

جزوه تهدیدات آب و فاضلاب

تهدیدات و آسیب شناسی مرتبط با صنعت آب و فاضلاب

ویژه داوطلبان مشاغل نگهداری و حفاظت فیزیکی

صفحه عنوان

عنوان: تهدیدات و آسیب شناسی مرتبط با صنعت آب و فاضلاب
مخاطب: داوطلبان و کارکنان تازه استخدام نگهداری و حفاظت فیزیکی
حوزه آموزشی: امنیت زیرساخت، حفاظت فیزیکی، مدیریت رخداد و واکنش اولیه
زبان: فارسی

فهرست مطالب

1. مقدمه و اهمیت صنعت آب و فاضلاب
2. جایگاه تأسیسات آب و فاضلاب در پدافند غیرعامل و امنیت زیرساختی
3. طبقه بندی تهدیدات در صنعت آب و فاضلاب
4. آسیب شناسی نقاط ضعف رایج در تأسیسات آب و فاضلاب
5. تهدیدات سایبری و سایبری - فیزیکی
6. تهدیدات داخلی، خطای انسانی و سوءاستفاده از دسترسی
7. مدیریت شرایط اضطراری و تداوم خدمت
8. سناریوهای عملی و نمونه رخدادها
9. اصول گزارش نویسی، ارتباطات و تحویل شیفت
10. جمع بندی

فصل اول: مقدمه و اهمیت صنعت آب و فاضلاب

۱-۱. آب و فاضلاب؛ زیرساختی حیاتی برای جامعه

آب سالم و خدمات دفع بهداشتی فاضلاب از مهم‌ترین نیازهای زندگی انسان، سلامت عمومی، تولید، آموزش، درمان و فعالیت اقتصادی هستند. شهروندان ممکن است در زمان عادی متوجه پیچیدگی و گستردگی این خدمات نباشند، اما هرگونه اختلال جدی در تأمین آب یا جمع‌آوری و تصفیه فاضلاب می‌تواند در مدت کوتاهی پیامدهای گسترده‌ای ایجاد کند.

تأسیسات آب و فاضلاب فقط ساختمان اداری یا مجموعه‌ای از لوله‌ها نیستند. این صنعت مجموعه‌ای به هم پیوسته از منابع آب، چاه‌ها، خطوط انتقال، تصفیه‌خانه‌ها، مخازن، ایستگاه‌های پمپاژ، شبکه توزیع، سامانه‌های اندازه‌گیری، مراکز کنترل، آزمایشگاه‌ها، انبار مواد شیمیایی و سامانه‌های ارتباطی است. هر بخش این زنجیره می‌تواند بر بخش‌های دیگر اثر بگذارد. برای نمونه، از کار افتادن یک ایستگاه پمپاژ ممکن است موجب کاهش فشار شبکه، قطع آب مناطق، سرریز مخزن یا ایجاد مشکل در فرآیند تصفیه شود.

در بخش فاضلاب نیز اختلال در پمپاژ، تصفیه یا دفع نهایی می‌تواند به پس‌زدگی فاضلاب، آلودگی محیط‌زیست، انتشار بوی نامطبوع، آلودگی منابع آب و تهدید سلامت عمومی منجر شود. بنابراین حفاظت از تأسیسات آب و فاضلاب، تنها حفاظت از اموال یک سازمان نیست؛ بلکه بخشی از حفاظت از سلامت و امنیت جامعه است.

۱-۲. اهمیت موضوع برای نگهبان

نگهبان معمولاً نخستین فردی است که در ورودی تأسیسات، محوطه پیرامونی، اتاق نگهبانی یا مسیرهای دسترسی حضور دارد. کارکنان فنی ممکن است در ساعات مشخصی در محل باشند، اما نگهبان مسئول مراقبت مستمر، کنترل ورود و خروج و مشاهده تغییرات غیرعادی است.

وظیفه نگهبان آن نیست که به تنهایی همه مشکلات فنی، امنیتی یا عملیاتی را حل کند. وظیفه اصلی او مشاهده دقیق، پیشگیری از ورود غیرمجاز، اجرای مقررات ابلاغ‌شده، حفظ آرامش، اطلاع‌رسانی سریع و ثبت صحیح رخدادهاست. یک گزارش دقیق و به موقع می‌تواند از تبدیل یک نشانه کوچک به حادثه‌ای بزرگ جلوگیری کند.

برای مثال، مشاهده باز بودن دری که معمولاً قفل است، حضور یک خودرو در محل غیرمعمول، تغییر بوی شدید مواد شیمیایی، صدای غیرعادی پمپ، مشاهده نشتی، قطع دوربین یا تردد فردی بدون کارت می‌تواند نشانه‌ای مهم باشد. ارزش این مشاهده زمانی بیشتر می‌شود که نگهبان آن را جدی بگیرد، بدون ایجاد خطر بررسی اولیه انجام دهد و موضوع را از مسیر تعیین‌شده گزارش کند.

۱-۳. مفهوم تهدید، آسیب‌پذیری و ریسک

برای تحلیل امنیتی باید سه مفهوم از یکدیگر تفکیک شوند:

تهدید به عامل یا رویدادی گفته می‌شود که توان ایجاد خسارت، اختلال یا آسیب را دارد. تهدید می‌تواند طبیعی، انسانی، فنی یا سایبری باشد.

آسیب‌پذیری ضعف یا نقصی است که امکان اثرگذاری تهدید را بیشتر می‌کند. نبود روشنایی، قفل معیوب، بی‌نظمی در ثبت ورود و خروج، رها بودن کلیدها یا نبود ارتباط مؤثر نمونه‌هایی از آسیب‌پذیری هستند.

ریسک حاصل ترکیب احتمال وقوع یک تهدید و شدت پیامد آن است. یک نقص کوچک در محل کم‌اهمیت ممکن است ریسک محدودی داشته باشد، اما همان نقص در ورودی مخزن اصلی یا اتاق کنترل می‌تواند بسیار مهم باشد.

