УТВЕРЖДЕНО

RU.96636777.62.01.29-02 103 01-1 ЛУ

Программный комплекс «АльтерОфис Специальный»/ «AlterOffice»
Процедуры устранения недостатков
RU.96636777.62.01.29-02 103 01-1

Листов 10

2025

СОДЕРЖАНИЕ

Перечень сокращений 3

Введение 4

1 Процедура отслеживания недостатков безопасности 5

2 Процедура устранения недостатков безопасности 7

3 Регламент работ по устранению недостатков 9

Перечень сокращений

ПК AlterOffice, Изделие	-	Программный комплекс «АльтерОфис Специальный»/ «AlterOffice»
ФСТЭК России	-	Федеральная служба по техническому и экспортному контролю
БДУ	-	Банк данных угроз безопасности информации
ООО	-	Общество с ограниченной ответственностью

Введение

Настоящий документ распространяется на изделие Программный комплекс «АльтерОфис Специальный»/«AlterOffice» (далее — ПК AlterOffice, Система, Изделие, ОО). ПК AlterOffice представляет собой совокупность интегрированных программных продуктов, в котором сделан упор на его эффективное использование в коммерческих и государственных учреждениях. ПК AlterOffice – это полнофункциональный набор офисных программ.

Разработчик: ООО «Алми Партнер» (юридический адрес: 117186, г.Москва, вн.тер.г. Муниципальный округ Котловка, ул. Нагорная, д. 24 к. 9, помещ. 1/1, лицензия ФСТЭК России на деятельность по разработке и производству средств защиты конфиденциальной информации № Л050-00107-00/00584159 от 08 августа 2019 г.).

Производитель: ООО «Алми Партнер» (юридический адрес: 117186, г.Москва, вн.тер.г. Муниципальный округ Котловка, ул. Нагорная, д. 24 к. 9, помещ. 1/1).

Настоящий документ содержит процедуры устранения недостатков Изделия.

1 Процедура отслеживания недостатков безопасности

С целью выявления недостатков безопасности Изделия ООО «Алми Партнер» периодически, не реже одного раза в месяц, должен проводить поиск известных уязвимостей в общедоступных источниках информации об уязвимостях. В качестве общедоступных источников в первую очередь должны использоваться БДУ в составе банка данных угроз безопасности информации ФСТЭК России (www.bdu.fstec.ru), а также следующие дополнительные источники:

- https://cve.mitre.org/ ,
- https://nvd.nist.gov/ ,
- https://www.exploit-db.com/ ,
- http://www.rapid7.com/db/ ,
- http://www.cvedetails.com/ ,
- http://www.securitylab.ru/ и другие.

- взаимодействие с пользователями посредством обратной связи.

По каждой актуальной уязвимости из общедоступных источников и каждому запросу от пользователей Изделия производится внутренняя независимая проверка на актуальной версии Изделия. Результатом проверки является вынесение вердикта о том, является ли заявленная уязвимость или поведение, описанное в запросе пользователя, недостатком безопасности.

При анализе уязвимостей учитываются следующие критерии:

- тип ошибки;
- версию программного обеспечения, подверженную уязвимости;
- уровни опасности уязвимости:
  - Критическая (Critical);
  - Высокая (High);
  - Средняя (Medium);
  - Низкая (Low);
- информацию об устранении.

В случае выявления информации об уязвимости изделия из различных источников и отсутствия информации об этой уязвимости в БДУ (базу данных уязвимостей), Производитель предоставляет информацию о данной уязвимости во ФСТЭК России для размещения в БДУ.

При выявлении в процессе эксплуатации уязвимостей и недостатков в ПК AlterOffice потребитель должен оповестить изготовителя по адресу 117186, г.Москва, вн.тер.г. Муниципальный округ Котловка, ул. Нагорная, д. 24 к. 9, помещ. 1/1, или по электронной почте support@alteroffice.ru, или по телефону 8 (495) 150-07-80 доб. 500.

2 Процедура устранения недостатков безопасности

При выявлении уязвимостей Изделия Производитель должен осуществить следующие мероприятия:

1) разместить информационное сообщение об уязвимостях в изделии на специализированном разделе своего сайта;

2) довести информацию до конечных потребителей изделия об организационно-технических мерах по устранению уязвимостей в изделии;

3) в случае невозможности устранения уязвимостей средства защиты информации, Производитель разрабатывает ограничения по применению средства защиты информации, которые незамедлительно доводит до испытательной лаборатории;

4) если в соответствии с заключением испытательной лаборатории ограничение по применению позволит устранить уязвимость, Производитель незамедлительно и гарантированно с подтверждением доводит его до пользователей;

5) Производитель вносит необходимые изменения в эксплуатационную документацию и направляет её совместно с заключением испытательной лаборатории в ФСТЭК России. Пользователи реализуют указанное ограничение по применению средства защиты информации;

6) если пользователь не может реализовать ограничение по применению средства защиты информации он прекращает его применение;

7) если уязвимость не устраняется путем установления ограничений по применению, Производитель незамедлительно и гарантированно, с подтверждением, сообщает об этом всем пользователям и в ФСТЭК России. Пользователи прекращают применение средства защиты информации.

