Дата поступления рукописи в редакцию: 23.04.2026 г.
Дата принятия рукописи в печать: 02.06.2026 г.
DOI: 10.24412/2782-3830-2026-5-437-441

ДМИТРИЕВ Григорий Геннадьевич,
доктор педагогических наук, профессор,
ведущий научный сотрудник НИЦ-2 ФКУ
НИИ ФСИН России,
г. Москва, Российская Федерация,
e-mail: vifk-nic@yandex.ru

ОСВОЕНИЕ БЕЗОПАСНОЙ РАБОТЫ В WEB 2.0 КАК НЕОБХОДИМЫЙ КОМПОНЕНТ УЧЕБНЫХ ПРОГРАММ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. *В работе авторы рассматривают Web 2.0 как вероятную угрозу информационной безопасности организации. Авторы отмечают что существующие технические и программные средств контроля не обеспечивают адекватную защиту от этих угроз, что придает большее значение надлежащему охвату таких угроз в ходе учебных программ по Информационной Безопасности и повышению осведомленности сотрудников не только подразделений информационной безопасности, но и обычного персонала организации. Лучшим активом компании в защите конфиденциальных данных являются сотрудники, которые прошли обучение по противодействию рискам, связанным с работой в мире Web 2.0.В статье приводятся практические рекомендации по использовании их в программах обучения.*

Ключевые слова: *Web 2.0, информационная безопасность, учебная программа, обучение сотрудников.*

DMITRIEV Grigoriy Gennadievich,
Doctor of Pedagogical Sciences, Professor,
Leading Researcher NITs-2 PKU Research Institute
of the Federal Penitentiary Service of Russia,
Moscow, Russian Federation

MASTERING SAFE WORK IN WEB 2.0 AS A NECESSARY COMPONENT OF TRAINING PROGRAMS INFORMATION SECURITY

Annotation. *In the work, the authors consider Web 2.0 as a likely threat to the information security of an organization. The authors note that the existing technical and software controls do not provide adequate protection against these threats, which attaches greater importance to the proper coverage of such threats during Information Security training programs and raising awareness among employees not only of information security units, but also of ordinary personnel of the organization. The company's best asset in protecting sensitive data is employees who have been trained on countering risks associated with working in the world of Web 2.0. The article provides practical recommendations for using them in training programs.*

Key words: *Web 2.0, information security, curriculum, employee training.*

Специалисты по обеспечению конфиденциальности и безопасности пришли к выводу, что технологии, которые сегодня работают для защиты компании, могут перестать быть эффективными завтра. Постоянно меняющиеся меры безопасности обусловлены не только внедрением новых технологий, но и быстрыми темпами адаптации и инноваций, которые демонстрируют злоумышленники. Злоумышленники используют новые уязвимости почти сразу же, как только исправляются существующие или возникают новые, создавая постоянную игру в догонялки между специалистами по безопасности и злоумышленниками. Хуже всего то, что за последние несколько лет появились различные сообщения о растущем подпольном рынке украденных электронных данных. Этот подпольный рынок достиг такого уровня, что хакеры могут зарабатывать большие деньги, используя небольшой набор специальных навыков таких как взлом почтового аккаунта, файрвола или браузера, а также взлом различных платных программных

продуктов, стоимость которых для корпоративных нужд составляет сотни тысяч долларов. При этом рынок хакеров не регулируется власти ни одного государства, что стирает границы для киберпреступности и значительно увеличивает ассортиментпредлогаемых услуг. Используя просторы интернета организованные преступные группы совершают нападения и организованные компании не зависимо от места расположения жертвы угрозы вовлекая в театр кибератаки участников из различных стран. Таким образом растущий спрос на персональные и конфиденциальные данные подогревает растущий криминальный бум хакерской активности.

Неспособность существующих технических средств контроля обеспечить адекватную защиту от этих угроз придает большее значение надлежащему охвату таких угроз в ходе учебных программ по Информационной Безопасности и повышению осведомленности сотрудников не только подразделений информационной безопасности, но и обычного персонала.

