مجله دستاوردهای نوین در مطالعات علوم انسانی
سال نهم، شماره ۹۷، خرداد ۱۴۰۵
ISSN: ۲۵۸۸-۶۹۶۷
www. jonahs.ir

چالش‌های امنیت سایبری در حفاظت از داده‌های حساس شرکت‌های آب و فاضلاب: مروری بر تهدیدها و راهکارها

عاطفه دانشور [۱] ، عیسی موسایی باغستانی [۲] ، سارا طغرالجردی [۳]

[۱] کارشناسی ارشد مدیریت بازرگانی – بازاریابی، شرکت آب و فاضلاب بندرعباس، استان هرمزگان، ایران (نویسنده مسئول)
[۲] کارشناسی کامپیوتر گرایش نرم افزار، شرکت آب و فاضلاب بندرعباس، استان هرمزگان، ایران
[۳] کارشناسی ارشد معماری کامپیوتر، شرکت آب و فاضلاب بندرعباس، استان هرمزگان، ایران

چکیده

با گسترش فناوری‌های دیجیتال و هوشمندسازی زیرساخت‌های شهری، امنیت سایبری به یکی از مهم‌ترین چالش‌های مدیریت زیرساخت‌های حیاتی تبدیل شده است. شرکت‌های آب و فاضلاب به عنوان یکی از مهم‌ترین ارائه‌دهندگان خدمات عمومی، به طور گسترده از سامانه‌های اطلاعاتی، سامانه‌های کنترل صنعتی و فناوری‌های ارتباطی برای مدیریت و پایش شبکه‌های آبرسانی استفاده می‌کنند. هرچند استفاده از این فناوری‌ها موجب افزایش کارایی عملیاتی و بهبود مدیریت منابع آب شده است، اما در عین حال سطح آسیب‌پذیری این زیرساخت‌ها در برابر تهدیدهای سایبری را نیز افزایش داده است. هدف از این پژوهش، بررسی و تحلیل چالش‌های امنیت سایبری در حفاظت از داده‌های حساس و زیرساخت‌های اطلاعاتی شرکت‌های آب و فاضلاب است. این پژوهش با استفاده از روش مرور نظام‌مند منابع علمی انجام شده است. در این راستا، مقالات و مطالعات مرتبط منتشرشده در پایگاه‌های علمی معتبر بین‌المللی و داخلی از جمله Scopus، ScienceDirect، IEEE Xplore، Web of Science و Google Scholar در بازه زمانی ۲۰۱۵ تا ۲۰۲۶ مورد بررسی قرار گرفتند. پس از فرآیند غربالگری و ارزیابی کیفیت مطالعات، مجموعه‌ای از پژوهش‌های مرتبط انتخاب و با استفاده از روش تحلیل محتوای کیفی مورد بررسی قرار گرفتند. نتایج پژوهش نشان می‌دهد که مهم‌ترین تهدیدهای سایبری در زیرساخت‌های آبی شامل حملات باج‌افزاری، نفوذ به سامانه‌های کنترل صنعتی، بدافزارها و دسترسی غیرمجاز به داده‌های حساس است. همچنین وجود تجهیزات قدیمی، ضعف در مدیریت دسترسی کاربران، نبود سامانه‌های پیشرفته تشخیص نفوذ و کمبود نیروی متخصص از جمله مهم‌ترین آسیب‌پذیری‌های امنیتی در این حوزه محسوب می‌شوند. یافته‌ها نشان می‌دهد که ارتقای امنیت سایبری در شرکت‌های آب و فاضلاب نیازمند ترکیبی از راهکارهای فنی و مدیریتی است. استفاده از سامانه‌های تشخیص نفوذ، رمزنگاری داده‌ها، احراز هویت چندمرحله‌ای، جداسازی شبکه‌های عملیاتی و توسعه سیاست‌های سازمانی امنیت اطلاعات از جمله مهم‌ترین راهکارهای پیشنهادی در مطالعات بررسی‌شده هستند. در مجموع، نتایج این پژوهش نشان می‌دهد که اتخاذ رویکردی جامع و چندبعدی در مدیریت امنیت سایبری می‌تواند نقش مهمی در افزایش تاب‌آوری زیرساخت‌های آبی در برابر تهدیدهای سایبری ایفا کند.

واژه‌های کلیدی: امنیت سایبری، زیرساخت‌های حیاتی، شرکت‌های آب و فاضلاب، سامانه‌های SCADA، امنیت داده‌ها، زیرساخت‌های آب

مقدمه

در دهه‌های اخیر، توسعه فناوری‌های دیجیتال و گسترش زیرساخت‌های اطلاعاتی موجب تحول اساسی در نحوه مدیریت و بهره‌برداری از زیرساخت‌های حیاتی شده است. یکی از مهم‌ترین این زیرساخت‌ها، سامانه‌های تأمین و توزیع آب و همچنین مدیریت شبکه‌های فاضلاب شهری است که نقش حیاتی در سلامت عمومی، پایداری محیط زیست و توسعه اقتصادی جوامع ایفا می‌کنند. شرکت‌های آب و فاضلاب برای مدیریت مؤثر منابع آبی، کنترل کیفیت آب، پایش شبکه‌های توزیع و ارائه خدمات به مشترکان، به طور گسترده از سامانه‌های اطلاعاتی، پایگاه‌های داده و سیستم‌های کنترل صنعتی استفاده می‌کنند. این روند موجب شده است که حجم قابل توجهی از داده‌های حساس شامل اطلاعات مشترکان، داده‌های عملیاتی شبکه، اطلاعات زیرساختی و داده‌های مربوط به کیفیت آب در سامانه‌های دیجیتال ذخیره و پردازش شوند. در نتیجه، حفاظت از این داده‌ها به یکی از مهم‌ترین چالش‌های مدیریتی و فنی در حوزه زیرساخت‌های آبی تبدیل شده است (بویس و همکاران، ۲۰۱۸؛ احمد و همکاران، ۲۰۲۱).

