СЪВРЕМЕННИТЕ СИСТЕМИ И ТЕХНИКА ЗА СИГУРНОСТ И РОЛЯТА ИМ ЗА СЪЗДАВАНЕ НА ЗАЩИТЕНА ОФИС СРЕДА

Илиана Димитрова
Университет по библиотекознание и информационни технологии

Резюме: Обезпечаването на сигурност на компанията е приоритетна задача на всяко ръководство. В ерата на бързо развиващите се нови технологии пред всеки собственик стои предизвикателството не само да защити фирмата, офиса, бизнеса си физически – от преки посегателства върху собствеността, имуществото, личния състав и клиентите си, но и да опази информационния и интелектуалния потенциал, които понастоящем са по-ценни от материалните придобивки. Частните охранителни компании са ценен партньор в съвместното изграждане на стратегии за охрана на недвижимото имущество и опазване на информационните масиви с помощта на съвременните системи и техника за сигурност.

Ключови думи: системи и техника за сигурност, контрол на достъп, СОТ и периметрова охрана, камери, видеонаблюдение.

Въведение

За успешното развитие на всяка фирма от изключителна важност са нивото на компетентност на собственика ѝ и на ръководния фактор, вижданията им за бъдещето на бизнеса и разработването на стратегии, които да водят успешно компанията напред. Повече от необходимо е фирмата да има изградена стабилна структура, ясни вътрешни правила за работа и поведение, добре подбран състав от компетентни кадри, умело стратегическо планиране, майсторски маркетинг и реклама и не на последно място, непрекъснато да се анализира бизнес и обществената среда и да се вземат възможно най-адекватни мерки и управленски решения за обезпечаването на сигурна работна среда. Като се има предвид, че всеки бизнес в определена ситуация може да бъде категоризиран като критична инфраструктура, обезпечаването на сигурност и защита е фактор, засягащ националната сигурност на страната. Както отбелязва В. Лазаров: „От края на XX в. защитата на критичната инфраструктура е съществен елемент от политиката за сигурност на много страни, които отчитат, от една страна, процесите на глобализация, а от друга, борбата срещу международния тероризъм. Другата основна причина за развитието на такава политика е появата и контролът над големите инфраструктурни проекти“ [1].

За да се гарантира безопасността на бизнеса, в процеса се включват частните охранителни компании – в ролята на партньори, които дават компетентна консултация и съвети за инсталирането на модерни средства за охрана на територията на офиса/фирмата. Повечето фирми, занимаващи се с охранителна дейност, освен стандартните услуги за охрана на обекти и хора предлагат и услугата „инженеринг“, която е насочена конкретно към конфигурирането и изграждането на системи за сигурност за всеки отделен клиент, съобразявайки се с дейността, изискванията, спецификите и възможните рискове. Частните охранителни компании работят в тясна връзка с фирмите, предлагащи на пазара специализирани системи и техника за сигурност, и са в течение на новостите, които големите световни производители анонсират всяка година.

Методология на изследването

На базата на анализ и оценка на дейностите в работата на охранителните фирми, в настоящия доклад ще бъде представен процесът за изграждане на системи и техника за сигурност на ниво фирма/офис.

Какъв е принципът на действие, когато става въпрос за изграждане на система за охрана на дадена компания? Независимо от спецификите на всеки отделен бизнес, има общи положения, представляващи базата, върху която се надграждат мерките, които ще подсигурят сигурността при функционирането на фирмата. Стандартната процедура започва с оглед на обекта, в който ще бъдат изграждани системи за сигурност. Много е важно да се обърне внимание на локацията. От това до голяма степен зависи колко и какви технически средства за охрана се налага да бъдат изградени, за да се подсигури сигурност на околоофисното пространство. Решенията за периметрова охрана включват няколко компонента – защитни заграждения, инфрачервени бариери, датчици за движение, бариери и рампи със специален режим за достъп – всички тези системи, в комбинация с камери за видеонаблюдение. Пазарът предлага модерни решения за отдалечен достъп и контрол на тези системи – с управление през мобилно или смартустройство, настройка за отложена във времето реакция, задействане на базата на разрешен достъп по предварително зададени критерии (лицево разпознаване, четене на номера на автомобили).

