9);
- неалфавитные символы (например: !, $, #, %);
3. пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии и т.д.), а также общепринятые сокращения (LAN, USER и т.п.);
4. при смене пароля новое значение должно отличаться от предыдущего не менее чем в 2 позициях;
5. Пароль желательно менять не реже 1 раза в 6 месяцев;
6. Пароль не должен совпадать с наименованием учетной записи.

При вводе пароля необходимо исключить возможность ознакомления с ними посторонних лиц. Должно быть обеспечено безопасное хранение пароля и (или) средств аутентификации, исключающее их утерю или разглашение. Категорически не рекомендуется хранить пароли в открытом доступе на предметах, бумажных носителях, дающих возможность ознакомления с ними других лиц.

Так же данный доступ должен осуществляться только под наблюдением со стороны сотрудника Компании, после выполнения работ учетная запись должна быть незамедлительно отключена.

Общие рекомендации по созданию безопасного пароля

1. Фраза

Придумайте фразу, которая имеет какое-либо значение только для Вас. Она не должна быть слишком короткой, но обязана быть запоминающейся. Например, «Каждый

охотник желает знать, где сидит фазан». Теперь возьмите первые буквы каждого слова и напишите их английскими буквами – получится неплохой пароль «Kojz,gsf».

2. Замена букв цифрами

Используем пароль из пункта 1 «Kojz,gsf» и изменим пару букв на цифры либо спецсимволы. В конечном итоге получится слово «K0jz,g$f».

3. Написание русских слов в английской раскладке клавиатуры

Придумайте слово, которая, имеет какое-либо значение только для Вас. Например, слово «Фиолетовый». Используя английскую раскладку клавиатуры, наберем данное слово. Получим «Abjktnjdsq». Для усложнения пароля используем рекомендация из пункта 2 - заменим буквы «И» на «!» и буквы «О» на «0»(ноль) и получим «A!0ktn0dsq».

4. Учет названия аккаунта

Использование одинакового пароля для различных аккаунтов – плохая идея, но простой прием может превратить Ваш единый пароль в такой пароль, который мог бы работать для каждого аккаунта. Например, если Вы хотите авторизоваться на персональном компьютере, Вы можете добавить «Pc» в начало или в конец пароля и может получиться, например, «Pc_Kojz,gsf» либо «Kojz,gsf _Pc». При необходимости авторизоваться, например, в почте добавить аналогично «M@iL», получится - «M@iL _Kojz,gsf» либо «Kojz,gsf _ M@iL».