با افزایش اتصال سامانه‌های صنعتی و مدیریتی به شبکه‌های ارتباطی، به‌ویژه در چارچوب تحول دیجیتال و استفاده از فناوری‌هایی نظیر اینترنت اشیا، رایانش ابری و سامانه‌های هوشمند مدیریت منابع آب، سطح آسیب‌پذیری این زیرساخت‌ها در برابر تهدیدهای سایبری نیز افزایش یافته است. بسیاری از شرکت‌های آب و فاضلاب از سامانه‌های کنترل صنعتی مانند SCADA برای پایش و کنترل فرآیندهای عملیاتی استفاده می‌کنند. این سامانه‌ها که در گذشته اغلب به صورت مستقل و بدون اتصال به شبکه‌های عمومی طراحی شده بودند، امروزه به منظور افزایش کارایی و امکان مدیریت از راه دور به شبکه‌های ارتباطی متصل شده‌اند. این اتصال، در کنار مزایای مدیریتی، فرصت‌های جدیدی را نیز برای مهاجمان سایبری فراهم کرده است (هومیِر و همکاران، ۲۰۲۱؛ چرادی و همکاران، ۲۰۱۸).

در سال‌های اخیر، نمونه‌های متعددی از حملات سایبری به زیرساخت‌های آبی در نقاط مختلف جهان گزارش شده است که نشان‌دهنده افزایش تهدیدات در این حوزه است. این حملات می‌توانند پیامدهای گسترده‌ای از جمله اختلال در ارائه خدمات، دستکاری داده‌های عملیاتی، افشای اطلاعات حساس مشترکان و حتی تهدید سلامت عمومی داشته باشند. برای مثال، برخی حملات سایبری توانسته‌اند به سامانه‌های کنترل صنعتی نفوذ کرده و پارامترهای عملیاتی تصفیه‌خانه‌های آب را تغییر دهند که در صورت عدم شناسایی به موقع می‌تواند پیامدهای جدی برای کیفیت آب آشامیدنی داشته باشد (کاردل و همکاران، ۲۰۱۷). علاوه بر این، افزایش حملات باج‌افزاری علیه سازمان‌های خدمات عمومی نیز نگرانی‌های جدیدی در خصوص امنیت داده‌ها و تداوم خدمات ایجاد کرده است.

از سوی دیگر، بسیاری از زیرساخت‌های فناوری اطلاعات در شرکت‌های آب و فاضلاب دارای ویژگی‌هایی هستند که آن‌ها را در برابر تهدیدهای سایبری آسیب‌پذیرتر می‌کند. استفاده از تجهیزات قدیمی، محدودیت منابع مالی برای به‌روزرسانی سامانه‌ها، نبود چارچوب‌های جامع امنیت سایبری و کمبود نیروی انسانی متخصص از جمله عواملی هستند که می‌توانند سطح امنیت این سازمان‌ها را کاهش دهند (رودریگز و همکاران، ۲۰۲۰؛ احمد و همکاران، ۲۰۲۱). علاوه بر این، پیچیدگی فنی سامانه‌های کنترل صنعتی و تفاوت آن‌ها با سامانه‌های فناوری اطلاعات متداول

باعث می‌شود که پیاده‌سازی راهکارهای امنیتی در این محیط‌ها با چالش‌های خاصی همراه باشد (بویس و همکاران، ۲۰۱۸).

در پاسخ به این چالش‌ها، پژوهش‌های متعددی در سال‌های اخیر به بررسی ابعاد مختلف امنیت سایبری در زیرساخت‌های آبی پرداخته‌اند. برخی از این مطالعات بر شناسایی تهدیدها و آسیب‌پذیری‌های موجود تمرکز داشته‌اند، در حالی که برخی دیگر به توسعه چارچوب‌ها و راهکارهای فنی برای افزایش سطح امنیت این زیرساخت‌ها پرداخته‌اند. برای مثال، پژوهش‌هایی در زمینه استفاده از سامانه‌های تشخیص نفوذ، روش‌های پیشرفته رمزنگاری، تحلیل رفتار شبکه و به‌کارگیری هوش مصنوعی برای شناسایی حملات سایبری در سامانه‌های کنترل صنعتی انجام شده است (چرادی و همکاران، ۲۰۱۸؛ احمد و همکاران، ۲۰۲۱). همچنین برخی مطالعات بر اهمیت رویکردهای مدیریتی و سیاست‌گذاری در ارتقای امنیت سایبری تأکید کرده‌اند و نشان داده‌اند که توسعه چارچوب‌های حکمرانی امنیت اطلاعات، آموزش کارکنان و مدیریت ریسک سایبری می‌تواند نقش مهمی در کاهش آسیب‌پذیری‌های سازمانی ایفا کند (هومیرِ و همکاران، ۲۰۲۱).

با وجود رشد قابل توجه مطالعات در این حوزه، بررسی ادبیات موجود نشان می‌دهد که پژوهش‌های انجام‌شده اغلب به صورت پراکنده و در چارچوب‌های تخصصی مختلف منتشر شده‌اند و هنوز نیاز به یک تحلیل جامع و نظام‌مند از یافته‌های پژوهشی وجود دارد. چنین مروری می‌تواند با تجمیع نتایج مطالعات مختلف، تصویری روشن‌تر از مهم‌ترین تهدیدها، آسیب‌پذیری‌ها و راهکارهای پیشنهادی در زمینه امنیت سایبری زیرساخت‌های آبی ارائه دهد. علاوه بر این، تحلیل تطبیقی مطالعات پیشین می‌تواند به شناسایی شکاف‌های پژوهشی و جهت‌گیری‌های آینده در این حوزه کمک کند.