نگهبان لازم نیست محاسبات پیچیده انجام دهد، اما باید بتواند با نگاه عملی تشخیص دهد کدام وضعیت عادی و کدام وضعیت نیازمند پیگیری فوری است. پرسش‌های زیر در این زمینه مفید هستند:

- چه چیزی ممکن است رخ دهد؟
- اگر رخ دهد، چه بخشی آسیب می‌بیند؟
- چه نشانه‌ای می‌تواند پیش از حادثه دیده شود؟
- چه اقدامی در حدود وظایف نگهبان می‌تواند احتمال یا پیامد حادثه را کاهش دهد؟
- چه کسی باید در سریع‌ترین زمان مطلع شود؟

۱-۴. اصول عمومی حفاظت

حفاظت مؤثر بر چند اصل استوار است:

1. پیشگیری: جلوگیری از ایجاد موقعیت خطرناک پیش از وقوع حادثه.

2. کشف: شناسایی سریع رفتار، وضعیت یا نشانه غیرعادی.
 3. تأخیر: ایجاد موانع و کنترل‌هایی که زمان لازم برای واکنش را فراهم کند.
 4. واکنش: اطلاع‌رسانی و اقدام مناسب مطابق دستورالعمل.
 5. بازیابی: کمک به بازگشت ایمن تأسیسات به وضعیت عادی.
 6. یادگیری: ثبت رخداد و اصلاح ضعف‌هایی که باعث تکرار حادثه شده‌اند.
- این اصول باید در کنار هم اجرا شوند. وجود دیوار مناسب بدون کنترل دروازه کافی نیست. دوربین بدون پایش و ثبت رخداد کافی نیست. حضور نگهبان بدون آموزش و ارتباط مؤثر نیز نمی‌تواند امنیت مطلوب ایجاد کند.

فصل دوم: جایگاه تأسیسات آب و فاضلاب در پدافند غیرعامل و امنیت زیرساختی

۲-۱. مفهوم زیرساخت حیاتی

زیرساخت حیاتی به سامانه‌ها و خدماتی گفته می‌شود که استمرار فعالیت جامعه به آن‌ها وابسته است و اختلال در آن‌ها می‌تواند پیامدهای گسترده اجتماعی، اقتصادی، بهداشتی یا امنیتی داشته باشد. آب و فاضلاب از مصادیق روشن این زیرساخت‌ها هستند.

وابستگی متقابل میان زیرساخت‌ها اهمیت موضوع را بیشتر می‌کند. تأسیسات آب به برق، مخابرات، سوخت، جاده و تجهیزات فنی وابسته است. از سوی دیگر، بیمارستان‌ها، صنایع، مراکز آموزشی، آتش‌نشانی و خانوارها به آب پایدار وابسته‌اند. در نتیجه، یک رخداد در صنعت آب ممکن است در بخش‌های دیگر نیز آثار زنجیره‌ای ایجاد کند.

درک این وابستگی برای نگهبان اهمیت دارد. قطع برق فقط یک مشکل برقی نیست؛ ممکن است به توقف پمپ‌ها، از کار افتادن سامانه‌های کنترل، کاهش فشار آب یا فعال شدن مولد اضطراری منجر شود. بارندگی شدید فقط یک پدیده جوی نیست؛ ممکن است دسترسی به تأسیسات، ایمنی مخازن، وضعیت فاضلاب‌روها و مسیرهای امدادی را تحت تأثیر قرار دهد.

۲-۲. پدافند غیرعامل و کاهش آسیب پذیری

پدافند غیرعامل به مجموعه اقداماتی گفته می شود که بدون استفاده از عملیات تهاجمی، آسیب پذیری افراد و زیرساخت ها را در برابر تهدیدها کاهش می دهد. پراکندگی مناسب، مقاوم سازی، ایجاد مسیرهای جایگزین، حفاظت فیزیکی، پشتیبان گیری، آموزش کارکنان و استمرار خدمت از نمونه های این اقدامات هستند.

در سطح نگهبانی، پدافند غیرعامل بیشتر در قالب رفتارهای روزمره دیده می شود:

- جلوگیری از ورود افراد فاقد مجوز؛
 - مراقبت از مسیرهای دسترسی و دروازه ها؛
 - توجه به نقاط کور، روشنایی و حصار؛
 - جلوگیری از تجمع افراد ناشناس در اطراف تأسیسات؛
 - گزارش خرابی قفل، دوربین، بی سیم و سامانه اعلام خطر؛
 - آشنایی با مسیرهای خروج، محل تجمع و تجهیزات اضطراری؛
 - حفظ محرمانگی اطلاعاتی که می تواند امنیت تأسیسات را کاهش دهد.
- پدافند غیرعامل به معنای ایجاد محدودیت بی دلیل برای مردم یا کارکنان نیست. هدف آن است که دسترسی ها متناسب با نیاز شغلی، قابل کنترل و قابل پیگیری باشند.

۲-۳. حفاظت لایه ای

حفاظت لایه ای یعنی امنیت به یک عامل واحد وابسته نباشد. یک تأسیسات مناسب، چند لایه حفاظتی دارد:

- لایه پیرامونی مانند دیوار، حصار، دروازه و روشنایی؛
- لایه کنترل ورود شامل نگهبانی، کارت، ثبت تردد و احراز هویت؛
- لایه داخلی شامل قفل گذاری، تفکیک مناطق و محدودیت دسترسی؛
- لایه نظارتی شامل دوربین، اعلام خطر و بازدید دوره ای؛
- لایه مدیریتی شامل دستورالعمل، آموزش، ثبت رخداد و ارزیابی؛
- لایه پشتیبان شامل برق اضطراری، ارتباط جایگزین و برنامه تداوم خدمت.

اگر یکی از لایه‌ها دچار نقص شود، لایه‌های دیگر باید تا حد امکان از وقوع یا گسترش حادثه جلوگیری کنند. برای مثال، اگر دوربین ورودی از کار افتاده باشد، افزایش بازدید فیزیکی و ثبت دقیق تردد می‌تواند بخشی از خلأ ایجادشده را جبران کند.

