

## ПЕДАГОГИЧЕСКИЙ ПРОЦЕСС ФОРМИРОВАНИЯ КУЛЬТУРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ФСИН РОССИИ

Борис Анатольевич Швырев<sup>1</sup>, Янина Николаевна Полякова<sup>2</sup>

<sup>1</sup> Московский университет МВД России имени В. Я. Кикотя, Москва, Россия

<sup>1</sup> Московский государственный лингвистический университет, Москва, Россия

<sup>2</sup> Научно-исследовательский институт ФСИН России, Москва, Россия

<sup>1</sup> i@bor2275.ru, <sup>2</sup> nii@fsin.su

**Аннотация.** Понятие культуры информационной безопасности (далее – ИБ) достаточно многогранное. Очевидные аспекты, влияющие на формирование культуры ИБ, – это информационные технологии, и они широко обсуждаются в литературе наравне с психологическими и культурологическими аспектами. Информационная безопасность по своей природе имеет ряд проблем: технических, связанных с непрерывным развитием аппаратно-программных вычислительных систем и пропорциональным увеличением их уязвимостей; правовых, обусловленных неустранимым отставанием нормативного правового регулирования и противодействия от возникающих угроз; персонала, получающего возрастающую осведомленность без осознанных норм поведения и принятия решений, связанных с обеспечением безопасности. Культура информационной безопасности не может сформироваться на пустом месте, для этого необходимо обучение персонала в области информационной безопасности, в связи с чем целесообразно иметь эффективное методическое обеспечение. В работе выделяются три элемента, составляющие и формирующие культуру ИБ: технологии, политики/правила и люди/компетентность. Проводится обсуждение рассматриваемых элементов и выделяется их значимость. Особое внимание отводится понятию осознания информационной безопасности. В работе рассматриваются этапы когнитивного процесса обучения культуре ИБ.

**Ключевые слова:** культура информационной безопасности, обучение, осознанность, развитие компетенции в области информационной безопасности.

**Для цитирования:** Швырев Б. А., Полякова Я. Н. Педагогический процесс формирования культуры информационной безопасности в ФСИН России // Вестник Уфимского юридического института МВД России. 2024. № 2 (104). С. 174–181.

Original article

## THE PEDAGOGICAL PROCESS OF FORMING AN INFORMATION SECURITY CULTURE IN THE FEDERAL PENITENTIARY SERVICE OF RUSSIA

Boris A. Shvyrev<sup>1</sup>, Yanina N. Polyakova<sup>2</sup>

<sup>1</sup> V. Ya. Kikot Moscow University of the Ministry of Internal Affairs of Russia, Moscow, Russia

<sup>1</sup> Moscow State Linguistic University, Moscow, Russia

<sup>2</sup> Scientific Research Institute of the Federal Penitentiary Service of Russia, Moscow, Russia

<sup>1</sup> i@bor2275.ru, <sup>2</sup> nii@fsin.su

**Abstract.** The concept of information security culture is quite multifaceted. The obvious aspects influencing the formation of the culture of information security are information technologies, and they are widely discussed in the literature along with psychological and cultural aspects. Information security by its nature has a number of problems: technical, related to the continuous development of hardware and software computing systems and a proportional increase in their vulnerabilities; legal, due to the unavoidable backlog of legal regulation and countering emerging threats; personnel receiving increasing awareness without conscious norms of

behavior and decision-making related to security. The culture of information security cannot be formed from scratch, for its formation it is necessary to train personnel in the field of information security, and for this it is advisable to have effective methodological support. The paper identifies three elements that make up and form the culture of information security: technologies, policies/rules and people/competence. The elements under consideration are discussed and their significance is highlighted. Special attention is paid to the concept of awareness of information security. The paper considers the stages of the cognitive process of teaching the culture of information security.

**Keywords:** information security culture, training, awareness, competence development in the field of information security.

**For citation:** Shvyrev B. A., Polyakova Y. N. The pedagogical process of forming an information security culture in the Federal penitentiary service of Russia // Bulletin of Ufa Law Institute of the Ministry of Internal Affairs of Russia. 2024. No. 2 (104). P. 174–181. (In Russ.)

