گزارپیش‌نویس طرح روردین ماه سال ۱۳۹۵

قسمت اول:مشخصات مربوط به طرح پژوهشی

۱-۱ـ عنوان طرح پژوهشی:

تحقیقاتی گزارش نهایی تائیدیه طرح:

عنوان طرح:

ارتقای ضریب امنیت پایگاههای اطلاعات پژوهشی استان مستقر در مرکزداده سازمان مدیریت و برنامه‌ریزی استان آذربایجان‌شرقی**واحد فناوری اطلاعات**

مقدمه:

ادی کاربردی

مقدمه

۱-۳ـ موضوع تحقیق:

با توجه به توانمندیهای بدنه کارشناسی سازمان، این طرح توسط نیروی انسانی سازمان انجام شد

۱-۴ـ توجیه اقتصادی و فنی:

امنیت شبکه شامل مقررات و سیاست‌های اتّخاذ شده توسط مدیریت شبکه است که به منظور جلوگیری و نظارت بر دسترسی غیرمجاز، سوءاستفاده، اصلاح، یا ایجاد محدودیت در شبکه‌های کامپیوتری و منابع قابل دسترس در شبکه، تدوین و اعمال می‌گردد. با توجه به اهمیت این موضوع و حفظ اطلاعات در مرکز داده خرید و نصب تجهیزات فایروال در راستای ارتقای امنیت اطلاعات دارای توجیه اقتصادی و فنی می‌باشد.

۱-۵- اهداف تحقیق:

دستیابی به یک پایگاه داده با ضریب امنیت بالا

دسترس پذیری بالا به سرور و اطلاعات و داده ها

ارتقای امنیت فضای تبادل اطلاعات

۱-۶- محدودهٔ مکانی تحقیق :

سازمان مدیریت و برنامه‌ریزی استان آذربایجان‌شرقی

۱-۷- محدودهٔ زمانی:

از مورخه ۹۴/۱۲/۱۵

۱-۸ـ اهمیت، ضرورت تحقیق:

با امنیت اقدامات زیر معمول گردد.

۱-۹- طرح موضوع و بیان مساله:

امنیت شبکه از تصدیق هویّت کاربر و معمولاً توسط یک نام کاربری و یک رمز عبور آغاز می‌شود. پس از تصدیق هویت، دیوارآتشین (فایروال) اجرای سیاست‌های دسترسی را اعمال می‌کند؛ از قبیل اینکه چه خدماتی مجاز هستند که در دسترس کاربران شبکه قرار بگیرند.
مدیریت امنیت برای شبکه‌ها، برای انواع شرایط مختلف، متفاوت است. یک خانه کوچک یا یک دفتر تنها به یک امنیت ابتدایی نیاز دارد؛ در حالی که کسب و کارهای بزرگ نیازمند محافظت در سطح بالا و داشتن نرم‌افزارها و سخت‌افزارهای پیشرفته برای جلوگیری از حملات بدخواهانه‌ای چون هک کردن و ارسال ایمیل‌های ناشناس هستند.

برای یک سازمان دولتی بزرگ در جهت حفظ امنیت اطلاعات انجام موارد زیر ضروریست :

- از یک دیوار آتش و پروکسی قوی استفاده کنید تا افراد ناخواسته را دور نگه دارید.
- از یک بسته حاوی نرم‌افزارهای آنتی ویروس قوی و نرم‌افزارهای امنیت اینترنت استفاده کنید.
- رمزنگاری قوی را به کار ببندید.
- همه سخت‌افزارهای شبکه در محل‌های امنی وجود دارند.
- همه میزبان‌ها می‌بایست در یک شبکه خصوصی باشند تا از زاویه بیرونی، نامرئی به نظر آیند.
- از خارج و از داخل، سرورها و تجهیزات در یک DMZ یا یک دیوار آتش قرار دهید.
- حصار امنیتی را برای علامت گذاری محیط و تخصیص محدوده‌های بی‌سیم به آنها، به کار ببندید.

با توجه به موراد مذکور استفاده از فایروال یا دیواره آتش بسیار مهم و حیاتی است. فایروال‌ها حفاظت لازم در مقابل مهاجمان خارجی را ایجاد و یک لایه و یا پوسته حفاظتی پیرامون کامپیوتر و یا شبکه را در مقابل کدهای مخرب و یا ترافیک غیرضروری اینترنت، ارائه می‌نمایند. با بکارگیری فایروال‌ها، امکان بلاک نمودن داده از مکانی خاص فراهم می‌گردد. امکانات ارائه شده توسط یک فایروال برای کاربرانی که همواره به اینترنت متصل هستند، بسیار حیاتی و مهم می‌باشد. فایروال ها به دو شکل سخت افزاری(خارجی) و نرم افزاری(داخلی)، ارائه می‌شوند. هر یک از مدل های فوق دارای مزایا و معایب خاص خود می‌باشند. فایروال های سخت افزاری نوعی از فایروال ها هستند که به آنان فایروال‌های شبکه نیز گفته می شود و بین کامپیوترهای شبکه و کابل و یا خط DSL قرار خواهند گرفت. فایروال های سخت افزاری، دستگاههای سخت افزاری مجزائی می باشند که دارای سیستم عامل اختصاصی خود می باشد. بنابراین بکارگیری آنان باعث ایجاد یک لایه دفاعی اضافه در مقابل تهاجمات می‌گردد.

۱-۹- خروجیها

۱) دسترس پذیری بالا به سرور و اطلاعات و داده ها
۲) ارتقای امنیت فضای تبادل اطلاعات

۱-۱۰- زمانبندی اجرای طرح

ردیف	فعالیت	مدت زمان
۱	**خرید و نصب فایروال**	خریداری و نصب گردید

قسمت دوم:اطلاعات مربوط به هزینه‌های اجرای طرح

۲-۱ـ هزینهٔ پرسنلی با ذکر مشخصات کامل و میزان اشتغال هریک و حق‌الزحمهٔ آنها:

۲-۲ـ فهرست دستگاه و وسایل: (غیر مصرفی)

۲-۳ سایر هزینه ها:

۲-۴ـ جمع هزینه‌های طرح: