Статья / Article

УДК / UDC 371.3

Формирование профессиональной компетенции в области кибербезопасности у будущих учителей информатики

А. А. Нечай

Ленинградский государственный университет имени А.С. Пушкина, Санкт-Петербург, Российская Федерация

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 ввиду выполнения ими на рабочих местах нештатных обязанностей специалиста по кибербезопасности. Представлены исследования угроз, которым подвержены современные образовательные организации, проведен анализ возможностей кибератак. Все это позволяет сделать вывод, что информационная безопасность образовательных организаций достигается не только применением средств защиты информации, она также 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 профессиональной компетенции учителя информатики. Делается вывод, что приобретение учителями информатики профессиональных знаний 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.

Для цитирования: Нечай А.А. Формирование профессиональной компетенции в области кибербезопасности у будущих учителей информатики // Вестник Ленинградского государственного университета имени А.С. Пушкина. 2020. № 1. С. 114–124.

Formation of professional competence in the field of cybersecurity for future computer science teachers

Aleksandr A. Nechai

Pushkin Leningrad State University,
Saint Petersburg, Russian Federation

The purpose of the research is to consider the specifics of the problems related to the need to improve the skills and develop 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, this article examines the threats that modern educational organizations are exposed to. An analysis of the possibilities of cyber attacks is conducted, which allows us to conclude that the information security of educational organizations is achieved not only by using 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.

Key words: cyber security, cyber attack, competence in the field of cyber security, computer science teacher, to develop the competence of cybersecurity.

For citation: Nechay, A. A. (2020) Formirovanie professionalnoi kompetencii v oblasti kiberbezopasnosti u budushchih uchitelej informatiki [Formation of professional competence in the field of cybersecurity for future computer science teachers]. *Vestnik Leningradskogo gosudarstvennogo universiteta imeni A.S. Pushkina – Pushkin Leningrad State University Journal.* 4. pp. 114–124. (In Russian).

Введение

В настоящей работе рассматривается проблема, связанная с необходимостью повышения квалификации и формирования профессиональной компетенции учителей информатики в области кибербезопасности. Образовательные учреждения хранят значительное количество конфиденциальных данных, начиная от исследовательских и тестовых документов и заканчивая личной информацией всех участников образовательного процесса. По мере того как школы будут внедрять все

больше технологий в компьютерные классы и административные кабинеты укомплектованные вычислительной техникой, кибербезопасность будет становиться все более важной.

По сравнению с критически важными объектами, финансовыми организациями и промышленными предприятиями образовательные организации фактически не обеспечиваются современными средствами защиты информации, что делает их более привлекательными для киберпреступников. Скомпрометированная киберпреступниками компьютерная сеть образовательной организации может сильно повлиять на ее репутацию и образовательный процесс в целом.

Отсутствие специалистов по кибербезопасности в образовательной организации, способных противостоять атакам, 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 совершенствования компетентности в области кибербезопасности.

Обзор литературы

Вопросам формирования профессиональных компетенций учителей информатики посвящено значительное количество научных публикаций. Так, в работе Горбачева А.В. исследуется обобщенная модель формирования профессиональных компетенций учителя информатики [2], описываются общие подходы к созданию такой модели. Родионов М.А., Акимов И.В., Губанов О.М. рассматривают различные составляющие, формирующие профессиональную компетенцию учителя информатики [13], в работе Шастун Т.А. анализируется 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. [15]. В работе Рихтер Т.В. [12], освещаются вопросы использования интерактивных методов обучения при формировании профессиональных компетенций учителей по обеспечению кибербезопасности обучающихся [8].

В научных трудах предлагаются разнообразные вариации повышения методического мастерства учителей информатики, касающиеся обучения школьников, но ни одна работа не раскрывает тематику того, что

именно должен знать сам учитель и чем владеть в области кибербезопасности. Одно дело – рассказывать о потенциальных угрозах кибератак [3; 7], совсем другое – показать на практике, как они реализуются [5], как проявляются [1; 6], и что можно предпринять [4; 17], чтобы не дать возможности нарушителям информационной безопасности реализовать свои планы [9; 16].