۲-۴. اصل حداقل دسترسی

هر فرد باید فقط به اندازه نیاز شغلی خود دسترسی داشته باشد. این اصل درباره ورود به محوطه، دریافت کلید، استفاده از کارت، مشاهده اطلاعات، دسترسی به اتاق کنترل و حضور در مناطق حساس کاربرد دارد.

نگهبان نباید صرفاً به دلیل آشنایی قبلی با یک فرد، مقررات احراز هویت را کنار بگذارد. کارکنان رسمی، پیمانکاران، رانندگان و نیروهای خدماتی نیز باید مطابق ضوابط شرکت شناسایی و ثبت شوند. در مواردی که مجوز یا وضعیت فرد روشن نیست، موضوع باید به مسئول شیفت یا مقام تعیین‌شده ارجاع شود.

هرگونه جزئیات مربوط به نقاط ضعف واقعی، مسیرهای حفاظتی، محل تجهیزات حساس یا برنامه شیفت‌ها باید فقط در چارچوب نیاز شغلی و دستورالعمل داخلی در اختیار افراد قرار گیرد. تطبیق سطح دسترسی و نحوه نگهداری اطلاعات با دستورالعمل داخلی شرکت الزامی است.

فصل سوم: طبقه‌بندی تهدیدات در صنعت آب و فاضلاب

۳-۱. تهدیدات طبیعی

تهدید طبیعی بدون دخالت مستقیم انسان ایجاد می‌شود، اما می‌تواند با ضعف طراحی یا نگهداری، خسارت بیشتری ایجاد کند. زلزله، سیل، بارندگی شدید، طوفان، صاعقه، گرمای شدید، یخبندان، خشکسالی و رانش زمین از نمونه‌های مهم هستند.

زلزله ممکن است به خطوط انتقال، مخازن، ساختمان‌ها، دیوارها، تابلوهای برق و تجهیزات فرایندی آسیب برساند. پس از زلزله، خطر ریزش، برق‌گرفتگی، نشت مواد شیمیایی و شکستگی لوله‌ها وجود دارد. نگهبان نباید برای بررسی خسارت وارد محل نایمن شود؛ اولویت با حفظ جان، اطلاع‌رسانی و جلوگیری از ورود افراد غیرمجاز است.

سیل می‌تواند مسیر ورود را مسدود کند، تابلوهای برق و اتاق‌های فنی را در معرض آب قرار دهد و مواد آلاینده را جابه‌جا کند. در چنین شرایطی، ورود خودرو یا افراد به محوطه آب‌گرفته ممکن

است خطر برق‌گرفتگی یا فروکش کردن زمین داشته باشد. هرگونه اقدام باید بر اساس دستور مسئولان فنی و ایمنی انجام شود.

گرمای شدید احتمال آتش‌سوزی، خرابی تجهیزات برقی و افزایش فشار کاری سامانه‌ها را بیشتر می‌کند. یخبندان نیز می‌تواند به لوله‌ها، شیرآلات و سامانه‌های آب‌رسانی آسیب برساند. نگهبان باید نشانه‌های ظاهری مانند ترک، نشستی، صدای غیرعادی، بخار، دود، تغییر رنگ آب یا تجمع غیرمعمول آب را گزارش کند.

۲-۳. تهدیدات انسانی عمدی

تهدید انسانی عمدی شامل ورود غیرمجاز، سرقت، خرابکاری، تخریب تجهیزات، آتش‌زنی، دستکاری شیرها و تابلوها، آلودگی عمدی، تهدید کارکنان و استفاده نادرست از اطلاعات است.

در حفاظت فیزیکی، نباید درباره انگیزه افراد بر اساس ظاهر یا حدس قضاوت کرد. معیار باید رفتار، مجوز، مقصد و انطباق با مقررات باشد. فردی که از پاسخ‌گویی درباره مقصد خودداری می‌کند، اصرار دارد بدون ثبت وارد شود، از مسیر غیرمعمول حرکت می‌کند یا درباره تجهیزات حساس پرسش‌های نامرتب دارد، نیازمند توجه و گزارش است؛ اما برخورد با او باید محترمانه، قانونی و مطابق اختیارات نگهبان باشد.

در صورت مشاهده رفتار مشکوک، نگهبان نباید به‌تنهایی وارد درگیری یا تعقیب خطرناک شود. فاصله ایمن، درخواست کمک، اطلاع به مسئول شیفت و حفظ اطلاعات مربوط به زمان، مکان، ظاهر و وسیله نقلیه اهمیت بیشتری دارد.

۳-۳. تهدیدات فنی و صنعتی

خرابی پمپ، شکستگی لوله، نقص شیر، آتش‌سوزی، انفجار، نشت مواد شیمیایی، قطع برق، از کار افتادن مولد اضطراری و خطای تجهیزات اندازه‌گیری از تهدیدات فنی هستند.

نگهبان وظیفه تعمیر یا دستکاری تجهیزات را ندارد. دستکاری تابلو برق، شیرهای فرایندی یا تجهیزات شیمیایی بدون مجوز می‌تواند خطر جانی داشته باشد. نقش او مشاهده، ایمن‌سازی اولیه محیط در حد توان، جلوگیری از ورود افراد غیرمسئول و تماس با واحد مربوط است.

در محیط‌های فاضلابی احتمال وجود گازهای خطرناک، کمبود اکسیژن و سطوح لغزنده بیشتر است. ورود به منهول، مخزن، کانال یا فضای بسته بدون مجوز، تجهیزات و نیروی آموزش‌دیده ممنوع است. حتی اگر فردی در داخل فضای بسته گرفتار شده باشد، ورود نجات‌دهنده آموزش‌ندیده ممکن است تعداد قربانیان را افزایش دهد.