## Введение

Понятие культуры ИБ достаточно многогранное. Известно много работ, посвященных формулированию определения культуры ИБ (Л. В. Астахова [1; 2], В. П. Поляков [3]). Культурологический подход к формированию культуры информационной безопасности у студентов педагогического вуза рассматривается Н. Н. Кузиной [4]. В структуре культуры ИБ автор выделяет аксиологический, технологический и личностно-творческий компонент и проводит культурологическое исследование аксиологического подхода. Рефлексивный подход к освоению культуры безопасности у студентов рассматривается М. В. Погодаевой и Т. Ф. Ушевой [5]. Рефлексия очень важна для саморазвивающейся личности и развития самообучения ИБ. В работе Н. Н. Кузиной [6] заявительно приводятся другие три аспекта формирования культуры ИБ студентов педагогических вузов: технический, гуманитарно-рефлексивный и гуманитарно-педагогический. Однако их всесторонний анализ не приводится. Следующие работы (Ю. С. Ерина и И. Ю. Кокаева [7]) направлены на изучение формирования культуры ИБ у студентов педагогических учебных заведений. В них проводится анализ программ обучения студентов и выделяется важность технических компонентов обеспечения информационной безопасности на протяжении всего обучения. Вопросы формирования культуры ИБ общества рассматривает А. А. Малюк. Автор выделяет важность «использования возможностей всех звеньев системы непрерывного образования, целенаправленной деятельности государ-

ственных органов, больших усилий в сфере законодательства и нормативного регулирования» [8]. Духовные аспекты формирования культуры ИБ рассматриваются О. К. Валитовым [9]. Очевидным аспектом, влияющим на формирование культуры ИБ, являются информационные технологии, достаточно широко представленные в научной литературе (Н. С. Шумилова [10], М. Ф. Алиева [11], А. С. Селиверстов [12]). Рассмотренные публикации составляют лишь часть работ, посвященных анализу и исследованиям понятия, аспектам, образующим понятие культуры ИБ. В приведенных работах анализируются либо отдельные компоненты культуры ИБ, либо компоненты узкой целевой аудитории, например, будущие учителя, курсанты и т. д.

## Методы

При рассмотрении понимания информационной безопасности учитывается идентификация применимых угроз и средств контроля, необходимых для предотвращения их возникновения. Средства (метод) – это способ, которым совершается несанкционированная деятельность нарушителя в отношении информационных ресурсов. Анализ способов и средств совершения несанкционированного доступа позволит повысить эффективность информационной безопасности и уменьшить связанные потери.

Основные способы несанкционированного доступа к информационным активам: подслушивание пакетов; атака по словарю паролей; кража ID/пароля при помощи социальной инженерии; несанкционированный доступ к информации системы управления

безопасностью деятельности (далее – СУБД) путем использования ошибок в настройках; несанкционированный доступ к информации СУБД путем использования уязвимости СУБД; несанкционированный доступ к информации СУБД путем изменения файлов базы данных; незаконный доступ к ID / паролю с помощью информации управления БД; создание бэкдоров; несанкционированный доступ к информации СУБД путем создания несанкционированного администратора СУБД или учетной записи оператора; несанкционированное удаление информации по несанкционированному маршруту; несанкционированный доступ к информации СУБД путем изменения информации управления; выполнение SQL с целью нарушения работы сервиса; несанкционированное удаление информации по авторизованному маршруту.

Несанкционированное действие является незаконной деятельностью и реализует способы незаконного доступа к информационным ресурсам.

### **Результаты**

Рассмотрим элементы, которые составляют и формируют культуру информационной безопасности: технологии, политики/правила и люди/компетентность.

Социальное поведение, идеи и обычаи в значительной степени основаны на правилах. Некоторые из них отражены в законах, нормах и стандартах. Другие правила, большинство из которых на самом деле являются неписаными и существуют в форме этических норм, моральных кодексов и общих представлений о том, что является приемлемым поведением в различных группах. Для обобщения представления будем считать «политикой» все правила, законы, нормы, моральные кодексы и т. д. Тогда политика организации в этом контексте – это нечто большее, чем просто письменная политика организации. В этом контексте «политики» включают в себя писанные и неписанные правила, которые регулируют творческие идеи, обычаи и социальное поведение.

Технологии также являются широкой областью, не ограниченной информационными технологиями в рамках рассматриваемой темы. Технологии в широком смысле – это применение научного знания для решения практических задач [13]. Она восходит к истокам человеческой жизни. Технология – это не только материальные вещи, такие как компьютеры, машины, молотки и т. д., но и модели: мысленные модели (шаблоны и схемы в нашем понимании), а также шаблоны, стандарты и модели, используемые в качестве шаблонов и отправных точек. Формирующий смысл понятия технологии определяется как: «средства или деятельность, с помощью которых человек изменяет свою среду обитания и манипулирует ею»<sup>1</sup>. Информационные технологии, как ни какие другие, в настоящее время активно подтверждают эту фразу.