Материалы и методы

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 [14], предназначенные для обучения и хранения персональных данных участников образовательного процесса и сотрудников образовательной организации [11]. Школы становятся все более технологичными, что в свою очередь повышает 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 [1; 10], а также организации, 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, касающихся 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 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 компетенций в соответствующих областях.

Результаты

В результате проведения анонимного опроса среди учителей информатики выяснилось, что их компетенции недостаточно, чтобы понимать, 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 только квалифицированные специалисты, обладающие знаниями и умениями по обучению узконаправленных специалистов в области информационной безопасности, и которые могут сформировать профессиональную компетенцию УИ (учителя информатики) в области кибербезопасности. Насколько это актуально, поможет ответить фактография кибератак на образовательные организации.

Анализ кибератак, проведенный компанией Positive Technologies, представленный в отчете за третий квартал 2019 г.[1], 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 данный факт не гарантирует отсутствия атак на их информационную инфраструктуру. Это свидетельствует о том, что на сегодняшний момент совершенствуются не только системы защиты от кибератак [5; 14], но и методы и средства, используемые злоумышленниками, становятся более технологичными.

[1] 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).

Из вышеуказанного отчета по кибератакам на образовательные организации[1] видно, что 93 % всех атак направлены на компьютеры, серверы и сетевое оборудование, 4 % – на 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[2]: персональные данные сотрудников (43 % от общего объема похищенных данных), потеря учетных данных сотрудников (15 %), утрата данных платежных карт сотрудников (14 %), коммерческая тайна (14 %) и другая информация (14 %). Наличие средств защиты информации у образовательных организаций не останавливает киберпреступников, потому что они применяют модифицированные, новые и комбинированные методы атак, одной из которых, к примеру, является APT-атака (advanced persistent threat)[3] – высокотехнологичная сложная целенаправленная атака, направленная на информационные ресурсы организации. Она реализуется таким образом, что остается невидимой для средств защиты.

Обсуждение и выводы

Исходя из вышеперечисленного, можно сделать вывод, что на сегодняшний день современными средствами защиты, которые используется в образовательных организациях, обнаружить и обезвредить высокотехнологичные целенаправленные атаки киберпреступников уже невозможно. Отсутствие в школе специалистов по кибербезопасности, способных противостоять атакам, ставит под угрозу информационную образовательную среду школы. Требуется не только усовершенствование технических средств и систем защиты информации, но и повышение квалификации специалистов в области кибербезопасности, что позволит более эффективно конфигурировать и настраивать средства защиты информации.

---

[1] 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).

[2] Там же.

[3] 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).

Учитывая вышесказанное, учителя информатики, прошедшие курсы повышения квалификации, должны: 1) знать основные методы и инструменты, которые используют киберпреступники для совершения атак, а также методы, которые используются специалистами для обнаружения, нейтрализации и профилактики этих атак; 2) уметь выполнять весь комплекс мероприятий по недопущению проникновения киберпреступников в информационную среду в зоне своей ответственности; 3) владеть навыками по проведению аудита и своевременного обнаружения проникновения злоумышленников в защищаемые информационные системы, а также способами нейтрализации киберпреступников в случае их своевременного обнаружения.

Таким образом, вышеуказанные компетенции необходимо включить в план повышения квалификации учителей информатики в области кибербезопасности.

