ВЪЗМОЖНОСТИ, ПРИЛОЖЕНИЕ И РИСКОВЕ ЗА КИБЕРСИГУРНОСТТА НА ИНФОРМАЦИОННИТЕ СИСТЕМИ ЗА УПРАВЛЕНИЕ НА ПРОМИШЛЕНИ ПРЕДПРИЯТИЯ

Николай Митев
Университет по библиотекознание и информационни технологии

Росица Митева
Технически университет – София

Резюме: С термина „Индустрия 4.0“ се обозначава съвременната концепция за развитие на индустрията чрез широко приложение на ИКТ за дигитализация на управлението на бизнес и производствените процеси. Чрез използването на интегрирани информационни системи за управление се извършват интеграция и обмен на данни в реално време и се осъществяват автоматизация и отимизация на управлението и контрола на процесите, което води до увеличаване на конкурентоспособността на компаниите. Същевременно, наред с предимствата, новите технологични решения увеличават уязвимостта на компаниите по отношение на киберзаплахи, тъй като те се превръщат в привлекателна цел за кибератаките, извършвани от разнообразни злонамерени лица, групи и организации.

Ключови думи: системи за управление, бизнес и производствените процеси, киберсигурност.

Въведение

Терминът „Индустрия 4.0“ се дефинира за първи път от Федералното правителство на Германия като основна инициатива за приемане на високотехнологична стратегия за развитие на немската индустрия през 2011 г., след което започва да се използва за обозначаване на тенденцията за широко прилагане на ИКТ за цифровизиране на управлението на бизнес и производствените процеси.

Индустрия 4.0 се определя като част от прилагането на новите цифрови технологии в производствения сектор и включва широк набор от технологични решения и бизнес модели, които допринасят за качествено нови форми на икономическа активност [1].

Индустрия 4.0 представлява съвкупност от свързани цифрови технологични решения, подпомагащи развитието на автоматизацията, интеграцията и обмена на данни в реално време в бизнес и

производствените процеси. По своята същност това представлява индустриален и технологичен трансформационен процес, който включва интернет свързаност и взаимодействие на кибернетично-физически системи без участието на човека, обработка и анализ на големи информационни масиви и вземане на решения от изкуствен интелект, роботика, ползване на облачни изчисления, цифрово моделиране и симулиране на производствените процеси чрез виртуална реалност, интелигентна автоматизация, масово производство на индивидуализирани продукти, поява на нови технологии, създаване на нови бизнес модели.

Съществуването на визия и оптимална стратегия за прилагане на ИТК при управление на бизнеса с цел адаптация към високо конкурентната глобална среда на цифровата икономика Индустрия 4.0, се превръща в основния фактор за създаването на дълготрайно конкурентно предимство и растеж на инвестиционната привлекателност на компаниите. В условията на Индустрия 4.0 ефективното управление на бизнес и производствените дейности представлява ценен ресурс за организацията, наред с традиционните финансови, материални, човешки и други ресурси. Именно този ресурс, чрез контрола върху всички страни на дейността на предприятието, помага за динамично реагиране на все по-бързо променящата се пазарна ситуация, за бързо идентифициране на проблемите и затрудненията, което позволява усилията да се концентрират точно там, където е най-необходимо в момента.

Интегрирани информационни системи за управление на предприятия

Оптимизацията и автоматизацията на управлението и контрола на бизнес и производствените процеси в съвременните компании се извършват чрез използване на *интегрирани информационни системи за управление* (наричани най-често ERP системи, като абревиатурата се получава от наименованието *Enterprise Resources Planning*). Единствено и еднозначно определение за ERP системите няма, но едно подходящо е: „ERP системата е компютърно интегрирана, многомерна и многофункционална система, изградена на база клиент-сървър технология, основана на бизнес модела за планиране, контрол и глобална оптимизация на цялостната логистична верига на процесите по доставката, производството и пласмента на готовите изделия и съпътстващите ги финансови операции“ [2].

