2019 IEEE International Systems Conference (SysCon), 2019, pp. 1–8.

37. Gazebo. Available at: http://gazebosim.org/ (accessed 17.02.2022).

38. ROS2. Available at: https://github.com/ros2/ros2/wiki/DDS-and-ROS-middlewareimplementations/ (accessed 17.02.2022).

39. Madhu, A., Harshith, M. B., Prajeesha. Positioning Optimization of Drones using IMU and Securing UAV Communication by implementing Hybrid Cryptosystem. *5th International Conference on Trends in Electronics and Informatics (ICOEI)*, 2021, pp. 681–686.

40. Khanh, T. D., Komarov, I., Don, L. D., Iureva, R., Chuprov, S. TRA: Effective Authentication Mechanism for Swarms of Unmanned Aerial Vehicles. *IEEE Symposium Series on Computational Intelligence (SSCI)*, 2020, pp. 1852–1858

41. Chen, A., Peng, K., Sha, Z. ToAM: a task-oriented authentication model for UAVs based on blockchain. *EURASIP Journal on Wireless Communications and Networking*, 2021, vol. 2021, no. 1, pp. 1–16.

42. Marinenkov, E. D., Viksnin, I. I., Zhukova, Yu. A., Usova, M. A. Analiz zashchishhennosti informatsionnogo vzaimodeystviya gruppy bespilotnykh letatelnykh apparatov [Security analysis of information interaction of a group of unmanned aerial vehicles]. *Nauchno-tekhnicheskiy vestnik informatsionnykh tekhnologiy, mekhaniki i optiki* [Scientific and Technical Journal of Information Technologies, Mechanics and Optics], 2018, vol. 18, no. 5, pp. 817–825.

43. Sánchez-Ibáñez, J. R., Pérez-del-Pulgar, C. J., García-Cerezo, A. Path Planning for Autonomous Mobile Robots: A Review. *Sensors*, 2021, vol. 21, no. 7898, pp. 1–29.

УДК 004.056

ПРОБЛЕМА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ПРИ СОЗДАНИИ ЦИФРОВОГО ДВОЙНИКА ДИСЦИПЛИНЫ

Статья поступила в редакцию 01.05.2022, в окончательном варианте – 10.05.2022.

Попов Алексей Михайлович, Сибирский государственный университет науки и технологий имени М.Ф. Решетнева, 660037, Российская Федерация, г. Красноярск, пр. им. газеты «Красноярский рабочий», 31,

доктор физико-математических наук, профессор, директор Института информатики и телекоммуникаций, ORCID: 0000-0002-6011-9375, e-mail: vm_popov@sibsau.ru

Золотарев Вячеслав Владимирович, Сибирский государственный университет науки и технологий имени М.Ф. Решетнева, 660037, Российская Федерация, г. Красноярск, пр. им. газеты «Красноярский рабочий», 31,

кандидат технических наук, доцент, заведующий кафедрой безопасности информационных технологий, ORCID: 0000-0002-8054-8564, e-mail: zolotorev@sibsau.ru

Кунц Екатерина Юрьевна, Сибирский государственный университет телекоммуникаций и информатики, 630102, Российская Федерация, г. Новосибирск, ул. Кирова, 86,

начальник отдела дистанционного обучения, ORCID: 0000-0003-3903-4737, e-mail: kuntsey@sibguti.ru

При формировании образовательного содержания дисциплин наблюдается проблема управления информационной безопасностью больших объемов накапливаемых данных. Особенно это характерно для дисциплин, предполагающих использование данных цифрового следа, виртуализации, конфигурационных файлов как средств подготовки среды развертывания образовательного контента. В случае обучения информационной безопасности такой оперативной информацией является цифровой след, формируемый на уровне лабораторных работ. В работе показаны некоторые схемы управления информационной безопасностью при использовании цифрового следа и виртуальных лабораторий на уровне формирования цифрового двойника дисциплины. Использование предлагаемых схем может быть полезно для создания индивидуальных образовательных траекторий обучающихся на основе оперативных данных, образовательного контента виртуальных лабораторий, накопления и использования опыта обучения.

Ключевые слова: цифровой двойник, цифровой след, индивидуальная траектория, рабочая программа, сбор цифрового следа, образовательный процесс, информационная инфраструктура, информационно-образовательная среда, виртуальная лаборатория

INFORMATION SECURITY MANAGEMENT PROBLEM FOR CREATING A DISCIPLINE DIGITAL TWIN

The article was received by the editorial board on 01.05.2022, in the final version – 10.05.2022.

