УДК 371.3
DOI: 10.26140/anip-2020-0904-0039

ФОРМИРОВАНИЕ КОМПЕТЕНЦИИ УЧИТЕЛЯ ИНФОРМАТИКИ В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ

SPIN: 1825-9435
AuthorID: 705412
ORCID: 0000-0003-1414-9220
ScopusID: 57193094949

Нечай Александр Анатольевич, аспирант
Ленинградский государственный университет имени А.С. Пушкина
(196605, Россия, Санкт-Петербург, Петербургское шоссе, 10, e-mail: webexpromt@mail.ru)

SPIN: 1713-3530
AuthorID: 732054
ORCID: 0000-0002-1202-4830

Краснов Сергей Александрович, кандидат технических наук, доцент
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
(197376, Россия, Санкт-Петербург, ул. Профессора Попова, дом 5, e-mail: kras25@rambler.ru)

Аннотация. *Цель исследования* – рассмотреть особенности проблематики связанной с необходимостью повышения квалификации и формирования профессиональной компетенции учителей информатики в области кибербезопасности. В статье показана актуальность освоения учителями информатики новой компетенции в виду выполнения ими на рабочих местах нештатных обязанностей специалиста по кибербезопасности. Кроме того, в данной статье авторами проведены исследования угроз, которым подвержены современные образовательные организации. Проведен анализ возможностей кибератак, который позволяет сделать вывод, что информационная безопасность образовательных организаций достигается не только применением средств защиты информации, но и зависит от квалификации специалистов в области кибербезопасности, которые должны учесть все факторы для обнаружения и пресечения высокотехнологичных целенаправленных атак. *Научная новизна* исследования заключается в анализе киберугроз и формировании на основе полученных данных требований к формированию профессиональной компетенции учителя информатики. При проведении исследования был проведен анализ требований руководящих документов и образовательных программы для получения высшего образования по специальностям связанным с информационными технологиями, защитой информации и кибербезопасностью. *В результате доказано*, что приобретение профессиональных знаний учителями информатики в области кибербезопасности это необходимое и важное условие существования безопасного образовательного процесса в учебных заведениях, в которых исполняет свои должностные обязанности данная категория лиц.

Ключевые слова: кибербезопасность, кибератака, компетенция в области кибербезопасности, учитель информатики, формирование компетенции кибербезопасности.

FORMING THE COMPETENCE OF A COMPUTER SCIENCE TEACHER IN THE FIELD OF CYBERSECURITY

Nechai Alexander Anatolievich, postgraduate student
Leningrad State University named after A. S. Pushkin
(196605, Russia, Saint Petersburg, Peterburgskoe shosse 10, e-mail: webexpromt@mail.ru)

Krasnov Sergey Aleksandrovich, candidate of technical Sciences, associate Professor
Saint Petersburg State Electrotechnical University "LETI" named after V. I. Ulyanov (Lenin)
(197376, Russia, Saint Petersburg, Professora Popova str., 5, e-mail: kras25@rambler.ru)

Abstract. The purpose of the research is to consider the specifics of the issues related to the need for professional development and formation of professional competence of computer science teachers in the field of cybersecurity. The article shows the relevance of computer science teachers ' development of a new competence in view of their performance of non-standard duties of a cybersecurity specialist in the workplace. In addition, in this article, the authors conducted research on threats to modern educational organizations. An analysis of the possibilities of cyber attacks has been conducted, which allows us to conclude that the information security of educational organizations is achieved not only by the use of information security tools, but also depends on the qualifications of specialists in the field of cybersecurity, who must take into account all factors for detecting and suppressing high-tech targeted attacks. The scientific novelty of the research consists in the analysis of cyber threats and the formation of requirements for the formation of professional competence of a computer science teacher based on the data obtained. The study analyzed the requirements of the guidelines and educational programs for higher education in the fields of information technology, information security and cybersecurity. As a result, it is proved that the acquisition of professional knowledge by computer science teachers in the field of cybersecurity is a necessary and important condition for the existence of a safe educational process in educational institutions where this category of persons performs their official duties.

Keywords: cybersecurity, cyberattack, competence in the field of cybersecurity, computer science teacher, formation of cybersecurity competence.

В настоящей работе рассматривается проблема, связанная с необходимостью повышения квалификации и формирования профессиональной компетенции учителей информатики в области кибербезопасности. Отсутствие специалистов по кибербезопасности способных противостоять атакам в школах ставит под угрозу информационную образовательную среду школы. Для решения этой проблемы предлагается реализация образовательных программ нацеленных на переподготовку и повышение квалификации учителей информатики, в плане повышения компетентности в области кибербезопасности.