Доработка Изделия должна осуществляться в срок не более 60 дней с момента выявления уязвимости заявителем.

Разработка компенсирующих мер по защите информации или ограничений по применению Изделия, а также доведение информации о таких мерах и ограничениях до потребителей должны осуществляться в срок не более 48 часов с момента выявления уязвимости.

Доведение информации об уязвимостях, а также о компенсирующих мерах по защите информации или ограничениях по применению Изделия должно осуществляться до

каждого потребителя путем отправки сообщений на электронные адреса потребителей, обеспечивающего доведение указанной информации до потребителя автоматически.

В случае невозможности устранения уязвимости, в том числе путем применения обновления, Производитель незамедлительно доводит до испытательной лаборатории информацию об ограничениях по применению Изделия. Если в соответствии с заключением испытательной лаборатории ограничения по применению позволит устранить уязвимость, Производитель незамедлительно и гарантированно с подтверждением доводит их до потребителя. Производитель вносит необходимые изменения в эксплуатационную документацию и направляет её совместно с заключением испытательной лаборатории в ФСТЭК России. Потребители реализуют указанное ограничение по применению Изделия. Если потребитель не может реализовать ограничение по применению Изделия, он прекращает его применение.

Если уязвимость не устраняется путем установления ограничений по применению, Производитель незамедлительно и гарантированно, с подтверждением, сообщает об этом потребителю и в ФСТЭК России.

3 Регламент работ по устранению недостатков

Инженер Предприятия-изготовителя, получивший заявку на устранение недостатков, производит ее первичное рассмотрение. На этом этапе перед ним ставится задача выяснить, решается ли проблема с помощью изменения настроек конфигурации той версии Изделия, которая стоит у заказчика, или же она связана с наличием ошибки в самом Изделии.

В первом случае инженер готовит рекомендации по изменению конфигурации Изделия и направляет их клиенту.

Если проблему решить удалось, то диспетчер Технического центра присваивает заявке статус завершенной. Для наиболее типичных случаев готовится краткое заключение с изложением способа решения и размещается в корпоративной информационной базе.

При невозможности разрешить проблему с помощью конфигурирования Изделия инженер Технического центра производит поиск в доступных источниках (интернете) информации о подобных ситуациях – недостатках средства, в том числе о недостатках в компонентах, заимствованных у сторонних изготовителей.

Инженер готовит рекомендации по изменению конфигурации Изделия и направляет их клиенту.

Во втором случае, при невозможности разрешить проблему с помощью конфигурирования Изделия, речь идет о недостатках безопасности самого Изделия. В этом случае инженер оформляет документ «Извещение об ошибке», и заявка в комплекте с этим документом направляется в группу тестирования подразделения разработчиков. «Извещении об ошибке» должно содержать:

- установленную у потребителя версию Изделия;
- условия эксплуатации, при которых возникла ошибка;
- частоту повторяемости ошибки;
- степень критичности для функционирования Изделия;
- данные о среде функционирования (информационное окружение).

Диспетчер Технического центра делает в базе заявок отметку о направлении Извещения и посылает потребителю уведомление, что его проблема может быть решена в новой версии Изделия.

Группа тестирования регистрирует поступающие извещения. Все сведения заносятся в специальную форму в базе данных Группы, что позволяет упростить (ускорить) решение «типовых» запросов.

Если в результате анализа неисправности не удалось найти решение, тогда ситуация моделируется на стенде Группы и приглашаются разработчики, которые должны устранить неисправность и представить Группе тестирования новую версию Изделия.

После устранения неисправности разработчиками, Группа тестирования осуществляет комплексные приемо-сдаточные испытания Изделия. Проверке подлежат:

- отсутствие заявленной аварийной ситуации;
- наличие у новой версии Изделия всех заявленных функциональных возможностей.

По результатам тестирования составляется протокол проверки и принимается решение о внесении необходимых изменений в эксплуатационную документацию – замечание исправлено, процесс устранения ошибки не затронул остальную часть функционала Изделия.

После внесения Предприятием-изготовителем необходимых изменений в эксплуатационную документацию, информация о них доводится до испытательной лаборатории, которая утверждает соответствие на измененные сведения.

Далее Производитель вносит необходимые изменения в эксплуатационную документацию и направляет её совместно с заключением испытательной лаборатории в ФСТЭК России. Пользователи реализуют указанное ограничение по применению средства защиты информации.

После получения от потребителя подтверждения о ликвидации проблемы, диспетчер Технического центра присваивает заявке статус завершенной.

Если пользователь не может реализовать ограничение по применению средства защиты информации, он прекращает его применение.

Если уязвимость не устраняется путем установления ограничений по применению, Производитель незамедлительно и гарантированно, с подтверждением, сообщает об этом всем пользователям и в ФСТЭК России. Пользователи прекращают применение средства защиты информации.