بر این اساس، هدف اصلی این مقاله ارائه یک مرور تحلیلی از مطالعات انجام‌شده درباره چالش‌های امنیت سایبری در حفاظت از داده‌های حساس در شرکت‌های آب و فاضلاب است. در این مقاله تلاش شده است تا با بررسی نظام‌مند پژوهش‌های منتشرشده در سال‌های اخیر، مهم‌ترین تهدیدهای سایبری در زیرساخت‌های آبی، آسیب‌پذیری‌های سامانه‌های اطلاعاتی و کنترل صنعتی، و همچنین راهکارهای فنی و مدیریتی برای ارتقای امنیت داده‌ها مورد تحلیل قرار گیرد. نتایج این مطالعه می‌تواند به مدیران زیرساخت‌های آبی، سیاست‌گذاران حوزه امنیت سایبری و پژوهشگران کمک کند تا درک جامع‌تری از چالش‌های موجود داشته باشند و راهبردهای مؤثرتری برای حفاظت از داده‌های حساس در این بخش حیاتی طراحی کنند.

ادبیات و پیشینه موضوع

با گسترش فناوری‌های دیجیتال و اتصال زیرساخت‌های حیاتی به شبکه‌های ارتباطی، موضوع امنیت سایبری به یکی از حوزه‌های مهم پژوهشی در مدیریت زیرساخت‌های عمومی تبدیل شده است. زیرساخت‌های آبی از جمله سامانه‌های تأمین، تصفیه و توزیع آب و همچنین شبکه‌های جمع‌آوری و تصفیه فاضلاب به دلیل وابستگی شدید به سامانه‌های اطلاعاتی و کنترل صنعتی، به طور فزاینده‌ای در معرض تهدیدهای سایبری قرار گرفته‌اند. پژوهش‌های

انجام‌شده در این حوزه نشان می‌دهند که آسیب‌پذیری‌های موجود در سامانه‌های فناوری اطلاعات و سامانه‌های کنترل صنعتی می‌توانند زمینه‌ساز حملات سایبری با پیامدهای گسترده برای خدمات عمومی و امنیت داده‌ها شوند (بویس و همکاران، ۲۰۱۸).

یکی از حوزه‌های مهم مطالعاتی در ادبیات امنیت سایبری زیرساخت‌های آبی، بررسی آسیب‌پذیری سامانه‌های کنترل صنعتی است. سامانه‌های SCADA و سایر سامانه‌های کنترل صنعتی به طور گسترده برای پایش و کنترل فرآیندهای عملیاتی در تصفیه‌خانه‌ها، ایستگاه‌های پمپاژ و شبکه‌های توزیع آب مورد استفاده قرار می‌گیرند. پژوهش‌ها نشان می‌دهند که بسیاری از این سامانه‌ها در زمان طراحی با فرض عدم اتصال به شبکه‌های عمومی توسعه یافته‌اند و به همین دلیل در برابر تهدیدهای سایبری جدید آسیب‌پذیر هستند. بویس و همکاران (۲۰۱۸) در مطالعه‌ای درباره امنیت سایبری سامانه‌های کنترل صنعتی در زیرساخت‌های حیاتی نشان دادند که ضعف در احراز هویت کاربران، استفاده از پروتکل‌های ارتباطی ناامن و نبود مکانیزم‌های پیشرفته تشخیص نفوذ از مهم‌ترین عوامل افزایش ریسک امنیتی در این سامانه‌ها محسوب می‌شوند.

در سال‌های اخیر، پژوهش‌های متعددی به بررسی تهدیدهای سایبری علیه زیرساخت‌های آبی پرداخته‌اند. کاردل و همکاران (۲۰۱۷) با تحلیل سناریوهای حملات سایبری به زیرساخت‌های آب نشان دادند که مهاجمان می‌توانند از طریق نفوذ به سامانه‌های کنترل صنعتی یا شبکه‌های فناوری اطلاعات، داده‌های عملیاتی را دستکاری کرده یا فرآیندهای تصفیه و توزیع آب را مختل کنند. این موضوع می‌تواند پیامدهایی از جمله اختلال در ارائه خدمات، افزایش هزینه‌های عملیاتی و حتی تهدید سلامت عمومی را به همراه داشته باشد.

علاوه بر تهدیدهای مرتبط با سامانه‌های کنترل صنعتی، برخی پژوهش‌ها به بررسی امنیت داده‌های حساس در شرکت‌های آب و فاضلاب پرداخته‌اند. داده‌های مربوط به مشترکان، اطلاعات زیرساخت‌های شبکه و داده‌های عملیاتی از جمله اطلاعات حساسی هستند که در صورت دسترسی غیرمجاز می‌توانند مورد سوءاستفاده قرار گیرند. احمد و همکاران (۲۰۲۱) در پژوهشی درباره امنیت سایبری زیرساخت‌های آبی نشان دادند که افزایش استفاده از سامانه‌های مدیریت داده، اینترنت اشیا و فناوری‌های ابری در این حوزه موجب افزایش سطح حملات سایبری شده است. این پژوهش تأکید می‌کند که بدون توسعه چارچوب‌های جامع امنیت سایبری، دیجیتالی شدن زیرساخت‌های آبی می‌تواند خطرات امنیتی جدیدی ایجاد کند.

بخش دیگری از ادبیات پژوهش به توسعه راهکارهای فنی برای مقابله با تهدیدهای سایبری اختصاص دارد. چرادی و همکاران (۲۰۱۸) در مطالعه‌ای درباره امنیت سامانه‌های کنترل صنعتی نشان دادند که استفاده از سامانه‌های تشخیص نفوذ مبتنی بر یادگیری ماشین می‌تواند به شناسایی سریع‌تر حملات سایبری در شبکه‌های صنعتی کمک کند. همچنین برخی پژوهش‌ها به کاربرد فناوری‌های رمزنگاری و روش‌های احراز هویت چندمرحله‌ای برای افزایش امنیت داده‌ها در زیرساخت‌های حیاتی اشاره کرده‌اند (رودریگز و همکاران، ۲۰۲۰).