Список литературы

1. Борисов А.А., Краснов С.А., Нечай А.А. Технология блокчейн и проблемы ее применения в различных информационных системах // Вестник Российского нового ун-та. Серия: Сложные системы: модели, анализ и управление. 2018. № 2. С. 63–67.
2. Горбачев А.В. Модель формирования профессиональных компетенций будущего учителя информатики // Проблемы совр. пед. образования. 2016. № 53-3. С. 146–152.
3. Котиков П.Е., Нечай А.А. Решение проблемы управления параллельным выполнением транзакций в распределенных базах данных для устранения опасной противоречивости // Вестник Российского нового ун-та. Серия: Сложные системы: модели, анализ и управление. 2015. № 2. С. 62–64.
4. Котиков П.Е., Нечай А.А. Репликация данных между серверами баз данных в среде геоинформационных систем // Вестник Российского нового ун-та. 2015. № 9. С. 88–91.
5. Нечай А.А. Формирование безопасной информационной среды // Актуальные проблемы современности: наука и общество. 2019. № 4 (25). С. 43-44.
6. Нечай А.А., Копьев А.И. Метод управляемого распределения ресурсов между ядрами процессора // Вестник Российского нового ун-та. Серия: Сложные системы: модели, анализ и управление. 2018. № 2. С. 101–106.
7. Нечай А.А., Котиков П.Е. Актуальные проблемы защиты информации в современных автоматических телефонных станциях // Вестник Российского нового ун-та. Серия: Сложные системы: модели, анализ и управление. 2015. № 2. С. 65–69.
8. Нечай А.А., Котиков П.Е. Методика комплексной защиты данных, передаваемых и хранимых на различных носителях информации // Вестник Российского нового ун-та. Серия: Сложные системы: модели, анализ и управление. 2015. № 1. С. 92–95.

9. Нечай А.А., Котиков П.Е. Методика повышения надежности функционирования систем, организованных на перепрограммируемых элементах // Вестник Российского нового ун-та. Серия: Сложные системы: модели, анализ и управление. 2016. № 1–2. С. 87–89.

10. 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 ун-та. Серия: Сложные системы: модели, анализ и управление. 2017. № 1. С. 72–79.

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

12. Рихтер Т.В. Использование интерактивных методов обучения при формировании профессиональных компетенций педагогов по обеспечению кибербезопасности подрастающего поколения // Активные и интерактивные методы обучения в естественно-математическом образовании: колл. моногр. Соликамск, 2018. С. 13–21.

13. 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.

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

15. Чусавитин М.О., Чусавитина Г.Н. Модель методики формирования у будущего учителя информатики компетенции в области обеспечения информационной безопасности // Новые информационные технологии в образовании: материалы VII междунар. науч.-практ. конф. Российский гос. проф.-пед. ун-т. 2014. С. 527–531.

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

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

Reference

1. Borisov, A.A., Krasnov, S.A., Nechaj, A.A. (2018) Tekhnologiya blokchejn i problemy ee primeneniya v razlichnykh informacionnykh sistemakh [Blockchain technology and problems of its application in various information systems]. *Vestnik Rossijskogo novogo universiteta. Seriya: Slozhnye sistemy: modeli, analiz i upravlenie – Bulletin of the Russian New University. Series: Complex systems: models, analysis and management.* Vol. 2. pp. 63–67. (In Russian).

2. Gorbachev, A.V. (2016) Model' formirovaniya professional'nykh kompetencij budushchego uchitelya informatiki [Model of formation of professional competencies of future computer science teacher]. *Problemy sovremennogo pedagogicheskogo obrazovaniya – Problems of modern pedagogical education.* Vol. 53-3. pp. 146–152. (In Russian).

3. Kotikov, P.E., Nechaj, A.A. (2015) Reshenie problemy upravleniya parallel'nym vypolneniem tranzakcij v raspredelennykh bazakh dannykh dlya ustraneniya opasnoj protivorechivosti [Address parallel transaction management in distributed databases to resolve dangerous inconsistencies]. *Vestnik Rossijskogo novogo universiteta. Seriya: Slozhnye sistemy: modeli, analiz i upravlenie – Bulletin of the Russian New University. Series: Complex systems: models, analysis and management.* Vol. 2. pp. 62–64. (In Russian).