Popov Alexey M., Reshetnev Siberian State University of Science and Technology, 31 Krasnoyarsky Rabochy Ave., Krasnoyarsk, 660037, Russian Federation,

Doct. Sci. (Physics and Mathematics), Professor, Director of the Institute of Informatics and Telecommunications, ORCID: 0000-0002-6011-9375, e-mail: vm_popov@sibsau.ru

Zolotarev Vyacheslav V., Reshetnev Siberian State University of Science and Technology, 31 Krasnoyarsky Rabochy Ave., Krasnoyarsk, 660037, Russian Federation,

Cand. Sci. (Engineering), Associate Professor, Head of Information Technologies Security Department, ORCID: 0000-0002-8054-8564, e-mail: zolotorev@sibsau.ru

Kunts Ekaterina Yu., Siberian State University of Telecommunications and Informatics, 86 Kirov St., Novosibirsk, 630102, Russian Federation,

Head of Distance Learning Department, ORCID: 0000-0003-3903-4737, e-mail: kuntsey@sibguti.ru

When forming the educational content of disciplines, there is a problem of information security management of large volumes of accumulated data. This is especially true for disciplines involving the use of digital footprint data, virtualization, and configuration files as means of preparing an educational content deployment environment. In the case of information security training, such operational information is a digital footprint formed at the level of laboratory work. The paper shows some information security management schemes when using a digital footprint and virtual laboratories at the level of forming a digital twin of the discipline. The use of the proposed schemes can be useful for creating individual educational trajectories of students based on operational data, educational content of virtual laboratories, accumulation, and use of learning experience.

Keywords: digital double, digital footprint, individual trajectory, work program, digital footprint collection, educational process, information infrastructure, information and educational environment, virtual laboratory

Graphical annotation (Графическая аннотация)

Введение. Цифровые двойники представляют собой технологию, создаваемую с целью упростить и усовершенствовать работу физических прототипов объектов, целых систем и отдельных процессов. К примеру, цифровой двойник РПД (ЦД РПД) – это виртуальный прототип РПД в электронной информационно-образовательной среде (ЭИОС) вуза. Целью разработки цифрового двойника дисциплины, в свою очередь, является возможность проактивного создания качественного образовательного контента, соответствующего требованиям рынка труда и регуляторов, а также цифровизации процесса формирования необходимой документации. Цифровые двойники дисциплины могут содержать как конфигурационные файлы применяемых лабораторных средств и их виртуальные копии, так и полноценные виртуальные лаборатории, реализующие определенные задачи внутри дисциплины. При этом перемещение цифрового двойника в рамках физического пространства лабораторий при наличии современной компьютерной техники существенно упрощено, так как среда развертывания и конфигурация могут быть подготовлены заранее, а наличие вписанного в требования университета цифрового двойника рабочей программы дисциплины позволяет автоматически (или в автоматизированном режиме) готовить документацию по объекту развертывания.

Цифровой след же представляет цифровые свидетельства достижения определенных результатов в ходе выполнения учебных задач. Работая с цифровым следом, возможно оперативно генерировать рекомендации к созданию образовательного контента, обогащая базы данных, необходимые для управления образовательным процессом, в том числе процессов управления информационной безопасностью в рамках такого управления.

Целью исследования, результаты которого приведены ниже, является улучшение интеграции реального образовательного процесса и его цифровых двойников через обогащение баз данных цифрового двойника, с учетом задач защиты информации, возникающих в процессе создания, обработки и интеграции. Проблема управления информационной безопасностью возникает на уровне поддерживающих (обеспечивающих) процессов и решается путем добавления указанных процессов в образовательную среду. В качестве инструментария используются:

- алгоритм сбора и анализа цифрового следа;
- технологии виртуализации;
- технологии работы с накапливаемыми данными как с едиными репозиториями.

Новыми результатами исследования, представленными ниже, стали изучение интеграционных процессов для цифровых двойников в образовании, формирование новых устойчивых связей поддерживающих процессов управления информационной безопасностью на уровне дисциплины или ее компонентов и цифрового двойника рабочей программы дисциплины, дисциплины, лабораторного оборудования, а также возможности комплексного использования возможностей применяемых технических средств в лабораторных работах и сборе цифрового следа.

Процесс управления образовательным процессом в обучении информационной безопасности. Рассматривая процесс управления образовательным процессом даже на уровне обучения информационной безопасности на специализированных направлениях (такие как 10.03.01, 10.05.02 и пр.), стоит уделить внимание проектированию образовательных программ (ОП) и факторам, под влиянием которых разрабатывается образовательная программа по данному направлению (требования образовательных и профессиональных стандартов, профессионального сообщества ИБ, потребностей физического лица или организации, по инициативе которых осуществляется дополнительное образование, ожиданий работодателя, возможностей образовательной организации).

Содержание ОП, а в частности содержательная часть РПД, должны учитывать требования профессиональных стандартов по соответствующим должностям. Неотъемлемой частью структуры ОП является описание перечня профессиональных компетенций в рамках имеющейся квалификации; конкретное описание планируемых результатов, которые формируются в компетентностной форме для всех видов ОП. В соответствии с нормативными документами, образовательная программа разрабатывается на основании установленных профессиональных стандартов в области информационной безопасности (ИБ) и требований соответствующих федеральных государственных образовательных стандартов (ФГОС) в области ИБ (рис. 1).

