**Министерство просвещения Российской Федерации**
**Федеральное государственное автономное образовательное учреждение высшего образования**
**«Государственный университет просвещения»**
**Факультет безопасности жизнедеятельности**
**Кафедра безопасности жизнедеятельности и методики обучения**

# Образование и безопасность: вызовы, тренды, перспективы

***Материалы международной научно-практической конференции***

***(27 марта 2026 г.)***

**Москва**
**2026 г.**

СОДЕРЖАНИЕ

**Аллахвердиева Лейла Матат кызы**

**ЦИФРОВЫЕ ТЕХНОЛОГИИ В ОБРАЗОВАНИИ КАК НОВАЯ ПЕДАГОГИЧЕСКАЯ ПРОБЛЕМА**.....7

**Анашкин Олег Анатольевич, Казорина Олеся Владимировна**

**ПСИХОЛОГО-ПЕДАГОГИЧЕСКИЕ АСПЕКТЫ БЕЗОПАСНОСТИ ВЗАИМОДЕЙСТВИЯ ПРЕПОДАВАТЕЛЯ И СТУДЕНТА В ВЫСШЕМ УЧЕБНОМ ЗАВЕДЕНИИ**.....17

**Барма Олег Анатольевич**

**ФОРМИРОВАНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СТУДЕНТОВ УЧРЕЖДЕНИЙ ВЫСШЕГО ОБРАЗОВАНИЯ ИНСТРУМЕНТАМИ КОРПОРАТИВНОГО МЕНЕДЖМЕНТА** .....35

**Власов Юрий Николаевич, Степанкова Лилия Сергеевна**

**ФОРМИРОВАНИЕ НАВЫКОВ ЦИФРОВОЙ ГИГИЕНЫ У МЛАДШИХ ШКОЛЬНИКОВ КАК ОСНОВА ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ И ПРОФИЛАКТИКИ ЦИФРОВОГО ПЕРЕУТОМЛЕНИЯ**.....46

**Гомзякова Наталия Юрьевна**

**ОСОБЕННОСТИ ПРАКТИКИ СТУДЕНТОВ – БУДУЩИХ ПРЕПОДАВАТЕЛЕЙ «ОСНОВ БЕЗОПАСНОСТИ И ЗАЩИТЫ РОДИНЫ»**.....54

**Горских Наталья Александровна**

**ИНТЕГРАТИВНАЯ КОНЦЕПЦИЯ ДИСЦИПЛИНЫ «БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ»: КЛЮЧЕВЫЕ ПРИНЦИПЫ, УРОВНИ РЕАЛИЗАЦИИ, ПЕРСПЕКТИВЫ ОБРАЗОВАТЕЛЬНОГО ВОЗДЕЙСТВИЯ**.....62

**Завадская Дарья Владимировна**

**ФОРМИРОВАНИЕ КУЛЬТУРЫ БЕЗОПАСНОСТИ ЛИЧНОСТИ ЧЕРЕЗ РЕАЛИЗАЦИЮ ВОСПИТАТЕЛЬНОГО ПОТЕНЦИАЛА УРОКОВ ХИМИИ**.....74

**Ковалев Денис Валерьевич, Гусева Анна Александровна**

**ИСТОРИЧЕСКИЕ АСПЕКТЫ, ЗАРОЖДЕНИЕ ПРЕДМЕТНОЙ ОБЛАСТИ БЕЗОПАСНОСТИ ЖИЗНЕДЕЯТЕЛЬНОСТИ И РАЗВИТИЕ ПРЕДМЕТА ОСНОВЫ БЕЗОПАСНОСТИ И ЗАЩИТЫ РОДИНЫ**....84

**Ковальский Виктор Брониславович**

**ДУХОВНО-НРАВСТВЕННОЕ ВОСПИТАНИЕ ПОДРАСТАЮЩЕГО ПОКОЛЕНИЯ – КЛЮЧЕВОЙ ФАКТОР ФОРМИРОВАНИЯ** .....92

**Койро Ольга Ивановна**

**МЕДИАГРАМОТНОСТЬ КАК ФАКТОР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ШКОЛЬНИКОВ (НА МАТЕРИАЛЕ УРОКОВ ЛИТЕРАТУРЫ)** .....101

