В. У. Ногаева*,
У. А. Долотенко**

Французские предприятия — жертвы киберпреступности

Аннотация. С появлением сети Интернет в современном мире возросла угроза распространения новых видов преступлений — киберпреступлений. По данным статистики, французские предприятия наиболее подвержены виртуальным атакам, что препятствует их нормальному функционированию и осуществлению деятельности. В данной статье сделана попытка анализа причин, видов и форм киберпреступлений, а также анализа возможных и наиболее действенных методов борьбы с виртуальными преступлениями как на национальном, так и международном уровне.

Ключевые слова: киберпреступность, кибератака, киберпреступление, виртуальное пространство, французское предприятие, борьба с киберпреступностью, защита, информационная система, Конвенция о киберпреступности, международное сотрудничество.

Entreprises françaises: victimes de la cybercriminalité

DOI: 10.17803/1994-1471.2017.80.7.214-217

La cybercriminalité, l'un des principaux défis que doit relever la société d'aujourd'hui, est en pleine croissance. Les entreprises françaises sont sous la pression constante des cyberattaques. Les cyberattaques contre lesquelles il est difficile de lutter sont devenues au fil des années un véritable fléau pour les entreprises françaises.

La cybercriminalité a beaucoup progressé depuis plusieurs années. Ainsi, l'année dernière, le nombre des cyberattaques a augmenté de 50 %¹.

Dans cet article sont abordés les points suivants: quel est le coût financier des cyberattaques; comment prévenir, gérer et défendre son entreprise face aux cybercrimes; quelles sanctions appliquer pour l'intrusion dans les systèmes informatiques; la solution de ce problème au niveau international.

Avant d'exposer tous ces points il faut définir la notion d'un cybercrime.

La cybercriminalité est une notion large ayant un grand nombre de définitions, mais elle re-

¹ Les 5 grandes tendances en matière de sécurité informatique pour 2016 // URL: https://www.expoprotection.com/site/FR/Les_5_grandes_tendances_en_matiere_de_securite_informatique (consulté le 15 avril 2017).

© Ногаева В. У., Долотенко У. А., 2017

* Ногаева Виктория Урузмаговна, кандидат педагогических наук, доцент кафедры иностранных языков Московского государственного юридического университета имени О.Е. Кутафина (МГЮА)
vnoagaeva@yandex.ru

125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9

** Долотенко Ульяна Алексеевна, студентка Международно-правового института Московского государственного юридического университета имени О.Е. Кутафина (МГЮА)

madam.dolotenko@yandex.ru

125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9

groupe généralement l'ensemble des infractions criminelles perpétrées à l'aide d'un ordinateur ou sur un réseau, ou à l'aide de matériel informatique. Située dans un espace virtuel appelé le «cyberespace», ce type de criminalité se transpose à des formes traditionnelles par le caractère virtuel d'action et par l'absence de contact direct avec les victimes. Phénomène récent, la cybercriminalité s'est amplifiée avec l'informatisation de la société, l'accès à l'informatique, la mondialisation des réseaux sociaux et nécessite de déterminer des infractions tout à fait nouvelles.

Une cyberattaque peut émaner de personnes isolées aussi bien que de groupes organisés. Les auteurs des cybercrimes s'appellent «cyber délinquants».

Quelles formes peuvent prendre les cyberattaques ?

En fonction des objectifs des criminels les cyberattaques peuvent être classées en 3 grandes familles :

- Le sabotage: cette forme d'attaque rend inopérant l'activité de l'entreprise en bloquant son système informatique ;
- La déstabilisation : cette forme d'attaque a pour but de porter atteinte à l'image de l'entreprise par la divulgation des données etc.;
- L'espionnage : cette forme d'attaque est destinée à capter les informations stratégiques importantes ;
- Le rançonnement : cette forme d'attaque est utilisée pour prendre en otage les données et de demander une rançon.

La Convention du Conseil de l'Europe sur la cybercriminalité définit quatre types de criminalité informatique :

- l'accès illégal (art. 2);
- interception illégale (art. 3);
- intervention dans les données (art. 4);
- intervention dans le système (art. 5)².

En parlant des domaines d'activité les plus touchés par la cybercriminalité, il est à noter qu'elle affecte les particuliers et les professionnels. Les cybercriminels s'attaquent à l'industrie aussi

bien qu'aux activités de services tels que, les télécommunications, l'hôtellerie/tourisme et, plus récemment, les entreprises de médias. Ainsi, par exemple, en avril 2015, des pirates ont mis hors de service les systèmes électroniques de la chaîne de télévision française TV5 Monde. Pendant plusieurs heures, tous les systèmes de l'obtention de l'information ont été bloqués, la chaîne a perdu la capacité de diffuser des bulletins de nouvelles. Les pirates ont aussi piraté le site officiel et ses comptes dans les réseaux sociaux.