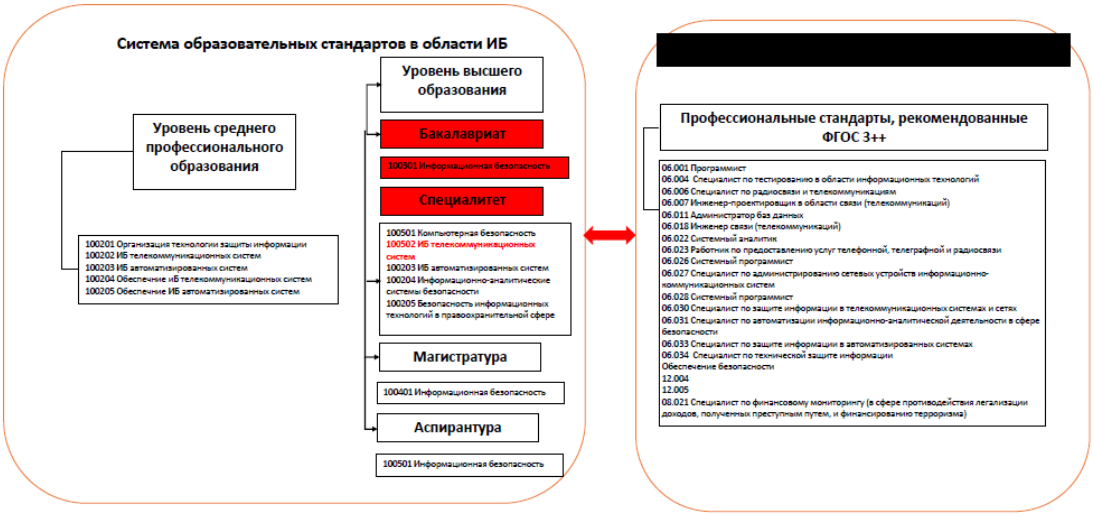

Рисунок 1 – Взаимосвязь ФГОС и профессиональных стандартов в области ИБ при проектировании образовательных программ

Однако в целом подход к разработке образовательных программ и дисциплин в области информационной безопасности гораздо шире, для формирования и описания профессиональных компетенций необходимо учитывать не только требования ФГОС и профессиональных стандартов, а также рекомендаций и стандартов профессионального сообщества, требования рынка труда. Анализ включает опрос работодателей, опрос образовательных организаций, реализующих программы в области ИБ, а также мониторинг сайтов-агрегаторов вакансий (рис. 2).

На данном этапе система подготовки специалистов в области информационной безопасности в Российской Федерации формируется и регламентируется нормативно-правовой документацией в сфере образования, в том числе путем разработки, обсуждения и принятия федеральных государственных образовательных стандартов высшего образования (ФГОС ВО), а также различными организациями [1].

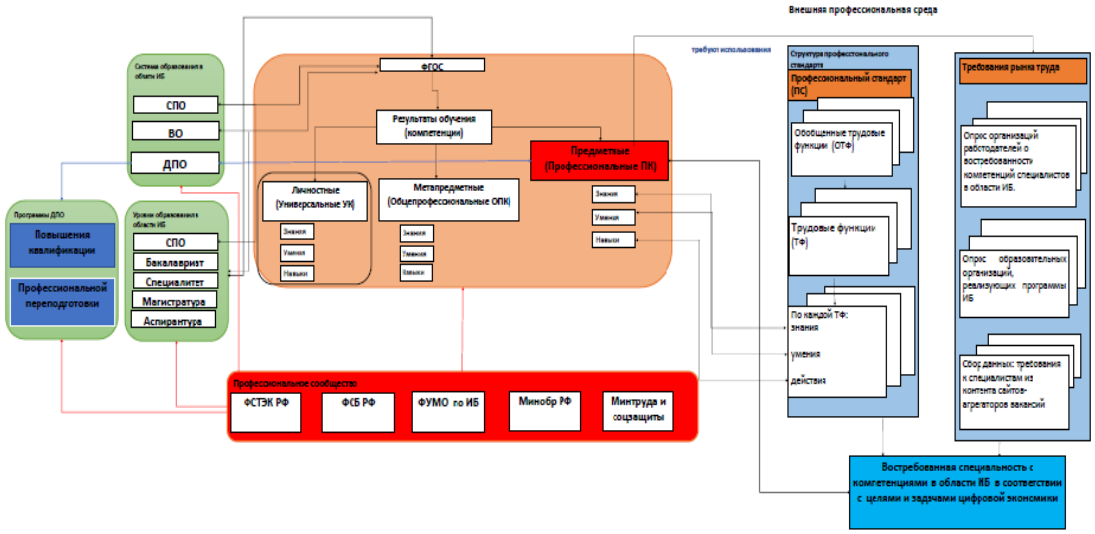

Рисунок 2 – Схема формирования профессиональной компетенции для программ ДПО в области ИБ

Процесс управления информационной безопасностью образовательного процесса. Таким образом, логично принять, что процесс управления образовательным процессом по направлению ИБ является серьезной задачей, требующей подробного анализа. К примеру, далее представлены некоторые варианты формирования цифрового следа, которые могут быть полезны для сбора оперативных данных для обогащения баз данных цифрового двойника дисциплины, схемы поддерживающих процессов, анализ формирования части цифрового двойника дисциплины на конкретных примерах.

