УДК 007.3 **DOI 10.52167/1609-1817-2023-124-1-334-338**

Е.Н.Емельянов ✉
АО"Государственная техническая служба", Алматы, Казахстан
E-mail: e_emelyanov@sts.kz

ПРЕДПОСЫЛКИ СОЗДАНИЯ КИБЕРПОЛИГОНА В РЕСПУБЛИКЕ КАЗАХСТАН

Аннотация. Данная статья рассматривает проблематику в сфере обеспечения информационной безопасности, а именно нехватку специалистов в данной области с практическими навыками по защите от киберугроз. С учетом современных вызовов вопрос обеспечения киберзащиты информационно-коммуникационной инфраструктуры является вопросом национальной безопасности государства, для обеспечения которой, должны применяться необходимые организационные, правовые и технические меры включая обеспечение необходимым количеством высококвалифицированных специалистов. В качестве одного из таких решений является построение в Республике Казахстан киберполигона, направленного на наработку навыков по противодействию киберугрозам, подготовке специалистов различных квалификаций. Опыт зарубежных исследований в данной области позволил определить необходимость создания идентичной платформы киберучений в Республике Казахстан, позволяющей повысить качество подготовки, выработать практические навыки и сократить сроки.

Ключевые слова. Кибербезопасность, подготовка специалистов, киберполигон, Казахстан.

Введение.

Киберпреступность является одна из основных угроз сегодняшнего цифрового мира. Ежедневно граждане сталкиваются с фактами и примерами того, как с помощью кибератак можно создать промышленную, финансовую, социальную и экологическую катастрофы. В то же время в сфере безопасности присутствует отставание в обеспечении защиты, связанное с подготовкой кадров, разработкой и внедрением технологий защиты, что естественно, так как злоумышленники ищут новые методы атак, на которые, в последствии, разрабатываются определенные методы защиты.

Материалы и методы.

Ведущие державы мира считают, что у каждого государства должен быть выстроен процесс подготовки специалистов, повышения квалификации и выработки новейших методик выявления кибератак и угроз по недопущению возникновения киберинцидентов и минимизации их последствий. Это означает что любое государство должно быть готово защите и противостоянию киберугрозам, оно должно обладать соответствующими и технологическими и кадровыми ресурсами

Текущая ситуация в Республике Казахстан как в частном, так и в государственном секторе требует большого количества именно узких специалистов-практиков, знающих тенденции угроз, методы атак и способных здесь и сейчас решать вопросы по обеспечению информационной безопасности. В связи с острой нехваткой таких специалистов, невозможно в полной мере противостоять сегодняшним угрозам информационной безопасности. Таким образом системное развитие кадрового потенциала Республики Казахстан в области информационной безопасности и формирование практических навыков защиты от угроз информационной безопасности и компьютерных атак у учащихся, специалистов, руководителей в области информационных технологий и

информационной безопасности, является актуальной задачей на сегодняшний день. Решением данных задач может стать создание киберполигона, позволяющее повысить уровень специализации экспертов, работающих над обеспечением информационной безопасности в стране.

Мировой опыт показывает наличие и успешность внедрения платформ для проведения обучения специалистов во многих странах. Огромное внимание в мире оказывается построению различных платформ для обучения специалистов и имитации различных атак, такая практика применяется в учебных заведениях, в военных и правоохранительных органах и т.д. Активное применение киберполигонов мы можем видеть в Международном союзе электросвязи, в рамках НАТО, в таких странах как Россия, США, Израиль и др. При этом необходимо отметить, что в настоящее время на территории Республики Казахстан аналога такого продукта как киберполигон не имеется.

Результаты и обсуждения.

В Казахстане, в последние годы, проводится ряд очень серьезных мероприятий по повышению уровня информационной безопасности в стране. Так, реализована концепция «Киберщит Казахстана», направленная на реализацию организационных и технических мер по защите киберпространства государства. В реализации данной концепции осуществлены изменения в нормативно-правовом регулировании сферы информационной безопасности. Появились такие институты как Национальный центр информационной безопасности, Службы реагирования на инциденты информационной безопасности, Оперативные центры информационной безопасности. Данные структуры призваны обеспечить мониторинг, защиту информационно-коммуникационных инфраструктур частных организаций, критически важных объектов информационно-коммуникационной инфраструктуры страны, государственного и квазигосударственного секторов, а также реагирования на инциденты информационной безопасности. Следует отметить создание лаборатории по исследованию вредоносного кода, лаборатории безопасности информационно-коммуникационных технологий, лаборатории исследования средств информационной безопасности. Осуществлено техническое оснащение Национального координационного центра информационной безопасности.

Национальный проект «Технологический рывок за счет цифровизации, науки и инноваций», является продолжением концепции «Киберщит Казахстана». Одними из мероприятий проекта являются создание Центра исследования вредоносного кода и дальнейшее оснащение средствами защиты информации государственных органов и ведомств. Таким образом видно, что данные реализованные и реализуемые меры, в первую очередь, требуют подготовки высококвалифицированных кадров, способных применить свои навыки, а также использовать новейшие технологии в обеспечении защиты киберпространства государства.