В своя първоначален вид ERP системите са представлявали отделни компютризирани информационни системи с ограничени възможности за планиране, управление и контрол на определени

ресурси, с ниска степен на интеграция и взаимодействие при обмена на данни помежду им. С развитието на ИКТ, ERP се превръща в многофункционална информационна система, задвижвана от интегриран набор от програмни модули, чрез която се осъществява цялостното управление на бизнеса на компаниите. Основно предимство на ERP системите и разлика спрямо традиционните системи за развитие и управление е, че те могат да работят при различни конфигурации на хардуера и компютърните мрежи, като обикновено информацията се съхранява в база данни, а достъпът на потребителите до нея се осигурява чрез прилагане и поддържане на гъвкава система за управление на достъпа. Една от основните характеристики на всички ERP системи е споделената база данни, която поддържа множество функции и информация, използвани от различни бизнес единици. Това означава, че информацията се въвежда само веднъж и без допълнителни обработки намира своето отражение във всички свързани модули на системата, като незабавно става достъпна в реално време за всички лица от различни поделения, оправомощени да я получават. Друго съществено предимство на тази интеграция е, че наличната информация вече може да бъде обработвана и комбинирана по нови начини, което дава на ръководството много по-цялостен поглед върху бизнес дейностите в компанията, не само от гледна точка на крайните резултати, но и на динамиката на реализирането и взаимодействие на процесите в реално време. С развитието на технологиите съвременните ERP все повече придобиват функции на експертни системи, с помощта на които се създават прогностични модели за средата и за очакваните резултати при реализирането на процесите, които помагат на ръководителите на различни нива да вземат обосновани бизнес решения [3].

Въпреки определените различия, в зависимост от областта на производството и услугите, в които работят компаниите, като цяло ERP системите, които те използват, имат някои общи черти по отношение на включените модули и предлаганите функционалности. В най-общия случай ERP софтуерът интегрира различните функции в компанията в една цялостна структурирана система чрез включване на модули, предназначени за:

- интегриране на финансовата информация;
- интегриране на информацията за движението на стоково-материалните запаси;
- стандартизиране и ускоряване на производството;
- стандартизиране и управление на доставките;
- управление на проекти и ресурси;
- управление на човешките ресурси;

- управление на взаимоотношенията с клиентите;
- улесняване на отчетността.

Интегрираните ERP системи предлагат функционалности, базирани на т.нар. „най-добри практики“, което означава, че софтуерът отразява начина, по който производителите интерпретират най-ефикасните начини за осъществяване на даден бизнес процес. Компаниите, които прилагат най-добрите практики, намаляват времето и повишават ефикасността при изпълнението на сложните задачи, свързани със събиране, съхраняване, управление, интегриране, анализ и тълкуване на данни за множество (в идеалния случай – всички) бизнес процеси в предприятието.

Интелигентни системи за управление на производството

Съвременното производство в повечето случаи е сложна, комплексна, високо автоматизирана, усъвършенствана дейност по създаване на продукти за потребление и средства за производство, която изисква правилно планиране на ресурсите, ефективно използване на техническите съоръжения в производствените звена, оптимизиране на управлението на оборудването и човешките ресурси, управляване на качеството и бързи реакции при прекъсвания и непланирани събития. Както много други организации, работещи в различни сфери на икономиката и финансите, съвременните производствени компании, за да бъдат конкурентни в глобален мащаб, използват ERP системи за организиране и управляване на своите производствени и бизнес процеси.

Въпреки че много от модулите на ERP системите имат пряко отношение към интегрирането на информацията и управлението на производствените процеси, в повечето случаи те не са достатъчни за тяхното автоматизиране и оптимизиране, защото производствата на огромната номенклатура от различни видове елементи, възли, модули, готови продукти и изделия са строго специфични и тяхното организиране и управляване не могат да се осъществят чрез използването на универсални модули или инструменти. Казано по друг начин, ERP са ефективни на високо ниво, в контекста на цялата организация, при управляване на бизнеса на предприятието. За да се произведе заявеният продукт своевременно, контролирано, безопасно и предсказуемо, в ERP системата трябва да има интегриран допълнителен слой за организиране, управляване и контрол на производството, който може да бъде наречен „интелигентно производство“ (smart factory).

Този допълнителен слой, известен като „Система за управление на производството“ (Manufacturing Execution System - MES), трябва не

само да отговаря непосредствено за производството на продукта, но също така да отговаря за събирането, съхраняването и предоставянето на данни относно действителното изпълнение на производствения процес, да осигурява подробна проследимост на стъпките в този процес и многократно и последователно да прилага същия процес, докато изискванията за неговото реализиране не бъдат умишлено променени.

Системата за управление на производството (MES) представлява компютризирана система, използваща специализирани софтуерни продукти за проследяване и документиране на трансформацията на суровините в готови изделия, която работи в реално време, за да даде възможност за контрол на множество елементи при реализиране на производствения процес. Освен това системите MES могат да събират, съхраняват и предоставят информация, която помага на ръководителите да анализират резултатите от изпълнението на производствените процеси и да вземат решения как да бъдат оптимизирани, за да се подобри производството.