Кроме всего указанного, здесь же необходимо учитывать и управление информационной безопасностью как часть указанного процесса. В основе своей это является следствием продолжающейся цифровой трансформации образовательного процесса. Управление информационной безопасностью в целом должно генерировать базовые процессы, применимые в задаче, такие как:

- управление требованиями к безопасности хранения, обработки, синтеза и анализа данных образовательного контента и цифрового следа;
- реализация процедур и сценариев обеспечения непрерывности образовательного контента, включая сценарии нарушения работоспособности при развертывании виртуальных стендов и контроля целостности цифровых двойников рабочих программ дисциплин;
- обучающие сценарии и сценарии оповещения при администрировании организационной и технической части образовательного процесса, в том числе и обучение действиям на основе стресс-тестов;
- управление уязвимостями используемого программного обеспечения для виртуальных лабораторий и виртуальной инфраструктуры в целом;
- управление рисками, включая правовые и юридические моменты, при формировании и использовании цифровых двойников дисциплин, рабочих программ, лабораторий и программных (программно-аппаратных) средств защиты информации (в рамках рассматриваемой проблематики; для иных областей образования – программных (программно-аппаратных) средств, используемых для формирования образовательного контента цифрового двойника дисциплины);
- управление инцидентами;
- целостное и непрерывное управление изменениями образовательного контента и цифровых двойников, включая процедуры синхронизации.

Далее будет показан план развертывания поддерживающих процессов для конкретных примеров – сбора цифрового следа, формирования виртуальной лаборатории.

Кроме того, необходимо отметить, что с точки зрения технологии управления информационной безопасностью не является критичным способ формирования цифрового двойника. К примеру, использование игровых сред на основе игровых технологий, в том числе с использованием элементов деловых игр и тренингов [2, 3], позволяет за счет высокого уровня вовлеченности обучающихся в процесс получать от них помощь в формировании указанных выше цифровых свидетельств. Использование же игровых вариантов типа Capture the Flag [4] генерирует хороший набор цифровых свидетельств автоматически, без привлечения участников. С точки зрения цифровых двойников рабочих программ также интересен опыт подготовки сотрудников организаций реального сектора, основанный на существующих программах security awareness [5], тренингов и обучения кибербезопасности в целом [6].

Далее показаны некоторые возможности работы с цифровым следом, формирования виртуальной лаборатории, порядок обогащения баз данных цифрового двойника и общая схема поддерживающих процессов, интегрированная в примеры развертывания.

Цифровой след и формирование цифрового двойника дисциплины. В рамках различных дисциплин образовательных программ в области информационной безопасности на стандартной основе предусмотрены лабораторные практикумы, основанные на фиксирующих цифровые свидетельства программных средствах. Цифровое свидетельство как способ документирования определенных действий в области защиты информации может быть легко использовано как компонент цифрового следа. К таким средствам формирования цифровых свидетельств как цифровых следов могут быть отнесены средства контроля утечек информации (DLP), средства анализа уязвимостей, системы анализа и управления информационными рисками, средства криптографической защиты информации (СКЗИ), средства криминалистического анализа. В обычном режиме не предполагается использование цифровых свидетельств, собранных на лабораторном практикуме, за рамками дисциплины; но в качестве первого шага обогащения баз цифрового двойника РПД это было бы полезным.

Второй шаг – это дообучение на основе использования цифрового следа. Внутри дисциплины создаются (корректируются) новые возможности, которые позволяют более полно использовать возможности лабораторных практикумов. Пока при этом не обновляются связи дисциплин, но возможны варианты корректировки лекционной или расчетной части дисциплины.

Основными процессами управления информационной безопасностью в данном случае должны быть:

- управление требованиями к безопасности хранения, обработки, синтеза и анализа данных образовательного контента и цифрового следа, основанное на непрерывном мониторинге цифровой среды, в которой развернут образовательный контент. При этом цифровая среда должна предполагать открытую (для внешнего мониторинга) и закрытую (для внутреннего использования) часть с соответствующим разграничением доступа;
- реализация процедур и сценариев обеспечения непрерывности образовательного контента, включая сценарии нарушения работоспособности при развертывании виртуальных стендов и контроля целостности цифровых двойников рабочих программ дисциплин. Этот процесс целесообразно кооперировать с процедурами разработки безопасного программного обеспечения, управления безопасностью развертывания виртуальных инфраструктур, управления нагрузкой и пр.;
- обучающие сценарии для формируемого набора действий при работе с цифровым следом.

Для поддерживающих процессов (рис. 3) в данном случае необходимо реализовать:

- управление записями и документацией дисциплины (разделов дисциплины);
- управление ресурсами в плане выделения процессорного времени, резервирования каналов передачи данных и оперативной памяти, резервирования времени использования инфраструктуры общего пользования;
- управление коммуникациями в плане формирования протоколов обмена данными цифрового следа, включая их безопасность.

На схеме ниже показан порядок использования таких данных для обогащения баз цифрового двойника дисциплины, включая поддерживающие процессы управления информационной безопасностью (рис. 3).

Образовательные ресурсы, используемые в данном случае, – любые вспомогательные источники информации, полезной для образовательного процесса, от форумов и баз данных до внешних источников, таких как агрегированные базы сетевых проектов или данные массовых онлайн-курсов. Как видно в примере, сбор цифрового следа может быть не только описан, но и алгоритмизирован на техническом уровне, приемлемом для реализации в образовательной системе, что через обучение может позволить постоянно повышать эффективность дообучения. При этом широкое использование именно цифровых свидетельств как компонентов цифрового следа является полезным, поскольку оставляет возможности для доказательства достижения определенного уровня и для ретроспективного анализа индивидуальной образовательной траектории.