Для сохранения эффективности программы обучения Информационной безопасности должны периодически пересматриваться, чтобы отражать политические реалии и существующую практику компаний, а также постоянно меняющуюся природу угроз и современного уровня программных и аппаратных средств. За последние десятилетия усовершенствования защиты сетей и защиты операционных систем привели к тому, что злоумышленники изменили свои стратегии атак на использование программных приложений (таких как браузеры, текстовые процессоры и цифровые форматы, такие как PDF) и социальных сетей, часто объединяя эти атаки в смешанном режиме.

Поскольку компании используют преимущества Web 2.0, т.е. интернет-приложения, программное обеспечение как услуги и облачные вычисления - у злоумышленников появляются новые возможности для получения, изменения или уничтожения данных компании. Существующие технологические средства контроля пока не доказали свою эффективность в противодействии этим новым и быстро развивающимся угрозам. Существующие политики должны быть обновлены (или созданы заново), а методы должны быть скорректированы, чтобы обеспечить постоянную безопасность и конфиденциальность персональных и коммерческих данных. На сегодняшний день лучшим активом компании в защите конфиденциальных данных являются сотрудники, которые прошли обучение по противодействию рискам, связанным с работой в мире Web 2.0.

Опытные пользователи информационных ресурсов часто хорошо разбираются в таких терминах, как брандмауэр и антивирус, они часто убеждены в том, что эти технологии обеспечивают практически непробиваемую защиту от всех потенциальных рисков атак. Однако после инцидента эти пользователи уверяют, что они были «в полной безопасности» при посещении Интернета, поскольку они были защищены популярной антивирусной программой. Имеющиеся в открытом доступе статистические обзоры киберпреступности по развитым странам, касающиеся безопасности в Интернете и утечки данных в 2018 и 2019 годах, показали, что хакеры используют вредоносное программное обеспечение (ПО) для обхода средств защиты, заражения компьютеров и установления долгосрочного контроля или наблюдения за пользовательской активностью и / или сетевым трафиком, несмотря на распространенные бытовые версии антивирусных программ. Из-за деликатного характера темы, немногие компании готовы поделиться уроками, извлеченными из расследования взлома данных.

Большинство взломанных записей осуществляется с использованием хакерских программ и вредоносных программ. При этом большинство атак являются простыми, только каждая десятая атака использует «сложные» методы. Эти атаки приносят наибольший вред порядка 90% потерянных данных, для их реализации злоумышленник использует специальные вредоносные программа которые крайне сложно обнаружить и удалить с помощью современных средств контроля безопасности.

Сотрудники должны знать, что текущее состояние технологий безопасности не может обеспечить полной защиты от современных атак, особенно от целевых атак. Причина этого (обычно временного) пробела в защите проста: антивирусные компании должны наблюдать и собирать образцы вредоносного программного обеспечения в естественных условиях, прежде чем они смогут обновить свои программы для правильного обнаружения и / или удаления вредоносного программного обеспечения. И все же процесс не идеален. Антивирусные программы всегда отстают от потенциальной угрозы. Используя аналогию текущего момента в мире, очевидно, что сначала население заболевает вирусом и спустя некоторое время разрабатывается вакцина. Противостоять такой ситуации возможно с использованием эвристического подхода к анализу программного обеспечения с целью обнаружения вредоносного кода. Но наиболее эффективным способом является своевременное обу-

чение сотрудников и актуализация программы повышения квалификации по информационной безопасности.

