- ОБРАЗОВАНИЕ В РОССИИ И МИРЕ -

Дата поступления рукописи в редакцию: 19.04.2026 г. DOI: 10.24412/2782-3830-2026-5-491-495
Дата принятия рукописи в печать: 02.06.2026 г.

ФИАЛКОВСКАЯ Екатерина Владимировна,
старший научный сотрудник ФКУ НИИ ФСИН России,
г. Москва, Российская Федерация;
кандидат педагогических наук,
e-mail: 19katrin81@bk.ru

РАЗРАБОТКА УЧЕБНОЙ ПРОГРАММЫ ПО ВЫЯВЛЕНИЮ И ПРОТИВОДЕЙСТВИЮ КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ ДЛЯ КУРСОВ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

Аннотация. *В работе авторы рассматривают образовательный процесс на курсах повышения квалификации по направлению информационная безопасность. Определены особенности разрабатываемой программы. Авторы определили исходя из актуальных угроз тематику занятий, порядок и последовательность их проведения. В статье приводится краткое описание каждого тематического образовательного периода. Выделена целевая аудитория и определены целевые умения, на формирование которых направлено обучение. Авторы уделяют большое внимание практическим занятием при освоении курса.*

Ключевые слова: *информационная безопасность, учебная программа, обучение сотрудников, угрозы, инцидент.*

FIALKOVSKAYA Ekaterina Vladimirovna,
leading researcher, Federal State Institution
Research Institute of the Federal
Penitentiary Service of Russia,
Moscow, Russian Federation;
Candidate of Pedagogical Sciences

DEVELOPMENT OF A TRAINING PROGRAM TO IDENTIFY AND COUNTERING COMPUTER INCIDENTS FOR REFRESHER COURSES

Annotation. *In the work, the authors consider the educational process in continuing education courses in the field of information security. The features of the developed program are determined. The authors determined the topic of classes, the order and sequence of their conduct based on current threats. The article provides a brief description of each thematic educational period. The target audience has been identified and the target skills for the formation of which the training is aimed are determined. The authors pay great attention to the practical lesson in mastering the course.*

Key words: *information security, curriculum, employee training, threats, incident.*

Разработка учебной программы по информационной безопасности для курсов повышения квалификации требует глубокого знания предметной области и современного её состояния, а также знать, уметь и владеть педагогическими приемами и методами, направленными на эффективное обучение за ограниченное время. Отличительной особенностью всех курсов повышения квалификации от классического обучения по программам высшей школы является ограниченный промежуток времени в который необходимо уложить актуальные очищенные от лишней академичности знания, при этом не скатываясь к сухому изложению информации и развитию навыков без осознания материала, а наоборот формируя опережающее эвристическое понимание проблем информационной безопасности.

Рассмотрим программу повышения квалификации по направлению Информационная безопасность с названием «Выявление и противодействие компьютерным инцидентам». Данное направление нацелено на системных администраторов, администраторов безопасности, сотрудников занимающихся обработкой инцидентов и других сотрудников ИТ отделов, занимающихся защитой информации, реагированием на атаки и угрозы.

Интернет полон мощных хакерских утилит, и злоумышленники широко их используют. Если в организации есть подключение к Интернету и один или два недовольных сотрудника, то информационная система гарантированно будет атакована. Начиная с единичных проверок интернет-инфраструктуры организации до сотен в день и злонамеренного инсайдера, злоумышленники медленно и скрытно проникают в самые важные информационные ресурсы, минуя системы защиты и обнаружения. Для противодействия этим вторжениям обучающиеся должны понимать инструменты и методы взлома компьютерных сетей. Они должны детально понимать тактику и стратегию злоумышленников, и для этого недостаточно теоретических занятий необходим практический опыт поиска уязвимостей и обнаружения вторжений, а также осознание комплексного плана обработки инцидентов. В нем рассматриваются последние передовые коварные векторы атак, классические атаки, которые все еще распространены, и достаточно часто встречаются. Эффективность обучения по данному направлению как ни с каким другим тесно переплетается с практическими занятиями. «Теория, мой друг, суха, / Но зеленеет жизни древо» (Из трагедии «Фауст» (ч. I, сцена IV) Иоганна Вольфганга Гете (1749-1832), перевод Бориса Пастернака). Вместо того, чтобы просто учить нескольким приемам хакерской атаки, эффективен пошаговый процесс реагирования на компьютерные инциденты и подробное описание того, как злоумышленники взламывают системы, чтобы системный администратор мог подготовиться, обнаружить и противостоять атакам. Отдельным направлением является рассмотрение правовых вопросов, связанных с реагированием на компьютерные атаки, включая мониторинг сотрудников, взаимодействие с правоохранительными органами и сбор и сохранение доказательств. Апогеем обучения по этой программе будет наличие знаний и умений, позволяющих обнаружить брешь в системе информационной безопасности организации раньше злоумышленников и устранить их.