۳-۴. تهدیدات سایبری

تأسیسات آب و فاضلاب از سامانه‌های رایانه‌ای، شبکه‌های ارتباطی، کنترل‌کننده‌ها، حسگرها و نرم‌افزارهای مدیریتی استفاده می‌کنند. حمله سایبری می‌تواند به افشای اطلاعات، اختلال در کنترل، نمایش داده نادرست یا تغییر عملکرد تجهیزات منجر شود.

برای نگهبان، تهدید سایبری ممکن است به شکل‌های زیر دیده شود:

- حضور فرد ناشناس در کنار اتاق کنترل یا رک ارتباطی؛
 - تلاش برای ورود به محل با عنوان پشتیبان فنی بدون هماهنگی؛
 - اتصال تجهیزات ناشناس به رایانه یا تابلو؛
 - درخواست غیرعادی برای دسترسی به رمز، کارت یا کلید؛
 - از کار افتادن هم‌زمان دوربین‌ها، ارتباطات یا نمایشگرها؛
 - مشاهده پیام‌های غیرعادی یا تغییر ناگهانی وضعیت سامانه‌ها.
- نگهبان نباید رمز عبور را دریافت، ثبت یا در اختیار دیگران قرار دهد و نباید تجهیزات ناشناخته را جابه‌جا یا خاموش کند؛ مگر طبق دستور مسئول مجاز. هر نشانه غیرعادی باید سریع گزارش شود.

۳-۵. تهدیدات ترکیبی

تهدید ترکیبی زمانی رخ می‌دهد که چند عامل هم‌زمان یا زنجیره‌ای عمل کنند. برای نمونه، قطع برق در اثر طوفان، از کار افتادن دوربین‌ها و تلاش فردی برای ورود غیرمجاز می‌تواند یک وضعیت ترکیبی ایجاد کند. یا خرابی ارتباطات هم‌زمان با حضور پیمانکار ناشناس، تشخیص رخداد را دشوارتر می‌کند.

در این وضعیت‌ها، حفظ نظم، اولویت‌بندی خطرها و استفاده از مسیرهای جایگزین ارتباطی اهمیت دارد. نگهبان باید نخست خطرهای فوری برای جان افراد را شناسایی کند، سپس از ورود غیرمجاز جلوگیری کرده و گزارش منظم ارائه دهد.

فصل چهارم: آسیب‌شناسی نقاط ضعف رایج در تأسیسات آب و فاضلاب

۴-۱. نقاط ضعف پیرامونی

حصار فرسوده، سوراخ یا کوتاه، دیوار بدون روشنایی، دروازه‌ای که کامل بسته نمی‌شود و مسیرهای فرعی بدون کنترل، از ضعف‌های رایج پیرامونی هستند. پوشش گیاهی بلند یا انباشت وسایل در کنار دیوار نیز می‌تواند دید نگهبان و دوربین را کاهش دهد.

بازدید پیرامونی باید با رعایت ایمنی و طبق برنامه انجام شود. نگهبان باید تغییرات قابل مشاهده مانند بریدگی حصار، آثار عبور، قفل شکسته، جابه‌جایی خاک، خودرو یا اشیای رها شده را گزارش کند. نزدیک شدن به بسته یا شیء مشکوک مجاز نیست و باید محدوده تا رسیدن فرد مسئول کنترل شود.

۴-۲. ضعف در ورودی و کنترل تردد

ثبت ناقص ورود و خروج، پذیرش کارت یا معرفی شفاهی بدون بررسی، نبود کنترل خودرو، تحویل کلید بدون ثبت و باز گذاشتن دروازه از آسیب‌پذیری‌های مهم هستند.

ثبت تردد باید خوانا، به‌موقع و قابل پیگیری باشد. اطلاعات معمول شامل نام، نام شرکت یا واحد، شماره وسیله نقلیه، زمان ورود، مقصد، نام فرد هماهنگ‌کننده و زمان خروج است؛ البته قالب دقیق باید با دستورالعمل داخلی شرکت تطبیق داده شود.

در خصوص پیمانکاران، صرف داشتن لباس کار یا خودرو سازمانی، به‌تنهایی مجوز ورود محسوب نمی‌شود. باید هماهنگی قبلی و محدوده فعالیت مشخص باشد. اگر فردی ادعا کند برای تعمیر فوری آمده است اما نام او در فهرست هماهنگی نیست، موضوع باید از طریق مسئول مربوط تأیید شود.

۴-۳. ضعف در نگهداری کلیدها و کارت‌ها

کلیدهای فیزیکی، کارت‌های دسترسی و تجهیزات ارتباطی دارای‌های امنیتی محسوب می‌شوند. نگهداری کلید در محل قابل دسترس، تحویل بدون ثبت، استفاده مشترک از کارت یا بی‌توجهی به مفقودی کارت می‌تواند امنیت چند بخش را کاهش دهد.

کلیدها باید طبق مقررات در محل تعیین شده نگهداری و تحویل آنها ثبت شود. در صورت مفقودی، نباید موضوع پنهان بماند؛ زیرا ممکن است لازم باشد قفل یا سطح دسترسی تغییر کند. استفاده از کارت فرد دیگر نیز نباید پذیرفته شود، حتی اگر فرد مدعی باشد کارت خود را فراموش کرده است.

۴-۴. ضعف در دوربین و سامانه‌های اعلام خطر

دوربین کثیف، زاویه نامناسب، نور ناکافی، ذخیره نشدن تصاویر یا ساعت نادرست سامانه باعث کاهش ارزش نظارتی می‌شود. سامانه اعلام خطر نیز اگر مرتباً هشدار کاذب بدهد، ممکن است کارکنان نسبت به هشدارها بی‌تفاوت شوند.

نگهبان باید وضعیت ظاهری تجهیزات و نمایشگرها را بررسی و خرابی‌ها را ثبت کند، اما نباید برای رفع نقص فنی اقدام غیرمجاز انجام دهد. قطع هم‌زمان چند سامانه باید به‌عنوان رخداد مهم تلقی و فوراً گزارش شود.

