ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ
Федеральное государственное образовательное
бюджетное учреждение
высшего профессионального образования
«Поволжский государственный университет телекоммуникаций и информатики»

Л. Толстого ул., 23, г. Самара, 443010. Телефон 846-333-58-56, www.psuti.ru, E-mail: info@psati.ru

_____№ _____ На № РШ-П30-2055 от 17.06.2014 г.

Заместителю руководителя
Федерального агентства связи

Р.В. Шередину

Уважаемый Роман Валериевич!

В соответствии с письмом РШ-П30-2055 от 17.06.2014 «О предоставлении информации» ФГОБУ ВПО «Поволжский государственный университет телекоммуникаций и информатики» направляет Вам доклад о состоянии технической защиты информации за июль 2014 года.

Приложения: доклад о состоянии технической защиты информации за июль.

Ректор В.А. Андреев

Осипов О.В. (846) 333-32-04

«Утверждаю»

Ректор ФГОБУ ВПО ПГУТИ

проф. _____ В.А. Андреев

«1» августа 2014 г.

Доклад о состоянии технической защиты информации в ФГОБУ ВПО «Поволжский государственный университет телекоммуникаций и информатики» за июль 2014 года

№	Объект защиты	Состояние технической защиты
1	Файловые сервера ПГУТИ	Для защиты информации на файловых серверов ФГОБУ ВПО ПГУТИ используется программное обеспечение Kaspersky EndPoint Security. Указанный программный продукт позволяет осуществлять защиту всех файловых серверов ПГУТИ, работающих как под управлением ОС Windows, так и Linux. Выбор антивирусного ПО обусловлен реализации в нем механизмов гибридной защиты. Также к информации на файловых серверах ПГУТИ применяется механизм разграничения доступа с использованием Active Directory. Определение прав доступа к информации осуществляется через доменные учетные записи пользователей.
2	Почтовый сервер	Для защиты почтового сервера применяется способ, базирующийся на доступе из внешних сетей только через web-интерфейс (блокировка доступа через 25 порт). Для фильтрации спама во входящих сообщениях используется совместное использование технологии Яндекс. Спамоборона и антиспам фильтра Microsoft.
3	Система контроля доступа в помещения	Для управления системой используется ПО ParsecNET. Контроль доступа осуществляется на основе учетных записей пользователей с разграничением прав.
4	Подключение к информационной системе ФИС-ЕГЭиП	Подключение к общероссийской информационной системе ФИС-ЕГЭиП осуществляется через автоматизированное рабочее место (АРМ), созданное по адресу: г. Самара, Московское шоссе, 77, ауд. 2-02-13. Взаимодействие между Федеральным центром тестирования и ФГОБУ ВПО ПГУТИ осуществляется посредством специализированного АРМ, оборудованного сертифицированными по требованиям безопасности информации ФСТЭК России и ФСБ России средств защиты информации и средств криптографической защиты информации (программа CryptoPro). Используется программное обеспечение ViPNet Client и средство защиты от несанкционированного доступа Dallas Lock 8.0.
5	Домен ПГУТИ	Контроль доступа к информационным ресурсам осуществляется на основе учетных записей пользователей с разграничением прав (механизм аутентификации пользователей).

№	Объект защиты	Состояние технической защиты
6	VPN-доступ	Контроль доступа к информационным ресурсам через VPN-доступ осуществляется на основе учетных записей пользователей с разграничением прав (механизм аутентификации пользователей). Для защиты передаваемой информации организован сетевой экран. Ежеквартальная смена паролей пользователей для доступа к VPN.
7	Web-сайты	В ПГУТИ используется nginx — web-сервер, работающий под управлением операционной системы Linux. Ежеквартальная смена паролей доступа администраторов сайтов к FTP и базам данных. Запрет создания новых баз данных администраторами сайтов. Еженедельное резервное копирование информации и сохранение дампов баз данных.
8	Wi-Fi	Защита Wi-Fi сети осуществляется на уровне настроек коммутатора Cisco — открыты только 80 порт и 443 порт (протокол HTTPS, SSL-соединение).
9	IP-телефония	Контроль доступа к информационным ресурсам осуществляется на основе учетных записей пользователей с разграничением прав (механизм аутентификации пользователей). Ежеквартальная смена паролей пользователей. Внешний выход IP-телефонов осуществляется только через сервер Ростелекома/
10	Персональные данные в финансово-экономическом управлении (ФЭУ)	Для защиты информации бухгалтерии используется контролируемый сервер доступа в сеть Интернет с рабочих мест сотрудников ФЭУ/
11	Система управления дистанционным обучением	Доступ осуществляется по защищенному протоколу HTTPS (SSL-соединение). Контроль доступа к информационным ресурсам системы дистанционного обучения осуществляется на основе учетных записей пользователей с разграничением прав (механизм аутентификации пользователей с реализацией технологии личных кабинетов).
12	Система электронного документооборота	Контроль доступа к информационным ресурсам осуществляется на основе учетных записей пользователей с разграничением прав (механизм аутентификации пользователей). Ежеквартальная смена паролей пользователей.

Проректор по информатизации
и образовательным технологиям О.В. Осипов

01.08.2014 г.