Третий элемент культуры информационной безопасности – это люди, персонал, сотрудники. Они имеют знания, компетенции, используют технологию и формируют политику, наполняют ее информацией. Инструменты и технологии, которые используют люди, определяются прежде всего той социальной средой, в которой они выросли и развивались. Стоит отметить, что социальное поведение, демонстрируемое ими, основано на знаниях.

Исходя из изложенного, культуру ИБ можно рассматривать как компетенцию сотрудников, их знания и понимание того, как правильно и безопасно функционировать в социальной группе, в информационном пространстве. Эти компетенции включают в себя безопасное использование информационных технологий и основных правил поведения в обществе.

Совокупность понятий «люди», «политика», «технологии» и взаимные связи между ними формируют представление о мире и определяют концепцию построения и поддержания культуры ИБ. Каждый из этих элементов непосредственно влияет на два

<sup>1</sup> Technology // Encyclopædia Britannica. Encyclopædia Britannica Online. Encyclopædia Britannica Inc., 2016.

других. Независимо от того, где происходят изменения, меняются и два других элемента.

Применительно к информационной безопасности очевидно, что «политика» стимулирует инновации. Требования к обеспечению конфиденциальности и ограничение доступа к информации инициируют создание новых технологий: инструменты оценки надежности информационных систем, инструменты сокрытия активности в системе и гарантия анонимности, – обеспечить неприкосновенность информации, обрабатываемой пользователями в системе.

Неизбежное развитие технологий и политики сказывается и на людях. Перемены в политике приводят к изменению взглядов и подходов к технологии обеспечения информационной безопасности, что в последующем гарантированно приводит к трансформации существующих технологий.

Поскольку культура ИБ определяется ансамблем идей, обычаев и социального поведения определенного народа или группы людей, очевидно, что окружение является важным фактором, который необходимо учитывать при обучении слушателей по направлению ИБ и формировании у них культуры ИБ. Изменения только одной части треугольника понятий приведет к изменению культуры ИБ и затронет другие две части треугольника. Сформированная при этом плоскость восприятия культуры ИБ будет уникальная, определяемая конкретной вовлеченностью каждого элемента треугольника понятий. Эта плоскость будет одной из бесконечного множества возможных вариантов и несравнимо маловероятно являться оптимальной и эффективной. Все три элемента должны развиваться и быть осознанными людьми в организации. Осознание персоналом этих элементов и вклад их в обеспечение безопасности улучшает и понимание культуры ИБ.

Понимание новой политики и технологий базируется на обучении и понимании

людьми в организации происходящих изменений, их причин и цели. Треугольник понятий не может существовать без «осознания». Осознание безопасности обращено к той части треугольника, которая относится к людям и их компетенции.

Осведомленность о безопасности – это узкое понятие, мало освещенное в литературе, и не имеет общепринятого определения. Известны отдельные публикации на эту тему,<sup>1</sup> затрагивающие в своем большинстве технологические вопросы информационной безопасности. Не существует общепринятого определения «осознание безопасности», что, в свою очередь, означает отсутствие общего понимания того, что такое «осознание безопасности» на самом деле. Известны отдельные попытки трактовать данное понятие<sup>2</sup> в большинстве своем применительно к технологическому компоненту отраслевой принадлежности.

Палитра идей трактования понятия «осведомленность о безопасности» простирается от использования палок и тяжелых предметов для обеспечения определенного поведения через проведение скучных и не приносящих результатов тренингов, до полного бездействия и нахождения в покое. Результаты формирования осведомленности на проводимых тренингах и курсах в большинстве своем или не оценивались, или имели малоинформативную оценку «Прошли обучение», «Осведомленность получена (освоена)». Отсутствие оценок после прохождения обучения обусловлено надуманным мифом о трудно формализуемом измерении «осведомленности» и невозможностью измерить осведомленность.

Понятие «осознанность» имеет больше психологические трактовки. В Википедии приводится определение: «Осознанность – понятие в современной психологии; определяется как непрерывное отслеживание текущих переживаний, то есть состояние, в

<sup>1</sup> History of technology // Encyclopædia Britannica. Encyclopædia Britannica Online. Encyclopædia Britannica Inc., 2016.