Il est évident que la motivation première d'une attaque est la fraude financière et le vol de données sur les clients. Dans ce contexte, combien coûte une cyberattaque pour l'entreprise victime?

Selon E. Kaspersky «en termes de rentabilité la cybercriminalité occupe aujourd'hui la deuxième place après le trafic de drogues. Le principal risque pour les entreprises est la fuite d'informations importantes»³.

Les pertes financières des cyberattaques peuvent entraîner de lourdes conséquences sur l'activité des entreprises. Il serait utile de citer les données statistiques concernant cyberattaques dans le monde entier. Le coût lié au cybercrime demeure très élevé. Les cyber-attaques coûtent aujourd'hui, au niveau mondial, plus de 400 milliards de dollars par an. Une cyberattaque en France coûte en moyenne 773 000 euros à une entreprise⁴. Les entreprises subissent en outre les coûts de la réparation des systèmes corrompus.

Le coût financier résultant des cyberattaques dans certains pays peuvent être chiffrées : environ 17 millions de dollars aux USA, 8 millions de dollars en Allemagne contre 4 millions de dollars en Australie.

Comment prendre des mesures efficaces en matière de cybercriminalité ?

Il existe des solutions, des outils disponibles pour la protection des systèmes ou limitation de l'impact des vols, mais il faut des moyens pour les mettre en place. Les mesures proposées pour la lutte contre cette forme de criminalité sont :

² Convention sur la cybercriminalité. Conseil de l'Europe // URL: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_fr.pdf (consulté le 24 avril 2017).

³ URL: <https://forum.kasperskyclub.ru/index.php?showtopic=27357> (consulté le 25 avril 2017).

⁴ Entreprises, une cyberattaque coûte en moyenne 773 000 euros // URL: <http://www.usine-digitale.fr/editorial/entreprises-une-cyberattaque-coute-en-moyenne-773-000-euros.N378944> (consulté le 30 mars 2017).

- 1) disposer d'informations sur les menaces existantes et sur les conséquences qu'elles peuvent avoir sur son activité et sur ses clients;
- 2) la création au sein des entreprises de centres opérationnels de sécurité;
- 3) former les collaborateurs, car un tiers des violations de données est dû à la négligence des collaborateurs. Il est donc recommandé d'inciter les salariés des entreprises à se montrer vigilants sur la confidentialité des données, sur les mots de passe (choisir des mots de passe complexes) à changer régulièrement, sur le fait de ne pas cliquer sur un mail suspect, de perte ou vol d'un matériel appartenant à l'entreprise, etc.

Du point de vue financier, cette sécurité coûte cher. Ainsi, TV 5 monde a dépensé pour sa sécurité environ 3,1 millions d'euros en 2016, et prévoit de dépenser 2,5 millions d'euros en 2017⁵. Après cette attaque TV 5 monde investit dans sa protection auprès d'Airbus, la filiale spatiale qui est spécialisée dans la défense.

Si malgré toutes ces mesures de prévention, il apparaît qu'un jour une entreprise soit un cible de cyberattaques, elle doit avant tout arrêter d'utiliser la machine corrompue, c'est ce que le personnel de la chaîne TV 5 monde a fait, il a identifié la machine attaquée et l'a déconnectée d'Internet, mettant ainsi fin à l'attaque. S'il ne l'avait pas fait tous ses systèmes, y compris les stocks, auraient été détériorés, et donc toute l'entreprise aurait été détruite.

En ce qui concerne les outils juridiques, les infractions à l'informatique en France sont régies au niveau national par le Code pénal (art. 321-1 — 321-8)⁶.

La réglementation juridique du cyberspace dans un pays est à peine possible. Compte tenu du fait que ce problème ne peut être résolu que dans le cadre du droit international, le Conseil des Ministres du Conseil de l'Europe a adopté en 2001 *la Convention sur la cybercriminalité* appelée aussi *la Convention de Budapest*. Entré en vigueur le 1er juillet 2004, c'est le seul instrument international contraignant dans ce domaine. La présente Convention est un ensemble

de principes de base pour tout pays adoptant des lois sur la cybercriminalité, ainsi qu'un cadre pour la coopération internationale entre les pays participants. Elle est complétée par un protocole sur la responsabilité pénale pour les actes de xénophobie et de racisme commis par le biais de systèmes informatiques, entré en vigueur le 1 mai 2006.