Примерная программа может иметь вид.

ДЕНЬ 1: Пошаговое расследование инцидентов и расследование компьютерных преступлений

В этом разделе рассматривается пошаговая модель обработки инцидентов, которая была отработана на практике с участием опытных специалистов по обработке инцидентов и доказала свою эффективность в сотнях организаций. Этот раздел предназначен для того, чтобы предоставить обучающимся полное погружение в процесс обработки инцидентов, используя шесть этапов (подготовка, идентификация, локализация, уничтожение, восстановление и извлеченные опыта), необходимых для подготовки к компьютерному инциденту и борьбы с ним. Во второй части этого раздела рассматриваются практические примеры из практики. В этом разделе представлена информация о шагах, которые может предпринять системный администратор для повышения шансов на поимку и преследование злоумышленников.

ДЕНЬ 2: Компьютерные и сетевые хакерские атаки (часть 1).

На первый взгляд безобидная утечка данных из сети организации может дать ключ, необходимый злоумышленнику для взлома системы. Этот однодневный курс охватывает первые две фазы многих компьютерных атак связанные с разведкой и сканированием.

ДЕНЬ 3: Компьютерные и сетевые хакерские атаки (часть 2).

Компьютерные злоумышленники постоянно совершенствуют свои методыи по-новому атакуют сети и системы. Этот день посвящен третьей фазе многих хакерских атак - получение доступа. Злоумышленники используют различные стратегии для перехода систем от уровня сети до уровня приложения. В этом разделе подробно рассматривают атаки, от переполнения буфера и методов форматной строковой атаки до перехвата сеансов предположительно безопасных протоколов.

ДЕНЬ 4: Компьютерные и сетевые хакерские атаки (часть 3).

Этот учебный день начинается с изучения одной из любимых техник злоумышленников для взлома систем: червей. Рассматривается эволюция червей за последние два года и экстраполяция этого процесса в будущее для анализа грядущих суперчервей, с которыми в будущем можно столкнуться. Обучение плавно переходит к веб-приложениям, часто используемым злоумышленниками. Поскольку самодельные веб-приложения большинства организаций используют открытое программное обеспечение, злоумышленники внедряют SQL запросы, осуществляют межсайтовый скриптинг, клонируют сеансы и множество других механизмов.

ДЕНЬ 5: Компьютерные и сетевые хакерские атаки (Часть 4).

Этот день обучения охватывает четвертый и пятый этапы многих хакерских атак: поддержание доступа и отслеживание следов. Компьютерные злоумышленники устанавливают черные ходы, применяют руткиты, а иногда даже манипулируют самим ядром системы, чтобы скрыть свои преступные следы. Каждая из этих категорий инструментов требует специальной защиты для базовой системы. В этот день рассматриваются наиболее часто используемые образцы вредоносного кода, а также обсуждаются будущие тенденции развития вредоносных программ, в том числе возможности вредоносного ПО на уровне BIOS и комбинированные вредоносные программы.

ДЕНЬ 6: Мастерская хакерских инструментов.

За прошедшие годы индустрия безопасности стала умнее и эффективнее противостоять хакерам. К сожалению, хакерские инструменты становятся умнее и сложнее. Один из наиболее эффективных способов остановить врага - это на самом деле проверить окружение с помощью тех же инструментов и тактик, которые атакующий может использовать против вас. Этот семинар позволит обучающимся применить на практике то, чему они научились за пройденный курс.

По окончанию обучения слушатели должны уметь:

– Для защиты корпоративной среды применять углубленные процессы обработки инцидентов, включая подготовку, идентификацию, локализацию, ликвидацию и восстановление.
– Проанализировать структуру общих методов атак, чтобы оценить распространение атакующего по системе и сети, предвидя и предотвращая дальнейшую активность атакующего.
– Использовать инструменты и доказательства для определения типа вредоносных программ, используемых в атаке, включая руткиты, трояны и бэкдоры, выбирая соответствующие средства защиты и тактику реагирования для каждого из них.
– Использовать встроенные средства командной строки, такие как Windows tasklist, wmic и reg, а также Linux netstat, ps и lsof, чтобы обнаружить присутствие злоумышленника на компьютере.
– Анализировать таблицы ARP маршрутизатора и системы вместе с таблицами CAM коммутатора для отслеживания активности злоумышленника по сети и идентификации подозреваемого.
– Использовать дампы памяти и инструмент Volatility для определения действий злоумышленника на компьютере, установленного вредоносного ПО и других вычислительных машин, которые злоумышленник использовал в качестве опорных точек в сети.
– Получать доступ к целевой машине с помощью Metasploit, а затем обнаруживать артефакты и последствия эксплуатации с помощью анализа процессов, файлов, памяти и журналов.
– Проанализировать систему, чтобы увидеть, как злоумышленники используют инструмент Netcat для перемещения файлов, создания бэкдоров и создания ретрансляторов в целевой среде.
– Запустить сканер портов Nmap и сканер уязвимостей Nessus, чтобы найти дыры в целевых системах, и применить такие инструменты, как tcpdump и netstat, для обнаружения и анализа последствий сканирования.