Однако, дефицит кадров в сфере информационной безопасности — это острая проблема всех государств на текущий момент. По данным исследования компании Cyberbit только в США наблюдается свыше 460 тысяч вакансий в сфере информационной безопасности. По данным Комитета информационной безопасности Министерства цифрового развития инноваций и аэрокосмической промышленности Республики Казахстан, общая потребность в специалистах информационной безопасности складывается в 35 000. При этом востребованность заключается в специалистах с разными уровнями квалификации и по разным направлениям. Так, например, согласно Приказу Председателя Комитета национальной безопасности Республики Казахстан от 30 января 2015 года №4 «Об утверждении квалифицированных требований и перечня документов, подтверждающих соответствие им, для осуществления деятельности в сферах обеспечения информационной безопасности и специальных технических средств,

предназначенных для проведения оперативно-розыскных мероприятий». Для осуществления деятельности Оперативного центра информационной безопасности и Службы реагирования на инциденты информационной безопасности в штатном расписании необходимы специалисты по аудиту информационной безопасности, по компьютерной криминалистике; реверс-инжинирингу и(или) анализу вредоносных программ; а также этичному хакингу и(или) тестированию на проникновение.

Для решения данных проблем и предназначен киберполигон, его аппаратно-программная и методологическая составляющая, которая должна обеспечивать выполнение таких функций как:

-отработка практических навыков выявления компьютерных атак, расследования инцидентов информационной безопасности, взаимодействия между подразделениями информационных технологий и информационной безопасности, внедрения превентивных мер по предупреждению компьютерных атак;

-исследование и тестирование компонентов автоматизированных систем управления технологическим процессом и промышленного Интернета, средств защиты информации и технических решений по защите информации, в том числе - моделирование атак на кибер-физические системы;

-проведение кибер-учений, соревнований и практических тренировок по информационной безопасности для учащихся, специалистов, экспертов разного профиля в области информационной безопасности систем промышленной автоматизации.

Немаловажную роль должно играть методологическое оснащение киберполигона материалом, позволяющим как подготовить нового специалиста, так и повысить профессиональный уровень уже готового эксперта.

По результатам прохождения обучения на платформе Киберполигона обучаемый должен приобрести/улучшить практические навыки в следующих направлениях:

- red team (специализация в нападении, атаке);
- blue team (специализация в защите);
- threat hunting (специализация в поиске следов взлома или функционирования вредоносных программ, не обнаруженых стандартными средствами защиты);
- digital forensics (специализации в форензике, имеющей отношение к доказательствам, обнаруженным в компьютерах и цифровых носителях);
- malware analysis (специализация в исследовании или процессе определения функциональности, происхождения и потенциального воздействия образца вредоносного программного обеспечения);
- incident response (специализация в реагировании на инциденты);
- mass incident response (специализация в реагировании на массовые инциденты);
- system hardening (специализация в защите системы за счет ее уязвимости).

Таким образом создание Киберполигона позволит обеспечить:

- сокращение срока подготовки специалистов информационной безопасности и введения в самостоятельную работу;
- системное развитие кадрового потенциала в области информационной безопасности в выявлении компьютерных атак, расследовании инцидентов информационной безопасности, взаимодействии между подразделениями, внедрении превентивных мер по предупреждению компьютерных атак;
- формирование практических навыков защиты от угроз информационной безопасности и компьютерных атак у студентов ВУЗов Республики Казахстан, специалистов, руководителей в области информационных технологий и области информационной безопасности, тем самым расширив круг потенциальных специалистов в этой сфере.

ЛИТЕРАТУРА

[1] Главные тренды кибербезопасности в 2022 годуhttps://www.kv.by/post/1064880-glavnye-trendy-kiberbezopasnosti-v-2022-godu

[2] Закон Республики Казахстан «Об информатизации» от 24 ноября 2015 года № 418-V ЗРК.

[3] Об утверждении квалификационных требований и перечня документов, подтверждающих соответствие им, для осуществления деятельности в сферах обеспечения информационной безопасности и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий Приказ Председателя Комитета национальной безопасности Республики Казахстан от 30 января 2015 года № 4. Зарегистрирован в Министерстве юстиции Республики Казахстан 17 марта 2015 года № 10473.

[4] Постановление Правительства Республики Казахстан от 30 июня 2017 года № 407 «Об утверждении Концепции кибербезопасности («Киберщит Казахстан»)»

[5] Постановление Правительства Республики Казахстан от 12 октября 2021 года № 727. Об утверждении национального проекта "Технологический рывок за счет цифровизации, науки и инноваций"

[6] Руководство по разработке национальной стратегии кибербезопасности. Международный союз электросвязи (МСЭ)

[7] Benoliel, Daniel. (2015). Towards a Cybersecurity Policy Model: Israel National Cyber Bureau Case Study. North Carolina Journal of Law & Technology, Vol. 16(3).

