# КОМПЛЕКСНАЯ ОЦЕНКА УЯЗВИМОСТЕЙ ИНФОРМАЦИИ В ЗОНЕ ДЗУ СЕТЕВОЙ ФАЙЛОВОЙ СИСТЕМЫ

***Абдоков Аслан Ращидович***

*Северо-Кавказская государственная академия, г.Черкесск*

*В ходе исследования проведена комплексная оценка уязвимостей информации в зоне ДЗУ сетевой файловой системы, проведен анализ типовых нападений на зону ДЗУ сетевой файловой системы. На основе полученных результатов предложены рекомендуемые рубежи защиты.*

**Ключевые слова:** информационная безопасность, ДЗУ, нападения, утечка данных, информация, защита, сетевая файловая система, оценка уязвимостей.

В современном мире широкое распространение получили сетевые технологии. Они используются как частными лицами для познавательно развлекательных целей, так и компаниями для обмена различного рода информацией. В ходе эксплуатации сетевых технологий для обмена данными встал вопрос удобства передачи и хранения данных, которые могли бы быть использованы разными людьми в одной сети. Для решения этого вопроса был придуман File Transfer Protocol (FTP) сервер. Он позволял скачивать и загружать на него информацию, но не позволял обрабатывать ее непосредственно на нем, что приводило к большим временным затратам.

Этих недостатков были лишены Network File System (NFS) сервера, которые могли быть подключены к компьютерам конечных пользователей, но при этом компьютер воспринимал информацию на нем так, словно это еще один жесткий диск внутри его корпуса. Это позволило значительно облегчить и ускорить обмен и обработку данных в современных сетях.

С развитием сетевых технологий были выявлены множество различных угроз информации, приводящих к её утечке\искажению, в то числе и в NFS. Так как, последние используются почти в каждой корпоративной сети, было необходимо произвести исследования основных угроз и найти способы противостоять им. Существуют различные виды угроз для различных контуров сети. Далее будут рассмотрены основные угрозы сетевой файловой системы в зоне долговременного запоминающего устройства (ДЗУ).

Основными видами угроза сетевой файловой системы в зоне ДЗУ являются:

1) загрузка с несанкционированного носителя; 2) прямой доступ к информации на носителе; 3) перехват информации.

Под загрузкой с несанкционированного носителя подразумевается возможность обхода встроенных сетевых средств защиты файлов путем загрузки с недоверенной операционной системы, которая позволит видоизменять файлы на доверенном ДЗУ или же заносить на него вредоносное ПО.

Данную угрозу можно нейтрализовать несколькими способами: средствами доверенной загрузки, например, Secret Net, блокировка недоверенных устройств при помощи антивирусного ПО, а также ограничением физического доступа к устройству.

Под прямой доступ к информации на носителе подразумевается возможность прочтения информации на носителе, например при похищении ДЗУ.

Данная угроза нейтрализуется шифрованием данных на ДЗУ любым из известных методов. Это может быть, как встроенное шифрование на системах Windows и Unix, так и отдельные шифрование специализированными программными продуктами.

Под угрозой перехвата информации подразумевается возможность считывания информации на выходе серверного или клиентского оборудования, а также перехвата информации во время её транспортировки по линиям связи.

Чтобы избежать этого типа атак необходимо: реализовать end-to-end шифрованные при передаче данных от сервера к клиенту и обратно, что позволить избежать легкого прочтения данных при реализации атаки. Так же необходимо максимально снизить паразитное электромагнитное излучение, что так затруднит попытку перехвата информации.

На основе проведенного исследования были выявлены возможные нападения на зону ДЗУ сетевой файловой системы и необходимые меры для нейтрализации этих угроз.

## Литература

1. Чипига А. Ф. Информационная безопасность автоматизированных систем. М: «Гелиос АРВ», 2010. 336 с.
2. Сагдеев К. М. Физические основы защиты информации: учебное пособие /

К. М. Сагдеев, В. И. Петренко, А. Ф. Чипига. Санкт-Петербург, 2017.

1. Чипига А. Ф. Модель трехмерной структуры объектов с матрицей доступа / А. Ф. Чипига, А. А. Ерещенко, Пелешенко В. С. // Известия ЮФУ. Технические науки. 2009.

С. 172-176.

1. Чипига А. Ф. Методология обнаружения и предотвращения угроз и компьютерных атак на информационные системы и психику людей / А. Ф. Чипига, В. С. Пелешенко // Информационное противодействие угрозам терроризма, 2010. С. 114-118.
2. Чипига А. Ф. Объектный подход к модели разграничения доступа в компьютерных системах / А. Ф. Чипига, А. А. Ерещенко // Информационное противодействие угрозам терроризма, 2005. С. 122-128.
3. Чипига А. Ф. Влияние упакованных форматов протоколов измерений на скорость обработки данных в адаптивных системах спутниковой связи / А. Ф. Чипига, Д. М. Марков, Г. В. Слюсарев // Фундаментальные исследования, 2015. С. 759.
4. Securelist. Лаборатория Касперского. [Электронный ресурс] URL:

https://securelist.ru/spam-and-phishing-in-2017/88630/

1. Infowatch. Аналитика. [Электронный ресурс] URL: https://www.infowatch.ru/analytics