Сериозно място за контрол както на външния периметър, така и на офисната част заема видеонаблюдението. Обикновено част от камерите следят пространството около офиса/сградата, а друга част –

самата офисна част, като се поставят на места с предполагаем повишен риск от нерегламентиран достъп.

Съвременните технологии позволяват да се направи избор сред множеството модели, предназначени за следене на специфични пространства и обекти. Притежаваща висока чуствителност, тази техника реагира на движение и звукови сигнали. Специално за външното наблюдение се препоръчват infra-red камери, с много високо ниво на резолюция и антимаскинг функции, което дава възможност да се наблюдава охраняемият периметър при всякакъв вид метеорологични условия и да се получава ясно и качествено изображение дори когато те са изключително неблагоприятни. Друга специфика на този тип камери е възможността да пренастройват наблюдението от дневен на нощен режим и обратно, без това да се отразява на качеството на получавания сигнал. Независимо дали са корпусни, или куполни, модерните камери за видеонаблюдение са снабдени с високо чувствителни обективи, способни да реагират и да се фокусират върху обектите независимо от разстоянието. Има модели, които следят периметъра на 360º.

Друг вид камери за външно наблюдение, които се използват и за нуждите на Пътна полиция и институции със специален статут, са оборудвани със специализиран софтуер, „четящ“ номерата на превозните средства, които преминават в близост до сградата. В зависимост от капацитета контролният софтуер е в състояние да фиксира и запише над 5000 поредни номера в рамките на една минута. Тази информация се съхранява в специализиран информационния масив и може да бъде ползвана за нуждите на компанията. Изкуственият интелект обработва постъпилата информация и в реално време индикира наличие на проблемни обекти в рамките на наблюдавания периметър. Паралелно с това тази техника предлага възможност за лицево разпознаване, като на тази база може да бъде настроен пропускателният режим в сградата или офиса и да се избегне достъпът на нежелани посетители.

След уточняване на външния периметър за охрана се преминава към прекия достъп до офиса на компанията. За тази цел може да бъдат приложени системи за контрол на достъпа на територията на обекта с няколко нива на сигурност – в зависимост от това дали става въпрос за собствениците на компанията, охраната, служителите на компанията, гости и клиенти. Съвременните системи за контрол на достъпа предлагат опцията посетителите да бъдат обособени в отделни потоци, към които се прилагат различни критерии за достъп на територията на обекта. Обикновено собствениците имат пълен достъп, а служителите имат частичен достъп до помещенията в обекта

в зависимост от ранга и отговорностите си. За гостите и клентите на фирмата обикновено се прилага сравнително рестриктивен режим. Влизането в сградата може да бъде посредством карти за достъп, посредством лицево разпознаване, а в определени случаи се използват сканиращи средства и устройства за проверка на посетителя и багажа.

Въпрос на предпочитания и индивидуално виждане е ползването на жива охрана, която да контролира и следи системите за достъп до сградата, или пък контролът да бъде управляван от специализиран софтуер, боравещ с необходимата база данни, за да контролира безпроблемното функциониране на системите за сигурност. Производителите предлагат опции за инсталиране на последно поколение IP домофонни системи с лицеви панели, осигуряващи до десет поста за вход и контрол. Всички външни модули са оборудвани с Fisheye IP камера с широк динамичен обхват, осигуряваща кристално изображение и позволяваща на потребителите ясно да видят кой е на входа, като по този начин се запазва високото ниво на сигурност. В допълнение, новите лицеви панели са оборудвани със система за намаляване на шума и затихване на ехото, LED осветление, безконтактен четец за контрол на достъпа и Wi-Fi свързаност. С помощта на мобилно приложение се осигурява възможност за наблюдение на обекта от дистанция.

Откакто през 2020 г. избухна световната пандемия от COVID-19, много компании се възползваха от възможността да инсталират на входа на фирмата си специални панели за лицево разпознаване, свързани с камера, отчитаща телесната температура на посетителите. По този начин, без да е необходим физически контакт, може да се контролира здравословното състояние на всеки, който иска да посети компанията. При наличие на висока температура системата не позволява достъп на болния на територията на сградата.