در کنار راهکارهای فنی، برخی مطالعات بر اهمیت رویکردهای مدیریتی و سیاست‌گذاری در حوزه امنیت سایبری تأکید کرده‌اند. هومیرِ و همکاران (۲۰۲۱) در پژوهشی درباره حکمرانی امنیت سایبری در زیرساخت‌های حیاتی نشان

دادند که توسعه سیاست‌های امنیت اطلاعات، آموزش کارکنان و ایجاد ساختارهای مدیریتی مناسب برای مدیریت ریسک سایبری می‌تواند نقش مهمی در کاهش آسیب‌پذیری سازمان‌ها ایفا کند. این پژوهش‌ها نشان می‌دهند که امنیت سایبری صرفاً یک مسئله فنی نیست، بلکه نیازمند رویکردی چندبعدی شامل فناوری، مدیریت و سیاست‌گذاری است.

در مجموع، بررسی ادبیات پژوهش نشان می‌دهد که مطالعات انجام‌شده در زمینه امنیت سایبری زیرساخت‌های آبی را می‌توان در سه محور اصلی طبقه‌بندی کرد: نخست، پژوهش‌هایی که به شناسایی تهدیدها و آسیب‌پذیری‌های سامانه‌های کنترل صنعتی و زیرساخت‌های اطلاعاتی پرداخته‌اند؛ دوم، مطالعاتی که راهکارهای فنی برای افزایش امنیت سامانه‌ها ارائه داده‌اند؛ و سوم، پژوهش‌هایی که بر ابعاد مدیریتی و سیاست‌گذاری امنیت سایبری در زیرساخت‌های حیاتی تمرکز داشته‌اند. با این حال، بسیاری از پژوهش‌ها به صورت موردی انجام شده‌اند و هنوز نیاز به تحلیل جامع و یکپارچه از یافته‌های مطالعات مختلف وجود دارد.

جدول ۱. نمونه‌ای از مهم‌ترین مطالعات انجام‌شده در حوزه امنیت سایبری زیرساخت‌های آبی

پژوهشگر	سال	موضوع پژوهش	مهم‌ترین یافته‌ها
کاردل و همکاران	۲۰۱۷	تحلیل تهدیدهای سایبری در زیرساخت‌های آب	حملات سایبری می‌توانند فرآیندهای عملیاتی شبکه آب را مختل کنند و پیامدهای جدی برای خدمات عمومی داشته باشند
بویس و همکاران	۲۰۱۸	امنیت سامانه‌های کنترل صنعتی در زیرساخت‌های حیاتی	آسیب‌پذیری‌های SCADA از مهم‌ترین نقاط ضعف امنیتی در زیرساخت‌های حیاتی هستند
چرادی و همکاران	۲۰۱۸	روش‌های تشخیص نفوذ در سامانه‌های صنعتی	استفاده از یادگیری ماشین می‌تواند دقت شناسایی حملات سایبری را افزایش دهد
رودریگز و همکاران	۲۰۲۰	راهکارهای امنیتی در شبکه‌های صنعتی	استفاده از رمزنگاری و احراز هویت چندمرحله‌ای موجب افزایش امنیت سامانه‌ها می‌شود
احمد و همکاران	۲۰۲۱	امنیت سایبری در زیرساخت‌های آبی هوشمند	گسترش اینترنت اشیا و دیجیتالی شدن زیرساخت‌ها موجب افزایش سطح حملات سایبری شده است
هومیِر و همکاران	۲۰۲۱	حکمرانی امنیت سایبری در زیرساخت‌های حیاتی	سیاست‌گذاری امنیتی و آموزش نیروی انسانی نقش مهمی در کاهش ریسک سایبری دارند

روش پژوهش

این پژوهش از نوع مطالعه مروری نظام‌مند است که با هدف تحلیل و تجمیع یافته‌های مطالعات پیشین در زمینه چالش‌های امنیت سایبری در حفاظت از داده‌های حساس شرکت‌های آب و فاضلاب انجام شده است. در پژوهش‌های مروری، به جای جمع‌آوری داده‌های میدانی، تمرکز اصلی بر بررسی و تحلیل نظام‌مند منابع علمی منتشرشده در یک

حوزه مشخص است تا از طریق مقایسه و ترکیب نتایج مطالعات مختلف، تصویری جامع از وضعیت دانش موجود ارائه شود (کیچنهام و چارترز، ۲۰۰۷).

در این مطالعه، فرآیند مرور منابع بر اساس چند مرحله اصلی شامل جستجوی نظام‌مند منابع، غربالگری مطالعات، انتخاب مقالات مرتبط و تحلیل محتوای آن‌ها انجام شده است. در مرحله نخست، برای شناسایی مطالعات مرتبط از پایگاه‌های علمی معتبر بین‌المللی و داخلی استفاده شد. مهم‌ترین پایگاه‌های مورد استفاده شامل اسکوپوس، ساینس دایرکت، آی‌تریپل‌ای (IEEE Xplore)، اسپرینگر، وب آو ساینس، گوگل اسکالر و پایگاه‌های علمی فارسی بوده است. انتخاب این پایگاه‌ها به دلیل پوشش گسترده پژوهش‌های مرتبط با امنیت سایبری، سامانه‌های کنترل صنعتی و زیرساخت‌های حیاتی انجام شده است.

در مرحله بعد، برای جستجوی مقالات از ترکیبی از کلیدواژه‌های مرتبط با موضوع پژوهش استفاده شد. برخی از مهم‌ترین کلیدواژه‌های مورد استفاده شامل «امنیت سایبری»، «زیرساخت‌های حیاتی»، «سامانه‌های کنترل صنعتی»، «امنیت داده‌ها»، «زیرساخت‌های آب»، «شرکت‌های آب و فاضلاب»، ««Cybersecurity، Critical Infrastructure Security»، ««Water Infrastructure Security» و «SCADA Security» بوده است. جستجوی منابع بر اساس این کلیدواژه‌ها در عنوان، چکیده و کلیدواژه‌های مقالات انجام شد.