В цялостната архитектура на управлението на бизнес и производствените процеси на предприятието MES може да бъдат разглеждани като междинен елемент (посредник) между ERP системата и системите за непосредствен контрол и управление на промишленото оборудване за производство (SCADA).

Системата за управление и контрол на производството MES осигурява и улеснява, от една страна, потока от данни и информация за производството в необходимия обем и формат към ERP системата като цяло и отделните модули за управление на бизнес процесите, и в обратна посока – към системите за автоматизация на производствените процеси SCADA. Затова ERP и MES системите, от една страна, и MES – SCADA, от друга, трябва да бъдат интегрирани, като изходът на едната система се превръща във вход на другата и обратно, при което производственият процес става по-прозрачен, мащабируем, предсказуем и надежден.

Системата за събиране на данни, наблюдение, контрол и управление на производството (SCADA – Supervisory control and data acquisition) представлява комбинация от хардуер, софтуер и комуникационна инфраструктура, която позволява извличане на данни в реално време от производствения процес, на базата на които се осъществяват неговото управляване, контрол и оптимизиране. Със своите възможности за локално или отдалечено управление на параметрите на автоматизирани технологични процеси и възможности за регистрация под формата на логове на събитията при

осъществяване на тези процеси, модерните решения за системите SCADA се превърнаха в интегрална част от дейността на промишлените предприятия.

Архитектурата на системите за автоматизация и управление на производствените процеси SCADA включва четири отделни нива с ясно разпределени функции: полево (технологично) оборудване и съоръжения; програмируеми логически контролери (Programmable Logic Controller – PLC) и/или отдалечени терминални възли (Remote Terminal Units – RTUs); комуникационна мрежа и настолни компютри или персонални мобилни устройства, на които е инсталиран софтуерът SCADA. Той обработва, разпределя и визуализира необходимите данни, осигурявайки възможност, с помощта на графични потребителски интерфейси (Graphical User Interfaces – GUI), на операторите на полевото оборудване, както и на управленския персонал, да вземат информирани решения и да предприемат нужните действия.

Основната функция на платформите SCADA е осигуряването на възможности за цялостен контрол на производствените системи от разстояние, но те осигуряват и възможност за локален контрол на процесите, така че полевите устройства (например вентили, помпи, двигатели, предаватели и т.н.) да се включват и изключват в подходящото време, допълвайки стратегията за отдалечено управление, събиране на данни и регистриране на различните събития при реализирането на производствените процеси. За целта съвременните софтуерни платформи SCADA предлагат множество опции, например задаване на аларми и изпращане на известия до потребителите, комплексни инструменти за съхраняване, обработване и анализиране на данни в реално време, включително статистическа обработка и идентифициране на тенденции в исторически план, и т.н. Това става възможно с прилагане на съвременни IT стандарти, практики и технологии при създаване софтуера SCADA, като използване на SQL и уеббазирани приложения, чрез които се оптимизират ефективността, сигурността, производителността и надеждността на системите SCADA.

Киберсигурност на производствените системи за управление

Индустрия 4.0 се основава на автономната комуникация на технологии, използвани за управляване на бизнес и производствени процеси, и производствено оборудване, включени в производствения процес по цялата верига на стойността. Тази концепция отчита увеличеното компютризиране на производствените сектори, където физическите обекти са плавно интегрирани в информационната

мрежа. По този начин модерните технологии все повече размиват границите между реален и виртуален свят, създавайки т.нар. киберфизически производствени системи, управлявани с помощта на интегрирани интелигентни системи за управление, означавани като „интелигентно производство“.

Заедно с посочените възможности и предимства системите за управление, поради своята висока степен на комплексност и интегритет, представляват голямо предизвикателство от гледна точка на осигуряване на необходимите нива на киберсигурност. Поради приложението им за автоматизация на всички процеси и за управляване на цялостната дейност на предприятието, както и поради размиването на границите на самата система в резултат на поддържане и осъществяване на голям брой външни комуникации, тя става уязвима за голям брой киберзаплахи.