Вопросам формирования профессиональных компетенций учителей информатики посвящено значительное количество научных публикаций, в работе Горбачева А.В. рассматривается обобщенная модель формирования профессиональных компетенций учителя информатики [1], описываются общие подходы к формированию

модели, в совместной работе Радионова М.А., Акимова И.В., Губанова О.М. рассматриваются различные составляющие формирующие проффессиональную компетенцию учителя информатики [2], в работе Шастун Т.А. рассматривается подход к формированию специально-технологических компетенций учителя информатики.

Формирование компетенций в области защиты информации у будущих учителей рассматривают Чусавитин М.О. и Чусавитина Г.Н. [3], вопросам формирования профессиональных компетенций учителей в области кибербезопасности посвящены работы Рихтер Т.В. [4], в которой рассматривается использование интерактивных методов обучения при формировании профессиональных компетенций учителей по обеспечению кибербезопасности обучающихся [5].

Все рассмотренные научные работы предлагают разнообразные вариации повышения методического мастерства учителей информатики, по обучению обучающихся, но не одна работа не раскрывает тематику того, что именно должен знать сам учитель в области кибербезопасности, что должен уметь и чем владеть. Одно дело рассказывать о потенциальных угрозах [6,7], совсем другое показать на практике как реализуются кибератаки [8], как они проявляется [9,10], что можно предпринять [11-14], чтоб не дать возможность нарушителям информационной безопасности реализовать свои планы [15-17].

Рассмотрим, текущее состояние дел связанных с кибербезопасностью в образовательных организациях. Современные организации общего образования представляют собой сложную распределенную инфраструктуру, в которой широко используются информационные технологии [18], предназначенные для обучения и хранения персональных данных участников образовательного процесса и сотрудников образовательной организации [19]. Школы становятся все более технологичными, что в свою очередь повышаются риски связанные с информационными преступлениями.

Образовательные учреждения находятся в особенно уязвимом положении, когда речь заходит о кибератаках. Нарушители информационной безопасности, мотивированные желанием похитить конфиденциальные данные или нарушить их целостность, или доступность все чаще выбирают менее защищенные организации, финансирование которых в недостаточной мере направлено на приобретение дорогостоящих средств защиты от кибератак [20, 21], а так же не имеющие квалифицированных специалистов которые могут противостоять угрозам кибербезопасности.

Согласно руководящим документам во всех школах осуществляется комплекс мероприятий по защите информации: организована работа нештатных ответственных за защиту информации, пишутся отчеты руководящим составом организаций, контролирующими организациями проводятся соответствующие проверки – но при этом не все замечания выявляются и отражаются в документах в области кибербезопасности.

Для объективности, проведем исследование, и попробуем ответить на несколько вопросов: «Кто в школе отвечает за информационную безопасность?», «Кто отвечает за кибербезопасность?», «Имеют ли соответствующую квалификацию (знания, навыки и умения) соответствующие должностные лица, отвечающие за кибербезопасность?», «Может ли школа противостоять целенаправленной высокотехнологичной кибератаке?».

Согласно руководящим документам в школе есть два нештатных специалиста по защите информации (кибербезопасности) – заместитель директора и учитель информатики. Но при этом ни заместитель директора, ни учитель информатики не имеют компетенции в соответствующих областях.

Проведя анонимный опрос среди учителей информатики было выяснено, что их компетенция не достаточна, чтоб знать, как организуется кибератака, как киберпреступник попадает на компьютер своей жертвы и как противостоять кибератаке, потому что они не проходили подготовку по соответствующим программам переподготовки и (или) повышения квалификации. Сложившуюся ситуацию могут решить квалифицированные специалисты, которые обладают знаниями и умениями по обучению узконаправленных специалистов в области информационной безопасности и могут сформировать профессиональную компетенцию учителя информатики в области кибербезопасности. На сколько актуально учить УИ, поможет ответить фактография кибератак на образовательные организации.

Анализ кибератак проведенный компанией Positive Technologies представленный в своем отчете за третий квартал 2019 года [22] показывает, что четвертое место в рейтинге атакуемых занимают образовательные организации.