Не менее опасными являются смешанные угрозы, атаки, использующие несколько вредоносных методов для достижения максимального вреда и быстрого заражения. По мере того, как корпорации экспериментируют с перемещением данных в облако или выходом в социальные сети, чтобы задействовать расширенную базу пользователей, пользователи обнаруживают, что взаимодействуют с новыми средами. Тем не менее, пользователи часто не знают о дополнительных векторах угроз, связанных с этими средами. Когда пользователи покидают хорошо охраняемые границы внутренней сети компании для доступа к службам Web 2.0, они часто делают это с помощью программных приложений, которые до сих пор оказывались весьма уязвимыми. Интернет-браузеры, которые обычно являются средством выбора для доступа к службам Web 2.0, легко подвергаются риску и часто используются на ранних стадиях атаки. Основной вектор доступа к сервисам Web 2.0 является не надежным с точки зрения безопасности. Наиболее распространенным методом доставки вредоносного ПО является сценарий, при котором злоумышленник скомпрометировал систему, а затем установил на нее вредоносное ПО. В то время как некоторые атаки требуют действий пользователя, таких как загрузка, установка или щелчок по пиктограмме, существует класс атак, называемых «атаками с диска», которые заражают компьютер без какого-либо вмешательства пользователя, кроме посещения зараженного сайта. Такие атаки входят в тройку наиболее распространенных в Web 2.0.

Чтобы минимизировать вероятность и потенциальный ущерб от современных вредоносных программ и смешанных угроз, отделы ИТ и безопасности могут применять технологические средства управления, такие как:

- Периодически проверять права доступа пользователей и удалять ненужные.
- Периодически просматривать журналы доступа на наличие признаков использования общих учетных данных.
- Предоставлять пользователям «усиленные» браузеры (или приложения Web 2.0).
- Предоставлять пользователям «изолированную» рабочую среду.
- Убедитесь, что процесс исправления распространяется как на операционные системы, так и на установленные приложения.
- Обеспечьте защиту пользователям дома и в дороге.

В то время как корпоративные пользователи обычно защищены несколькими уровнями технологий безопасности, пользователи дома или в дороге часто более уязвимы. Таким образом описанный выше материал целесообразно включать в эффективную программу обучения сотрудников по направлению Информационная безопасность.

Список литературы:

[1] Вилкова, А. В. Проблемы непрерывного обучения персонала информационной безопасности / А. В. Вилкова,В. М. Литвишков, Б. А. Швырев // Мир науки, культуры, образования. – 2019. – № 4 (77). – С. 29–31.

[2] James Governor, Dion Hinchcliffe, Duane Nickull. Web 2.0 Architectures: What Entrepreneurs and Information Architects Need to Know. — O'Reilly, 2009. — 276 p. — ISBN 978-0596514433.

[3] Amy Shuen. Web 2.0: A Strategy Guide. — O'Reilly, 2008. — 272 p. — ISBN 978-0-596-52996-3.

[4] Bernd W. Wirtz et al. Strategic Development of Business Models (англ.) // Long Range Planning. — 2010. — Vol. 43, no. 2-3. — P. 272-290. — ISSN 0024-6301. — doi:10.1016/j.lrp.2010.01.005. Архивировано 5 ноября 2012 года.

[5] Jones, B. Web 2.0 Heroes: Interviews with 20 Web 2.0 Influencers. — Wiley, 2008. — 273 p. — ISBN 9780470241998.

[6] Skudalova, O. V. Personal factor of a social entrepreneur in the context of the inclusive economy development /O. V. Skudalova et al. // International Journal of Innovative Technology and Exploring Engineering. – 2019. – Vol. 8, no. 8.– Pp. 2996–3002.

[7] Pedley, D. Understanding the UK cyber security skills labour market / D. Pedley, D. McHenry, H. Motha, J. Shah.– URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/767422/Understanding_the_UK_cyber_security_skills_labour_market.pdf.

[8] Policy paper «Initial National Cyber Security Skills Strategy: increasing the UK's cyber security capability – a callfor views, Executive Summary. – URL: https://www.gov.uk/government/publications/cyber-security-skills-strategy/initial-national-cyber-security-skills-strategy-increasing-the-uks-cyber-security-capability-a-call-for-views-executive-summary.

[9] Вилкова А. В., Тищенко Ю. Ю. Социально-педагогическая запущенность и делинквентность несовершеннолетних // В сборнике: Уголовно-исполнительная система: история и современность. Сборник материалов Межвузовской научно-практической конференции с международным участием. Псков. 2025. С. 65-68.