Также возможно и целесообразно использование цифрового следа для формирования индивидуальной образовательной траектории (ИОТ) обучающегося. В области информационной безопасности существуют ограничения, формируемые в рамках консервативных пожеланий регулирующих органов, но при этом возможности работы с индивидуальной траекторией не закрыты – существуют возможности использования блока дисциплин по выбору или факультативных дисциплин, дисциплин дополнительного обучения и блоков (модулей), представленных партнерами образовательного учреждения.

Рисунок 3 – Цифровой след для обогащения баз данных цифрового двойника дисциплины

Для реализации технической части управления информационной безопасностью необходимо рассмотреть отдельно вопрос обеспечения защиты информации при работе с цифровым следом. Целесообразной для организации минимально допустимого уровня защищенности будет следующая последовательность действий:

1. Оценка снимаемых параметров, их формата и способа считывания для анализа возможности применения защитных мер. Цифровой след, собираемый для обогащения баз данных цифрового двойника, должен применяться достаточно широко и в различных задачах, поэтому анализ должен быть проведен комплексно, для всей информационной инфраструктуры.

2. Анализ протоколов обмена данными для получения информации о способе передачи, формате данных и заголовков, служебной информации, промежуточных коммуникационных устройствах. Если данные передаются между потребителями, необходимо обеспечить их недоступность третьим лицам, к примеру, за счет реализации виртуальной частной сети.

3. Анализ системы управления хранением данных и их обработкой. В большинстве случаев речь будет идти либо о работе с файлами, в том числе большого размера, либо о системе управления базами данных. Соответственно меры по защите информации будут сосредоточены либо на безопасности штатных средств обработки данных, либо на защите учетных записей, привязанных к их обработке. Также допустимо сквозное шифрование. Для цифрового следа значимыми процессами также будут подтверждение авторства и неотказуемость от операций, реализуемых с применением электронной подписи.

4. Анализ порядка доступа к данным. Варианты доступа к данным, с одной стороны, должны учитывать необходимость их использования, а с другой – возможность сохранения их целостности, конфиденциальности и доступности. Работая с порядком доступа к данным, необходимо обеспечить и быстрое восстановление, в том числе резервное копирование.

На уровне реализации цифрового двойника должны быть предусмотрены и возможности интеграции в программу электронного обучения различного типа [7]. Результатом такой интеграции может и должна стать единая система формирования ИОТ внутри дисциплин, в том числе защищенной среды работы с данными цифрового следа, используемой для поддержки формирования ИОТ.

Процессы управления информационной безопасностью здесь должны быть представлены как основными, так и поддерживающими компонентами. К основным должны быть отнесены:

- управление требованиями к безопасности хранения, обработки, синтеза и анализа данных образовательного контента и цифрового следа – в части сохранения персональных данных и данных ИОТ для задач формирования и поддержки образовательной траектории. Здесь существенное значение может иметь даже не конфиденциальность, а целостность и сохранность данных;

- реализация процедур и сценариев обеспечения непрерывности образовательного контента, включая сценарии нарушения целостности данных, собранных при прохождении индивидуальной траектории, в том числе и для цифровых следов различных типов;
- управление уязвимостями используемого программного обеспечения для управления индивидуальной образовательной траекторией, в том числе собственной разработки;
- управление рисками, включая риск нарушения аккредитационных требований;
- управление инцидентами, связанными с невыполнением требований защиты контента, данных обучающихся и пр.;
- целостное и непрерывное управление изменениями образовательного контента и цифровых двойников, включая процедуры синхронизации.

Поддерживающие процессы, в свою очередь, сосредоточены в этом случае на управлении коммуникациями, в особых случаях добавляется управление знаниями, а также на управлении безопасностью взаимоотношений с заинтересованными сторонами.

Возникает положительная обратная связь между сбором цифровых свидетельств, в том числе различных записей, и формированием образовательной траектории. Центральное место при этом занимает цифровой двойник дисциплины – РПД и соответствующие базы записей, используемые образовательным учреждением. Наборы цифровых двойников дисциплин формируют с учетом взаимных связей цифровую модель образовательного процесса, на основе которой и будут сформированы образовательные траектории.

Пример формирования части цифрового двойника – формирование виртуальной образовательной лаборатории. Здесь актуальными будут поддерживающие процессы управления данными, управления безопасностью взаимоотношений с заинтересованными сторонами. Основные процессы показаны на схеме ниже (рис. 4).