Государственные, промышленные и финансовые компании более надежно защищены от кибератак чем образовательные организации, но и это не гарантирует отсутствия атак на их информационную инфраструктуру. Это свидетельствует о том, что на сегодняшний момент совершенствуются не только системы защиты от кибератак [8,18] но и методы и средства, используемые злоумышленники, становятся более технологичными.

Из отчета по выявленным кибератакам на образовательные организации за третий квартал 2019 года [22] видно, что 93% всех атак направлены на компьютеры, серверы и сетевое оборудование, 4% атак направлено людей и 3% на веб-ресурсы образовательной организации.

Цели кибератак на образовательные организации, прослеживаются из той информации, которая была похищена или изменена в результате совершенных кибератак [22]. Наибольший процент составляют персональные данные сотрудников образовательной организации, это 43% от общего объема похищенных данных, потеря учетных данных сотрудников составила 15%, утрата данных платежных карт сотрудников составила 14%, комерческая тайна 14% и другая информация, которая попала в руки злоумышленников, составила оставшиеся 14%. Наличие средств защиты информации у образовательных организаций не останавливает киберпреступников, потому что они применяют модифицированные, новые и комбинированные методы атак, подробно эти методы описаны в работе [23]. Злоумышленниками применяются APT (advanced persistent threat) – атаки [23]. APT атака, это высокотехнологичная сложная целенаправленная атака, направленная на информационные ресурсы организации, которая реализуется таким образом, что она остается невидимой для средств защиты.

Исходя из вышеперечисленных возможностей кибератак можно сделать вывод, что на сегодняшний день современными средствами защиты который используется в образовательных организациях обнаружить и обезвредить высокотехнологичные целенаправленные атаки киберпреступников уже не возможно. А отсутствие специалистов по кибербезопасности способных противостоять атакам в школах ставит под угрозу информационную образовательную среду школы. Для этого требуется усовершенствование не только технических средств и систем защиты информации, но и повышение квалификации специалистов в области кибербезопасности, что позволит более эффективно конфигурировать и настраивать средства защиты информации.

Учителя информатики прошедшие курс повышения квалификации должны будут знать основные методы и инструменты, которые используют киберпреступники для совершения атак, а также методы, которые используются специалистами для обнаружения, нейтрализации и профилактики этих атак. Уметь выполнять весь комплекс мероприятий по недопущению проникновения киберпреступников в информационную среду в зоне своей ответственности. Владеть навыками по проведению

аудита и своевременного обнаружения проникновения киберпреступников в защищаемые информационные системы и нейтрализации киберпреступников в случае их своевременного обнаружения.

В план повышения квалификации учителей информатики в области кибербезопасности необходимо включить следующее компетенции:

• Знать основные методы и инструменты, которые используют киберпреступники для совершения атак, а также методы, которые используются специалистами для обнаружения, нейтрализации и профилактики этих атак.

• Уметь выполнять весь комплекс мероприятий по недопущению проникновения киберпреступников в информационную среду в зоне своей ответственности.

• Владеть навыками тестирования и своевременного обнаружения проникновения киберпреступников в защищаемые информационные системы и нейтрализации киберпреступников в случае их своевременного обнаружения.

СПИСОК ЛИТЕРАТУРЫ:

1. Горбачев А.В. Модель формирования профессиональных компетенций будущего учителя информатики // Проблемы современного педагогического образования. 2016. № 53-3. С. 146-152.

2. Родионов М.А., Акимова И.В., Губанова О.М. Формирование предметной составляющей профессиональной компетенции учителя информатики // Вопросы современной науки и практики. Университет им. В.И. Вернадского. 2017. № 2 (64). С. 129-139.

3. Чусавитин М.О., Чусавитина Г.Н. Модель методики формирования у будущего учителя информатики компетенции в области обеспечения информационной безопасности // В сборнике: Новые информационные технологии в образовании Материалы VII международной научно-практической конференции. Российский государственный профессионально-педагогический университет. 2014. С. 527-531.

4. Рихтер Т.В. Использование интерактивных методов обучения при формировании профессиональных компетенций педагогов по обеспечению кибербезопасности подрастающего поколения // В книге: активные и интерактивные методы обучения в естественно-математическом образовании коллективная монография. Соликамский государственный педагогический институт (филиал) ФГБОУ ВО «Пермский государственный национальный исследовательский университет». Соликамск, 2018. С. 13-21.

5. Нечай А.А., Котиков П.Е. Методика комплексной защиты данных, передаваемых и хранимых на различных носителях информации // Вестник Российского нового университета. Серия: Сложные системы: модели, анализ и управление. 2015. № 1. С. 92-95.

