Приложение № 1

Требования к Исполнителю по защите информации

Работы, выполняемые Исполнителем на инфраструктуре Заказчика удалённо, должны осуществляться по защищённым каналам связи, с применением сертифицированных средств криптографической защиты информации. Дистрибутив средства криптографической защиты информации и ключевую информацию предоставляет Заказчик, Заказчик также проводит настройку средства криптографической защиты информации. Порядок доступа, перечень узлов Системы (IP-адреса, протоколы, порты) и иных узлов инфраструктуры, к которым должен иметь доступ Исполнитель, время и срок доступа, также определяется Соглашением о конфиденциальности.

Исполнитель должен обеспечить защиту автоматизированного рабочего места, с которого будут проводиться удалённо работы (далее – АРМ Исполнителя) от несанкционированного доступа, обеспечить защиту переданной ему идентификационной, аутентификационной и ключевой информации. На АРМ Исполнителя должны быть установлены актуальные версии общесистемного и прикладного программного обеспечения, а также критические обновления и обновления безопасности общесистемного и прикладного программного обеспечения. На АРМ Исполнителя должно быть установлено и корректно функционировать средство антивирусной защиты, имеющее сертификат ФСТЭК, обеспечивающее функции как сигнатурного анализа, так и проактивной защиты. Работы на АРМ Исполнителя должны проводиться из-под непривилегированной учётной записи.

По окончании работ по разработке Системы Заказчиком совместно с Исполнителем должно быть проведено тестирование корректного функционирования Системы с установленными и настроенными в соответствии с политиками Заказчика средствами защиты информации

В случае выявления конфликта совместимости средств защиты информации и компонентов Системы, Исполнитель должен доработать/донастроить Систему для разрешения конфликта со средствами защиты информации.

Исполнитель не должен удалять или вносить изменения в настройки средств защиты информации на инфраструктуре Заказчика.

Исполнитель обязан обеспечить персонификацию учётных данных, используемых для доступа к Системе, т.е. у каждого работника Исполнителя должна быть персональная учётная запись для доступа к Системе.

Исполнителем при проведении работ должны выполняться организационно-распорядительные акты Заказчика в части, касающейся безопасности информации.

На компонентах Системы должно быть установлено только необходимое для функционирования программное обеспечение.

В случае возникновения у Исполнителя необходимости установки дополнительного программного обеспечения для доработки, настройки или мониторинга состояния Системы, Исполнитель в обязательном порядке согласовывает данные действия с Заказчиком. По окончании работ данное программное обеспечение должно быть удалено.

Работы по установке и настройке, техническому обслуживанию и мониторингу средств защиты информации выполняются Заказчиком по согласованию с Исполнителем. Исполнитель подтверждает работоспособность компонентов и узлов

серверов. Исполнитель принимает меры по обеспечению штатной работы Системы при выявлении негативного влияния сертифицированных СЗИ, рекомендованных для эксплуатации в составе с используемой операционной системы.

Для работы Системы должны использоваться актуальные версии общесистемного и прикладного программного обеспечения.

По итогам доработки должен быть проведен анализ избыточности компонентов Системы (изначально ненужных или необходимость в которых отпала при внесении изменений в проект), в частности, должно быть реализовано отключение функций, блоков конфигурационных файлов, учётных записей, не задействованных при функционировании Системы.

В случае возникновения у Исполнителя необходимости создания новых персональных или служебных учётных записей на серверах Заказчика (уровня операционной системы, уровня СУБД, уровня приложения), необходимо согласовать данные действия с Заказчиком. Исполнитель передает Заказчику перечень требуемых для создания учётных записей, прав доступа с обоснованием необходимости создания учётных записей и предоставления им соответствующих прав доступа. Создание идентификаторов, аутентификаторов, настройка свойств, в частности прав доступа, учётной записи проводится Заказчиком.

Исполнитель должен предоставить Заказчику перечень сетевых узлов, протоколов, портов необходимых для обеспечения взаимодействия компонентов Системы с другими информационными системами, для доступа пользователей к Системе. Также Исполнитель предоставляет Заказчику схему потоков данных между компонентами Системы, с другими информационными системами и ресурсами с указанием IP-адресов, портов, протоколов, передаваемых данных.