برای افزایش دقت مرور، معیارهایی برای انتخاب منابع در نظر گرفته شد. نخست آنکه تنها مطالعات منتشرشده بین سال‌های ۲۰۱۵ تا ۲۰۲۶ مورد بررسی قرار گرفتند تا تمرکز پژوهش بر یافته‌های جدید و به‌روز باشد. دوم آنکه تنها مقالات منتشرشده در نشریات علمی معتبر، کنفرانس‌های بین‌المللی و گزارش‌های پژوهشی معتبر در فرآیند مرور قرار گرفتند. همچنین مطالعاتی که به طور مستقیم به موضوع امنیت سایبری در زیرساخت‌های حیاتی، سامانه‌های کنترل صنعتی یا زیرساخت‌های آب مرتبط نبودند از فرآیند تحلیل حذف شدند.

پس از مرحله جستجو، فرآیند غربالگری منابع انجام شد. در این مرحله ابتدا عنوان و چکیده مقالات بررسی شد و مطالعات غیرمرتبط حذف گردیدند. در مرحله بعد، متن کامل مقالات منتخب مورد بررسی قرار گرفت و تنها مطالعاتی که دارای ارتباط مستقیم با موضوع پژوهش و دارای کیفیت علمی مناسب بودند در تحلیل نهایی استفاده شدند. در نهایت، مجموعه‌ای از مطالعات منتخب به عنوان مبنای تحلیل ادبیات پژوهش مورد استفاده قرار گرفت.

در مرحله نهایی، برای تحلیل مطالعات منتخب از روش تحلیل محتوای کیفی استفاده شد. در این روش، یافته‌های پژوهش‌های مختلف بر اساس موضوعات مشترک دسته‌بندی شده و سپس مورد مقایسه و تحلیل قرار گرفتند. مهم‌ترین محورهای تحلیل شامل انواع تهدیدهای سایبری در زیرساخت‌های آبی، آسیب‌پذیری‌های سامانه‌های اطلاعاتی و کنترل صنعتی، و راهکارهای پیشنهادی برای ارتقای امنیت سایبری بوده است. این رویکرد تحلیلی امکان شناسایی روندهای پژوهشی، نقاط اشتراک و تفاوت مطالعات و همچنین خلأهای موجود در ادبیات علمی را فراهم می‌کند.

جدول ۲. مراحل انجام مرور نظام‌مند منابع در پژوهش

مرحله	شرح فعالیت
مرحله اول	تعیین موضوع پژوهش و تعریف کلیدواژه‌های جستجو
مرحله دوم	جستجوی مقالات در پایگاه‌های علمی معتبر داخلی و بین‌المللی
مرحله سوم	غربالگری اولیه بر اساس عنوان و چکیده مقالات
مرحله چهارم	بررسی متن کامل مطالعات و حذف منابع غیرمرتبط
مرحله پنجم	انتخاب مقالات نهایی برای تحلیل
مرحله ششم	تحلیل کیفی یافته‌های پژوهش‌ها و دسته‌بندی موضوعی نتایج

جدول ۳. معیارهای انتخاب و حذف منابع در مرور پژوهش

معیار انتخاب منابع	توضیح
بازه زمانی انتشار	مطالعات منتشرشده بین سال‌های ۲۰۱۵ تا ۲۰۲۶
نوع منبع	مقالات علمی معتبر، کنفرانس‌های بین‌المللی و گزارش‌های پژوهشی
ارتباط موضوعی	تمرکز بر امنیت سایبری زیرساخت‌های آبی و سامانه‌های کنترل صنعتی
کیفیت علمی	انتشار در نشریات معتبر یا پایگاه‌های علمی شناخته‌شده
معیار حذف منابع	**توضیح**
عدم ارتباط با موضوع	مطالعاتی که به امنیت سایبری زیرساخت‌های آب مرتبط نبودند
منابع قدیمی	مطالعات منتشرشده قبل از سال ۲۰۱۵
منابع غیرعلمی	گزارش‌ها یا مطالب فاقد اعتبار علمی

یافته‌های پژوهش

تحلیل مطالعات منتشرشده در حوزه امنیت سایبری زیرساخت‌های آبی نشان می‌دهد که پژوهش‌های انجام‌شده عمدتاً بر چند محور اصلی تمرکز دارند. این محورها شامل شناسایی انواع تهدیدهای سایبری در زیرساخت‌های آبی، بررسی آسیب‌پذیری سامانه‌های کنترل صنعتی و سامانه‌های اطلاعاتی، توسعه راهکارهای فنی برای مقابله با حملات سایبری و همچنین ارائه چارچوب‌های مدیریتی و سیاست‌گذاری برای ارتقای امنیت سایبری در سازمان‌های خدمات عمومی است. بررسی تطبیقی این مطالعات نشان می‌دهد که امنیت سایبری در شرکت‌های آب و فاضلاب یک مسئله چندبعدی است که علاوه بر جنبه‌های فنی، به عوامل مدیریتی، سازمانی و سیاست‌گذاری نیز وابسته است.

۱. تهدیدهای سایبری در زیرساخت‌های آب و فاضلاب

یکی از موضوعات اصلی در مطالعات امنیت سایبری زیرساخت‌های آبی، شناسایی انواع تهدیدهای سایبری است که می‌توانند سامانه‌های اطلاعاتی و عملیاتی این سازمان‌ها را هدف قرار دهند. پژوهش‌ها نشان می‌دهند که

زیرساخت‌های آبی به دلیل اتصال به شبکه‌های ارتباطی، استفاده از سامانه‌های کنترل صنعتی و ذخیره حجم زیادی از داده‌های حساس، به هدف جذابی برای مهاجمان سایبری تبدیل شده‌اند (کاردل و همکاران، ۲۰۱۷).