По отношение на фирмения персонал се прилага и друга система – за контрол на работното време. Във всеки момент, когато има влизане в/излизане от сградата, системата отчита статуса на служителите, като по този начин се следи за коректността на персонала по отношение на спазването на договорените условия за работа и почивка в течение на работния ден. Самата система анализира данните и може да индикира проблемни служители, които не спазват установеното работно време, както и движението им в зони, в които достъпът е ограничен. Режимът на придвижване трябва да е строго регламентиран. Всеки служител има достъп до работното си място, до общи сервизни и санитарни помещения, до зоните за почивка и хранене. Чекирането сутрин на влизане и вечер при напускане на сградата се отразява в системата за работно време

посредством специализиран софтуер, който отчита реалното физическо присъствие на служителя на територията на офиса.

Така получената информация се систематизира от системата и се предоставя на съответните отдели, които на тази база могат да правят корекции в заплащането, да предлагат санкции, глоби или друг тип наказания и рестрикции за некоректните служители.

На пазара вече се предлагат и нови решения за контрол на достъпа и работното време – терминали за разпознаване на лица и модули за вграждане в турникети. Тази технология е на базата на Deep learning алгоритъм, който увеличава точността на разпознаване на лица до над 99% и увеличава скоростта на проверка до под 0,2 секунди. Повишената степен на проверка и точност гарантират достъп без докосване за потребителите – огромно подобрение в сравнение с проверката на лични карти, карти за достъп или сканирането на пръстови отпечатъци. Този тип терминали за разпознаване на лица реагират еднакво добре и в среда с ниска и дори нулева светлина. Снабдени са с два обектива – един за видимата светлина и един инфрачервен. След сканирането на лицата те предоставят достъп само когато и двата обектива открият едно и също лице, както и определят дали лицето е действително, а не изображение. Тази технология за защита от измама прави управлението на контрола на достъпа много по-безопасно и предотвратява неоторизиран достъп със снимка вместо с истинско лице.

Камерите и видеонаблюдението са основната система за поддържането на реда и сигурността и на територията на офиса. Разположени на ключови места, така че да покриват голям периметър от вътрешността на сградата и помещенията, те предават информацията в реално време в контролен център, който може да бъде обслужван от физически лица или изкуствен интелект. Тази информация се записва на сървър и може да се съхранява за определено време в зависимост от важността си. При необходимост може да бъде преглеждана и възпроизвеждана, както и предоставяна за ползване на съответните органи, които имат право да я изискват.

Помещенията в офиса обикновено са с различен статут и към всяко от тях има определен оперативен интерес. Във връзка с това фирменото ръководство преценява какъв достъп да има до всяко помещение и каква система за контрол да бъде инсталирана. Вътрешен СОТ и специализирани четци с карти или друг тип идентификация са основно системите, използвани за охрана на помещенията, съдържащи и съхраняващи чуствителна и важна фирмена информация. Специално внимание се отделя на фирмения архив, сървърното помещение, или т.нар. data-center, трезора, касата,

счетоводството, кабинетите на управляващите и собствениците. При наличие на трезор се предвижда изграждане на допълнителна защитна бариера, защитни стени, както и индивидуални системи за защита на касетите. В помещение, където би била разположена каса или се работи с пари, обикновено се инсталират паникбутони и специални сигнализационни бутони на самите хранилища за пари и ценности, които са директно свързани с охраната на сградата, с охранителната фирма или с полицията (в зависимост от вида и дейността на компанията). Голям интерес представляват и системите FOGGY, които освен в банки и финансови институции имат приложение и във фирмена среда. При наличие на критична ситуация, индикирана от софтуера на камерите за видеонаблюдение или от реакция на служители, системата се активира и разпръсква „мъгла“, която да дезориентира нарушителите, а в това време да се задействат останалите структури за охрана и да се очаква пристигане на охранителите или представителите на органите на реда.