Список мер, которые Исполнитель выполняет при выявлении негативного влияния СЗИ на Систему по итогам выполнения работ:

- предоставление Заказчику информации об отклонении параметров работы компонентов и узлов серверов Системы от описанной в базовых характеристиках инфраструктуры серверов;
- предоставление Заказчику информации о возможных причинах таких отклонений;
- предоставление Заказчику информации о работе системы мониторинга до и после включения СЗИ;
- восстановление работоспособности Системы совместно с Заказчиком.

Анализ инцидентов, которые могут быть связаны с работой СЗИ, проводится, прежде всего, с привлечением Заказчика. Заказчик в том числе проверяет корректность настройки СЗИ, в случае необходимости отключается СЗИ для формирования заключения о влиянии или не влиянии применяемых СЗИ на компоненты и узлы серверов Системы. После формирования заключения Стороны восстанавливают эксплуатацию СЗИ и принимают совместные меры по устранению инцидентов, связанных с совместимостью СЗИ и Системы, а также меры по устранению инцидентов, связанных с совместимостью СЗИ и эксплуатируемой инфраструктуры, в т.ч. системы виртуализации, применяемой Заказчиком.

Анализ событий безопасности, которые регистрируются на серверах Системы, выполняется Заказчиком. В случае выявления в Системе инцидентов информационной безопасности, связанных с доработкой функционала в соответствии с данным техническим заданием, Заказчик привлекает Исполнителя к расследованию инцидента.

Исполнитель в свою очередь должен предоставлять всю имеющуюся у него информацию в отношении инцидента.

По окончании работ Заказчиком может быть проведён анализ уязвимостей Системы. В случае выявления уязвимостей, их устранение должно быть проведено Исполнителем в рамках текущего технического задания.

Требования к мерам защиты информации при доработках и модификациях Системы

Все новые и изменённые компоненты информационной системы должны быть совместимы с сертифицированными ФСТЭК России средствами защиты информации от несанкционированного доступа, а также средствами антивирусной защиты.

Все новые и изменённые компоненты должны соответствовать уже реализованным требованиям защиты информации существующей Системы.

При внедрении новых компонентов Системы должно быть обеспечено изменение аутентификационной информации (в частности, паролей), заданных их производителями по умолчанию (учётные записи уровня операционной системы, уровня СУБД, уровня приложения).

Требования к мерам защиты информации в Системе

Все компоненты Системы должны быть совместимы с сертифицированными ФСТЭК России средствами защиты информации от несанкционированного доступа, а также средствами антивирусной защиты.

Пользователи Системы должны однозначно идентифицироваться и аутентифицироваться для всех видов доступа, кроме тех видов доступа, которые определяются, как действия по ознакомлению с общедоступной информацией, опубликованной в Системе для доступа неограниченного числа пользователей в сети Интернет.

Доступ в Систему должен осуществляться с обязательным вводом пароля. «Прозрачный» вход в систему без ввода пароля должен быть исключён.

Если в Системе не используется идентификация и аутентификация через ЕСИА, то в Системе должна присутствовать возможность установить следующие минимальные характеристики пароля:

— длина пароля не менее восьми символов;

— длина пароля привилегированной учётной записи (администратор) не менее шестнадцати символов;

— алфавит пароля не менее 70 символов (например, прописные и строчные символы английского алфавита, цифры и специальные символы);

— максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки от 3 до 8 попыток;

— блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации от 10 до 30 минут;

— срок действия паролей не более 90 дней.

Вводимые символы пароля должны отображаться условными знаками (например, «*», «•») или не отображаться вовсе.

При внедрении компонентов Системы должно быть обеспечено изменение аутентификационной информации (в частности, паролей), заданных их

производителями по умолчанию (учетные записи уровня операционной системы, уровня СУБД, уровня приложения).

Механизмы Системы должны позволять создавать различные типы учётных записей, указанные в техническом задании, например, внутреннего пользователя, внешнего пользователя; администратора Системы, пользователя Системы, гостевая (анонимная), временная и (или) иные типы записей (при необходимости).