Тези общи киберзаплахи за системите за управление, които се отнасят за всички информационни системи и комуникационни мрежи, може да се групират на такива:

- свързани с технологиите (хардуерни системи и мрежи – архитектура, конфигурация, капацитет, резервиране и т.н.; софтуерни продукти – функционални възможности на операционни системи, универсални и потребителски приложения, системи за сигурност, настройки, персонализиране и поддръжка, уязвимости, актуализации, управление на достъпа и т.н.);
- свързани с хората – в повечето случаи служителите на компаниите са главен обект на киберпрестъпниците, които се възползват от слабости като небрежност, невнимание, доверчивост, неглижиране, за осъществяване на кибератаки от типа „социален инженеринг“. Допълнителна заплаха представляват недоволни или злонамерени служители. Затова особено внимание трябва да се обърне на подбора и осигуряването на необходимия персонал, със съответното образование, професионална квалификация, опит и умения, на осигуряването на допълнително обучение и тренировки за подобряване на уменията на служителите както от гледна точка на изпълнението на професионалните им задължения, така и по отношение на спазването на правилата и мерките за киберсигурност [4].

Особено чувствителни по отношение на киберзаплахите са информационните системи за управление на производствените процеси, защото, както вече отбелязахме, част от техните функции, в рамките на концепцията „интелигентно производство“, са за

непосредствено управляване на физическото оборудване (чрез модулите SCADA). Всякакъв вид пробив в сигурността не само може да предизвика отказ, блокиране, възможност за манипулиране или за получаване на контрол от страна на атакуващите върху определени информационни ресурси или дори върху цялата информационна система на компанията, но и да им даде възможност за получаване на достъп до управлението на физическото производствено оборудване.

Последствията от пробиви в сигурността на системи за управление на производствените процеси MES, в частност при компрометиране на модулите SCADA, може да включват спиране на производството, повреди на производственото оборудване или на спомагателни системи (снабдяване с електричество, газ, климатизация и т.н.), които могат да доведат до катастрофални последици за съоръженията, до производствени аварии, а в крайни случаи – и до загуба на живот. Въпреки че е възможно да се получи загуба на интелектуална собственост (данни за параметри и настройки на процеси, ноу-хау, производствени данни и т.н.) и на друга чувствителна информация, която може да бъде използвана за изнудване на компаниите, все пак основните опасности при кибератаки срещу интелигентното производство са свързани по-скоро с функционирането и параметрите на физическите производствени процеси, отколкото с поверителността и целостта на информацията, като е при традиционните киберрискове [5].

Днес чрез автоматизирани информационни системи се извършват управление на производството и доставка на жизненоважни продукти, както и предоставяне, мониторинг, контрол и управляване на достъпа до услуги, които са критично важни за функционирането на обществото, като производство и доставка на храна, електричество, вода, газ, петролни продукти, отвеждане на отпадни води и обработка на отпадъци, транспорт и системи за управление на транспорта, медицински услуги и т.н.

Прекъсването или нарушаването на доставката на жизненоважни продукти и услуги от предприятията от критичните инфраструктура в резултат на технически откази или кибератаки могат не само да нанесат икономически вреди и финансови загуби на държавите, но и пряко да причинят затруднения в дейността на структури, отговорни за гарантирането на националната сигурност, или да застрашат националната сигурност чрез дезорганизиране на обществото и предизвикване на социални вълнения, например чрез създаване на дефицити (или повишаване на цените) на критични продукти и услуги, т.е. кибератаките могат да се окажат елемент на хибридни войни или

да представляват терористичен акт, целящи провокиране на хаос, противоречия, противопоставяне и дезинтеграция на обществото.

Заключение

В условията на Индустрия 4.0 широкото прилагане на новите решения, предоставяни в процеса на развитие на ИТ за дигитална трансформация на управлението на бизнеса и производството на продукти и услуги, е единственият начин за компаниите да останат конкурентоспособни в условията на съществуващия глобален пазар, който съвременната цифровата икономика предлага. Дигитализацията води до създаването на киберфизически производствени системи, чрез които се извършват автоматизация и оптимизация на производствените и бизнес процесите, осигуряващи повишаване на производителността и ефективността на дейността на компаниите, което съответно води до предлагане на голям обем разнообразни и качествени продукти и услуги за задоволяване на нуждите на потребителите и обществото. Същевременно масовото навлизане на ИТ и промяната на модела на работа на компаниите (като децентрализация, работа от разстояние, постоянна свързаност и комуникация през интернет и т.н.), както и тоталната им зависимост от правилното функциониране на техните информационни и комуникационни системи, водят до увеличаване на рисковете за прекъсвания, откази, аварии и прекратяване на дейността при нарушаване на киберсигурността. От глобалната свързаност на информационните системи и мрежи, която се разглежда като едно от основните предимства, предлагани от съвременната цифрова икономика, се възползват не само легитимните участници, но и зловредни лица, групи и организации, които за изпълнение на своите престъпни намерения използват същите тези авангардни решения и постижения, които се осигуряват с развитието на ИТ. Затова за съвременните компании, наред с осъществяването на дигиталната трансформация, приоритет трябва да бъдат усилията (създаване на политики, стратегии, осигуряване на ресурси – финансови, материални, човешки) за намаляване на рисковете и постигане на адекватни нива на киберсигурност.