**Король Владимир Вячеславович**

**СОВРЕМЕННЫЕ АСПЕКТЫ ОБЩЕНАУЧНЫХ ОСНОВ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ** ..... 111

**Корягина Ольга Васильевна, Илларионов Сергей Васильевич**

**ПРОБЛЕМЫ ПРОФИЛАКТИКИ ДЕСТРУКТИВНОГО ПОВЕДЕНИЯ ПОДРОСТКОВ В ОБЕСПЕЧЕНИИ БЕЗОПАСНОЙ ОБРАЗОВАТЕЛЬНОЙ СРЕДЫ**.....129

**Махонин Евгений Владимирович**

**БЕЗОПАСНОСТЬ ОБРАЗОВАТЕЛЬНЫХ УЧРЕЖДЕНИЙ**.....139

**Муродова Нигина Сулаймоновна**

**ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ И УГРОЗЫ ТЕРРОРИЗМА В СОВРЕМЕННОМ ОБЩЕСТВЕ** ..... 147

**Политевич Елена Эдуардовна**

**ФОРМИРОВАНИЕ ПРОФЕССИОНАЛЬНЫХ КОМПЕТЕНЦИЙ БИБЛИОТЕЧНЫХ СПЕЦИАЛИСТОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ В ИНСТИТУЦИАЛИЗИРОВАННОЙ СИСТЕМЕ ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ** ..... 162

**Серебрякова Наталья Владимировна**

**К ВОПРОСУ БЕЗОПАСНОСТИ ДЕТСТВА: ИСТОРИЧЕСКИЙ ОПЫТ ПЕРВОЙ ТРЕТИ XX**..... 178

**Сморчкова Валентина Петровна**

**БЕЗОПАСНЫЙ ТИП ЛИЧНОСТИ В БУДУЩЕМ: СТРАТЕГИЯ РАЗВИТИЯ В СОВРЕМЕННЫХ УСЛОВИЯХ**..... 186

**Стаценко Ольга Алексеевна**

**ТЕНДЕНЦИИ РАЗВИТИЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В ОБРАЗОВАТЕЛЬНЫХ УЧРЕЖДЕНИЯХ КАЗАХСТАНА**..... 201

**Тытар Владимир Александрович**

**К ВОПРОСУ О ПОСТРОЕНИИ СИСТЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ** ..... 212

**Чихорич Сандра**

**РАБОТА С ТЕКСТОМ НА ЗАНЯТИЯХ РКИ В СЛОЖНЫХ РЕАЛИЯХ СОВРЕМЕННОГО МИРА: СОДЕРЖАТЕЛЬНАЯ БЕЗОПАСНОСТЬ ТЕКСТА** ..... 232

**Барма Олег Анатольевич**

магистр педагогических наук, старший преподаватель
кафедры менеджмента социально-культурной деятельности
учреждения образования «Белорусский государственный
университет культуры и искусств»
E-mail: o.barma@buk.by

# ФОРМИРОВАНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СТУДЕНТОВ УЧРЕЖДЕНИЙ ВЫСШЕГО ОБРАЗОВАНИЯ ИНСТРУМЕНТАМИ КОРПОРАТИВНОГО МЕНЕДЖМЕНТА

Аннотация: рассматривается проблематика формирования информационной безопасности студентов учреждений высшего образования, активных пользователей общественных и ведомственных (корпоративных) цифровых экосистем, инструментами корпоративного менеджмента. Принимая во внимание общественную опасность социальной инженерии и ее активное применение для совершения противоправных действий посредством информационно-коммуникационных технологий, использование инструментов корпоративного менеджмента позволяет сформировать у студентов целостное представление о системе защиты своих персональных данных, определить общий алгоритм действий в случаях явной или скрытой угрозы.

Ключевые слова: информационная безопасность студентов, цифровые экосистемы, социальная инженерия, защита персональных данных.

**Barma Aleh Anatolyevich**
Master of Pedagogical Sciences, Senior Lecturer, the department of management in socio-cultural activity Establishment of education
«Belarusian State University of Culture and Arts»
E-mail: o.barma@buk.by

# FORMATION OF INFORMATION SECURITY OF STUDENTS OF HIGHER EDUCATION INSTITUTIONS BY MEANS OF CORPORATE MANAGEMENT TOOLS

**Abstract:** the problems of formation of information security of students of higher education institutions, active users of public and departmental (corporate) digital ecosystems, corporate management tools are considered. Taking into account the public danger of social engineering and its active use for committing illegal actions through information and communication technologies, the use of corporate management tools allows students to form a holistic view of the system of protecting their personal data, to determine the general algorithm of actions in cases of explicit or hidden threat.