<sup>2</sup> Осведомленность о безопасности: 6 мешающих факторов // SecurityLab.ru. URL: <https://www.securitylab.ru/blog/personal/bezmaly/345865.php> (дата обращения: 15.03.2024).

котором субъект фокусируется на переживании настоящего момента, не вовлекаясь в мысли о событиях прошлого или будущего»<sup>1</sup>. В ресурсе «Словари и энциклопедии»<sup>2</sup> имеется следующее высказывание: «Осознанность – это состояние или способность воспринимать, чувствовать или осознавать события, объекты и чувственные установки». Для понимания педагогического контекста в рамках обсуждаемой темы развития культуры ИБ рассмотрим определение одного из словарей: «Осознанность – это знание чего-то; знание того, что что-то существует и является важным»<sup>3</sup>. Это определение показывает основу осознанности в «знании, восприятии ситуации или факта». Можно увидеть в этом определении два компонента: правильную компетентность и способность применять эту компетентность в конкретной ситуации.

Формирование компетентности происходит непрерывно как на занятиях, так и в повседневной жизни [14]. Все, что нас окружает и встречается нам в жизни, учит нас новым навыкам. Информация непрерывно поступает в мозг человека. Человеческий разум – это удивительная машина, когда речь заходит о сборе, анализе и использовании новой информации и навыков. Чем больше человек знает, тем легче нашему мозгу делать еще больше новых умозаключений. Однако, если обучение происходит по неправильным навыкам, недостоверной информации и ошибочным ментальным образцам, мозг также продолжает мыслительный процесс, но конструируемые им умозаключения неверные, неправильные.

Различие между осознанием безопасности и культурой безопасности заключается в том, что культура – это нечто большее, чем

просто осознание. Осознанность или компетентность жизненно важна для того, чтобы люди поступали правильно. Компетентность в вопросах ИБ – это всего лишь один из способов построения культуры ИБ, а не самоцель. Осознание безопасности само по себе только помогает людям узнать или осознавать проблему безопасности, в которой они находятся. Знание чего-либо – совсем не то же самое, что делать – это, соответственно, изменять свое поведение. Знание о проблеме – это только один из шагов к изменению поведения и начало формирования культуры ИБ.

Рассмотрим четырехэтапный когнитивный процесс обучения:

1. Внимание.
2. Удержание.
3. Воспроизведение.
4. Мотивация.

Каждый из этих шагов важен, и осознание часто в основном связано с первыми двумя.

Внимание заключается в том, что учащийся обращает внимание на процесс обучения. Учащийся должен присутствовать, обращать внимание и проявлять интерес ко всему, что происходит при обучении. На этот шаг влияют сам обучающийся, непосредственно образовательный процесс, а также его содержание. Усиление внимания обучающихся может быть обеспечено убеждением в важности полученных знаний и их большим влиянием не только на поведение и безопасность обучающихся, но и общества в целом. Также может быть создана среда, в которой желаемое целевое поведение уже смоделировано и наглядно продемонстрировано обучающимся.

Образовательные программы повышения квалификации по направлению ИБ,

---

<sup>1</sup> Осознанность // Википедия. URL: <https://ru.wikipedia.org/wiki/%D0%9E%D1%81%D0%BE%D0%B7%D0%BD%D0%B0%D0%BD%D0%BD%D0%BE%D1%81%D1%82%D1%8C> (дата обращения: 15.03.2024).

<sup>2</sup> Осознанность // Словари и энциклопедии на Академике. URL: <https://dic.academic.ru/dic.nsf/ruwiki/1844538> (дата обращения: 15.03.2024).

<sup>3</sup> Awareness // Oxford learner's dictionaries. URL: <https://www.oxfordlearnersdictionaries.com/definition/english/awareness?q=awareness> (дата обращения: 15.03.2024).

ограничивающиеся этим уровнем, измеряют результат изменения поведения и формирования осознанности путем оценки посещаемости занятий и количеством людей, проходящих тот или иной курс.

Удержание – это способность учащегося сохранять информацию. Необходимо создать среду, помогающую обучающимся сохранить знания. Такая среда должна облегчать обучение, быть адаптирована к уровню знаний обучающегося и многократно повторяться по мере необходимости. Одним из возможных вариантов является игровая форма занятий, на которой учащиеся находятся в среде с целевым поведением и закрепляют полученные знания повторением.