Механизмы Системы должны позволять объединять учётные записи в группы.

Механизмами Системы должны быть реализованы требуемые методы управления доступом, назначены типы доступа субъектов к объектам доступа и реализованы правила разграничения доступа субъектов доступа к объектам доступа.

Должны быть минимизированы права доступа как пользовательских и административных, так и служебных учетных записей.

Должно осуществляться блокирование анонимного доступа к базе данных, подключения должны производиться только для авторизованных пользователей.

Механизмами Системы должно быть реализовано блокирование учётной записи пользователя через период времени неиспользования не более 90 дней.

Механизмами Системы должно быть реализовано блокирование учётной записи в случае утраты и (или) компрометации пароля.

Механизмы Системы не должны использовать NTML в качестве протокола сетевой аутентификации. При прохождении процедуры аутентификации пользователей в web-приложении должны использоваться защищённые протоколы Kerberos (в случае доменной аутентификации) или TLS (v1.2 и выше).

Механизмами Системы должна быть реализована возможность самостоятельной смены пароля учётной записи пользователем.

В случае внесения изменений пользователем в принадлежащий ему профиль, изменения необходимо подтверждать дополнительной процедурой аутентификации.

Механизмами Системы должна быть реализована защита аутентификационной информации от неправомерного доступа к ней и модифицирования. В частности, не допускается размещение пароля для доступа к базе данных в тексте кода веб-приложения. Пароли должны храниться в Системе не в открытом, а в преобразованном виде (например, с использованием хеш-функций). При этом не допускается использовать слабые алгоритмы преобразования (например, md5, sha-1). Пароли между клиентом и Системой должны передаваться в преобразованном виде.

Должна быть реализована защита от подбора паролей и имен пользователей Системы.

При вводе неверного логина или пароля сообщения об ошибке не должны различаться. После определенного количества неверных попыток ввода пароля выдавать Captcha. Captcha должна быть защищена от автораспознавания.

Должен быть реализован функционал восстановления пароля, в котором Captcha должна выдаваться сразу.

При использовании восстановления пароля должен выдаваться ответ, не позволяющий определить наличие или отсутствие учетной записи с предъявленным идентификатором.

Механизмы Системы должны обеспечивать блокирование сеанса доступа пользователя после 15-30 минут бездействия (неактивности) пользователя. В пользовательском интерфейсе Системы после блокировки сеанса не должна отображаться информация сеанса пользователя.

Механизмы Системы должны обеспечивать ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы. Должна быть предусмотрена возможность задавать ограничения на число параллельных (одновременных) сеансов (сессий), основываясь на идентификаторах пользователей и (или) принадлежности к определенной роли. При превышении параллельных сеансов пользователь должен попадать в систему, а самая ранняя сессия должна завершаться с показом уведомления о новом входе в систему.

Механизмами Системы должен быть реализован контроль точности, полноты и правильности вводимых данных. В случаях, когда возможные значения пользовательского ввода известны заранее, рекомендуется использовать механизмы «белого списка» для проверки входных данных.

Должна быть обеспечена фильтрация загружаемых пользователями Системы файлов по расширению и mime-типу (по белому списку) во избежание передачи в Систему исполняемых файлов, в том числе на стороне сервера. В рамках данной фильтрации должны отбрасываться с уведомлением пользователя файлы бинарные и интерпретируемые, файлы у которых MIME-тип не соответствует расширению, файлы у которых MIME-тип не соответствует белому списку, файлы с двойным расширением, файлы без имени, например, .htaccess.

В случае наличия в системе интерфейсов взаимодействия (api), доступных извне необходимо ограничить доступ к api для неавторизованных запросов.

Пользователь Системы не должен иметь доступа к директориям сервера за пределами веб-приложения Системы.

В Системе должны быть минимизированы возможности пользователей по использованию функций обращения к операционной системе, при обращении к указанным функциям должна быть реализована проверка на специальные символы (символы пути к файлам и каталогам - ../, ./, консольные команды - ls, cd, dir, tree, type, systeminfo).

