۱- محور پروژه

☐ تولید ☐ عمومی ☒ توزیع ☐ مطالعات کلان انرژی، اقتصادی و مدیریتی ☐ انرژی‌های نو و تجدید پذیر

۲ - عنوان دقیق پروژه:

طراحی و پیاده سازی سیستم مدیریت رویداد و اطلاعات امنیتی (SIEM)

۳ - تعریف مسئله / دلایل اولویت داشتن تحقیق: (سابقه موضوعی، اقدامات انجام‌شده و نتایج به‌دست‌آمده، سابقه استفاده کاربردی در کشورهای پیشرفته بیان شود- انجام پروژه چه مشکلی از صنعت برق را حل خواهد نمود، صرفه‌جویی ناشی از انجام پروژه اعلام گردد- زیان‌های ناشی از عدم انجام پروژه روی سایر تجهیزات ذکر شود- تعداد موردنیاز اعلام گردد و ...)

با افزایش سطح دیجیتال‌سازی و استفاده از سیستم‌های کنترل صنعتی(ICS) ، سیستم‌های نظارت و کنترل(SCADA) ، شبکه‌های هوشمند (Smart Grid) و سامانه‌های اطلاعاتی یکپارچه، زیرساخت‌های فناوری اطلاعات شرکت توزیع نیروی برق در معرض تهدیدات متعدد سایبری و فیزیکی قرار گرفته‌اند. این تهدیدات می‌توانند منجر به اختلال در عملیات، نشت اطلاعات حساس، خسارات مالی و کاهش قابلیت اطمینان شبکه توزیع شوند.

شبکه‌های توزیع برق به‌عنوان یک زیرساخت حیاتی ملی، همواره هدف اصلی حملات سایبری و اقدامات تخریبی فیزیکی بوده‌اند. وقوع حملاتی مانند استاکس‌نت(Stuxnet) ، حمله به شبکه برق اوکراین (۲۰۱۵) و سریال حملات به شبکه‌های انرژی ایران، ضرورت ایجاد سیستم‌های جامع مدیریت ریسک را به‌طور جدی آشکار کرده است.

در حال حاضر، ارزیابی ریسک‌های سایبری و فیزیکی در شرکت توزیع خراسان جنوبی به‌صورت پراکنده، غیرسیستماتیک و عمدتاً مبتنی بر تجربه انجام می‌شود. عدم وجود یک چارچوب یکپارچه ارزیابی ریسک، منجر به شکاف‌های امنیتی، عدم شناسایی به‌موقع نقاط بحرانی و عدم اولویت‌بندی صحیح اقدامات ایمن‌سازی شده است. همچنین، یکپارچه‌سازی بین امنیت سایبری و امنیت فیزیکی در سطح عملیاتی ضعیف است.

اجرای این پروژه می‌تواند به شناسایی جامع نقاط ضعف، اولویت‌بندی ریسک‌ها، ارائه راهکارهای فنی و اداری، و در نهایت افزایش مقاومت شبکه کمک کند. صرفه‌جویی‌های انتظاری شامل کاهش ۴۰-۶۰٪ در خطر وقوع حوادث سایبری، کاهش هزینه‌های بازیابی پس از حادثه، جلوگیری از جریمه‌های نظارتی و افزایش اعتماد عمومی به خدمات برق است.

عدم انجام این پروژه می‌تواند منجر به قطعی‌های گسترده، خسارت به تجهیزات حساس (مانند ترانسفورماتورها و سرورهای کنترل)، نشت اطلاعات مشترکان و کارکنان، و حتی تهدید امنیت ملی شود. همچنین، عدم تطابق با الزامات ملی (سازمان تنظیم مقررات، مرکز ملی فضای مجازی) و بین‌المللی (ISO/IEC ۲۷۰۰۱, NIST) می‌تواند مانع از دریافت گواهی‌های امنیتی و همکاری‌های فنی شود.

در کشورهای پیشرفته مانند آمریکا، آلمان و سوئد، سیستم‌های مدیریت یکپارچه ریسک سایبری-فیزیکی (Cyber-Physical Risk Management) به‌عنوان بخشی از استراتژی امنیت زیرساخت‌های حیاتی اجرا می‌شوند. استفاده از چارچوب‌هایی مانند NIST CSF، ISO/IEC ۲۷۰۰۵ و IEC ٦٢٤٤٣، به این سازمان‌ها کمک کرده تا به‌صورت پیشگیرانه و سیستماتیک با تهدیدات روبرو شوند.

۴ - وجوه تمایز و اشتراک اولویت پیشنهادی نسبت به کارهای انجام شده قبلی یا جاری مشابه چیست؟

وجه تمایز اصلی این پروژه، یکپارچه‌سازی ارزیابی ریسک‌های سایبری و فیزیکی در یک چارچوب واحد و منطقه‌محور است. برخلاف اقدامات قبلی که عمدتاً بر یکی از این دو حوزه (سایبری یا فیزیکی) متمرکز بوده‌اند، این پروژه به‌طور همزمان بر هر دو بعد تمرکز دارد و تأثیر متقابل آن‌ها را بررسی می‌کند (مثلاً: دسترسی فیزیکی به سرور باعث فعال‌سازی بدافزار می‌شود).