References/Литература

1. **Kontseptsiya** za tsifrova transformatsiya v bŭlgarskata industriya (Industriya 4.0). https://www.mi.government.bg/bg/themes/koncepciya-za-cifrova-transformaciya-na-balgarskata-industriya-industriya-4-0-1862-468.html.

[**Концепция** за цифрова трансформация на българската индустрия (Индустрия 4.0). https://www.mi.government.bg/bg/themes/koncepciya-za-cifrova-transformaciya-na-balgarskata-industriya-industriya-4-0-1862-468.html.]

2. **Petkov**, A. Upravlenski informatsionni sistemi. Ruse: Primaks, 2004.
[**Петков**, А. Управленски информационни системи. Русе: Примакс, 2004.]

3. **Boneva**, M., A. **Petkov**, A. **Nedyalkov**, I. **Sheludko**, P. **Vitliemov**. Prilozhenie na integrirani informatsionni sistemi zaupravlenie na protsesite v organizatsiite. Ruse: Primaks, 2017.
[**Бонева**, М., А. **Петков**, А. **Недялков**, И. **Шелудко**, П. **Витлиемов**. Приложение на интегрирани информационни системи за управление на процесите в организациите. Русе: Примакс, 2017.]

4. **Semerdzhiev**, Ts., N. **Mitev**. Upravlenie na informatsionnata sigurnost v organizatsiite. Sofia: Softtreyd, 2020.
[**Семерджиев**, Ц., Н. **Митев**. Управление на информационната сигурност в организациите. София: Софттрейд, 2020.]

5. **Mitev**, N., R. **Miteva**. Upravlenie i zashtita na intelektualnite aktivi v kiber prostranstvoto. Sofia: Softtreyd, 2019.
[**Митев**, Н., Р. **Митева**. Управление и защита на интелектуалните активи в кибер пространството. София: Софттрейд, 2019.]

За авторите

Николай Митев е доцент, преподавател в катедра „Национална сигурност“ в УниБИТ. Чете лекции, автор е и участва като съавтор при издаването на 7 учебника и учебни пособия в областта на ефективното използване на информационните системи и управлението и защитата на информацията.

За контакт с автора: n.mitev@unibit.bg

Росица Митева е доцент, преподавател в катедра „Прецизна техника и уредостроене“ в ТУ – София. Чете лекции по „Системи за управление на качеството“, автор е и участва като съавтор при издаването на 5 учебника и учебни пособия в областта на ефективното използване на информационните системи и управлението и защитата на информацията, на метрологията и управление на качеството.

За контакт с автора: rosimiteva@tu-sofia.bg

OPPORTUNITIES, APPLICATION AND RISKS FOR CYBER SECURITY OF INDUSTRIAL ENTERPRISE MANAGEMENT INFORMATION SYSTEMS

Nikolay Mitev
University of Library Studies and Information Technologies

Rositsa Miteva
Technical University – Sofia

Abstract: The term "Industry 4.0" refers to the modern concept of industrial development through the widespread use of ICT for digitalization of management of business and production processes. Through the use of integrated management information systems, the integration and exchange of data in real time is performed and automation and optimization of the management and control of the processes is carried out, which leads to an increase in the competitiveness of the companies. At the same time, along with the benefits, new technology solutions increase companies' vulnerability to cyber threats, as they become an attractive target for cyberattacks carried out by a variety of malicious individuals, groups and organizations.

Keywords: Management systems, Business and production processes, Cybersecurity.

About the authors

Nikolay Mitev, Assoc. Prof. PhD is a lecturer at the Department of "National Security" at ULSIT. He delivers lectures, is an author and participates as a co-author in the publishing of 7 textbooks and teaching materials in the field of effective use of information systems, management and protection of information.

To contact the author: n.mitev@unibit.bg

Rositsa Miteva, Assoc. Prof. PhD is a lecturer at the Department of "Precision Technique and Instrumentation" at the Technical University of Sofia. She lectures on "Quality Management Systems", author and co-author of 5 textbooks and teaching materials in the field of effective use of information systems and information management and protection, of metrology and quality management.

To contact the author: rosimiteva@tu-sofia.bg