Должно осуществляться журналирование действий пользователей Системы. В Системе как минимум подлежат регистрации следующие события:

— вход (выход), попытки входа в Систему;

— изменение настроек Системы, в частности, изменение прав доступа пользователей, создание новых пользователей;

— выполнение задачи резервного копирования данных и настроек Системы.

В Системе, обрабатывающей персональные данные, должно осуществляться журналирование следующих операций, выполняемых с этими данными:

— редактирование;

— удаление;

— добавление;

— импорт/экспорт (в том числе в другие информационные системы);

— запрос персональных данных;

— построение отчётов.

При регистрации событий должна быть зафиксирована следующая информация:

— дата и время действия;

— описание действия (для входа (выхода) должно быть зафиксировано под какой учётной записью произведён вход/выход, для изменения настроек Системы должно быть указано, какие настройки на какие значения изменены);

— результат действия (успех/неудача).

В Системе должна быть предусмотрена возможность настроить доступ учётных записей к журналу событий. Администратор Системы и пользователи не должны иметь возможности редактировать журнал событий.

Исполнителем совместно с Заказчиком должны быть определены файлы Системы, изменение которых, критично для безопасности и/или работоспособности Системы.

Средствами Системы или механизмами средства защиты информации от несанкционированного доступа должен быть обеспечен контроль целостности указанных файлов, а также определено поведение Системы в случае изменения указанных файлов (оповещение администратора, блокировка работы Системы).

В Системе должны присутствовать механизмы по оповещению администратора о нарушениях работоспособности Системы.

В Системе должны присутствовать механизмы резервного копирования конфигурации Системы.

Сообщения об ошибках должны фиксироваться в специальных журналах, доступ к которым ограничен для посторонних лиц.

Требования к мерам защиты web-компонентов

Доступ пользователей к веб-интерфейсу Системы должен осуществляться по протоколу https. Для реализации https должен использоваться протокол TLS v1.2 и выше с запретом использования шифра RC4 и с расширением Extended Master Secret и поддержкой псевдошифронабора Fallback Signaling Cipher Suite Value). При обращении пользователя по протоколу http к веб-интерфейсу Системы он должен быть перенаправлен на соединение по https.

Доступ к административному разделу веб-приложения Системы должен быть возможен только из инфраструктуры Заказчика.

Необходимо использовать директивы в заголовках сообщений HTTP, определяющие применяемую кодировку и исключить использование разных кодировок для разных источников входных данных. Заголовок REFERER не должен использоваться в качестве основного механизма авторизации.

Использовать параметризованные SQL-запросы.

Осуществлять экранирование специальных символов (замена управляющих символов на безопасные подстановки) в отношении всех данных пользовательского ввода, использующихся в динамических SQL-запросах.

При этом должны быть учтены данные, передаваемые всеми методами HTTP-запросов (POST, GET, PUT, DELETE), в том числе, данные передаваемые через скрытые поля форм ввода, поля ввода имени пользователя и пароля, а также данные из заголовков (например, Cookie, Referer).

Реализовать функцию отслеживания источника поступающих данных путем:

- проверки его в $S_SERVERP[‘HTTPREFERER’];
- созданием скрытого поля: в форме для отслеживания источника;
- указывания имени формы при отправке на веб-сервер;
- указывания имени кнопки отправки, поля и других структурных элементов формы при отправке на веб-сервер.

Использовать фреймворки (программные платформы) с автоматической проверкой и преобразованием пользовательских данных. Должна быть реализована проверка входных данных по «белым спискам» (осуществлять проверку полей для всех

входных данных, включая заголовки, cookies, строки запросов, скрытые поля, а также длины полей форм, их тип, синтаксис, допустимые символы и другие правила, прежде чем принять данные, которые будут сохранены и отображены на сайте).

Должны быть минимизированы права доступа как пользовательских и административных, так и служебных учетных записей (в частности, учетная запись веб-сервиса не должна иметь в операционной системе прав локального администратора, подключение веб-сервиса к базе данных не должно осуществляться с правами администратора базы данных, сценарии веб-приложения не должны иметь прав по созданию и удалению каких-либо объектов в базе данных).