همچنین، این پروژه با تمرکز بر ویژگی‌های منحصر به فرد استان خراسان جنوبی — از جمله مناطق مرزی، شبکه‌های طولانی، شرایط اقلیمی سخت و توزیع جغرافیایی پراکنده — راهکارهای سفارشی‌سازی شده و قابل اجرا ارائه می‌دهد. این رویکرد منطقه‌محور، فراتر از اجرای یک چارچوب عمومی است.

استفاده از روش‌های پیشرفته و استاندارد بین‌المللی مانند NIST SP ۸۰۰-۳۰، ISO/IEC ۲۷۰۰۵، و ماتریس ریسک TARA (Threat and Risk Assessment) برای سیستم‌های سایبرفیزیکی، از دیگر وجوه تمایز است. همچنین، توسعه یک سامانه تعاملی یا داشبورد مدیریت ریسک (به‌عنوان خروجی نرم‌افزاری) برای نمایش نقشه ریسک، پیگیری اقدامات و گزارش‌دهی دوره‌ای، این پروژه را از گزارش‌های کاغذی و غیرعملیاتی متمایز می‌کند.

در نهایت، تمرکز بر ارائه راهکارهای عملیاتی و اولویت‌بندی شده (فنی، اداری، آموزشی و تجهیزاتی) برای هر ریسک شناسایی شده، این پروژه را به یک بسته اجراپذیر و تصمیم‌سازی برای مدیریت شرکت تبدیل می‌کند.

۵ – اهداف مورد انتظار و مراحل کلی انجام تحقیق :

- اهداف کلی:

شناسایی جامع ریسک‌های سایبری و فیزیکی در زیرساخت‌های IT و OT شرکت توزیع برق.

ارزیابی و رتبه‌بندی ریسک‌ها بر اساس احتمال وقوع و شدت پیامد.

ارائه راهکارهای فنی، اداری و تجهیزاتی برای کاهش یا حذف هر ریسک.

توسعه یک چارچوب مستند و قابل تکرار برای مدیریت ریسک در آینده.

افزایش آگاهی و ظرفیت سازمانی در حوزه امنیت سایبری و فیزیکی.

طراحی و پیاده‌سازی سیستم SIEM متمرکز برای پایش امنیت سایبری.

- مراحل کلی اجرا:

❖ تشکیل تیم چند رشته‌ای و تعریف محدوده (۱,۵ ماه):

شامل متخصصان امنیت سایبری، امنیت فیزیکی، شبکه، و مدیریت بحران.

❖ شناسایی دارایی‌های حیاتی و نقشه‌برداری زیرساخت‌ها (۲ ماه):

شناسایی سرورها، شبکه‌ها، سیستم‌های SCADA، مراکز کنترل، ایستگاه‌ها و نقاط دسترسی فیزیکی.

❖ شناسایی تهدیدات و آسیب‌پذیری‌ها (۲ ماه):

استفاده از روش‌های STRIDE (سایبری)، TARA (فیزیکی)، و بازدید میدانی.

❖ ارزیابی ریسک و رتبه‌بندی (۱,۵ ماه):

استفاده از ماتریس ریسک (احتمال × پیامد) و اولویت‌بندی ریسک‌های بحرانی.

❖ توسعه راهکارهای مدیریت ریسک (۲ ماه):

ارائه راهکارهای فنی (فایروال، رمزگذاری، نظارت مرکزی)، اداری (سیاست‌های دسترسی)، آموزشی و تجهیزاتی (دوربین، کنترل دسترسی).

❖ پیاده‌سازی آزمایشی و آموزش (۲ ماه):

اجرای راهکارها در یک منطقه نمونه و آموزش کارکنان.

❖ گزارش نهایی و ارائه نقشه راه (۱ ماه):

ارائه گزارش جامع، داشبورد مدیریت ریسک و برنامه گسترش.

❖ ارائه سامانه تحت وب شناسایی ریسک (۲ ماه):

امکان شناسایی ریسک و فرایند های مرتبط با قابلیت بروزرسانی ریسک ها پس از انجام اقدامات و یا توسعه زیرساخت ها

۶ – الزامات واستانداردهای لازم جهت رعایت در انجام این پروژه چیست؟

اسناد بالادستی ملی:

سند ملی انرژی

برنامه‌های توسعه پنج‌ساله کشور
مصوبات شورای عالی انرژی
دستورالعمل‌های سازمان تنظیم مقررات و ارتباطات رادیویی (ATIC)
ضوابط مرکز ملی فضای مجازی
استانداردهای بین‌المللی:
ISO/IEC ۲۷۰۰۱ (مدیریت امنیت اطلاعات)
ISO/IEC ۲۷۰۰۵ (ارزیابی ریسک)
NIST Cybersecurity Framework (CSF)
NIST SP ۸۰۰-۳۰ (ارزیابی ریسک)
IEC ٦٢٤٤٣ (امنیت سیستم‌های اتوماسیون صنعتی)
ISO ۳۱۰۰۰ (مدیریت ریسک)
الزامات فنی و امنیتی:
عدم تداخل با سیستم‌های کنترل عملیاتی (OT) در حین تست
رعایت حریم خصوصی و امنیت داده‌ها
استفاده از ابزارهای تست نفوذ مجاز و ثبت تمامی فعالیت‌ها
رمزگذاری داده‌های حساس و دسترسی مبتنی بر نقش (RBAC)