4. Kotikov, P.E., Nechaj, A.A. (2015) Replikaciya dannykh mezhdu serverami baz dannykh v srede geoinformacionnykh sistem [Replication between database servers in a geographic information system environment]. *Vestnik Rossijskogo novogo universiteta. Seriya: Slozhnye sistemy: modeli, analiz i upravlenie – Bulletin of the Russian New University. Series: Complex systems: models, analysis and management.* Vol. 9. pp. 88–91. (In Russian).

5. Nechaj, A.A. (2019) Formirovanie bezopasnoj informacionnoj sredy [Creating a Secure Information Environment]. *Aktual'nye problemy sovremennosti: nauka i obshchestvo – Current problems of our time: science and society.* Vol. 4. pp. 43–44. (In Russian).

6. Nechaj, A.A., Kop'ev, A.I. (2018) Metod upravlyaemogo raspredeleniya resursov mezhdu yadrami processor [Managed resource allocation method for processor cores]. *Vestnik Rossijskogo novogo universiteta. Seriya: Slozhnye sistemy: modeli, analiz i upravlenie – Bulletin of the Russian New University. Series: Complex systems: models, analysis and management.* Vol. 2. pp. 101–106. (In Russian).

7. Nechaj, A.A., Kotikov, P.E. (2015) Aktual'nye problemy zashchity informacii v sovremennykh avtomaticheskikh telefonnykh stanciyakh [Current issues of information protection in modern automatic telephone exchanges]. *Vestnik Rossijskogo novogo universiteta. Seriya: Slozhnye sistemy: modeli, analiz i upravlenie – Bulletin of the Russian New University. Series: Complex systems: models, analysis and management.* Vol. 2. pp. 65–69. (In Russian).

8. Nechaj, A.A., Kotikov, P.E. (2015) Metodika kompleksnoj zashchity dannykh, peredavaemykh i khranimykh na razlichnykh nositelyakh informacii [Method of integrated protection of data transmitted and stored on various media]. *Vestnik Rossijskogo novogo universiteta. Seriya: Slozhnye sistemy: modeli, analiz i upravlenie – Bulletin of the Russian New University. Series: Complex systems: models, analysis and management.* Vol. 1. pp. 92–95. (In Russian).

9. Nechaj, A.A., Kotikov, P.E. (2016) Metodika povysheniya nadezhnosti funkcionirovaniya sistem, organizovannykh na pereprogrammiruemykh ehlementakh [Procedure for improving the reliability of systems organized on reprogrammed elements]. *Vestnik Rossijskogo novogo universiteta. Seriya: Slozhnye sistemy: modeli, analiz i upravlenie – Bulletin of the Russian New University. Series: Complex systems: models, analysis and management.* Vol. 1-2. pp. 87–89. (In Russian).

10. Novikov, A.N., Nechaj, A.A., Malakhov, A.V. (2017) O podkhode k obosnovaniyu racional'noj nomenklatury ehtalonnoj bazy izmeritel'nykh kompleksov na osnove nechetkikh modelej [On approach to justification of rational nomenclature of reference base of measuring complexes based on fuzzy models]. *Vestnik Rossijskogo novogo universiteta. Seriya: Slozhnye sistemy: modeli, analiz i upravlenie – Bulletin of the Russian New University. Series: Complex systems: models, analysis and management.* Vol. 1. pp. 72–79. (In Russian).

11. Novikov, A.N. Nechaj, A.A., Malakhov, A.V. (2016) Matematicheskaya model' obosnovaniya variantov rekonfiguracii raspredelennoj avtomatizirovannoj kontrol'no-izmeritel'noj sistemy [Mathematical model of substantiation of options for reconfiguration of distributed automated control and measurement system]. *Vestnik Rossijskogo novogo universiteta. Seriya: Slozhnye sistemy: modeli, analiz i upravlenie – Bulletin of the Russian New University. Series: Complex systems: models, analysis and management.* Vol. 1–2. pp. 56–59. (In Russian).