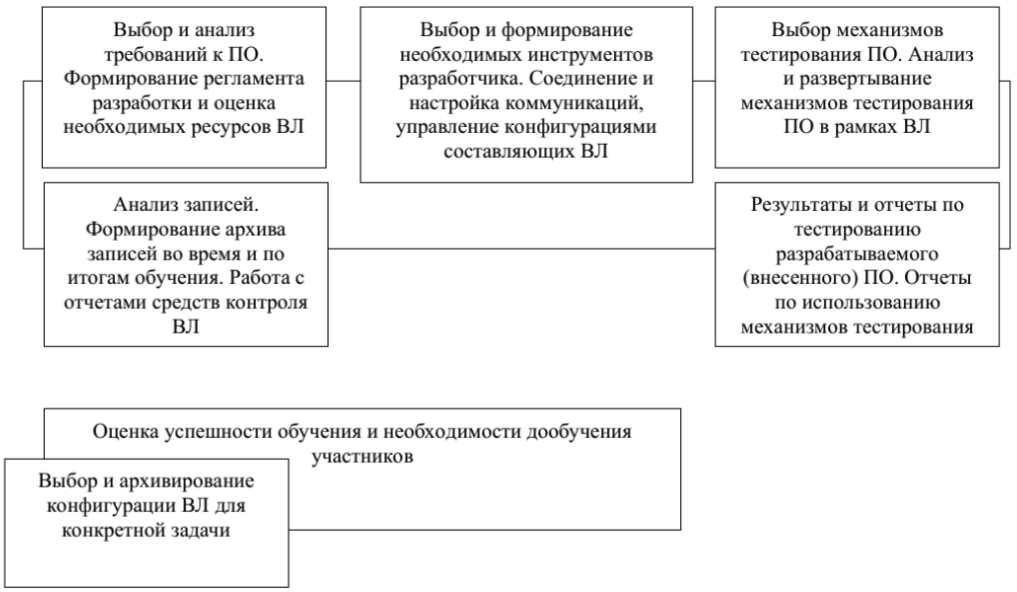

Рисунок 4 – Формирование виртуальной лаборатории, включая поддерживающие процессы управления ИБ

Технически в рамках предложенной концепции [8] формирование РПД инициируется из «1С: Университет ПРОФ» ответственными лицами, формируется структура документа с данными из учебного плана, содержащая объем нагрузки, виды занятий, предусмотренные в учебном плане, компетенции, аудиторный фонд, материально-техническое обеспечение. Данная структура после инициации формирования загружается в систему управления обучением (LMS), где с ней начинает работать научно-педагогический работник. Имея доступ к базам цифровых следов, система может автоматически назначать или корректировать составляющие дисциплин, что позволяет оперативно управлять индивидуальной образовательной траекторией каждого обучающегося. Дополнение образовательного процесса новыми модулями может быть реализовано не только за счет изменения РПД, но и в рамках работы с цифровым двойником с применением инструментов интеграции дополнительных обучающих практик, таких как квизы [9] и различного типа кейсовые задания [10]. Формально эти практики могут иметь статус внеучебной деятельности, но, так как на уровне цифрового двойника эта работа предусмотрена как дополнительная развивающая, ее результаты могут быть учтены для корректного формирования ИТ как в рамках обучения в целом, так и в рамках отдельных дисциплин. При этом возможно формировать специальные цифровые двойники для отдельных задач, в том числе цифровые двойники обучающихся [11].

При формировании образовательной траектории критичным является актуализация баз цифровых двойников дисциплины и РПД. При формировании баз данных возможно использовать различные источники (рис. 5).

Рисунок 5 – Обогащение баз данных цифрового двойника

Как видно из схемы, можно работать с различными источниками данных, но для их обобщения требуется работа по формализации записей. На настоящий момент это представляется большой сложностью и фактически не решено ни в одной образовательной программе в области информационной безопасности.

Рассмотрим конкретный пример. Если принять, что главной целью формирования цифрового двойника является управление реализацией (в том числе с учетом упомянутых выше требований управления информационной безопасностью) дисциплины (см. выше), то интересны возможности использования алгоритма обогащения на конкретных примерах. В данном случае рассмотрено обучение по учебному плану набора 2021 г. в Сибирском государственном университете науки и технологий (Красноярск) по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем», специализация «Разработка защищенных телекоммуникационных систем». Пример использования алгоритма показан в таблице 1 ниже. Формат, как видно из примера, учитывает работу поддерживающих процессов управления ИБ в части работы с данными и пользователями, оповещения и управления непрерывностью.

Таблица 1 – Пример использования алгоритма

Семестр	Назначение	СЗИ	Формат	Дисциплина
3	Сбор цифрового следа при формировании ЭП обучающегося – общие требования, формирование подписи и документации на нее, сертификата	УЦ КриптоПро	БД цифровых сертификатов обучающихся	Основы информационной безопасности
4	Сбор цифрового следа в автоматическом режиме при использовании DLP – общие вопросы, настройка, обнаружение фиксированных записей	Infowatch/ Staffcop	Общий архив отчетов на сервере. Архивы подписаны персональной ЭП	Гуманитарные аспекты информационной безопасности
5	Сбор цифрового следа при настройке сетевого подключения сервер-клиент на примере сетевых СЗИ с агентами-сборщиками данных	Staffcop	Конфигурационные файлы пользователей. Подписаны персональной ЭП	Вычислительные сети передачи данных открытых информационных систем
6	Сбор цифрового следа при использовании аутентификационных параметров и протоколов аутентификации	КриптоПро, Infowatch	Дампы трафика учебных задач, аналитика по траффику. Подписаны персональной ЭП	Безопасность вычислительных сетей
7	Сбор цифрового следа по результатам решения кейсов по применению DLP в задачах обнаружения инсайдера во внутренней инфраструктуре организации	Infowatch/ Staffcop, УЦ КриптоПро	Решения кейсов по применению DLP. Подписаны персональной ЭП. Аналитика учебных чатов обучающихся. Аналитика социальных графов при решении задачи	Управление информационной безопасностью

Как видно из таблицы, последовательность действий обучающегося может содержать вариативность как внутри одной дисциплины, так и внутри набора дисциплин в зависимости от формируемой компетенции.