۷- مشخصات محصول نهایی پروژه: ☑ گزارش ☑ نرم افزار ☐ سخت افزار ☐ دستورالعمل

در صورتی‌که خروجی به‌صورت نرم‌افزار باشد- سیستم‌عامل پیشنهادی: **تحت وب** ☒ **ویندوز** ☐ **اندروید** ☐

سایر .....

مشخصات فنی محصول:

سامانه شناسایی ریسک و ثبت فرایندهای پیگیری

نقشه تعاملی ریسک: نمایش نقاط بحرانی در شبکه با رنگ‌بندی (قرمز، نارنجی، زرد)

ثبت و پیگیری ریسک: ثبت ریسک، انتساب مسئول، وضعیت اجرا، تاریخچه تغییرات

ماتریس ریسک پویا: محاسبه خودکار سطح ریسک بر اساس احتمال و پیامد

پیشنهاد راهکار: ارائه خودکار راهکارهای فنی، اداری و تجهیزاتی برای هر ریسک

۸- واحد بهره‌بردار نتایج تحقیق: دفتر IT معاونت برنامه ریزی و تحقیقات

۹ - پیش‌بینی مدت‌زمان اجرای پروژه (ماه) : ۱۴ ماه	**۱۰- پیش بینی مبلغ (میلیون ریال): ۲۰۰۰۰۰۰۰۰۰**
نام شخص پیشنهاددهنده پروژه :	**شماره تماس:**

دلایل تحقیقاتی بودن

امضاء

☐ پروژه‌های بهینه‌سازی سیستم‌ها و روش‌ها که با تغییر یا اصلاح در طراحی، عملکرد و بهره‌برداری و با روش‌های شناخته‌شده یا ابداعی و یا تلفیقی انجام‌پذیر می‌باشند.

☐ پروژه‌های طراحی و ساخت سیستم‌ها و دستگاه‌ها برای اولین بار در کشور (مشابه‌سازی و نمونه‌سازی) که باهدف کسب هرگونه دانش فنی طراحی، ساخت و تکمیل تجهیزات و سیستم‌ها انجام می‌شوند.

☐ پروژه‌های بررسی‌های فنی که با بهبود و تغییر روش‌ها و یا توسعه در سیستم‌ها، کاهش هزینه‌های سرمایه‌گذاری و یا بهره‌برداری را به دنبال داشته باشند.

☐ پروژه‌هایی که شامل تلفیق روش‌های موجود و انتخاب روش تلفیقی درزمینهٔ موردنظر باشند. در این پروژه‌ها، بایستی برتری روش تلفیقی بر روش‌های موجود نشان داده شود.

☐ پروژه‌هایی که متضمن کار در مرزهای دانش و فن باشند.

☐ پروژه‌هایی که برای اولین بار روش‌های شناخته‌شده روی سیستم‌ها و تجهیزات را پیاده می‌کنند. فاز اجرایی (عملیاتی) این پروژه‌ها باکار عملی توأم با آزمایش همراه است.

☐ پروژه‌هایی که برای اولین بار با انجام مطالعات موردی مشکلی از مشکلات صنعت برق را حل نمایند.

☐ پروژه‌هایی که شامل آزمایش‌های خاص و غیرمعمول روی سیستم‌ها با روش‌های شناخته‌شده باشند. این آزمایش‌ها، بایستی استاندارد بوده و یا توسط مرجع معتبری تائید شده باشند.

☐ پروژه‌هایی که شامل آزمایش‌های خاص روی سیستم‌ها با روش‌های ابداعی به‌صورت شبیه‌سازی نرم‌افزاری یا سخت‌افزاری باشند. در این پروژه‌ها روش‌های ابداعی با روش‌های استاندارد مقایسه می‌شوند.

☐ مطالعات مرتبط با مدیریت، نیروی انسانی و مسائل اجتماعی که برای اولین بار انجام‌شده و نتایج آن‌ها مورداستفاده در صنعت برق باشد.

☐ مطالعات مرتبط با مسائل مالی و اقتصادی در جهت کاهش هزینه‌های جاری و سرمایه‌گذاری در صنعت برق که برای اولین بار انجام گیرد.

☐ پروژه‌های مشابه با تفاوت اصولی درروش تحقیق، اجرا و یا کاربرد در مناطق مختلف

☐ پروژه‌های باهدف تداوم و تکمیل پروژه‌های انجام‌شده قبلی

☐ پروژه‌های مشابه با تکنولوژی بالا و یا به‌منظور تسریع یا اطمینان در حصول نتیجه و دست‌یابی به فنون مختلف