بررسی مطالعات مختلف نشان می‌دهد که حملات باج‌افزاری، نفوذ به سامانه‌های کنترل صنعتی، حملات بدافزاری، دستکاری داده‌های عملیاتی و دسترسی غیرمجاز به اطلاعات مشترکان از جمله مهم‌ترین تهدیدهای سایبری در این حوزه هستند. احمد و همکاران (۲۰۲۱) نشان می‌دهند که با گسترش زیرساخت‌های هوشمند و اینترنت اشیا در مدیریت منابع آب، سطح حملات سایبری نیز افزایش یافته است. همچنین برخی پژوهش‌ها به خطر حملات هدفمند علیه زیرساخت‌های حیاتی اشاره کرده‌اند که می‌توانند با هدف ایجاد اختلال در خدمات عمومی انجام شوند (بویس و همکاران، ۲۰۱۸).

جدول ۴. مهم‌ترین تهدیدهای سایبری در زیرساخت‌های آب

نوع تهدید	توضیح	پیامدهای احتمالی
حملات باج‌افزاری	رمزگذاری داده‌ها و درخواست باج برای بازیابی آن‌ها	اختلال در ارائه خدمات و از دست رفتن داده‌ها
نفوذ به سامانه‌های SCADA	دسترسی غیرمجاز به سامانه‌های کنترل صنعتی	دستکاری فرآیندهای عملیاتی
بدافزارها	نفوذ نرم‌افزارهای مخرب به شبکه سازمانی	سرقت اطلاعات و اختلال در سیستم‌ها
حملات مبتنی بر اینترنت اشیا	سوءاستفاده از تجهیزات هوشمند متصل به شبکه	دسترسی غیرمجاز به شبکه‌های عملیاتی
دسترسی غیرمجاز به داده‌ها	نفوذ به پایگاه‌های داده مشترکان	افشای اطلاعات حساس

۲. آسیب‌پذیری‌های سامانه‌های اطلاعاتی و کنترل صنعتی

مطالعات مختلف نشان می‌دهند که بسیاری از زیرساخت‌های آبی دارای آسیب‌پذیری‌های فنی و ساختاری هستند که می‌توانند زمینه‌ساز حملات سایبری شوند. یکی از مهم‌ترین این آسیب‌پذیری‌ها مربوط به سامانه‌های کنترل صنعتی است که در بسیاری از موارد با در نظر گرفتن ملاحظات امنیت سایبری طراحی نشده‌اند (چرادی و همکاران، ۲۰۱۸).

برخی از پژوهش‌ها نشان می‌دهند که استفاده از تجهیزات قدیمی، نبود به‌روزرسانی‌های امنیتی، ضعف در مدیریت دسترسی کاربران و نبود سامانه‌های پیشرفته تشخیص نفوذ از جمله مهم‌ترین نقاط ضعف در امنیت سایبری زیرساخت‌های آبی هستند (رودریگز و همکاران، ۲۰۲۰). همچنین پیچیدگی فنی شبکه‌های صنعتی و تفاوت آن‌ها با

شبکه‌های فناوری اطلاعات متداول باعث می‌شود که بسیاری از راهکارهای امنیتی رایج به سادگی در این محیط‌ها قابل پیاده‌سازی نباشند.

جدول ۵. مهم‌ترین آسیب‌پذیری‌های امنیتی در زیرساخت‌های آبی

نوع آسیب‌پذیری	توضیح
تجهیزات قدیمی	استفاده از سامانه‌هایی که به‌روزرسانی امنیتی ندارند
ضعف در مدیریت دسترسی	نبود کنترل مناسب برای دسترسی کاربران
نبود سامانه‌های تشخیص نفوذ	دشواری در شناسایی سریع حملات سایبری
اتصال ناامن شبکه‌های صنعتی	اتصال مستقیم SCADA به شبکه‌های عمومی
کمبود نیروی متخصص امنیت سایبری	محدودیت در مدیریت و پایش امنیت سیستم‌ها

۳. راهکارهای فنی برای افزایش امنیت سایبری

در پاسخ به تهدیدهای سایبری، پژوهشگران راهکارهای فنی مختلفی برای افزایش امنیت سامانه‌های اطلاعاتی و کنترل صنعتی در زیرساخت‌های آبی ارائه کرده‌اند. یکی از مهم‌ترین این راهکارها استفاده از سامانه‌های **تشخیص نفوذ** برای شناسایی حملات سایبری در شبکه‌های صنعتی است. چرادی و همکاران (۲۰۱۸) نشان می‌دهند که استفاده از الگوریتم‌های یادگیری ماشین در سامانه‌های تشخیص نفوذ می‌تواند دقت شناسایی حملات را به طور قابل توجهی افزایش دهد.

علاوه بر این، برخی مطالعات بر اهمیت استفاده از رمزنگاری پیشرفته، احراز هویت چندمرحله‌ای و جداسازی شبکه‌های عملیاتی از شبکه‌های فناوری اطلاعات تأکید کرده‌اند (رودریگز و همکاران، ۲۰۲۰). این اقدامات می‌توانند احتمال دسترسی غیرمجاز به سامانه‌های حیاتی را کاهش دهند.

جدول ۶. مهم‌ترین راهکارهای فنی امنیت سایبری در زیرساخت‌های آب

راهکار فنی	توضیح
سامانه‌های تشخیص نفوذ	شناسایی و تحلیل رفتارهای مشکوک در شبکه
رمزنگاری داده‌ها	حفاظت از اطلاعات حساس در برابر دسترسی غیرمجاز
احراز هویت چندمرحله‌ای	افزایش امنیت دسترسی کاربران
جداسازی شبکه‌ها	تفکیک شبکه‌های صنعتی از شبکه‌های عمومی

پایش مداوم شبکه	نظارت مستمر بر فعالیت‌های شبکه

۴. راهکارهای مدیریتی و سیاست‌گذاری امنیت سایبری

علاوه بر راهکارهای فنی، بسیاری از مطالعات بر اهمیت رویکردهای مدیریتی و سازمانی در ارتقای امنیت سایبری تأکید دارند. هومیرِ و همکاران (۲۰۲۱) نشان می‌دهند که توسعه چارچوب‌های حکمرانی امنیت سایبری و مدیریت ریسک می‌تواند نقش مهمی در کاهش آسیب‌پذیری زیرساخت‌های حیاتی داشته باشد.