Пример работы алгоритма для одной дисциплины показан в таблице 2.

Таблица 2 – Пример ИОТ внутри одной дисциплины (СибГУ им. М.Ф. Решетнева, специальность 10.05.02 «Информационная безопасность телекоммуникационных систем», набор 2020 г., дисциплина «Средства криптографической защиты информации»)

Модуль	**Действие**	**СЗИ**	**Модуль**	**Лабораторная работа**
Компетенция ПК-6		Способность применять технологии обеспечения информационной безопасности телекоммуникационных систем и нормы их интеграции в государственную и международную информационную среду		
1	Сбор цифрового следа при развертывании СКЗИ – журнал развертывания, отчеты, протоколы защиты лабораторных работ	КриптоПро CSP	Назначение шифровальных средств	Развертывание КриптоПро CSP
2	Сбор цифрового следа в автоматическом режиме при работе с УЦ КриптоПро (альтернатива)	УЦ КриптоПро	Симметричное и асимметричное шифрование	Развёртывание сервера центр сертификации ПАК «КриптоПро УЦ 2.0»
2	Сбор цифрового следа при настройке сетевого подключения СКЗИ «Континент» (альтернатива, дополнительная работа)	Криптошлюз «Континент» (вирт.)	Симметричное и асимметричное шифрование	Развёртывание VPN
3	Выполнение дополнительных заданий (сертификация) по направлению «Инфраструктура открытых ключей»		Дополнительный	Работа по треку партнера образовательной организации
3	Выполнение дополнительных заданий (сертификация) по направлению «СКЗИ Континент»		Дополнительный	Работа по треку партнера образовательной организации

При этом у него также сохраняется набор показателей цифрового следа, который свидетельствует о развитии soft skills. Таким образом, кроме реализации задач управления ИБ, в образовательных целях можно считать полезным применение методики как для наддисциплинарных треков в индивидуальной образовательной траектории, так и для внутридисциплинарных корректировок.

Заключение. Показанный подход применим к различным программам в области информационной безопасности. При этом необходимо соблюдение нескольких условий, которые открывают возможности подхода и не противоречат требованиям ФГОС и регуляторов.

Это использование общих баз данных и сохранение записей, корректные формальные структуры записей и способы автоматического исследования записей и результатов опросов данных.

Управление информационной безопасностью в данном случае решает задачу поддержки основных процессов для гарантированного соблюдения определенных требований. Показанные варианты интеграции основных и поддерживающих процессов управления информационной безопасностью могут быть реализованы как универсальные, но для технических дисциплин с возможностью виртуализации лабораторных работ предлагаемый подход наиболее интересен.

Предлагаемый подход может быть сложным в реализации в традиционной программе, без использования соответствующих инструментов, таких как цифровые двойники РПД и цифровая модель образовательного процесса. При этом в рамках последних программ поддержки университетов – «Приоритет-2030», цифровая трансформация – предполагается поддержка внедрения именно таких инструментов, и учет требований информационной безопасности для них является крайне актуальным и важным как с технической стороны, так и со стороны политик безопасности и общих концепций (процессных моделей) управления информационной безопасностью.

Библиографический список

1. Анурьева, М. С. Современная система образования в области информационной безопасности в Российской Федерации / М. С. Анурьева // Вестник ТГУ. – 2018. – № 3 (173).

2. Tang, S., Hanneghan, M. A Model-Driven Framework to Support Development of Serious Games for Game based Learning / S. Tang, M. Hanneghan // The 3rd International Conference on Developments in e-Systems Engineering. – London, UK, 2010. – DOI: 10.1109/DeSE.2010.23.

3. Jin, G. Game based Cybersecurity Training for High School Students / G. Jin, M. Tu, T.-H. Kim, J. Heffron, J. White // SIGCSE'18 Proceedings of the 49th ACM Technical Symposium on Computer Science Education. – P. 68–73. – DOI: 10.1145/3159450.3159591.

4. Trickel, E. Shell We Play A Game? CTF-as-a-service for Security Education / E. Trickel, F. Disperati, E. Gustafson et al. // USENIX Workshop on Advances in Security Education (ASE). – 2017. – Режим доступа: https://www.researchgate.net/publication/319141725_Shell_We_Play_A_Game_CTF-as-a-service_for_Security_Education, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения: 20.10.2021).

5. Ali Zani, A. A review of security awareness approaches: Towards achieving communal awareness / Editor(s): Vladlena Benson, John Mcalaney / A. Ali Zani, A. Norman, N. Ghani // Cyber Influence and Cognitive Threats. – Academic Press, 2020. – P. 97–127. – Режим доступа: https://aisel.aisnet.org/pacis2018/278, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения: 20.10.2021).

6. Арифуллина, С. Б. Концепция создания цифрового двойника рабочей программы дисциплины с использованием решений на платформе «1С:Предприятие» / С. Б. Арифуллина, Е. Ю. Кунц, Д. Г. Ли, А. В. Ильенко // Новые информационные технологии в образовании : сборник научных трудов 21-й Международной научно-практической конференции / под общ. ред. Д. В. Чистова. – Москва, 2021. – С. 50–52.