[10] Мудрецы России под ред. Сапунов В. Б., Ермилова М. В., Колесов В. И. (2-е издание). Санкт-Петербург, 2023.

[11] Траектория развития субъектов образовательного процесса. Материалы II Международной научно-практической конференции. Воронеж. 2024.

[12] Научные труды ФКУ НИИ ФСИН России. Научно-практическое ежеквартальное издание / Том Выпуск 4. Москва. 2021.

[13] Научные труды ФКУ НИИ ФСИН России. Научно-практическое ежеквартальное издание / Том Выпуск 1. Москва. 2022.

[14] Научные труды ФКУ НИИ ФСИН России. Научно-практическое ежеквартальное издание / Том Выпуск 2. Москва. 2022.

[15] Научные труды ФКУ НИИ ФСИН России. Научно-практическое ежеквартальное издание / Том Выпуск 3. Москва. 2022.

[16] Вилкова А. В., Лукашенко Д. В. Самооценка личности несовершеннолетних осужденных / В сборнике: Уголовно-исполнительная система: законодательство, теория и практтика. Материалы Всероссийской научно-практической конференции с международным участием, посвященной памяти российского ученого-пенитенциариста заслуженного юриста Российской Федерации доктора юридических наук, профессора О. В. Филимонова. В 2-х частях. Самара, 2025. С. 87-93. Сборник статей круглого стола. Тверь, 2025. С. 87-93.

[17] Вилкова А. В., Полякова Я. Н. Подготовка кадров высшей категории в уголовно-исполнительной системе/ Антропогогика. 2025. № 3(19). С. 8-16.

[18] Фадеева С. А., Вилкова А. В. Уголовно-исполнительная система и пенитенциарная пробация: профессиональная готовность // В сборнике: Научные труды ФКУ НИИ ФСИН России. Научно-практическое ежеквартальное издание. Москва, 2025. С. 147-154.

[19] Вилкова А. В., Полякова Я. Н. Трудности подготовки научно-педагогических кадров высшей категории в уголовно-исполнительной системе // в сборнике: XI педагогические чтения, посвященные памяти профессора С. И. Злобина. Сборник материалов. Пермь. 2025. С. 14-22.

[20] Мешкова Л. В., Вилкова А. В. К вопросу о развитии социальной активности будущих сотрудников ФСИН в процессе социально-психологического тренинга // Военно-правовые и гуманитарные науки Сибири. 2025. № 3(25). С. 212-218.

[21] Вилкова А. В., Ковтуненко Л. В., Лукашенко Д. В. Программа подготовки педагогических кадров: структурно-содержательная модель обучения взрослых / Проблемы современного педагогического образования. 2025. № 89-2. С. 68-71.

[22] Лукашенко Д. В. Содержание и структура плана внеурочной деятельности для воспитанников воспитательных колоний / А. В. Вилкова, Д. В. Лукашенко // Антропогогика. 2024. № 3(15). С.5-16.

References:

[1] Vilkova, A. V. Problems of continuous training of information security personnel/A. V. Vilkova, V. M. Litvishkov, B. A. Shvyrev//World of Science, Culture, Education. – 2019. – № 4 (77). - S. 29-31.

[2] James Governor, Dion Hinchcliffe, Duane Nickull. Web 2.0 Architectures: What Entrepreneurs and Information Architects Need to Know. — O'Reilly, 2009. — 276 p. — ISBN 978-0596514433.

[3] Amy Shuen. Web 2.0: A Strategy Guide. — O'Reilly, 2008. — 272 p. — ISBN 978-0-596-52996-3.

[4] Bernd W. Wirtz et al. Strategic Development of Business Models (англ.) // Long Range Planning. — 2010. — Vol. 43, no. 2-3. — P. 272-290. — ISSN 0024-6301. — doi:10.1016/j.lrp.2010.01.005. Archived 5 November 2012 at the Wayback Machine.

[5] Jones, B. Web 2.0 Heroes: Interviews with 20 Web 2.0 Influencers. — Wiley, 2008. — 273 p. — ISBN 9780470241998.

