Оригинальная статья

УДК 338.97:622.33

О противодействии киберпреступной деятельности

DOI: http://dx.doi.org/10.18796/0041-5790-2021-3-14-15

СТЕПАНОВ О.А.
Доктор юрид. наук, профессор,
главный научный сотрудник
Центра уголовного, уголовно-процессуального
законодательства и судебной практики
Института законодательства
и сравнительного правоведения
при Правительстве Российской Федерации,
117218, г. Москва, Россия,
e-mail: o_stepanov28@mail.ru

СТЕПАНОВ А.О.
Учащийся факультета экономических наук
НИУ «Высшая школа экономики»
101000, г. Москва, Россия,
e-mail: stepanov.alexey99@gmail.com

Рассматриваются особенности осуществления информационного противоборства с киберпреступными группами на предприятиях угольной отрасли в современных условиях.
Ключевые слова: *атаки киберпреступных групп, информационное противоборство, функции.*
Для цитирования: Степанов О.А., Степанов А.О. О противодействии киберпреступной деятельности // Уголь. 2021. № 3. С. 14-15. DOI: 10.18796/0041-5790-2021-3-14-15.

ВВЕДЕНИЕ

По оценкам Минэнерго России, после 2021 г. производство угля в России будет расти и в 2024 г. достигнет 450 млн т. При этом производство и экспорт угля из России будут соответствовать динамике мирового потребления. Исходя из этого на 2021 г. рассчитываются параметры федерального бюджета и тарифы естественных монополий [1]. Вместе с тем таким крупным производителям, как АО «СУЭК», АО «УК «Кузбассразрезуголь», АО ХК «СДС-Уголь», ООО «Компания «Востсибуголь», в рамках осуществления своей финансово-экономической политики следует обратить более пристальное внимание на сферу кибербезопасности.

СОСТАВЛЯЮЩИЕ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА

Так, по оценкам СМИ, в течение 2019-2020 гг. хакерская группировка XDSpy провела как минимум четыре успешные атаки на государственный сектор и промышленные предприятия. Эти атаки были успешными – анализ образцов вредоносного программного обеспечения подтвердил сбор, шифровку и отправку данных на серверы хакеров, которые остались безнаказанными.

Атаки XDSpy начинаются с фишингового письма по электронной почте с вложениями (файлами PowerPoint, ZIP или ярлыками, загрузка которых заражает жертву вредоносными программами). Эксперты полагают, что целью XDSpy является дальнейшая продажа полученных противоправным путем доступов к корпоративным и государственным сетям, то есть промышленный шпионаж. При этом жертвы XDSpy находятся в основном на территории России [2].

Анализу киберугроз, а также особенностям предотвращения неправомерного доступа к информации, обрабатываемой значимым объектом критической информационной инфраструктуры на предприятиях угольной промышленности, в 2019-2020 гг. были посвящены авторские публикации в журнале «Уголь» [3, 4, 5]. Однако проблема информационного противоборства с киберпреступными группами в этих публикациях не затрагивалась. С учетом того, что информационное противоборство включает в себя три основных компонента: стратегический анализ, информационное воздействие, информационное противодействие менеджменту ведущих угольных компаний, необходимо принимать во внимание перспективы создания организационно-управленческого и информационно-аналитического механизма. Такой механизм призван выполнять «оборонительные» задачи в рамках осуществления информационного противоборства с профессиональными хакерскими группировками.

Каждое противоправное действие, связанное даже с локальным вмешательством в работу компьютерной системы компании, как правило, имеет экономическую составляющую, т.е. может повлечь за собой совершенно неожиданные финансовые последствия. В целях недопущения развития «хаоса» в деятельности компании из-за несанкционированного доступа к ее электронным ресурсам в качестве ключевых функций такого механизма следует выделить: диагностическую, прогностическую, организационно-управленческую, методическую, профилактическую, контрольную, коррекционную [6].

Реализация диагностической функции предполагает оценку полноты охвата вниманием IT-специалистов компании результатов работы всех основных звеньев коммуникации, связанных с критически значимой для компании информации, а также диагностику соответствующих знаний и умений IT-специалистов, изучение их профессиональных намерений.

Прогностическая функция связана с разработкой индивидуальных планов повышения уровня профессиональных достижений IT-специалистов компании.

Организационно-управленческая функция связана с индивидуальной и организационной работой по формированию необходимых профессиональных навыков и умений у IT-специалистов компании в сфере осуществления информационного противоборства.

Методическая функция связана с разработкой методов принятия решений по оперативному реагированию на факты постороннего воздействия на деятельность компании, а также с оценкой результатов такого воздействия.

Профилактическая функция *связана с повышением уровня защиты собственной информации компании и с повышением эффективности мер противодействия попыткам взлома такой защиты.*

Контрольная функция предполагает анализ соответствия содержания контроля цели, виду, форме и совокупности осуществления его методов.

Коррекционная функция связана с коррекцией знаний IT-специалистов компании в сфере осуществления информационного противоборства с хакерскими группами, обеспечивающих поддержание возможностей системы защиты информации на заданном уровне.