6. Котиков П.Е., Нечай А.А. Решение проблемы управления параллельным выполнением транзакций в распределенных базах данных для устранения опасной противоречивости // Вестник Российского нового университета. Серия: Сложные системы: модели, анализ и управление. 2015. № 2. С. 62-64.

7. Нечай А.А., Котиков П.Е. Актуальные проблемы защиты информации в современных автоматических телефонных станциях Вестник Российского нового университета. Серия: Сложные системы: модели, анализ и управление. 2015. № 2. С. 65-69.

8. Нечай А.А. Формирование безопасной информационной среды // Актуальные проблемы современности: наука и общество. 2019. № 4 (25). С. 43-44.

9. Нечай А.А., Копьев А.И. Метод управляемого распределения ресурсов между ядрами процессора // Вестник Российского нового университета. Серия: Сложные системы: модели, анализ и управление. 2018. № 2. С. 101-106.

10. Борисов А.А., Краснов С.А., Нечай А.А. Технология блокчейн и проблемы ее применения в различных информационных системах. // Вестник Российского нового университета. Серия: Сложные системы: модели, анализ и управление. 2018. № 2. С. 63-63.

11. Котиков, П.Е., Нечай А.А. Репликация данных между серверами баз данных в среде геоинформационных систем // Вестник Российского нового университета. Москва, 2015. №9. С. 88-91.

12. Широбоков В.В., Нечай А.А. Алгоритм планирования энергосберегающей параллельной обработки информации с учетом информационной важности и времени поступления задач // Вестник Российского нового университета. Москва, 2017. № 1. С. 88-93.

13. Васильев Н.Г. Система передачи данных, защита информации при обмене информации // Научный вектор Балкан. 2019. Т. 3. № 2 (4). С. 104-107.

14. Стадников М.Д. Педагогические условия формирования профессионально-коммуникативной компетентности специалистов по технической защите информации // Балтийский гуманитарный журнал. 2016. Т. 5. № 1 (14). С. 150-153.

15. Шаймарданов А.М., Нечай А.А., Лепехин С.В. Математическая модель систем автоматического управления с широтно-импульсной модуляцией // Вестник Российского нового университета. Серия: Сложные системы: модели, анализ и управление. 2019. № 2. С. 27-39.

16. Нечай, А.А., Котиков П.Е. Методика повышения надежности функционирования систем, организованных на перепрограммируемых элементах // вестник Российского нового университета. Серия: Сложные системы: модели, анализ и управление. Москва, 2016. № 1-2. С. 87-89.

17. Фарниев С.А. Теоретико-концептуальные аспекты изучения феномена информационной безопасности // Азимут научных исследований: экономика и управление. 2018. Т. 7. № 3 (24). С. 397-399.

18. Свинарчук А.А., Нечай А.А. Использование квантовых вычислений при выборе управленческого решения // Вестник Российского нового университета. Серия: Сложные системы: модели, анализ и управление. 2018. № 2. С. 31-36.

19. Новиков, А.Н. Нечай А.А., Малахов А.В. Математическая модель обоснования вариантов реконфигурации распределенной автоматизированной контрольно-измерительной системы // вестник Российского нового университета. Серия: Сложные системы: модели, анализ и управление. Москва, 2016. № 1-2. С. 56-59.

20. Борисов А.А., Краснов С.А., Нечай А.А. Технология блокчейн и проблемы её применения в различных информационных системах // Вестник Российского нового университета. Серия: Сложные системы: модели, анализ и управление. 2018. № 2. С. 63-67.

21. Новиков А.Н., Нечай А.А., Малахов А.В. О подходе к обоснованию рациональной номенклатуры эталонной базы измерительных комплексов на основе нечетких моделей // Вестник Российского нового университета. Серия: Сложные системы: модели, анализ и управление. 2017. № 1. С. 72-79.

22. Актуальные киберугрозы III квартал 2019 года: [Электронный ресурс] // Positive Technologies URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/cybersecurity-threatscape-2019-q3-rus.pdf (Дата обращения: 30.04.2020).

23. APT-атаки на госучреждения в России: обзор тактик и техник 2019: [Электронный ресурс] // Positive Technologies URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/apt-attacks-government-2019-rus.pdf (Дата обращения: 30.04.2020).

Статья поступила в редакцию 30.04.2020
Статья принята к публикации 27.11.2020