12. Rihter, T.V. (2014) Ispol'zovanie interaktivnykh metodov obucheniya pri formirovanii professional'nykh kompetencij pedagogov po obespecheniyu kiberbezopasnosti podrastayushchego pokoleniya [The use of interactive training methods in the formation of professional competencies of teachers in ensuring cybersecurity of the younger generation]. *V knige: Aktivnye i interaktivnye metody obucheniya v estestvenno-matematicheskom obrazovanii kollektivnaya monografiya. – In the book: Active and interactive methods of learning in natural and mathematical education:* collective monograph. Solikamsk. pp. 13–21. (In Russian).

13. Rodionov, M.A., Akimova, I.V., Gubanova, O.M. (2017) Formirovanie predmetnoj sostavlyayushchej professional'noj kompetencii uchitelya informatiki [Formation of the subject component of the professional competence of the computer science teacher]. *Voprosy sovremennoj nauki i praktiki. Universitet im. V.I. Vernadskogo – Issues of modern science and practice. University ime V.I. Vernadsky.* Vol. 2 (64). pp. 129–139. (In Russian).

14. Svinarchuk, A.A., Nechaj, A.A. (2018) Ispol'zovanie kvantovykh vychislenij pri vybore upravlencheskogo resheniya [Using Quantum Computing to Choose a Management Solution]. *Vestnik Rossijskogo novogo universiteta. Seriya: Slozhnye sistemy: modeli, analiz i upravlenie – Bulletin of the Russian New University. Series: Complex systems: models, analysis and management.* Vol. 2. pp. 31–36. (In Russian).

15. Chusavitin, M.O., Chusavitina, G.N. (2014) *Model' metodiki formirovaniya u budushchego uchitelya informatiki kompetencii v oblasti obespecheniya informacionnoj bezopasnosti* [Model of methodology for formation of competence in the field of information security in future informatics teacher]. *Novye informacionnye tekhnologii v obrazovanii* [New information technologies in education]. Materials of the VII International Scientific and Practical Conference. Russian State Vocational Pedagogical University. pp. 527–531. (In Russian).

16. Shajmardanov, A.M., Nechaj, A.A., Lepekhin, S.V. (2019) Matematicheskaya model' sistem avtomaticheskogo upravleniya s shirotno-impul'snoj modulyaciej [Mathematical model of automatic control systems with pulse width modulation]. *Vestnik Rossijskogo novogo universiteta. Seriya: Slozhnye sistemy: modeli, analiz i upravlenie – Bulletin of the Russian New University. Series: Complex systems: models, analysis and management.* Vol. 2. pp. 27–39. (In Russian).

17. Shirobokov, V.V., Nechaj, A.A. (2017) Algoritm planirovaniya ehnergosberegayushchej parallel'noj obrabotki informacii s uchetom informacionnoj vazhnosti i vremeni postupleniya zadach [Algorithm for planning energy-saving parallel processing of information taking into account information importance and time of tasks arrival]. *Vestnik Rossijskogo novogo universiteta. Seriya: Slozhnye sistemy: modeli, analiz i upravlenie – Bulletin of the Russian New University. Series: Complex systems: models, analysis and management.* Vol. 1. pp. 88–93. (In Russian).

Об авторе

Нечай Александр Анатольевич, преподаватель, Ленинградский государственный университет имени А.С. Пушкина, Санкт-Петербург, Российская Федерация, ORCID ID: 0000-0002-1202-4830, e-mail: webexpromt@mail.ru

About the author

Aleksandr A. Nechai, Cand. Sci. (Ped.), teacher, Pushkin Leningrad State University, Saint Petersburg, Russian Federation, ORCID ID: 0000-0002-1202-4830, e-mail: webexpromt@mail.ru

Поступила в редакцию: 14.10.2020 | Received: 14 October 2020

Принята к публикации: 24.11.2020 | Accepted: 24 November 2020

Опубликована: 28.12.2020 | Published: 28 December 2020