۴-۵. ضعف در محوطه داخلی

قرار دادن مواد، ابزار یا خودرو در مسیرهای اضطراری، نبود نظم در انبار، باز بودن اتاق‌های حساس، انباشت ضایعات قابل اشتعال و مسدود شدن تابلوهای هشدار از مشکلاتی هستند که احتمال حادثه را افزایش می‌دهند.

نظم محیط فقط مسئله زیبایی نیست؛ در زمان حادثه، مسیر آزاد می‌تواند سرعت امدادرسانی را افزایش دهد. نگهبان باید انسداد مسیرهای خروج، پارک خودرو در محل ممنوع، باز بودن درهای غیرعادی و وجود مواد ناشناخته را گزارش کند.

۴-۶. ضعف‌های انسانی و سازمانی

خستگی، بی‌توجهی، عادی شدن هشدارها، ارتباط ضعیف بین شیفت‌ها، آموزش ناکافی و ترس از گزارش‌دادن، از ضعف‌های مهم انسانی هستند. بسیاری از رخدادها نه به دلیل نبود تجهیزات، بلکه به علت اجرا نشدن رویه‌های ساده اتفاق می‌افتند.

تحویل شیفت باید شامل وضعیت دروازه‌ها، کلیدها، افراد حاضر، خودروهای داخل محوطه، خرابی تجهیزات، رخدادهای ثبت شده و موارد پیگیری نشده باشد. تحویل شفاهی بدون ثبت می‌تواند باعث فراموشی یا اختلاف در مسئولیت شود.

فصل پنجم: تهدیدات سایبری و سایبری - فیزیکی

۵-۱. پیوند امنیت دیجیتال و فیزیکی

در تأسیسات مدرن، امنیت فیزیکی و امنیت سایبری از یکدیگر جدا نیستند. فردی که بدون مجوز وارد اتاق کنترل شود، ممکن است به سامانه‌های رایانه‌ای دسترسی پیدا کند. همچنین یک اختلال سایبری ممکن است به صورت تغییر ناگهانی در عملکرد پمپ، نمایش نادرست سطح مخزن یا قطع ارتباط آشکار شود.

بنابراین نگهبان باید از اتاق‌های کنترل، تابلوهای ارتباطی، رک‌ها و تجهیزات اندازه‌گیری مانند سایر مناطق حساس حفاظت کند.

۵-۲. نشانه‌های اولیه رخداد سایبری

نشانه‌های زیر الزاماً به معنی حمله سایبری نیستند، اما باید بررسی و گزارش شوند:

- خاموش شدن ناگهانی چند نمایشگر؛
- تغییر غیرمنتظره وضعیت تجهیزات؛
- مشاهده حساب کاربری ناشناس یا پیام هشدار غیرمعمول؛
- اتصال حافظه یا لپ‌تاپ ناشناس؛
- حضور فرد فنی بدون هماهنگی؛
- قطع هم‌زمان ارتباط دوربین، تلفن یا سامانه کنترل؛
- درخواست برای عبور از روال‌های احراز هویت.

نگهبان نباید سیستم را خودسرانه خاموش یا راه‌اندازی مجدد کند. این اقدامات ممکن است داده‌های مهم را از بین ببرد یا وضعیت را بدتر کند. باید موضوع به مسئول فناوری اطلاعات، کنترل فرایند یا مدیر شیفت اعلام شود.

۳-۵. مهندسی اجتماعی

مهندسی اجتماعی یعنی فریب دادن افراد برای دریافت اطلاعات یا دسترسی. فرد ممکن است خود را مدیر، کارشناس فوری، پیمانکار یا مأمور امدادی معرفی کند و با ایجاد فشار زمانی بخواهد مقررات را دور بزند.

راهکار مناسب، حفظ ادب و ارجاع به روال رسمی است. جمله‌هایی مانند «طبق مقررات، ورود شما پس از تأیید واحد مربوط انجام می‌شود» می‌تواند بدون ایجاد تنش، مانع عبور غیرمجاز شود.

۴-۵. حفاظت از تجهیزات ارتباطی

بی‌سیم، تلفن، رایانه ثبت تردد و سامانه‌های تصویری باید فقط در اختیار افراد مجاز باشد. رمز عبور نباید روی کاغذ کنار دستگاه نوشته شود. تجهیزات مفقودشده باید فوراً گزارش شوند.

استفاده از حافظه‌های ناشناس، نصب نرم‌افزار، تغییر تنظیمات یا اتصال تلفن شخصی به تجهیزات سازمانی باید مطابق مقررات فناوری اطلاعات انجام شود. در صورت نبود دستور روشن، نگهبان نباید تصمیم فنی مستقل بگیرد.

فصل ششم: تهدیدات داخلی، خطای انسانی و سوءاستفاده از دسترسی

۱-۶. تهدید داخلی چیست؟

تهدید داخلی می‌تواند از سوی کارمند، پیمانکار، نیروی موقت یا فردی باشد که به دلیل شغل خود به بخشی از تأسیسات دسترسی دارد. این تهدید ممکن است عمدی یا ناشی از بی‌احتیاطی باشد.

نمونه‌های آن عبارت‌اند از:

- واگذاری کارت یا کلید به فرد دیگر؛
- ورود به بخش خارج از محدوده کاری؛
- افشای اطلاعات حفاظتی؛

- ثبت نکردن تردد؛
 - بی‌توجهی به هشدارها؛
 - خارج کردن ابزار یا قطعه بدون مجوز؛
 - استفاده از تلفن همراه در محل ممنوع؛
 - انجام تعمیرات بدون رعایت الزامات ایمنی.
- نباید هر خطا را نشانه خیانت دانست. اما هر تخلف باید طبق مقررات ثبت و گزارش شود تا مسئولان بتوانند درباره علت و اقدام مناسب تصمیم بگیرند.

۲-۶. کنترل دو نفره و تأیید متقابل

در برخی فعالیت‌های حساس، حضور یا تأیید دو فرد مجاز احتمال خطا و سوءاستفاده را کاهش می‌دهد. نگهبان باید بداند چه اقداماتی نیازمند تأیید دو نفر یا اجازه مسئول ارشد است. اگر دستور داخلی شرکت در این زمینه وجود دارد، اجرای آن الزامی است و جزئیات آن باید از همان دستورالعمل دریافت شود.