Живеем в ерата на информационното общество, което освен възможности за достъп до информационни ресурси носи и сериозни зависимости по отношение на опазването им на всяко ниво – и в обществено-политическия живот, и в бизнеса, и в частното битие. Както отбелязват И. Петева и В. Лазаров: „Информационното общество, икономиката на знанието, информацията като стратегически ресурс, е-управлението и достъпът до информация са вече признати съществени страни на глобалното общество. Днес информацията се определя като основен ресурс за всички сфери – политика, държавно управление, икономика, образование, здравеопазване, култура. Процесът на промяна обхваща целия спектър на обществения живот, той е повсеместен и необратим“ [2].

Във връзка с това освен на чисто физическия аспект на сигурността на офиса и работещите в него всяка компания трябва да обърне сериозно внимание и на опазването на сигурността на информацията, която е от изключителна важност в съвременните условия. В повечето случаи изтичането на важна фирмена информация или кражбата на такава могат да нанесат много по-големи щети на бизнеса, отколкото посегателстсвото върху материалната собственост. На всеки служител трябва да се предоставя индивидуална магнитна карта, с която да се обозначава в компанията. С помощта на тази карта, освен че ще има достъп до сградата и определени сектори в нея, той ще може да ползва периферните компютърни устройства в офиса. По този начин може да бъде проследявано дали се злоупотребява с офис консумативите, дали се използват печатащите и сканиращите устройства за несвойствени на

фирмата дейности и дали се извършват зловредни действия и се ползват користно вътрешнофирмената информация и инфраструктура.

За съхраняването на цялата фирмена информация се обособява специализиран информационен масив – обикновено сървърно помещение или data-center, – в който се съхранява цялата база данни за компанията. Самото сървърно помещение е със специален статут и към него се прилагат специфични мерки за сигурност. Специална система за контрол на достъпа, СОТ, камери, пожароизвестителна система и система за пожарогасене са задължително оборудване на подобно помещение. Достъпът до него е крайно ограничен и под специален и непрекъснат контрол. Освен по отношение на физическата сигурност сървърният сектор трябва да бъде много добре подсигурен и по отношение на информационната сигурност. Антивирусни системи и програми, защитни стени, филтри за проверка и пропуск на входящата и изходящата информация, редовна проверка и профилактика на базата данни, сървър за дублиране и съхраняване на данните – всичко това в комбинация с изградените системи за сигурност е най-чувствителният сектор в рамките на всеки офис.

Цялата комуникационно-информационна база трябва да се организира във вътрешна мрежа. Всеки служител, в зависимост от заеманата позиция, компетентности и задължения, има определен достъп до ограничена част или до цялата база данни на фирмата.

Изрично трябва да се подчертае сериозното внимание, което всяка компания е нужно да отделя на съхраняването и ползването на лични данни и на стриктното спазване на изискванията и условията за работа с тях. Важно е да се разпише специален регламент за работа и съхранение на договори и документи, съдържащи лични данни на клиенти, партньори, доставчици и служители. Строго определени да бъдат редът и списъкът на служителите, които биха могли да боравят с тази информация, както и местата за физическо съхранение при съответните условия на документи на хартиен носител.

Изводи

Осигуряването на контрол за достъп и защита на техническите и информационните ресурси в една компания не е никак лека задача. За да се достигне високо ниво на сигурност на фирмата, трябва да се познава изключително добре нормативната уредба, от една страна, и да се вложат достатъчно средства за техническо обезпечаване на сигурността, от друга. Далновидността и верният бизнес усет на всеки собственик на фирма са разковничето за успешното представяне на компанията като надежден бизнес партньор. Съвременната бизнес

среда изисква ясна стратегия по отношение на контрола на сигурността, която позволява на собственика на фирма да е поне с крачка пред криминалния контингент и недоброжелателните бизнес конкуренти. Да се възползва максимално от услугите, предлагани от частния сектор за сигурност и високите технологии, с които частните охранителни фирми разполагат – това е основен фактор за спокойното функциониране на всеки бизнес в този толкова неспокоен свят.