[8] Carr, Madeline. (2016). Public-private partnerships in national cyber-security strategies. International Affairs, Vol. 92(1), 43-62.

[9] ENISA. (2014). An Evaluation Framework for National Cyber Security Strategies .

[10] Henschke, Adam and Shannon Brandt Ford. (2017). Cybersecurity, trustworthiness and resilient systems: guiding values for policy. Journal of Cyber Policy, Vol. 2(1), 82-95.

[11] Роль киберполигона в обеспечении ИБ. https://www.securityvision.ru/blog/rol-kiberpoligona-v-obespechenii-ib/

REFERENCES*

[1] Glavnye trendy kiberbezopasnosti v 2022 goduhttps://www.kv.by/post/1064880-glavnye-trendy-kiberbezopasnosti-v-2022-godu

[2] Zakon Respubliki Kazahstan «Ob informatizacii» ot 24 nojabrja 2015 goda № 418-V ZRK.

[3] Ob utverzhdenii kvalifikacionnyh trebovanij i perechnja dokumentov, podtverzhdajushhih sootvetstvie im, dlja osushhestvlenija dejatel'nosti v sferah obespechenija informacionnoj bezopasnosti i special'nyh tehnicheskih sredstv, prednaznachennyh dlja provedenija operativno-rozysknyh meroprijatij Prikaz Predsedatelja Komiteta nacional'noj bezopasnosti Respubliki Kazahstan ot 30 janvarja 2015 goda № 4. Zaregistrirovan v Ministerstve justicii Respubliki Kazahstan 17 marta 2015 goda № 10473.

[4] Postanovlenie Pravitel'stva Respubliki Kazahstan ot 30 ijunja 2017 goda № 407 «Ob utverzhdenii Koncepcii kiberbezopasnosti («Kibershhit Kazahstan»)»

[5] Postanovlenie Pravitel'stva Respubliki Kazahstan ot 12 oktjabrja 2021 goda № 727. Ob utverzhdenii nacional'nogo proekta "Tehnologicheskij ryvok za schet cifrovizacii, nauki i innovacij"

[6] Rukovodstvo po razrabotke nacional'noj strategii kiberbezopasnosti. Mezhdunarodnyj sojuz jelektrosvjazi (MSJe)

Евгений Емельянов, қызметкер, "Мемлекеттік техникалық қызмет" акционерлік қоғамы Алматы, Қазақстан, e_emelyanov@sts.kz

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНДА КИБЕРПОЛИГОНДЫ ҚҰРУ АЛҒЫШТТАРЫ

Аңдатпа. Бұл мақалада ақпараттық қауіпсіздікті қамтамасыз ету саласындағы мәселелер, атап айтқанда, киберқауіптерден қорғау бойынша іс жүзіндегі дағдылары бар осы саладағы мамандардың жетіспеушілігі қарастырылады. Қазіргі заманның сын-тегеуріндерін ескере отырып, ақпараттық-коммуникациялық инфрақұрылымның киберқорғауын қамтамасыз ету мәселесі мемлекеттің ұлттық қауіпсіздік мәселесі болып табылады, ал оны қамтамасыз ету үшін жоғары білікті мамандарды қажетті бірліктермен қамтамасыз етуді қоса алғанда, қажетті ұйымдастырушылық, құқықтық және техникалық шаралар қолданылуы керек. Осындай шешімдердің бірі ретінде Қазақстан Республикасында киберқауіптерге қарсы іс-қимыл, түрлі біліктілік мамандарын даярлау бойынша дағдыларды дамытуға бағытталған киберполигон құру болып табылады. Осы саладағы шетелдік зерттеулердің тәжірибесі Қазақстан Республикасында даярлық сапасын арттыруға, іс жүзіндегі дағдыларды дамытуға және мерзімдерді қысқартуға мүмкіндік беретін бірден бір кибер оқыту платформасын құру қажеттілігін айқындауға мүмкіндік берді.

Түйінді сөздер. Киберқауіпсіздік, мамандар даярлау, киберполигон, Қазақстан.

Yevgeniy Yemelyanov, employee, Joint Stock Company" State Technical Service"Almaty, Kazakhstan, e_emelyanov@sts.kz

PREREQUISITES FOR CREATING A CYBERPOLYGON IN THE REPUBLIC OF KAZAKHSTAN

Abstract. The article examines information security problems, namely the need for specialists with practical skills in protecting against cyber threats. Considering modern challenges, the issue of ensuring cyber protection of information and communication infrastructure is a matter of national security of the state to ensure that the necessary organizational, legal, and technical measures must be applied, including the provision of the necessary number of highly qualified specialists. One such solution is constructing a cyber training ground in the Republic of Kazakhstan, aimed at developing skills to counter cyber threats and training specialists of various qualifications. The foreign research experience in this area made it possible to determine the need to create an identical platform for cyber exercises in the Republic of Kazakhstan, which would improve the quality of training, develop practical skills, and reduce time.

Keywords. Cybersecurity, training of specialists, cyberpolygon, Kazakhstan.

****