۳-۶. تعارض منافع و فشار بیرونی

ممکن است فردی از نگهبان بخواهد به دلیل آشنایی، نسبت خانوادگی، فشار اداری یا وعده پاداش، مقررات را رعایت نکند. پاسخ مناسب، خودداری محترمانه و ارجاع به مسئول رسمی است.

پذیرش هدیه یا وجه در برابر تسهیل ورود یا ثبت نکردن رخداد، علاوه بر آسیب امنیتی، می‌تواند پیامد قانونی و اداری داشته باشد. نگهبان باید هرگونه فشار غیرعادی یا پیشنهاد مشکوک را به روش امن و تعیین‌شده گزارش کند.

فصل هفتم: مدیریت شرایط اضطراری و تداوم خدمت

۱-۷. اصول اولویت‌بندی در بحران

در هر حادثه، اولویت‌ها معمولاً به ترتیب زیر دنبال می‌شوند:

۱. حفظ جان افراد؛
 ۲. جلوگیری از گسترش خطر؛
 ۳. اطلاع‌رسانی و درخواست کمک؛
 ۴. حفاظت از تجهیزات و محیط؛
 ۵. حفظ شواهد و ثبت رخداد؛
 ۶. کمک به بازگشت خدمات.
- این ترتیب ممکن است بر اساس نوع حادثه تغییر کند، اما جان انسان‌ها همواره اولویت اساسی است.

۲-۷. آتش‌سوزی

در صورت مشاهده دود یا آتش، نگهبان باید محل، نوع ظاهری خطر و افراد در معرض را اعلام کند. فعال کردن سامانه اعلام حریق یا تماس با آتش‌نشانی باید طبق رویه انجام شود. استفاده از خاموش‌کننده فقط زمانی مجاز است که فرد آموزش دیده، مسیر خروج باز و خطر در حد قابل کنترل باشد.

در صورت وجود مواد شیمیایی یا کابل برق، نزدیک شدن بی‌احتیاط می‌تواند خطرناک باشد. درهای مشکوک نباید بدون ارزیابی باز شوند؛ زیرا ورود ناگهانی هوا ممکن است آتش را تشدید کند. مسیر خروج باید برای کارکنان و نیروهای امدادی باز نگه داشته شود.

۳-۷. نشت مواد شیمیایی

مواد مورد استفاده در تصفیه آب و فاضلاب ممکن است خورنده، سمی یا واکنش پذیر باشند. در صورت مشاهده نشتی، بخار، بوی شدید یا علائم تحریک چشم و تنفس، نگهبان باید از نزدیک شدن خودداری کند، افراد را دور کند و موضوع را به واحد ایمنی و مسئول فنی اطلاع دهد.

هرگز نباید ماده ناشناخته را لمس، بو یا با آب مخلوط کرد. استفاده از تجهیزات حفاظت فردی باید به افراد آموزش دیده واگذار شود. مسیر باد و محل تجمع افراد باید در تصمیم گیری مسئولان فنی مورد توجه قرار گیرد.

۴-۷. زلزله و پس لرزه

پس از زلزله، خطرهای ثانویه مانند ریزش، آتش سوزی، نشتی، برق گرفتگی و پس لرزه وجود دارد. نگهبان باید از ورود افراد غیرمسئول به ساختمان های آسیب دیده جلوگیری کند و مسیرهای امدادی را باز نگه دارد.

در صورت قطع ارتباط، استفاده از روش جایگزین مانند بی سیم یا مراجعه به نقطه تجمع تعیین شده باید مطابق برنامه اضطراری انجام شود. اطلاعات مربوط به افراد حاضر، مصدومان و وضعیت دروازه ها برای مدیریت بحران ارزشمند است.

۵-۷. سیل و بارندگی شدید

در زمان سیل، رانندگی در آب، نزدیک شدن به تابلوهای برق و ورود به فضاهای آب گرفته ممنوع است. نگهبان باید از تجمع افراد در مسیر خطرناک جلوگیری کند و وضعیت راه های دسترسی را گزارش دهد.

پس از فروکش کردن آب نیز خطر آلودگی، ریزش زمین و برق گرفتگی باقی است. بازگشت به محل باید پس از تأیید مسئولان فنی و ایمنی انجام شود.

۶-۷. قطع برق و از کار افتادن سامانه ها

قطع برق ممکن است باعث توقف پمپ ها، از کار افتادن روشنایی، دوربین و سیستم کنترل شود. نگهبان باید وضعیت مولد اضطراری، دروازه ها و ارتباطات را طبق دستورالعمل بررسی ظاهری کند، اما نباید به تابلوهای برق دست بزند.

اگر سامانه‌های نظارتی از کار افتادند، افزایش مراقبت فیزیکی و ثبت دستی تردد اهمیت پیدا می‌کند. قطعی برق باید از نظر زمان شروع، بخش‌های تحت تأثیر و اقدام‌های انجام‌شده ثبت شود.

فصل هشتم: سناریوهای عملی و نمونه رخدادها

۸-۱. ورود پیمانکار بدون هماهنگی

فردی با لباس کار و خودرو وانت به دروازه مراجعه می‌کند و می‌گوید برای تعمیر پمپ آمده است، اما نام او در فهرست روزانه نیست. او اصرار دارد کار فوری است و از نگهبان می‌خواهد فقط دروازه را باز کند.

اقدام مناسب این است که نگهبان با احترام، ورود را تا زمان تأیید مسئول مربوط متوقف کند. مشخصات فرد و خودرو ثبت می‌شود و با واحد فنی یا مدیر شیفت تماس گرفته می‌شود. اگر هماهنگی تأیید نشد، ورود انجام نمی‌شود. نگهبان نباید خودسرانه درباره ضرورت تعمیر یا اعتبار ادعا تصمیم بگیرد.