Программы по развитию культуры ИБ должны быть по своему содержанию адаптированы к уровню знаний аудитории и их потребности в обучении. Фактическое содержание обучения корректируется после анализа аудитории. Все люди разные, и им могут понадобиться разные подходы, чтобы лучше обучаться.

Программы повышения осведомленности, реализующие этот этап, измеряют результат изменения поведения и формирования осознанности путем измерения посещаемости и повторения одной и той же учебной программы через определенные промежутки времени, например, как ежегодная программа обучения антифишингу.

Воспроизведение – это демонстрация того, что безопасное поведение освоено. На этой стадии обучающийся воспроизводит усвоенное поведение и показывает, что он не только знает, как и что делать, но и поступает, руководствуясь полученными знаниями.

Программы повышения осведомленности, останавливающиеся на этом уровне для оценки результатов изменения поведения, используют тесты навыков, опросники и другие инструменты оценки качества во время и сразу после учебной программы, демонстрируя определенный уровень воспроизводства. Примером может служить учебная программа по антифишингу, в которой

измеряется, сколько учеников нажимают на ссылку в электронном письме во время обучения и после него.

Мотивация – это последний этап, состоящий в том, чтобы мотивировать ученика последовательно воспроизводить поведение вне учебной ситуации. Учащийся принимает во внимание как формальную, так и неформальную информацию, чтобы решить, следует ли воспроизводить то или иное поведение или нет.

### **Заключение**

Как технология, так и политика играют важную роль в мотивации обучающегося. Если, например, исправительное учреждение или любая другая организация требует, чтобы сотрудники обнаруживали и сообщали о фишинговых письмах и заполняли при этом многостраничный отчетный документ для службы реагирования на угрозы ИБ, то очевидна низкая мотивация у сотрудников. Еще один пример. Допустим, сотрудники очень хорошо осознают проблему ИБ и знают, как с ней справиться, однако технология, позволяющая сделать это, является для организации слишком большим финансовым бременем при ее использовании.

Оценка результатов после обучения на программах, учитывающих этот уровень, строится на измерениях на всех четырех этапах. Анализируется посещаемость учебных курсов, но полученное число будет использоваться только как показатель того, что есть активность. Тесты позволяют измерить фактическую компетентность или способность к воспроизведению.

Для измерения изменения поведения обучающихся используются журналы событий вычислительных систем и анализ данных, инцидентов безопасности и т. д.

Организации дополнительного образования сотрудников ФСИН России, реализующие программы осведомленности на этом уровне, используют структурный подход, который помогает им сосредоточиться на повышении культуры ИБ. В ходе реализации всех четырех этапов обучения осведомленности обеспечивается формирование поведения каждого обучающегося на осно-

ве полученных знаний, что, в свою очередь, приводит к установлению, изменению культуры ИБ в организации. Изменение культу-

ры – это задача, выполняемая целым рядом людей, и задача педагога – быть частью этой команды.

### СПИСОК ИСТОЧНИКОВ

1. Астахова Л. В. Понятие культуры информационной безопасности // Научно-техническая информация. Серия 1: Организация и методика информационной работы. 2014. № 2. С. 1–8.
2. Астахова Л. В. От культуры – к культурному капиталу информационной безопасности организации // Вестник культуры и искусств. 2018. № 3 (55). С. 85–101.
3. Поляков В. П. Развитие культуры информационной безопасности в вузе // Акмеология. 2006. № 4 (20). С. 80–82.
4. Кузина Н. Н. Культурологический подход и его методологическое значение в формировании культуры информационной безопасности у студентов педагогического вуза // Kant. 2017. № 2 (23). С. 38–42.
5. Погодаева М. В., Ушева Т. Ф. Формирование культуры безопасной жизнедеятельности студентов на основе рефлексивного подхода // Казанский педагогический журнал. Издательство: Институт педагогики, психологии и социальных проблем (Казань). 2014. № 4 (105). С. 91–100.
6. Кузина Н. Н. Культура информационной безопасности личности учителя и процесс ее формирования у студентов педагогического вуза // Kant. 2018. № 2 (27). С. 88–91.
7. Ерина Ю. С., Кокаева И. Ю. Формирование культуры информационной безопасности у студентов будущих учителей в процессе профессиональной подготовки // Вестник Кем ГУКИ. 2017. 41. С. 168–176.
8. Ерина Ю. С., Саханский Ю. В. Формирование информационной безопасности будущих педагогов в процессе профессиональной подготовки // Вестник Северо-Осетинского государственного университета имени К. Л. Хетагурова. Издательство. 2017. № 2. С. 84–87.
9. Малюк А. А. Формирование культуры информационной безопасности общества // Педагогика. М.: Изд-во: ООО «Педагогика», 2009. № 3. С. 33–39.
10. Валитов О. К. Правовая культура и информационная безопасность // Вестник Башкирского университета. 2012. Т. 17. № 1-1. С. 580–585.
11. Шумилова Н. С. Влияние компьютерных технологий на формирование культуры информационной безопасности // Специфика педагогического образования в регионах России. 2012. № 1. С. 189–190.
12. Алиева М. Ф. Информационная безопасность как элемент информационной культуры // Вестник Адыгейского государственного университета. Серия 1: Регионоведение: философия, история, социология, юриспруденция, политология, культурология. 2012. № 4 (108). С. 97–102.
13. Селиверстов А. С. К вопросу об актуальности формирования культуры информационной безопасности у курсантов военных вузов // Вестник современных исследований. 2018. № 6.3 (21). С. 190–192.
14. Nate Kornell. A Stability Bias in Human Memory. Encyclopedia of the Sciences of Learning, 2012. P. 4–7.