ЗАКЛЮЧЕНИЕ

Все отмеченное выше носит особенно актуальный характер в условиях, когда *отечественные платежные системы, а также системы поддержки документооборота реализованы на основе зарубежных либо собственных несертифицированных криптографических средствах, что делает их весьма уязвимыми с точки зрения информационной безопасности.* Кроме того, следует обратить внимание на то, что в обозримой перспективе развитие в России сетей 5G связано с серьезными проблемами из-за разногласия различных государственных ведомств. Это обстоятельство может привести к тому, что отечественные алгоритмы шифрования трафика для 5G не будут приняты на глобальном уровне [7]. С учетом этого возрастает роль менеджмента ведущих угольных компаний в обеспечении их информационной безопасности.

Список литературы

1. Углю нарисовали светлое будущее // Коммерсантъ. № 181/П от 5.10.2020. С. 7 URL: https://www.kommersant.ru/doc/4519426 (дата обращения: 15.02.2021).

2. В хакерах узнали шпионов // Коммерсантъ. № 181/П от 5.10.2020. С. 7 URL: https://www.kommersant.ru/doc/4519427 (дата обращения: 15.02.2021).

3. Степанов О.А., Печегин Д.А. Право как средство обеспечения безопасности объектов угольной промышленности в условиях цифровизации // Уголь. 2019. № 9. С. 54-55. DOI: 10.18796/0041-5790-2019-9-54-55.

4. Степанов О.А. О перспективах развития надзора в угольной промышленности в условиях совершенствования законодательства о госконтроле // Уголь. 2020. № 2. С. 51-52. DOI: 10.18796/0041-5790-2020-2-51-52.

5. Степанов О.А. Об особенностях предотвращения неправомерного доступа к информации, обрабатываемой значимым объектом критической информационной инфраструктуры // Уголь. 2020. № 10. С. 40-41. DOI: 10.18796/0041-5790-2020-10-40-41.

6. Панарин И. Система информационного противоборства // ВПК. Военно-промышленный курьер. 15 октября 2008. URL: https://vpk-news.ru/articles/3672 (дата обращения: 15.02.2021).

7. Криптозащит и меч // Коммерсантъ. № 184/П от 8.10.2020. С. 1 URL: https://www.kommersant.ru/doc/4521511?query=Криптозащит (дата обращения: 15.02.2021).

Original Paper

UDC 338.97:622.33 © O.A. Stepanov, A.O. Stepanov, 2021
ISSN 0041-5790 (Print) • ISSN 2412-8333 (Online) •
Ugol' – Russian Coal Journal, 2021, № 3, pp. 14-15
DOI: http://dx.doi.org/10.18796/0041-5790-2021-3-14-15

Title
ON COUNTERACTING CYBERCRIMES

Authors
Stepanov O.A.[1], Stepanov A.O.[2]
[1] Institute of Legislation and Comparative Law under the Government of the Russian Federation, Moscow, 117218, Russian Federation
[2] HSE University, Moscow, 101000, Russian Federation

Authors' Information
Stepanov O.A., Doctor of Law Sciences, Professor, Chief Researcher of the Center for Criminal Law, Criminal Procedure Legislation, Judicial Practice, e-mail: o_stepanov28@mail.ru
Stepanov A.O., Student of Economic Sciences Department, e-mail: stepanov.alexey99@gmail.com

Abstract
The paper examines specific features of the information warfare against cybercrime groups in the coal mining industry in the current context.

Keywords
Attacks by cybercrime groups, Information warfare, Functions.

References
1. Coal is promised a better tomorrow. Kommersant, No. 181/P, dated 5.10.2020, p. 7. Available at: https://www.kommersant.ru/doc/4519426 (accessed 15.02.2021). (In Russ.).
2. Hackers recognized as spies. Kommersant, No. 181/P, dated 5.10.2020, p. 7. Available at: https://www.kommersant.ru/doc/4519427 (accessed 15.02.2021). (In Russ.).
3. Stepanov O.A. & Pechegin D.A. Law as a means of ensuring the safety of coal industry facilities in the context of digitalization. Ugol', 2019, (9), pp. 54-55. (In Russ.). DOI: 10.18796/0041-5790-2019-9-54-55.
4. Stepanov O.A. On the prospects for the development of supervision in the coal industry in the context of improving legislation on state control. Ugol', 2020, (2), pp. 51-52. (In Russ.). DOI: 10.18796/0041-5790-2020-2-51-52.
5. Stepanov O.A. On specific features of access management to information processed by a significant facility of critical IT infrastructure. Ugol', 2020, (10), pp. 40-41. (In Russ.). DOI: 10.18796/0041-5790-2020-10-40-41.
6. Panarin I. A system of information counteraction. Voenno-promyšlenniy kur'er, 15 October 2008. Available at: https://vpk-news.ru/articles/3672 (accessed 15.02.2021). (In Russ.).
7. The crypto shield and the sword. Kommersant", No. 184/P, dated 8.10.2020, p. 1. Available at: https://www.kommersant.ru/doc/4521511?query=Криптозащит (accessed 15.02.2021). (In Russ.).

For citation
Stepanov O.A. & Stepanov A.O. On counteracting cybercrimes. Ugol', 2021, (3), pp. 14-15. (In Russ.). DOI: 10.18796/0041-5790-2021-3-14-15.

Paper info
Received October 14, 2020
Reviewed November 11, 2020
Accepted February 17, 2021