۸-۲. باز بودن درِ اتاق فنی

در گشت شبانه، نگهبان متوجه می‌شود درِ اتاقی که معمولاً بسته است، نیمه‌باز مانده است. صدای مشخصی از داخل شنیده نمی‌شود.

نگهبان نباید بلافاصله وارد محل تاریک شود. ابتدا از فاصله ایمن وضعیت را بررسی، مسئول شیفت را مطلع و در صورت امکان محدوده را کنترل می‌کند. اگر نشانه ورود غیرمجاز وجود داشت، صحنه نباید دست‌کاری شود. زمان مشاهده، وضعیت قفل و افراد مطلع باید ثبت شود.

۸-۳. قطع دوربین‌ها هم‌زمان با حضور فرد ناشناس

چند دوربین یک بخش از محوطه از کار افتاده و فردی در نزدیکی همان محدوده دیده شده است. این وضعیت می‌تواند خرابی فنی یا رخداد عمدی باشد.

نگهبان باید موضوع را فوری گزارش کند، از نزدیک شدن غیرضروری به فرد یا محل خودداری کند و مسیرهای خروج را زیر نظر بگیرد. در صورت امکان، تصویر ظاهری فرد، لباس، وسیله نقلیه و جهت حرکت ثبت می‌شود. دستکاری دوربین یا تعقیب خطرناک مجاز نیست.

۴-۸. بوی شدید و مشاهده بخار در محل مواد شیمیایی

در زمان گشت، بوی تند و بخار در نزدیکی انبار مواد شیمیایی دیده می‌شود. اقدام درست، نزدیک نشدن، دور کردن افراد، اطلاع به واحد ایمنی و فنی و رعایت جهت باد تا حد امکان است. نگهبان نباید برای پیدا کردن منشأ نشتی وارد محل شود یا شیرها را ببندد، مگر اینکه آموزش و مجوز مشخص داشته باشد.

۵-۸. شیء ناشناس در کنار حصار

یک بسته بدون صاحب در کنار حصار مشاهده می‌شود. نگهبان نباید آن را جابه‌جا یا باز کند. باید فاصله ایمن ایجاد و مسیر عبور افراد محدود شود. موضوع با ذکر محل، ساعت و ویژگی ظاهری به مسئولان اعلام می‌شود. تصمیم نهایی درباره بررسی یا انتقال بسته با مراجع مجاز است.

۶-۸. اختلاف با مراجعه‌کننده

مراجعه‌کننده‌ای به دلیل درخواست کارت شناسایی عصبانی می‌شود و نگهبان را تهدید می‌کند. نگهبان باید آرامش خود را حفظ کند، وارد بحث طولانی نشود و از الفاظ تحریک‌آمیز استفاده نکند. در صورت ادامه تهدید، درخواست کمک و اطلاع به مسئول شیفت یا نیروی انتظامی طبق مقررات انجام می‌شود. حفظ امنیت دروازه و جلوگیری از ورود اجباری اولویت دارد.

فصل نهم: اصول گزارش‌نویسی، ارتباطات و تحویل شیفت

۱-۹. گزارش خوب چه ویژگی‌هایی دارد؟

گزارش باید روشن، دقیق، بی‌طرفانه و قابل پیگیری باشد. گزارش خوب به پرسش‌های «چه چیزی، کجا، چه زمانی، توسط چه کسی و چه اقدامی» پاسخ می‌دهد.

در گزارش باید میان مشاهده و برداشت تفاوت گذاشت. عبارت «قفل دروازه پشتی شکسته بود» مشاهده است؛ اما «حتماً سرقت انجام شده است» نتیجه‌گیری است و ممکن است هنوز ثابت نشده باشد.

۲-۹. اجزای گزارش رخداد

گزارش معمولاً شامل موارد زیر است:

- تاریخ و ساعت رخداد؛
 - محل دقیق؛
 - شرح عینی وضعیت؛
 - مشخصات افراد یا خودروهای مرتبط، در صورت امکان؛
 - اقدامات انجام شده؛
 - افراد و واحدهای مطلع شده؛
 - وضعیت نهایی تا زمان تحویل گزارش؛
 - نام و امضای گزارش دهنده.
- قالب رسمی گزارش باید با فرم‌های شرکت تطبیق داده شود. اطلاعات حساس نباید از مسیرهای غیرمجاز ارسال شود.

۳-۹. ارتباط رادیویی و تلفنی

در ارتباط اضطراری، پیام باید کوتاه و روشن باشد. ابتدا نام یا شناسه گوینده، سپس محل، نوع خطر و نیاز فوری اعلام می‌شود. از شوخی، شایعه، پیام‌های طولانی و بیان اطلاعات غیرضروری در کانال عمومی باید خودداری کرد.

اگر ارتباط اصلی قطع بود، از مسیر جایگزین تعیین شده استفاده می‌شود. شماره‌های اضطراری و مسئولان باید در محل مجاز و به‌روز نگهداری شوند.

۴-۹. تحویل شیفت

تحویل شیفت فقط جابه‌جایی نفرات نیست؛ انتقال وضعیت امنیتی و عملیاتی تأسیسات است. نگهبان خروجی باید موارد زیر را به نگهبان ورودی منتقل کند:

- افراد و خودروهای حاضر؛
- کلیدها و تجهیزات تحویلی؛

- خرابی‌ها و هشدارهای فعال؛
 - پیمانکاران داخل مجموعه؛
 - رخدادهای ثبت‌شده؛
 - مواردی که هنوز پیگیری نشده‌اند؛
 - وضعیت دروازه‌ها و مسیرهای پیرامونی.
- در صورت امکان، تحویل باید با ثبت کتبی یا الکترونیکی انجام شود. موضوعات مهم نباید تنها به حافظه افراد وابسته باشد.