Заключение

Освен партньорство с бизнеса, този тип консултантска и инженерна дейност, предлагана от частните охранителни компании, би могла да бъде полезна и на държавните институции, като се има предвид сериозният технически потенциал в сферата на системите и техниката за сигурност. Големите фирми за охрана имат капацитет да поемат отговорност за градското видеонаблюдение. При желание и законодателна инициатива работата на Единния телефонен номер за спешни случаи 112 може да бъде подпомогната от колцентровете за централизирана охрана и СОТ на частните охранителни фирми. Дирекциите за реагиране на централизираната охрана биха могли успешно да се включат в звеното за бърза и неотложна медицинска помощ. Още немалко идеи и инициативи може да бъдат реализирани в посока на опазване на обществения ред и защита на националната сигурност, ако държавата обърне по-сериозно внимание на сектора на частна охранителна дейност.

За злонамерените няма спирачки и ограничения, няма и почивен ден. Затова всеки трябва да бъде подготвен – независимо дали става въпрос за опазване на държавна, частна, или бизнес собственост. И тук е мястото на сериозните компании, занимаващи се с частна охранителна дейност, които могат да предложат съвременни иновативни решения и технологии, гарантиращи спокойствие и сигурност за развитието на успешен бизнес.

Настоящият Доклад е подготвен за представяне с ексклузивното разрешение на собственика на фирмите „СОТ – сигнално охранителна техника“ ЕООД и „Сектрон“ ООД да се използва информацията, засягаща услуги, системи и техника за сигурност, предлагани от двете компании. Представените данни са изцяло базирани на информация, предоставена от компаниите.

Бележки

[1] **Zakon** za chastnata ohranitelna deynost. – V: *Darzhaven vestnik,* br. 10, 2018 g; izm. *Darzhaven vestnik,* br. 69 ot 04.08.2020 g.

[**Закон** за частната охранителна дейност. – В: *Държавен вестник*, бр. 10, 2018 г.; изм. *Държавен вестник*, бр. 69 от 04.08.2020 г.]

[1] **Targovski** zakon. – V: *Darzhaven vestnik*, br. 48 ot 18.06.1991 g.; izm. *Darzhaven vestnik*, br. 104 ot 08.12.2020 g.

[**Търговски** закон. – В: *Държавен вестник*, бр. 48 от 18.06.1991 г.; изм. *Държавен вестник*, бр. 104 от 08.12.2020 г.]

[2] **Strategia** za natsionalna sigurnost na Republika Bulgaria. – V: *Darzhaven vestnik*, br. 26 ot 23.03.2018 g.

[**Стратегия** за национална сигурност на Република България. – В: *Държавен вестник*, бр. 26 от 23.03.2018 г.]

[3] **Kontseptsia** za natsionalnata sigurnost na Republika Bulgaria. – V: *Darzhaven vestnik*, br. 46 ot 22.04.1998 g.

[**Концепция** за националната сигурност на Република България. – В: *Държавен вестник*, бр. 46 от 22.04.1998 г.]

[4] **Naredba № 8121z-610** ot 11 yuni 2018 g. za reda, po koyto litsata udostoveryavat, che otgovaryat na iziskvaniyata na Zakona za chastnata ohranitelna deynost. – V: *Darzhaven vestnik*, br. 52 ot 22.06.2018 g.

[**Наредба № 8121з-610** от 11 юни 2018 г. за реда, по който лицата удостоверяват, че отговарят на изискванията на Закона за частната охранителна дейност. – В: *Държавен вестник*, бр. 52 от 22.06.2018 г.]

[5] **Naredba** № 8121z-611 ot 11 yuni 2018 g. za usloviyata i reda za organizatsia i izvarshvane na vidovete chastna ohranitelna deynost po chl. 5, al. 1 ot Zakona za chastnata ohranitelna deynost i za opredelyane na primerna tipova klasifikatsia na obektite, na koito se osashtestvyava ohrana po chl. 5, al. 1, t. 2 i 3 ot Zakona za chastnata ohranitelna deynost. – V: *Darzhaven vestnik*, br. 52 ot 22.06.2018 g.