[6] Skudalova, O. V. Personal factor of a social entrepreneur in the context of the inclusive economy development /O. V. Skudalova et al. // International Journal of Innovative Technology and Exploring Engineering. – 2019. – Vol. 8, no. 8.– Pp. 2996–3002.

[7] Pedley, D. Understanding the UK cyber security skills labour market / D. Pedley, D. McHenry, H. Motha, J. Shah.– URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/767422/Understanding_the_UK_cyber_security_skills_labour_market.pdf.

[8] Policy paper «Initial National Cyber Security Skills Strategy: increasing the UK's cyber security capability – a callfor views, Executive Summary. – URL: https://www.gov.uk/government/publications/cyber-security-skills-strategy/initial-national-cyber-security-skills-strategy-increasing-the-uks-cyber-security-capability-a-call-for-views-executivesummary.

[9] Vilkova A. V., Tishchenko Yu. Yu. Socio-pedagogical neglect and delinquency of minors//In the collection: The penal system: history and modernity. Collection of materials of the Interuniversity Scientific and Practical Conference with international participation. Pskov. 2025. S. 65-68.

[10] Sages of Russia ed. Sapunov V. B., Ermilova M. V., Kolesov V. I. (2nd edition). St. Petersburg, 2023.

[11] Trajectory of educational process subjects. Materials of the II International Scientific and Practical Conference. Voronezh. 2024.

[12] Scientific works of the PKU Research Institute of the Federal Penitentiary Service of Russia. Scientific and practical quarterly publication/Volume Issue 4. Moscow. 2021.

[13] Scientific works of the PKU Research Institute of the Federal Penitentiary Service of Russia. Scientific and practical quarterly publication/Volume Issue 1. Moscow. 2022.

[14] Scientific works of the PKU Research Institute of the Federal Penitentiary Service of Russia. Scientific and practical quarterly publication/Volume Issue 2. Moscow. 2022.

[15] Scientific works of the PKU Research Institute of the Federal Penitentiary Service of Russia. Scientific and practical quarterly publication/Volume Issue 3. Moscow. 2022.

[16] Vilkova A. V., Lukashenko D. V. Self-assessment of the personality of juvenile convicts/In the collection: The penal system: legislation, theory and practice. Materials of the All-Russian Scientific and Practical Conference with international participation, dedicated to the memory of the Russian scientist-penitentiary Honored Lawyer of the Russian Federation, Doctor of Law, Professor O. V. Filimonov. In 2 parts. Samara, 2025. S. 87-93. Collection of roundtable articles. Tver, 2025. S. 87-93.

[17] Vilkova A.V., Polyakova Y. N. Training of the highest category in the penal system/Anthropology. 2025. № 3(19). S. 8-16.

[18] Fadeeva S. A., Vilkova A. V. Criminal executive system and penitentiary probation: professional readiness//In the collection: Scientific works of the PKU Research Institute of the Federal Penitentiary Service of Russia. Scientific and practical quarterly publication. Moscow, 2025. S. 147-154.

[19] Vilkova A.V., Polyakova Y. N. Difficulties in training scientific and pedagogical personnel of the highest category in the penal system//in the collection: XI pedagogical readings dedicated to the memory of Professor S. I. Zlobin. Collection of materials. Perm. 2025. S. 14-22.

[20] Meshkova L.V., Vilkova A.V. On the development of social activity of future employees of the Federal Penitentiary Service in the process of social and psychological training//Military legal and humanitarian sciences of Siberia. 2025. № 3(25). S. 212-218.

[21] Vilkova A. V., Kovtunenko L. V., Lukashenko D. V. Teacher training program: structural-content model of adult education/Problems of modern pedagogical education. 2025. № 89-2. S. 68-71.

[22] Lukashenko D.V. Content and structure of the plan of extracurricular activities for pupils of educational colonies/A.V. Vilkov, D.V. Lukashenko// Anthropology. 2024. № 3(15). S.5-16.