7. Kim B.-H. Development of cyber information security education and training system / B.-H. Kim, K.-C. Kim, S.-E. Hong, S.-Y. Oh // Multimedia Tools and Applications. – 2017. – № 76 (4). – P. 6051–6064.

8. Джанелли, М. Электронное обучение в теории, практике и исследованиях / М. Джанелли // Вопросы образования. – 2018. – № 4. – С. 81–98.

9. Pape, S. Conceptualization of a CyberSecurity Awareness Quiz / S. Pape, L. Goeke, A. Quintanar, K. Beckers // Proc. ESORICS 2020 International Workshops MSTEC. – 2020.

10. Sillanpää, M. Social Engineering Intrusion: A Case Study / M. Sillanpää, J. Hautamäki // Proc. IAIT2020 : The 11th International Conference on Advances in Information Technology. – 2020. – P. 1–5.

11. Казначеева, Н. В. Прототип цифрового двойника обучающегося для построения индивидуального образовательного маршрута / Н. В. Казначеева, Е. Ю. Кунц, И. О. Сучков, А. Н. Полетайкин // Современное образование: повышение конкурентоспособности университетов : материалы Междунар. науч.-метод. конф. : в 2 ч., 28–29 января 2021 г., Томск, Россия / отв. ред. В. М. Рулевский. – Томск : Изд-во Томск. гос. ун-та систем управления и радиоэлектроники, 2021. – Ч. 1. – С. 89–94.

References

1. Anuryeva, M. S. Sovremennaya sistema obrazovaniya v oblasti informatsionnoy bezopasnosti v Rossiiskoy Federatsii [Modern system of education in the field of information security in the Russian Federation]. *Vestnik Tomskogo gosudarstvennogo universiteta* [Bulletin of Tomsk State University], 2018, no. 3 (173).

2. Tang, S., Hanneghan, M. A Model-Driven Framework to Support Development of Serious Games for Game based Learning. *The 3rd International Conference on Developments in e-Systems Engineering*. London, UK, 2010. DOI: 10.1109/DeSE.2010.23.

3. Jin, G., Tu, M., Kim, T.-H., Heffron, J., White, J. Game based Cybersecurity Training for High School Students. *SIGCSE'18 Proceedings of the 49th ACM Technical Symposium on Computer Science Education*, pp. 68–73. DOI: 10.1145/3159450.3159591.

4. Trickel, E., Disperati, F., Gustafson, E. et al. Shell We Play A Game? CTF-as-a-service for Security Education. *USENIX Workshop on Advances in Security Education (ASE)*, 2017. Available at: https://www.researchgate.net/publication/319141725_Shell_We_Play_A_Game_CTF-as-a-service_for_Security_Education (accessed 20.10.2021).

5. Ali Zani, A., Norman, A., Ghani, N. A review of security awareness approaches: Towards achieving community awareness / Editor(s): Vladlena Benson, John Mcalaney. *Cyber Influence and Cognitive Threats*. Academic Press, 2020, pp. 97–127. Available at: https://aisel.aisnet.org/pacis2018/278 (accessed 20.10.2021).

6. Arifullina, S. B., Kunts, E. Yu., Li, D. G., Ilyenko, A. V. Kontseptsiya sozdaniya tsifrovogo dvoynika rabochey programmy s ispolzovaniem resheniy na platforme “1C: Predpriyatie” [The concept of creating a digital double of the discipline's work program using solutions on the 1C platform:Enterprise"]. *Novie informatsionnie technologii v obrazovanii : sbornik nauchnykh trudov 21-y Mezhdunarodnoy nauchno-prakticheskoy konferentsii* [New information technologies in education : Collection of scientific papers of the 21st International Scientific and Practical Conference]. Moscow, 2021, pp. 50–52.

7. Kim, B.-H., Kim, K.-C., Hong, S.-E., Oh, S.-Y., Development of cyber information security education and training system. *Multimedia Tools and Applications*, 2017, no. 76 (4), pp. 6051–6064.

8. Janelli, M. Electronnoe obuchenie v teorii, praktike i issledovaniyakh [E-learning in theory, practice and research]. *Voprosy obrazovaniya* [Education Issues], 2018, no. 4, pp. 81–98.

9. Pape, S., Goeke, L., Quintanar, A., Beckers, K. Conceptualization of a CyberSecurity Awareness Quiz. *Proc. ESORICS 2020 International Workshops MSTEC*, 2020.

10. Sillanpää, M., Hautamäki, J. Social Engineering Intrusion: A Case Study. *Proc. IAIT2020 : The 11th International Conference on Advances in Information Technology*, 2020, pp. 1–5.

11. Kaznacheeva, N. V., Kunts, E. Yu., Suchkov, I. O., Poletaykin, A. N. Prototype of a student's digital double for building an individual educational route [Prototip tsifrovogo dvoynika obuchaushegosya dlya postroeniaya individualnogo obrazovatelnogo marshruta]. *Sovremennoe obrazovanie: povyshenie konkurentosposobnosti universitetov : materialy Mezhdunarodnoy nauchno-metodicheskoy konferentsii* [Modern education: improving the competitiveness of universities : materials of the international scientific methodical conference], in 2 parts, January 28–29, 2021, Tomsk, Russia. Tomsk : Publishing House of Tomsk State University of Control Systems and Radioelectronics, 2021, part 1, pp. 89–94.