[**Наредба № 8121з-611** от 11 юни 2018 г. за условията и реда за организация и извършване на видовете частна охранителна дейност по чл. 5, ал. 1 от Закона за частната охранителна дейност и за определяне на примерна типова класификация на обектите, на които се осъществява охрана по чл. 5, ал. 1, т. 2 и 3 от Закона за частната охранителна дейност. – В: *Държавен вестник*, бр. 52 от 22.06.2018 г.]

[6] **SECTRON** OOD. https://sectron.com.

[**СЕКТРОН** ООД. https://sectron.com.]

[7] **SOT** – signalno-ohranitelna tehnika EOOD. https://sot.bg.

[**СОТ** – сигнално-охранителна техника ЕООД. https://sot.bg.]

References/Литература

1. **Lazarov**, Vladislav. Uyazvimost na kritichnata infrastruktura. Monografia. Sofia: Za bukvite – O pismenehy, 2019. 210 s. ISBN 978-619-185-384-7, s. 12.

[**Лазаров**, Владислав. Уязвимост на критичната инфраструктура. Монография. София: За буквите – О писменехъ, 2019. 210 с. ISBN 978-619-185-384-7, с. 12.].

2. **Peteva**, Irena, Vladislav **Lazarov**. Strategicheskite energiyni resursi vav fokusa na informatsionnata tsivilizatsia. Monografia. Sofia: Za bukvite – O pismenehy, 2020, s. 207. ISBN 978-619-185-438-7.

[**Петева**, Ирена, Владислав **Лазаров**. Стратегическите енергийни ресурси във фокуса на информационната цивилизация. Монография. София: За буквите – О писменехъ, 2020, с. 207. ISBN 978-619-185-438-7.]

За автора

Илиана Димитрова е работила дълги години като „специалист, доставки“ в частния охранителен сектор – по-специално търговия със системи и техника за сигурност. През 1987 г. завършва средното си образование в Гимназия с преподаване на чужди езици „Васил Левски“ в град Правец – паралелка с преподаване на френски език. В периода 1988 – 1994 г. завършва семестриално специалност „Педагогика“ в Софийски университет „Свети Климент Охридски“. През 2020 г. придобива бакалавърска степен по „Обществени политики и практики“ в Университета по библиотекознание и информационни технологии – град София. През 2021 г. защитава магистърска степен по „Бизнес и административни информационни технологии и комуникации“ в УниБИТ. От Октомври 2021 г. е зачислена като редовен докторант в докторска програма „Национална сигурност“ – факултет „Информационни науки“, Катедра „Национална сигурност“ в УниБИТ.

За контакт с автора: i.a.dimitrova@unibit.bg

MODERN SYSTEMS AND TECHNIQUES FOR SECURITY AND THEIR ROLE FOR CREATING A SECURE OFFICE ENVIRONMENT

Iliana Dimitrova
University of Library Studies and Information Technologies

Abstract: Ensuring the security of the company is a priority of every management. In the era of rapidly evolving new technologies, every owner faces the challenge to protect his company, office, business not only physically – from direct encroachments on property, staff and customers, but also to preserve the information and intellectual potential that, at present, are more valuable than material gains. Private security companies are a valuable partner in the joint development of strategies for the protection of real estate and protection of information files, using modern systems and security techniques.

Keywords: security systems and equipment, access control, security and perimeter security, cameras, video surveillance.

About the author

Iliana Dimitrova has worked for years as a "Specialist, Purchasing" in the private security sector – in particular trade with security systems and equipment. In 1987 she graduated the foreign language high school Vasil Levski – Pravetz with French. Between 1988 – 1994 she studied for a degree in Pedagogy and Psychology from Sofia University "St. Kliment Ohridski". In 2020 she received a BA degree in "Public Policy and Practices" from the University of Library Studies and Information Technologies. In 2021 she defended her MA degree in "Business and Administrative Information Technologies and Communications" at ULSIT. Since October 2021 she's been a full-time PhD student in the doctoral program "National Security" – Faculty of Information Sciences, Department of National Security at ULSIT.

To contact the author: i.a.dimitrova@unibit.bg