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. Преодоление отклоняющегося поведения несовершеннолетних осужденных / В сборнике: Духовно-нравственное воспитание личности в пенитенциарной системе: педагогические и социально-психологические аспекты. Сборник научных статей по материалам Всероссийского научно-практического круглого стола, посвященного памяти ученых-пенитенциаристов: доктора педагогических наук, профессора В. М. Литвишкова и доктора психологических наук, профессора Сочивко Д. В., Рязань, 2026. С. 23-29.

[10] Вилкова А. В., Антипов А. Н., Строгович Ю. Н. О средствах исправления осужденных в современных реалиях // Уголовно-исполнительная система: право, экономика, управление. 2026. № 1. С. 22-26.

[11] Вилкова А. В., Фиалковская Е. В., Полякова Я. Н. Подходы к изучению агрессивности в рамках пенитенциарной психологии / Образование и право. 2026. № 1. С. 214-218.

[12] Вилкова А. В., Фадеева С. А. О профессиональной готовности специалистов уголовно-исполнительной системы Российской Федерации к осуществлению пенитенциарной пробации // Ведомости уголовно-исполнительной системы. 2026. № 3 (286). С, 45-51.

[13] Вилкова А. В., Тищенко Ю. Ю. Особенности реализации дисциплинарной практики в отношении несовершеннолетних в следственных изоляторах / Международный научный вестник. 2026. № 1. С. 81-84.

[14] Вилкова А. В., Полякова Я. Н. Роль научного коллектива как субъекта профессионального становления молодого ученого / В сборнике: Уголовно-исполнительная система сегодня: взаимодействие науки и практики. Материалы XXV Всероссийской научно-практической конференции. Новокузнецк, 2025. С. 253-256.

[15] Вилкова А. В., Полякова Я. Н. Научно-педагогические кадры и их подготовка в адъюнктуре образовательных организаций ФСИН России // Вопросы современной науки и практики. 2025. № 2(13). С. 47-54.

[16] Вилкова А. В., Лукашенко Д. В. Теории и концепции о происхождении обучения и воспитания / Международный научный вестник.2025. № 10. С. 374-379.

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. Overcoming the deviating behavior of juvenile convicts/In the collection: Spiritual and moral education of a person in the penitentiary system: pedagogical and socio-psychological aspects. Collection of scientific articles based on the materials of the All-Russian Scientific and Practical Round Table dedicated to the memory of penitentiary scientists: Doctor of Pedagogical Sciences, Professor V. M. Litvishkov and Doctor of Psychological Sciences, Professor D. Sochivko, Ryazan, 2026. S. 23-29.

[10] Vilkova A.V., Antipov A.N., Strogovich Yu.N. On the means of correcting convicts in modern realities//Penal system: law, economics, management. 2026. № 1. S. 22-26.

[11] Vilkova A. V., Fialkovskaya E. V., Polyakova Y. N. Approaches to the study of aggressiveness in the framework of penitentiary psychology/Education and law. 2026. № 1. S. 214-218.

[12] Vilkova A. V., Fadeeva S. A. On the professional readiness of specialists of the penitentiary system of the Russian Federation to carry out penitentiary probation//Vedomosti of the penitentiary system. 2026. № 3 (286). S, 45-51.

[13] Vilkova A. V., Tishchenko Yu. Yu. Peculiarities of the implementation of disciplinary practice against minors in pre-trial detention centers/International Scientific Bulletin. 2026. № 1. S. 81-84.

[14] Vilkova A.V., Polyakova Y. N. The role of the scientific team as a subject of professional development of a young scientist/In the collection: The penal system today: the interaction of science and practice. Materials of the XXV All-Russian Scientific and Practical Conference. Novokuznetsk, 2025. S. 253-256.

[15] Vilkova A.V., Polyakova Y. N. Scientific and pedagogical personnel and their training in the adjunct of educational organizations of the Federal Penitentiary Service of Russia//Issues of modern science and practice. 2025. № 2(13). S. 47-54.

[16] Vilkova A.V., Lukashenko D.V. Theories and concepts about the origin of education and upbringing/International Scientific Bulletin .2025. № 10. S. 374-379.