فصل دهم: جمع‌بندی

صنعت آب و فاضلاب یکی از مهم‌ترین زیرساخت‌های حیاتی کشور است و استمرار فعالیت آن با سلامت، رفاه و امنیت جامعه ارتباط مستقیم دارد. تهدیدهای این صنعت تنها به سرقت یا ورود غیرمجاز محدود نمی‌شوند، بلکه مجموعه‌ای از تهدیدهای طبیعی، انسانی، فنی، سایبری، محیط‌زیستی و ترکیبی را دربرمی‌گیرند.

نگهبان در خط مقدم حفاظت قرار دارد. ارزش کار او در مشاهده دقیق، رعایت مقررات، کنترل دسترسی، گزارش به موقع، رفتار حرفه‌ای و خودداری از اقدامات پرخطر است. نگهبان موفق کسی نیست که در هر حادثه به تنهایی وارد عمل شود؛ بلکه کسی است که خطر را زود تشخیص دهد، جان افراد را در اولویت قرار دهد، از حدود اختیار خود تجاوز نکند و اطلاعات درست را سریع به فرد مسئول برساند.

مهم‌ترین اصول عملی این جزوه عبارت‌اند از:

- هیچ ورود، خروج یا تحویلی را بدون رعایت روال ثبت و تأیید نپذیرید؛
- به نشانه‌های کوچک مانند قفل معیوب، روشنایی خاموش یا تردد غیرعادی بی‌توجه نباشید؛
- در برابر بسته ناشناس، نشت مواد، کابل آسیب‌دیده و فضای بسته، فاصله ایمن را حفظ کنید؛
- اطلاعات امنیتی و رمزها را محرمانه نگه دارید؛
- خرابی دوربین، بی‌سیم، تلفن و سامانه اعلام خطر را فوراً گزارش کنید؛
- با مردم و کارکنان محترمانه اما قاطع رفتار کنید؛

- در شرایط اضطراری، جان انسان‌ها را بر اموال مقدم بدانید؛
 - هیچ دستورالعمل عمومی را جایگزین دستورالعمل داخلی شرکت ندانید.
- جزئیات مربوط به سطح‌بندی مناطق، شماره تماس‌ها، نحوه بازرسی، استفاده از تجهیزات، شرایط حمل مواد شیمیایی، مدیریت تهدیدهای خاص و اختیارات نیروهای حفاظت باید با دستورالعمل داخلی شرکت، ضوابط ایمنی و مقررات مراجع ذی‌صلاح تطبیق داده شود.

منابع

1. قانون تشکیل شرکت‌های آب و فاضلاب، مصوب مجلس شورای اسلامی و اصلاحات بعدی، پایگاه مرکز پژوهش‌های مجلس و سامانه قوانین و مقررات جمهوری اسلامی ایران.
2. قانون مدیریت بحران کشور، مصوب ۱۳۹۸، سامانه ملی قوانین و مقررات جمهوری اسلامی ایران.
3. سازمان پدافند غیرعامل کشور، اسناد و مطالب آموزشی عمومی درباره پدافند غیرعامل و حفاظت از زیرساخت‌های حیاتی، وبگاه رسمی سازمان پدافند غیرعامل کشور.
4. شرکت مهندسی آب و فاضلاب کشور، گزارش‌ها و مطالب عمومی مرتبط با صنعت آب و فاضلاب، وبگاه رسمی شرکت مهندسی آب و فاضلاب کشور.
5. وزارت نیرو، اطلاعات و گزارش‌های عمومی درباره تأمین آب، جمع‌آوری و تصفیه فاضلاب و مدیریت زیرساخت‌های آب، وبگاه رسمی وزارت نیرو.
6. سازمان ملی استاندارد ایران، استانداردها و راهنماهای منتشرشده در حوزه ایمنی، مدیریت بحران و سامانه‌های مدیریتی، وبگاه رسمی سازمان ملی استاندارد ایران.
7. سازمان حفاظت محیط‌زیست ایران، قوانین و ضوابط عمومی مرتبط با آلودگی آب، فاضلاب و حفاظت محیط‌زیست، وبگاه رسمی سازمان حفاظت محیط‌زیست.
8. سازمان آتش‌نشانی و خدمات ایمنی، راهنماهای عمومی ایمنی در برابر حریق، تخلیه اضطراری و استفاده از خاموش‌کننده‌ها.
9. ISO 31000:2018, Risk ,International Organization for Standardization
.management — Guidelines

- ISO 22301:2019, Security ,International Organization for Standardization .10
— and resilience — Business continuity management systems
.Requirements
- ISO 27001:2022, Information ,International Organization for Standardization .11
security, cybersecurity and privacy protection — Information security
.management systems — Requirements
- IEC 62443 series, Industrial ,International Electrotechnical Commission .12
.communication networks — Network and system security
- Framework for Improving ,National Institute of Standards and Technology .13
.NIST, 2018 ,Critical Infrastructure Cybersecurity, Version 1.1
- Guide to Industrial Control ,National Institute of Standards and Technology .14
.NIST, 2023 ,Systems Security, SP 800-82 Rev. 3
- America's Water Infrastructure Act ,U.S. Environmental Protection Agency .15
of 2018: Risk and Resilience Assessment and Emergency Response Plan
Guidance , منابع و راهنماهای عمومی بخش آب.
- Water Safety Plan Manual: Step-by-step risk ,World Health Organization .16
.second edition, WHO, 2023 ,management for drinking-water suppliers
- fourth ,Guidelines for Drinking-water Quality ,World Health Organization .17
.edition incorporating the first and second addenda, WHO
- Sendai Framework for ,United Nations Office for Disaster Risk Reduction .18
.Disaster Risk Reduction 2015–2030
- Occupational Safety and Health Administration , منابع عمومی مربوط به ایمنی .19
فضاهای بسته، مواد شیمیایی، واکنش اضطراری و حفاظت کارکنان، وبگاه رسمی OSHA.
- دستورالعمل‌ها، نقشه‌ها، برنامه‌های اضطراری، نظام‌نامه‌های حفاظتی و ضوابط ایمنی .20
اختصاصی هر شرکت آب و فاضلاب؛ نیازمند تطبیق با دستورالعمل داخلی شرکت.