À ce jour la convention est ratifiée par 53 pays, y compris la France. La Russie est le seul membre du Conseil de l'Europe qui s'est abstenue, car elle n'est pas d'accord avec l'article sur «l'accès transfrontalier aux données informatiques stockées», qui, selon les autorités russes, menacent la sécurité et la souveraineté du pays. Cet article permet à différents services de sécurité de mener sans autorisation des opérations dans les réseaux informatiques des pays tiers. La Russie a proposé aux Nations Unies son projet de la Convention sur la coopération dans le domaine de la lutte contre la cybercriminalité. Le projet russe exclut la possibilité d'une intervention des services de renseignement de pays tiers aux systèmes informatiques d'autres personnes et un de ses articles prescrit le mécanisme de protection de la souveraineté. Le but des auteurs du document est défini comme la prévention des crimes et des actes illégaux dans le domaine des technologies d'information et de communication. Ceux-ci comprennent, en particulier, l'accès illégal à l'information, le développement et l'utilisation des logiciels malveillants et le spam, la pédopornographie, la violation du droit d'auteur.

Des experts mondiaux estiment que les nouvelles menaces les plus dangereuses pour la sécurité informatique sont la croissance de cybercrime, de cyberterrorisme et l'utilisation des technologies d'information et de communication (TIC) pour la solution des conflits entre Etats.

Il est à conclure que tous les pays sont touchés par ce problème et en même temps, ils ne sont pas prêts à faire le pas nécessaire pour se défendre. L'absence de règles juridiques internationales régissant les relations entre États en matière des cybercrimes empêche de créer un système de sécurité cybernétique international.

⁵ Le piratage de TV5 monde coûte 4,6 millions d'euros à la chaîne // URL: <http://www.clubic.com/antivirus-securite-informatique/actualite-798224-tv5-cout-piratage.html> (consulté le 16 avril 2017).

⁶ Le Code pénal (Articles 323-1 à 323-8) // URL: <https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT00000607071> (consulté le 27 avril 2017).

Les différences dans les législations nationales et le déficit de la coopération internationale permet aux cyber délinquants de rester impunis.

La cybercriminalité, étant un problème mondial, tous doivent unir leurs efforts afin de se

protéger contre cette menace. Les moyens traditionnels n'étant plus suffisants, avec la croissance d'attaques ciblées et de menaces avancées persistantes une nouvelle approche en matière de sécurité est nécessaire.

BIBLIOGRAPHIE

1. *Chekunov I. G.* Ponyatie i otlichitel'nye osobennosti kiberprestupnosti // Rossijskij sledovatel'. — 2014. — № 18. — S. 53 — 56.
2. *Freyssinet E.* La cybercriminalité en mouvement. — Hermes Science Publications, 2012. — 226 p.
3. Le piratage de TV5 monde coûte 4,6 millions d'euros à la chaîne // URL: <http://www.clubic.com/antivirus-securite-informatique/actualite-798224-tv5-cout-piratage.html> (consulté le 16 avril 2017).
4. Cyber-attaques: quels risques, quelles solutions? // URL: <http://www.entreprises.gouv.fr/politique-et-enjeux/cyber-attaques-quels-risques-queles-solutions> (consulté le 27 avril 2017).
5. Conseil de l'Europe. Convention sur la cybercriminalité. // URL: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_fr.pdf (consulté le 24 avril 2017).
6. Les 5 grandes tendances en matière de sécurité informatique pour 2016 // URL: https://www.expoprotection.com/site/FR/Les_5_grandes_tendances_en_matiere_de_securite_informatique (consulté le 15 avril 2017).
7. Entreprises, une cyberattaque coûte en moyenne 773 000 euros // URL: <http://www.usine-digitale.fr/editorial/entreprises-une-cyberattaque-coute-en-moyenne-773-000-euros.N378944> (consulté le 30 mars 2017).

Материал поступил в редакцию 30 апреля 2017 г.

FRENCH ENTERPRISES ARE CYBERCRIME VICTIMS

NOGAEVA Victoria Uruzmagovna — PhD in Pedagogical Sciences, Associate Professor of the Department of Foreign Languages at the Kutafin Moscow State Law University (MSAL)
vnogaeva@yandex.ru
125993, Russia, Moscow, Sadovaya-Kudrinskaya Str., 9

DOLOTENKO Ulyana Alekseevna — Student of the International Law Institute at the Kutafin Moscow State Law University (MSAL)
madam.dolotencko@yandex.ru
125993, Russia, Moscow, Sadovaya-Kudrinskaya Str., 9

Review: *The threat of proliferation of new types of crime – cybercrime – has increased nowadays. According to statistics, the French companies are most susceptible to virtual attacks that interferes with their normal functioning and enjoyment of activity. This article makes an attempt to analyze the causes, types and forms of cybercrimes, some possible and most effective methods to combat virtual crime at the national and international levels.*

Keywords: *cybercrime, cyber-attack, virtual space, French enterprise, fight against cybercrime, protection, information system, Convention on Cybercrime, international cooperation.*