### REFERENCES

1. Astakhova L. V. The concept of information security culture // Scientific and technical information. Series 1: Organization and methodology of information work. 2014. No. 2. P. 1–8. (In Russ.)
2. Astakhova L. V. From culture to cultural capital of information security of an organization // Bulletin of culture and arts. 2018. No. 3 (55). P. 85–101. (In Russ.)
3. Polyakov V. P. Development of a culture of information security at a university // Acmeology. 2006. No. 4 (20). P. 80–82. (In Russ.)
4. Kuzina N. N. Culturological approach and its methodological significance in the formation of a culture of information security among students of a pedagogical university // Kant. 2017. No. 2 (23). P. 38–42. (In Russ.)

5. Pogodaeva M. V., Usheva T. F. Formation of a culture of safe life of students based on a reflexive approach // Kazan Pedagogical Journal. Publisher: Institute of Pedagogy, Psychology and Social Problems (Kazan). 2014. No. 4 (105). P. 91–100. (In Russ.)
6. Kuzina N. N. Culture of information security of the teacher's personality and the process of its formation among students of a pedagogical university // Kant. 2018. No. 2 (27). P. 88–91. (In Russ.)
7. Erina Yu. S., Kokaeva I. Yu. Formation of a culture of information security among students - future teachers in the process of professional training // Vestnik Kem GUKI. 2017. 41. P. 168–176. (In Russ.)
8. Erina Yu. S., Sakhansky Yu. V. Formation of information security of future teachers in the process of professional training // Bulletin of the North Ossetian State University named after K. L. Khetagurov. Publishing house. 2017. No. 2. P. 84–87. (In Russ.)
9. Malyuk A. A. Formation of a culture of information security of society // Pedagogy. M.: Publishing house: Pedagogika LLC, 2009. No. 3. P. 33–39. (In Russ.)
10. Valitov O.K. Legal culture and information security // Bulletin of the Bashkir University. 2012. Vol. 17. No. 1-1. P. 580–585. (In Russ.)
11. Shumilova N. S. The influence of computer technologies on the formation of a culture of information security // Specifics of pedagogical education in the regions of Russia. 2012. No. 1. P. 189–190. (In Russ.)
12. Alieva M. F. Information security as an element of information culture // Bulletin of the Adygea State University. Series 1: Regional studies: philosophy, history, sociology, jurisprudence, political science, cultural studies. 2012. No. 4 (108). P. 97–102. (In Russ.)
13. Seliverstov A. S. On the issue of the relevance of developing a culture of information security among cadets of military universities // Bulletin of modern research. 2018. No. 6.3 (21). P. 190–192. (In Russ.)
14. Nate Kornell. A Stability Bias in Human Memory. Encyclopedia of the Sciences of Learning, 2012. P. 4–7. (In Russ.)

***Информация об авторах:***

Б. А. Швырев, кандидат физико-математических наук, доцент;  
Я. Н. Полякова, кандидат психологических наук.

***Information about the authors:***

B. A. Shvyrev, Candidate of Physics and Mathematics, Associate Professor;  
Ya. N. Polyakova, Candidate of Psychology.

Статья поступила в редакцию 01.04.2024; одобрена после рецензирования 04.04.2024; принята к публикации 21.06.2024.

The article was submitted 01.04.2024; approved after reviewing 04.04.2024; accepted for publication 21.06.2024.