**Key words:** student information security, digital ecosystems, social engineering, personal data protection.

Информационная безопасность представляется сегодня актуальным направлением исследовательских штудий специалистов в области социогуманитаристики. Интерес к данной проблематике эксплицитно определен общими тенденциями развития человечества и доминирующими трендами общественного бытия. В первую очередь

актуализация рассматриваемой темы в новом тысячелетии обусловлена стремительной цифровизацией всех сфер жизнедеятельности личности. Немаловажным фактором является и стремление общественных институтов (субъектов жилищно-коммунального хозяйства, здравоохранения, образования, сферы развлечений и досуга и других) к максимальному использованию цифровых технологий в реализации своей сервисной политики, где человеку (пользователю) отводится роль «актора». Одним из таких примеров является создание цифровых экосистем – внешнего закрытого электронного пространства, в котором функционирует множество сервисов, предназначенных для предоставления услуг по индивидуальным запросам пользователей в режиме реального времени. Как отмечает Е.Э. Политевич, «цифровые экосистемы по географическому принципу могут быть: международные (мировые/транснациональные), национальные, региональные. Экосистемы, функционирование которых соотносится с ведомством (ведомственные), созданы для корпоративного взаимодействия (корпоративные), общественного пользования (общественные), индивидуальной работы (индивидуализированные). Можно разделить экосистемы по уровню доступа (открытые, закрытые, смешанные) и форме функционирования и отношения к объекту (внешние и внутренние)» [1, с. 174].

Сегодня цифровые экосистемы являются технико-технологической основой для реализации программ регулирования потребительских практик и социального поведения граждан (как на уровне государства – «Цифровое государство», «Электронное правительство» или отдельно взятого региона – «Умный город», так и на уровне ведомства – «Талон.бай»), что позволяет каждому человеку, субъекту цифрового пространства совершать действия, направленные на решение своих личных вопросов или профессиональных обязанностей в установленном законодательством порядке. Повсеместно использование цифровых экосистем в сфере логистики, медицины, юриспруденции, образования, досуга является сегодня экономически выгодным и востребованным обществом. Их основные функциональные характеристики – удобство в использовании, надежность в осуществлении операций, высокий уровень защищенности данных, экономичность в себестоимости, – сделали их частью повседневной жизни человека. В тоже время, рассматривая цифровые экосистемы как пространство реализации своих потребительских практик, человек сталкивается с проявлением по отношению к себе элементов социальной инженерии. С развитием цифровых экосистем и повсеместным увеличением технических возможностей их применения, возрастает и уровень преступности в сфере защиты информации.

На сегодняшний день социальная инженерия является наиболее серьезной угрозой безопасности для пользователей сети Интернет, в общем, и цифровых экосистем – в частности. Наиболее часто встречающими видами социальной инженерии являются: фишинг – цель которого заключается в получении доступа к конфиденциальным данным – логинам и паролям; претекстинг – атака, в которой злоумышленник представляется другим человеком и по заранее подготовленному сценарию узнает конфиденциальную информацию. Подвержены социальной инженерии все слои населения, но наиболее уязвимой группой является студенческая молодежь и сферы их активных потребительских практик.

Современное поколение студентов, поколение Z, является наиболее мобильной группой общества, активными пользователями цифровых экосистем, представленными информационно-поисковыми системами, социальными сетями, банковскими сервисами, облачными хранилищами, маркетплейсами, стриминговыми и нейросетевыми сервисами. Они чаще других выходят в Интернет, преследуя в основном развлекательные, коммуникативные и образовательные цели.

Понимая риск быть объектом социальной инженерии со стороны злоумышленников, студенческая молодежь ищет способы защиты своих данных от несанкционированного

использования, пути реализации своих прав на неприкосновенность в цифровом пространстве. Наличие нормативного правового инструмента – законодательства в области защиты персональных данных, принятых в сетевом сообществе правил поведения (например, политика «цифровой гигиены», «цифровых привычек» и т.д.), позволяет реализовывать свои потребительские модели поведения в интернет-пространстве. Все вышеперечисленное гарантирует только институциализированную систему защиты. Остается открытым вопрос о психологических аспектах манипуляции и других видов давления, повсеместно применяемых мошенниками для получения необходимой информации – личных данных, паролей, сведений конференциального характера. Данный вопрос может быть решен за счет проведения на базе учреждения высшего образования образовательных мероприятий, цель которых – формирование информационной безопасности студентов посредством использования инструментария корпоративного менеджмента. Необходимо учитывать и тот факт, что современный университет – это целостная, многоуровневая цифровая экосистема, одновременно субъектом и объектом которой выступает сам студент. Как отмечает М.В. Сомов, «Проблемы информационной безопасности в системе высшего образования выходят за рамки технической защиты данных. Они затрагивают вопросы формирования цифровой культуры

у обучающихся <…>, ответственности преподавателей и административного персонала за соблюдение правил кибербезопасности <…>, а также необходимость разработки и реализации комплексной политики защиты информации на институциональном уровне» [2, с. 74].