همچنین پژوهش‌ها نشان می‌دهند که آموزش کارکنان، تدوین سیاست‌های امنیت اطلاعات، انجام ارزیابی‌های دوره‌ای ریسک و توسعه برنامه‌های واکنش به حوادث سایبری از جمله مهم‌ترین اقدامات مدیریتی در این حوزه هستند. این اقدامات می‌توانند به سازمان‌ها کمک کنند تا علاوه بر پیشگیری از حملات، در صورت وقوع حمله نیز واکنش سریع و مؤثری داشته باشند.

جدول ۷. مهم‌ترین راهکارهای مدیریتی برای ارتقای امنیت سایبری

راهکار مدیریتی	توضیح
توسعه سیاست‌های امنیت اطلاعات	تدوین دستورالعمل‌های امنیتی در سازمان
آموزش کارکنان	افزایش آگاهی کارکنان درباره تهدیدهای سایبری
مدیریت ریسک سایبری	شناسایی و ارزیابی آسیب‌پذیری‌ها
برنامه واکنش به حوادث	آمادگی برای مقابله با حملات سایبری
همکاری بین‌سازمانی	تبادل اطلاعات امنیتی میان سازمان‌ها

بحث و نتیجه‌گیری

نتایج حاصل از مرور نظام‌مند مطالعات انجام‌شده در حوزه امنیت سایبری زیرساخت‌های آبی نشان می‌دهد که با گسترش فناوری‌های دیجیتال در مدیریت منابع آب، سطح تهدیدهای سایبری علیه شرکت‌های آب و فاضلاب به طور قابل توجهی افزایش یافته است. در سال‌های اخیر بسیاری از این سازمان‌ها برای بهبود کارایی عملیاتی، مدیریت هوشمند شبکه‌های توزیع و افزایش دقت پایش مصرف از سامانه‌های کنترل صنعتی، اینترنت اشیا و زیرساخت‌های داده‌محور استفاده کرده‌اند. هرچند این تحولات موجب افزایش کارایی و کیفیت خدمات شده است، اما در عین حال سطح حملات سایبری و آسیب‌پذیری‌های امنیتی نیز افزایش یافته است.

یکی از مهم‌ترین یافته‌های این پژوهش آن است که زیرساخت‌های آبی به دلیل ماهیت حیاتی خدماتی که ارائه می‌کنند، از اهداف بالقوه برای حملات سایبری محسوب می‌شوند. مطالعات مختلف نشان می‌دهند که حملاتی نظیر باج‌افزار، نفوذ به سامانه‌های SCADA، بدافزارها و دستکاری داده‌های عملیاتی می‌توانند اختلالات جدی در فرآیندهای عملیاتی شرکت‌های آب و فاضلاب ایجاد کنند. این موضوع به ویژه در شرایطی اهمیت بیشتری پیدا می‌کند که بسیاری از سامانه‌های کنترل صنعتی مورد استفاده در این سازمان‌ها در زمان طراحی، با در نظر گرفتن ملاحظات امنیت سایبری توسعه نیافته‌اند. در نتیجه، وجود تجهیزات قدیمی، ضعف در مدیریت دسترسی و نبود سامانه‌های پیشرفته پایش امنیتی می‌تواند احتمال وقوع حملات سایبری را افزایش دهد.

یافته‌های پژوهش همچنین نشان می‌دهد که امنیت سایبری در زیرساخت‌های آبی صرفاً یک مسئله فنی نیست، بلکه به طور مستقیم با عوامل مدیریتی و سازمانی نیز ارتباط دارد. بسیاری از مطالعات تأکید کرده‌اند که حتی در صورت استفاده از فناوری‌های امنیتی پیشرفته، نبود سیاست‌های سازمانی مناسب و ضعف در مدیریت ریسک سایبری می‌تواند اثربخشی اقدامات امنیتی را کاهش دهد. در این زمینه، توسعه چارچوب‌های حکمرانی امنیت سایبری، تدوین سیاست‌های امنیت اطلاعات و ایجاد ساختارهای مدیریتی برای پایش مستمر تهدیدها از اهمیت ویژه‌ای برخوردار است.

از سوی دیگر، بررسی مطالعات نشان می‌دهد که استفاده از فناوری‌های نوین مانند سامانه‌های تشخیص نفوذ مبتنی بر یادگیری ماشین، رمزنگاری پیشرفته و احراز هویت چندمرحله‌ای می‌تواند نقش مهمی در افزایش امنیت زیرساخت‌های آبی ایفا کند. این فناوری‌ها امکان شناسایی سریع فعالیت‌های مشکوک در شبکه‌های صنعتی و جلوگیری از دسترسی غیرمجاز به سامانه‌های حیاتی را فراهم می‌کنند. با این حال، اجرای موفق این راهکارها نیازمند زیرساخت‌های مناسب، نیروی انسانی متخصص و سرمایه‌گذاری سازمانی است.

یکی دیگر از نتایج مهم این پژوهش، نقش کلیدی آموزش و آگاهی کارکنان در کاهش خطرات امنیت سایبری است. بسیاری از حملات سایبری از طریق خطاهای انسانی، استفاده از گذرواژه‌های ضعیف یا بی‌توجهی به دستورالعمل‌های امنیتی رخ می‌دهند. بنابراین آموزش مستمر کارکنان، ارتقای فرهنگ امنیت اطلاعات در سازمان و افزایش سطح آگاهی نسبت به تهدیدهای سایبری می‌تواند به عنوان یکی از مؤثرترین راهکارهای پیشگیرانه در نظر گرفته شود.

