АДМИНИСТРАЦИЯ МУНИЦИПАЛЬНОГО РАЙОНА «АЛДАНСКИЙ РАЙОН» РЕСПУБЛИКИ САХА (ЯКУТИЯ)

САХА ӨРӨСПҮҮБҮЛҮКЭТИН «АЛДАН ОРОЙУОНА» МУНИЦИПАЛЬНАЙ ОРОЙУОН ДЬАhАЛТАТА

РАСПОРЯЖЕНИЕ

ДЬАhАЛ

№ 1869 **от** 29.06. **20**22 **г.**

О мероприятиях по переносу Интернет-ресурсов (сайтов)

На основании перечня поручений Главы Республики Саха (Якутия) по итогам заседания оперативного штаба по обеспечению экономического развития Республики Саха (Якутия) от 5.04.2022 г. № Пр-748-А1 распоряжаюсь:

1. Администрации МР «Алданский район» РС (Я), МКУ «Алданская централизованная бухгалтерия»; МКУ «Томмотская централизованная бухгалтерия»; МКУ «Контрактная служба МР «Алданский район»»; МУ АР «Земельно-имущественное управление»; МКУ «Департамент образования МР «Алданский район»; МКУ «Управление сельского хозяйства» МР «Алданский район»; МКУ «Управление культуры и искусства» МР «Алданский район»; МБУ «Бизнес-инкубатор Алданского района»; МКУ «Служба управления строительством МР «Алданский район»; МУП «Алданские пассажирские перевозки» выполнить мероприятия по переносу Интернет-ресурсов (сайтов), размещенных за пределами Российской Федерации на хостинг на территории Российской Федерации в соответствии с обобщенными рекомендациями по усилению мер защиты информации интернет ресурсов, разработанными на основании рекомендаций ФСТЭК России, Национального координационного центра по компьютерным инцидентам (ФСБ России), согласно приложению №1 к настоящему распоряжению.

Срок – до 06.07.2022 г.

2. Исполнить при проведении работ по созданию или модернизации информационных систем мероприятия в соответствии с обобщенными рекомендациями по усилению мер защиты информации интернет ресурсов, разработанными на основании рекомендаций ФСТЭК России, Национального координационного центра по компьютерным инцидентам (ФСБ России).

Срок – до 23.12.2022 г.

3. Контроль распоряжения оставляю за собой.

Глава района А.В. Шестопалов

Исп. Винокуров А.С.
Тел: 6-55-55 доб. 190

Приложение 1
к постановлению №186
от «29» 06. 2022 г.

Обобщенные рекомендации по усилению мер защиты информации интернет ресурсов

1. Обеспечить размещение технических средств, используемых для обеспечения функционирования системы, на территории Российской Федерации. При этом не использовать технологические площадки филиалов иностранных компаний.
2. Отключить неиспользуемые в работе сетевые службы (сервисы).
3. Для корректной работы веб-сайтов (порталов) обеспечить использование DNS-серверов, размещенных на территории РФ. Так же убедится в отсутствии в цепочке серверов публичных иностранных серверов.
4. В случае использования для публичных ресурсов основных иностранных доменных зон (например, .com, .org и других иностранных доменных зон), перейти на использование отечественной доменной зоны .ru.
5. Ограничить использование небезопасных протоколов управления информационными ресурсами организации (например: TELNET, SNMPv1, v2, HTTP).
6. Использовать защищенные протоколы TLS v1.2 (и выше) при прохождении процедуры аутентификации пользователей в веб-приложении.
7. Запретить предоставлять в выводе сообщений об ошибках следующую информацию:
   - данные о структуре файловой системы (информация о версии операционной системы, директориях с системными файлами и системным программным обеспечением, включая пути к директориям и файлам);
   - фрагменты программного или конфигурационного кода;
   - сообщения об ошибках при передаче запросов в СУБД;
   - SQL-выражения, используемые при доступе к базе данных.
8. Выдавать пользователю страницу-заглушку с кодом HTTP-ответа веб-сервера «200» при обработке ошибок веб-сервером.
9. По возможности ограничить использование при обработке веб-сервером данных в формате XML внешних сущностей (External Entity), внешних параметров сущностей (External Parameter Entity) и внешних описаний типа документа (External Doctype), а также JSON.

10. Запретить кеширование веб-форм ввода конфиденциальной информации. Выставить атрибут HTTPOnly у параметров cookie, значения которых не должны быть доступны сценариям, выполняемым браузером. У параметров cookie, содержащих чувствительную информацию, необходимо выставить атрибут secure.

11. Проводить проверку корректности вводимых пользователем данных как на стороне клиента (с использованием сценариев, исполняемых браузером), так и на стороне сервера.

12. Использовать директивы в заголовках сообщений HTTP, определяющие применяемую кодировку. Исключить использование разных кодировок для разных источников входных данных.

13. Использовать параметризованные запросы (например, хранимые процедуры) для построения SQL-запросов. В случае отсутствия такой возможности, организовать процедуру предварительной обработки получаемых от пользователя данных (путем удаления метасимволов « ` – / *», а также следующих SQL-операторов: SELECT, UNION, ALTER, UPDATE, EXEC, DROP, DELETE и INSERT).

14. Осуществлять преобразование HTML-кода входного потока данных следующим образом:

- заменить < > на &lt и >
- заменить () на &#40 и)
- заменить # на #
- заменить & на &#38.

15. Осуществлять фильтрацию входного потока данных (например, с использованием методов Server.HTMLEncode и HttpServerUtility.HTMLEncode в ASP и ASP.NET).

16. Запретить пользователю ввод данных, в которых допустимы HTML-теги <IMG> или <TABLE>.

17. Для подсистем управления сессиями пользователей:

- организовать авторизованному пользователю веб-приложения возможность самостоятельного завершения сеанса работы в веб-приложении.
- обеспечить гарантированное удаление идентификатора соответствующей сессии по завершении сеанса работы клиента веб-приложения.
- ограничить время жизненного цикла сессии пользователя.

18. Для подсистем разграничения доступа:

- организовать доступ к защищенным ресурсам веб-приложения только после прохождения процедуры аутентификации;
- обеспечить хранение аутентификационных данных пользователей веб-приложения только в криптографически защищенном виде;
- исключить хранение аутентификационных данных (от веб-приложений, СУБД, ТКО, FTP и т.п.) в файлах конфигурации, доступных путем обращения к ним по URL;
- исключить хранение в HTML-страницах аутентификационных данных, а также информации, позволяющей сделать вывод о структуре каталогов веб-приложения на вебсервере;
- в случае, если в веб-приложении предусматривается возможность внесения изменений пользователем в принадлежащий ему профиль, внесенные изменения необходимо подтверждать дополнительной процедурой аутентификации;
- запретить использование заголовка REFERER в качестве основного механизма авторизации.

19. Отказаться от использования на веб-ресурсах (в том числе веб-сайтах) компонентов и контента, подгружаемых с внешних ресурсов, не контролируемых организацией.

20. В случае невозможности отказа от использования указанных компонентов и контента осуществлять их проверку на предмет вредоносного воздействия на отображаемую в браузерах пользователя информацию, а также возможность кражи аутентификационных данных и файлов-cookie пользователей. Далее осуществлять периодическую проверку их хэш-сумм. В случае изменения хэш-сумм – блокировать использование указанных компонентов и контента на веб-ресурсе и осуществлять их повторную проверку функциональности. В случае отсутствия потенциально вредоносного функционала – проводить дальнейшее сравнение по новой хэш-сумме.