В веб-приложениях, написанных на ASP.NET, также должна быть запрещена загрузка web.config. Каталоги, в которых будут храниться загруженные файлы (с наследованием), не должны иметь разрешения на запуск.

Идентификаторы сессии (cookie) должны передаваться только по защищенному каналу связи (https) и должно быть реализовано ограничение, что только сценарии на сервере могут читать идентификаторы сессии (cookie). Необходимо выставить атрибут HTTPOnly у параметров cookie, значения которых не должны быть доступны сценариям, выполняемым браузером.

Идентификатор сессии (cookie) должен быть достаточно сложен и уникален для подбора во избежание атак типа подмена пользователя. В идентификаторе сессии (cookie) не должна присутствовать аутентификационная информация (логины и пароли) пользователя Системы, а также иная информация в открытом виде, позволяющая идентифицировать пользователя. У параметров cookie, содержащих чувствительную информацию, необходимо выставить атрибут secure.

В html-коде страниц Системы, в частности, в комментариях, скрытых формах и параметрах, не должно присутствовать информации, раскрывающей логику работы кода веб-приложения, критичных технических данных (логинов, паролей, IP-адресов и доменных имен, структуры файловой системы веб-приложения и веб-проекта). Также в директориях веб-приложениях не должны располагаться файлы предыдущих версии сценариев веб-приложения.

Не использовать (по возможности) метод GET в формах сайта. Если информация представляет важность, необходимо использовать метод POST.

При обработке ошибок web-сервером необходимо выдавать пользователю страницу-заглушку с кодом HTTP-ответа web-сервера «200».

Веб-сервер должен обрабатывать ошибки, генерируемые сервисом приложений, интерпретатором языка, на котором написано веб-приложение, СУБД, передавая в клиентскую часть сообщение об ошибке, не содержащее критичной технической информации (в частности, информация об наименовании и версии используемых в Системе приложений, путях к файлам и каталогам, IP-адресах и доменных именах компонентов Системы).

Необходимо ограничить использование на веб-страницах серверов информационных ресурсов (видеофайлов, электронных документов, изображений и других файлов), размещенных на сторонних серверах.

Доступ к каталогам систем контроля версий и их содержимому (таким как *.git, *.svn и другие каталоги) должен быть ограничен.

Должен быть настроен запрет выдачи листинга каталогов при отсутствии в них индексируемых файлов (если иное не предусмотрено функциональными возможностями веб-сервера).

Разрешенные, запрещенные для индексации каталоги и файлы настроить с использованием robots.txt.

Перед использованием на web-ресурсах JavaScript-кода, подгружаемого со сторонних ресурсов, должна осуществляться его проверка на предмет вредоносного воздействия на отображаемую в браузерах пользователя информацию и возможность кражи его аутентификационных данных и файлов-cookie. Должна осуществляться периодическая проверка хэш-сумм используемых JavaScript. В случае изменения хэш-сумм прекращать использование JavaScript на сайте и выполнять повторную проверку функциональности. Динамически формируемые коды JavaScript на web-ресурсе использоваться не должны.

В целях предотвращения возможности реализации атак межсайтового скриптинга по рекомендациям ФСТЭК необходимо принять следующие дополнительные меры:

- по возможности указывать кодировку на каждой веб-странице;
- использовать политику защиты содержимого (Content Security Policy, CSP);
- использовать заголовок X-XSS-Protection, предназначенный для фильтра межсайтового скриптинга, встроенного во всех современных браузерах, путем установки значения «mode=block» и внесения изменений следующего содержания:

а) для веб-сервера Apache в файле дополнительной конфигурации .htaccess необходимо добавить следующую запись:

<ifModule mod_headers.c> Header set X-XSS-Protection "1; mode=block" </IfModule>

б) для веб-сервера Nginx необходимо дополнить файл nginx.conf в разделе HTTP записью:

add_header X-XSS-Protection "1; mode=block";

в) для веб-серверов, поддерживающих PHP, необходимо использовать следующую функцию:

<?php header("X-XSS-Protection: 1; mode=block"); ?>;

- использовать экранирование входных (выходных) данных, путём применения встроенных функций для очистки кода от вредоносных скриптов, такие как htmlspecialchar(), htmlentities() и strip_tags().