در مجموع، نتایج این مطالعه نشان می‌دهد که ارتقای امنیت سایبری در شرکت‌های آب و فاضلاب نیازمند یک رویکرد چندبعدی است که شامل ترکیبی از راهکارهای فنی، مدیریتی و سازمانی باشد. تمرکز صرف بر ابزارهای امنیتی بدون توجه به سیاست‌های مدیریتی و آموزش منابع انسانی نمی‌تواند امنیت پایدار زیرساخت‌های حیاتی را تضمین کند. در این راستا، توسعه چارچوب‌های جامع امنیت سایبری، سرمایه‌گذاری در فناوری‌های امنیتی پیشرفته و تقویت همکاری میان سازمان‌های مسئول در حوزه زیرساخت‌های حیاتی می‌تواند نقش مهمی در افزایش تاب‌آوری این زیرساخت‌ها در برابر تهدیدهای سایبری ایفا کند.

با توجه به یافته‌های این پژوهش، پیشنهاد می‌شود که مطالعات آینده به بررسی تجربی پیاده‌سازی چارچوب‌های امنیت سایبری در شرکت‌های آب و فاضلاب، توسعه مدل‌های پیش‌بینی تهدیدهای سایبری و همچنین تحلیل

اقتصادی سرمایه‌گذاری در امنیت زیرساخت‌های آبی بپردازند. انجام چنین پژوهش‌هایی می‌تواند به توسعه دانش کاربردی در حوزه امنیت سایبری زیرساخت‌های حیاتی و بهبود سیاست‌گذاری‌های مرتبط با حفاظت از داده‌ها و سامانه‌های عملیاتی در صنعت آب کمک کند.

منابع

عسکری، مهدی و حیدری، رضا. (۱۳۹۹). بررسی چالش‌های امنیت اطلاعات در زیرساخت‌های حیاتی کشور. *فصلنامه مدیریت فناوری اطلاعات*، ۱۲(۳)، ۸۵–۱۰۲.

حسینی، علی و موسوی، حمید. (۱۴۰۰). تحلیل آسیب‌پذیری‌های امنیت سایبری در سامانه‌های کنترل صنعتی. *نشریه مهندسی فناوری اطلاعات*، ۱۴(۲)، ۵۵–۷۰.

رحیمی، سارا و کریمی، محمد. (۱۴۰۱). بررسی تهدیدهای سایبری در زیرساخت‌های شهری هوشمند. *فصلنامه مطالعات امنیت اطلاعات*، ۹(۱)، ۳۳–۴۹.

Ahmed, S., Mahmood, A., & Hu, J. (٢٠٢١). Cybersecurity challenges in smart water infrastructure: A review. *Journal of Water Resources Planning and Management*, ١٤٧(٦), ٠٤٠٢١٠٢٥.

Boyes, H., Isbell, R., & Watson, T. (٢٠١٨). Critical infrastructure cyber security and the water sector. *Computer Law & Security Review*, ٣٤(٢), ٣٦٧–٣٧٩.

Cardell, J., Anderson, K., & McDonald, J. (٢٠١٧). Cybersecurity of critical infrastructures: Challenges and opportunities in the water sector. *Energy Policy*, ١٠٣, ٨٥–٩٢.

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (٢٠١٨). A review of cyber security risk assessment methods for SCADA systems. *Computers & Security*, ٥٦, ١–٢٧.

Humayer, S., Niyaz, Q., Javaid, A., Shafiq, M., & Kim, K. (٢٠٢١). Cybersecurity for industrial control systems: A survey. *IEEE Communications Surveys & Tutorials*, ٢٣(٣), ١٧٥٢–١٧٧٨.

Rodriguez, M., Perez, J., & Lopez, D. (٢٠٢٠). Security challenges in industrial control systems for water utilities. *International Journal of Critical Infrastructure Protection*, ٢٩, ١٠٠٣٤١.

Cybersecurity Challenges in Protecting Sensitive Data in Water and Wastewater Utilities: A Review of Threats and Mitigation Strategies

Atefeh Daneshvar, Isa Mousaei Baghestani, Sara Toghroljerdi

M.A. in Business Administration – Marketing, Bandar Abbas Water and Wastewater Company, Hormozgan Province, Iran (Corresponding Author)

B.Sc. in Computer Engineering (Software), Bandar Abbas Water and Wastewater Company, Hormozgan Province, Iran

M.Sc. in Computer Engineering (Computer Architecture), Bandar Abbas Water and Wastewater Company, Hormozgan Province, Iran

Abstract

With the rapid expansion of digital technologies and the increasing smartization of urban infrastructure, cybersecurity has become one of the most critical challenges in the management of critical infrastructures. Water and wastewater utilities, as key providers of essential public services, widely rely on information systems, industrial control systems, and communication technologies to manage and monitor water supply networks. While the adoption of these technologies has improved operational efficiency and enhanced water resource management, it has simultaneously increased the vulnerability of these infrastructures to cyber threats. The objective of this study is to examine and analyze cybersecurity challenges related to the protection of sensitive data and information infrastructures in water and wastewater utilities. This research employs a systematic literature review approach. Relevant studies and scholarly articles published in reputable international and national databases, including Scopus, ScienceDirect, IEEE Xplore, Web of Science, and Google Scholar, were reviewed for the period between ۲۰۱۵ and ۲۰۲٦. Following the screening process and quality assessment of the studies, a set of relevant publications was selected and analyzed using a qualitative content analysis method. The results indicate that the most significant cyber threats targeting water infrastructures include ransomware attacks, intrusions into industrial control systems, malware, and unauthorized access to sensitive data. In addition, the presence of legacy equipment, weaknesses in user access management, the lack of advanced intrusion detection systems, and the shortage of specialized cybersecurity professionals are among the most important security vulnerabilities in this sector. The findings further suggest that enhancing cybersecurity in water and wastewater utilities requires a combination of both technical and managerial approaches. The implementation of intrusion detection systems, data encryption, multi-factor authentication, network segmentation between operational and information technology networks, and the development of organizational information security policies are among the most frequently recommended strategies identified in the reviewed studies. Overall, the results of this research indicate that adopting a comprehensive and multidimensional cybersecurity management approach can significantly enhance the resilience of water infrastructures against cyber threats.

Keywords:

Cybersecurity, Critical Infrastructure, Water and Wastewater Utilities, SCADA Systems, Data Security, Water Infrastructure.