Корпоративный менеджмент, в первую очередь, комплекс организационно-управленческих механизмов, направленных на обеспечение устойчивости развития организации, защиту интересов ее сотрудников, информационных ресурсов от внутренних и внешних угроз. Использование инструментов корпоративного менеджмента позволяет разработать мероприятия, направленные на формирование у студентов целостного представления о существующих способах защиты своих персональных данных, алгоритмов действий в случаях явной или скрытой угрозы своей информационной безопасности – применения к ним технологий социальной инженерии. Данные мероприятия направлены на регламентирование поведения студентов внутри корпоративной системы университета как единой цифровой экосистемы, и обеспечение их информационной безопасности при работе с внешними цифровыми экосистемами (общественными, ведомственными (корпоративными)). Примерами мероприятий, направленных на поддержание внутренней информационной безопасности

университета как цифровой экосистемы и студента, как ее субъекта и объекта, являются:

1. разработка, утверждение и ознакомление студентов с правилами информационной безопасности университета в отношении использования ее информационных ресурсов (определение компетенций каждого участника информационных процессов, норм и правил использования информационных ресурсов, персональной ответственности за соблюдение правил информационной безопасности, наличие системы наказания);

2. создание единого информационного пространства размещения, хранения и распространения управленческой информации, а также определение точек доступа к информации, системы ограничений по отношению к каждому пользователю;

3. создание персональных аккаунтов студентов в корпоративной системе коммуникации (корпоративная почта, мессенджеры, сообщества в социальных сетях) и определение правил их использования для общения, передачи данных, взаимодействия с администраторами; недопустимость использования других почтовых сервисов в пространстве университета;

4. определение лиц, ответственных за информирование студентов по вопросам внутренней

корпоративной информационной безопасности, проведение обучающих мероприятий;

5. определение алгоритма действий студента при выявлении информационной угрозы или предпосылок для ее возникновения (разработка соответствующих документов);

6. проведение интерактивных занятий для студентов по вопросам их когнитивной безопасности, обучению алгоритмам действий при применение по отношением к ним технологий социальной инженерии.

Среди мероприятий, контент которых ориентирован на формирование информационной безопасности при работе с внешними, по отношению к университету, цифровыми экосистемами (общественными, ведомственными (корпоративными), можно выделить в качестве приоритетных проведение:

1. обучающих тренингов по работе с:

1.1 почтовым сервисами (mail.ru, Яндекс Почта, Gmail), определение их возможностей в защите персональных данных, уязвимости перед кибератаками;

1.2 социальными сетями как цифровым экосистемами: возможности использования их сервисов для хранения и передачи информации, совместной работы по генерации медиаконтента;

1.3 файлохранилищами как платформами для размещения текстовой информации, фото-, аудио-, видеоконтента;

2. обучающих семинаров с использованием в качестве обучающего материала протоколов безопасности ведущих цифровых экосистем, пользователями которых являются студенты. Семинары направленны, в первую очередь, на изучения алгоритмов их действий при регистрации (правила и порядок предоставления персональных данных, генерирование безопасных паролей, работы с функциональными инструментами), работы с сервисами (подача запроса, работа с дескрипторами), восстановление паролей (заполнение формы восстановления доступа к аккаунту, обращения в службу технической поддержки). С приглашением профильных специалистов, администраторов данных цифровых экосистем, возрастает эффективность данных мероприятий;

3. психологических тренингов, способствующих формированию эмоциональной устойчивости к технологиям социальной инженерии.

Таким образом, использование инструментов кадрового менеджмента в процессе организационно-управленческой и образовательной деятельности учреждения высшего образования, позволяет сформировать у студентов, активных пользователей цифрового пространства, целостного

представления о системах защиты своих персональных данных, алгоритмах действий в случаях явной или скрытой угрозы, тем самым увеличить их уровень информационной безопасности, а через них и уровень безопасности цифровых экосистем, субъектами и объектами которых они являются.

**Список литературы**

1. Политевич, Е.Э. Пользователь в цифровой экосистеме библиотеки колледжа технического профиля: клиентоориентированный подход / Е. Э. Политевич // Наука. Библиотека. Информация : материалы Междунар. науч.-практ. конф., посвященной 100-летию Центральной научной библиотеки имени Якуба Коласа Национальной академии наук Беларуси, Минск, 12-13 фев. 2025 г. / НАН Беларуси, Центр. науч. б-ка им. Я. Коласа ; сост.: Ю. А. Переверзева, О. В. Пирогова, Е. Е. Купрещенкова ; редкол.: С. С. Юрецкий (пред.) [и др.]. – Минск : ИВЦ Минфина, 2025. – С. 171-177. – Текст: непосредственный.

**2.** Сомов, М.В. Информационная безопасность в системе высшего образования: сборник трудов конференции / М.В. Сомов // Социально-педагогические вопросы образования и воспитания : материалы II Всерос. науч.-практ. конф. с междунар. участ. (Чебоксары, 10 окт. 2025 г.) / редкол.: Ж. В. Мурзина [и др.] – Чебоксары: ИД «Среда», 2025. – С. 74-76. – Текст: непосредственный.