Требования по защите контейнеров виртуализации

В случае использования технологий контейнеризации необходимо реализовать:

1) доступ пользователей к контейнерам с минимально необходимыми для выполнения задач правами доступа;

2) возможность работы в контейнерах пользователям, обладающим минимальными правами доступа;

3) отключение возможности повышения привилегий пользователей при работе в контейнерах (например, security-opt=no-new-privileges);

4) обеспечение доступа пользователей к контейнерам с применением защищенных протоколов передачи данных;

5) ограничение доступа контейнеров к вычислительным ресурсам хостовой операционной системы (например, квоты на использование ресурсов, AppArmor, SELinux и другие ограничения);

6) ограничение доступа контейнеров к вычислительным ресурсам узлов компьютерной сети (например, ограничить доступ к следующим параметрам: - т или —memory — доступная память до OOM; —cpus — сколько процессоров доступно

(например, 1.5); —cpuset-cpus — можно указать, какие именно процессоры доступны (ядра); —restart=on-failure : — убираем вариант Restart Always, чтобы контролировать количество перезапусков и вовремя обнаруживать проблемы; —read-only — файловая система настраивается только на чтение при запуске, особенно если контейнер отдает статику);

7) управление системным окружением контейнеров;

8) управление доступом пользователей к системе управления контейнеризацией;

9) обеспечение целостности настроек контейнеров, содержащихся в системе управления контейнеризацией.

Приложение № 2

Памятка по повышению защищённости публичных веб-ресурсов (сайтов)

1. Выполнить внеплановую смену и усилить требования к парольной политике администраторов и пользователей сайтов, исключив при этом использование паролей, заданных по умолчанию; усилить парольную политику (рекомендованная сложность пароля администратора не менее 16 символов, алфавит пароля должен содержать заглавные и строчные буквы, специальные символы и не менее трех цифр).
2. Организовать смену паролей не реже 1 раза в 90 дней.
3. Отключить сервисные и неиспользуемые учётные записи.
4. Выполнить внеплановую смену и усиление парольной политики учётных записей администраторов зоны доменных имен (DNS), проверить доступ в личный кабинет и корректность DNS-записей.
5. Обеспечить поддержку сайтами соединения с применением актуальных защищенных протоколов сетевого взаимодействия (HTTPS, SSH и других протоколов).
6. Регулярно обновлять компоненты платформы управления сайтом. При использовании Bitrix обязательно обновить модуль "Polls, Votes" (vote) до версии 21.0.100 или выше.
7. Исключить возможность применения на сайтах сервисов подсчёта сбора данных о посетителях, сервисов предоставления информации о месторасположении и иных сервисов, разработанных иностранными организациями (например, сервисов onthe.ioReCAPTCHA, YouTube, Google Analytics, Google Maps, Google Translate).
8. Исключить возможность использования встроенных видео- и аудиофайлов, интерфейсов взаимодействия API, «виджетов» и других ресурсов, загружаемых со сторонних сайтов, заменив их при необходимости гиперссылкой на такие ресурсы.
9. Провести инвентаризацию служб и веб-сервисов, используемых для функционирования сайтов, отключить неиспользуемые службы и веб-сервисы.
10. При наличии возможности подключить защиту от DdoS и Web Application Firewall.
11. Ограничить доступ к каталогам систем контроля версий и их содержимому (таким как *.git, *.svn и другие каталоги).
12. В случае использования свободно распространяемого программного обеспечения и программного кода не выполнять обновление без проверки работоспособности в тестовой среде.
13. Сократить регламентные сроки создания резервных копий, проводить регулярную проверку работоспособности резервных копий, организовать раздельное хранение копий и ресурса с ограничением доступа к резервным копиям.
14. По возможности ограничить доступ к ресурсу по географическому признаку: оставить только Россию.
15. Заключить договор на постоянную техническую поддержку ресурса с обязательным включением пунктов об обеспечении информационной безопасности ресурса и ответственностью (юридической и материальной) в случае взлома, недоступности и других инцидентов, связанных с информационной безопасностью ресурса.