DOI: 10.18137/RNU.V9187.25.01.P.20 УДК 004.056:004.94

Яничкин Александр Юрьевич
начальник учебной части – заместитель начальника Военного учебного центра, Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет), Москва.
Электронный адрес: janichkin@bmstu.ru
Aleksandr Yu. Yanichkin
The chief academic officer – Deputy Head of the Military Training Center, Bauman Moscow State Technical University, Moscow.
E-mail address: janichkin@bmstu.ru

ПОКАЗАТЕЛЬ КОНФИДЕНЦИАЛЬНОСТИ В МАТЕМАТИЧЕСКИХ МОДЕЛЯХ ОЦЕНКИ КАЧЕСТВА ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Аннотация. Обеспечение требуемого уровня профессиональной подготовки специалистов, обучающихся в высших учебных заведениях, предусматривает проведение оценки качества образовательного процесса с использованием информации, содержащей государственную тайну. В связи с этим необходимо учитывать характерные особенности проведения такой оценки. В статье рассмотрены вопросы применения показателя конфиденциальности при оценке качества образовательного процесса.

Ключевые слова: образовательный процесс, конфиденциальность, информация, содержащая гостайну, показатель качества, военно-профессиональная подготовка.

Для цитирования: *Яничкин А.Ю.* Показатель конфиденциальности в математических моделях оценки качества образовательного процесса // Вестник Российского нового университета. Серия: Сложные системы: модели, анализ, управление. 2025. № 1. С. 20 – 26. DOI: 10.18137/RNU.V9187.25.01.P.20

CONFIDENTIALITY AS AN INDICATOR OF THE QUALITY OF THE EDUCATIONAL PROCESS IN HIGHER EDUCATIONAL INSTITUTION

Abstract. Ensuring the required level of professional training of specialists studying at higher education institutions involves assessing the quality of the educational process using information containing state secrets. In this regard, it is necessary to take into account the characteristic features of such an assessment. The article examines the issues of applying the confidentiality indicator when assessing the quality of the educational process.

Keywords: educational process, confidentiality, information containing state secrets, quality indicator, military professional training.

For citation: Yanichkin A.Yu. (2025) Confidentiality index in mathematical models of educational quality assessment. *Vestnik of Russian New University. Series: Complex Systems: Models, analysis, management*. No. 1. Pp. 20 – 26. DOI: 10.18137/RNU.V9187.25.01.P.20 (In Russian).

Введение

Совершенствование образовательного процесса направлено на обеспечение требуемого уровня профессиональной подготовки специалистов, обучающихся в высших учебных заведениях, и требует проведения оценки качества такого вида деятельности [1–3].

Для решения указанной задачи применяются различные методики и показатели. При оценке качества профессиональной подготовки специалистов, обучение которых осуществляется по учебным дисциплинам, содержащим информацию, составляющую государственную тайну, необходимо учитывать такой показатель, как конфиденциальность образовательного процесса. Дадим определение информационной и образовательной безопасности образовательного процесса, рассмотрим конфиденциальность как показатель качества такого процесса и сформулируем математическое выражение рассматриваемого показателя.

Понятие информационной и образовательной безопасности в образовательной организации

Информационная безопасность (далее – ИБ) – это совокупность средств защиты информации от случайного или преднамеренного воздействия[1].

ИБ образовательной организации назовем *образовательной безопасностью* (далее – ОБ), которая определяет комплекс мер, направленных на решение следующих задач:

• защита персональных данных и образовательного пространства от несанкционированного ознакомления, хищения информации и изменения конфигурации системы поддержки образовательной деятельности со стороны третьих лиц;

• защита обучаемых от любых видов пропаганды, рекламы, запрещенной законом информации, а также дезинформации.

В рамках решаемых задач в соответствии с действующим законодательством ОБ предусматривает защиту сведений и данных, относящихся к трем группам:

1) персональные данные и сведения, которые имеют отношение к обучаемым, преподавательскому составу, персоналу организации и оцифрованные архивные документы;

2) обучающие программы, базы данных, библиотеки, другая структурированная информация, применяемая для обеспечения учебного процесса;

3) защищенная законом интеллектуальная собственность.

Спецификой обеспечения ОБ в сфере образовательных технологий в организациях является состав характерных угроз. К ним относится как возможность хищения или повреждения данных хакерами, так и деятельность обучаемых, которые могут сознательно или ненамеренно повредить оборудование или заразить систему вредоносными программами.

К объектам, которые могут подвергаться воздействию, относятся:

• компьютерное и другое оборудование образовательной организации, в отношении которого возможны воздействия вредоносного программного обеспечения (далее – ПО), физические и другие воздействия;

• ПО, применяемое в учебном процессе или для работы системы;

---

[1] Об утверждении Доктрины информационной безопасности Российской Федерации : Указ Президента РФ от 05.12.2016 N 646 // КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_208191/?ysclid=m8ht8nsau8860132924 (дата обращения: 17.01.2025).

Вестник Российского нового университета
Серия «Сложные системы: модели, анализ и управление», выпуск 1 за 2025 год

• данные, хранящиеся на жестких дисках или портативных носителях;

• сами обучаемые, которые могут подвергаться стороннему информационному воздействию;

• персонал, поддерживающий работу ИТ-системы [4].

• Угрозы ИБ образовательной организации могут носить непреднамеренный и преднамеренный характер. К непреднамеренным угрозам относятся:

• аварии и чрезвычайные ситуации (затопление, отключение электроэнергии и др.);

• программные сбои;

• ошибки работников;

• поломки оборудования;

• сбои систем связи.

Намеренные угрозы могут исходить от обучаемых, персонала организации, конкурентов, хакеров. Наиболее уязвимыми являются сети с удаленным в пространстве расположением элементов системы поддержки образовательной деятельности. Злоумышленники могут достаточно легко нарушать связи между такими удаленными элементами, что может полностью вывести систему из строя.

Существенную угрозу представляет хищение интеллектуальной собственности и нарушение авторских прав. Внешние атаки на компьютерные сети образовательной организации могут предприниматься для воздействия на сознание обучаемых, в том числе с целью вовлечения их в криминальную или террористическую деятельность.

Для хищения данных, создания нарушений в работе информационной системы и других действий требуется несанкционированный доступ. Различают следующие виды несанкционированного доступа.

Человеческий. Предусматривает хищение сведений методом их отправки по электронной почте или копирования на портативные носители, внесение вручную изменений в базы данных при наличии физического доступа к серверу.

Аппаратный. Применение специального оборудования для хищения данных или внесения изменений в систему. В том числе может применяться оборудование для перехвата электромагнитных сигналов.

Программный. Применение специального программного обеспечения для перехвата данных, копирования паролей, дешифровки и перенаправления трафика, внесения изменений в функционирование другого софта.

Современные технологии информационной безопасности образовательной организации предусматривают необходимость защиты на нормативно-правовом, морально-этическом, административно-организационном, физическом и техническом уровне[2].

На нормативно-правовом уровне определены данные, которые должны быть защищены от несанкционированного доступа третьих лиц. Порядок обеспечения безопасности персональных данных регламентируется Трудовым кодексом РФ, Гражданским кодексом РФ, Федеральным законом «Об информации» и другими актами. Конкретные меры по защите данных, используемое для этого аппаратное и методическое обеспечение определяются законами и профильными государственными стандартами.

---

[2] Об информации, информационных технологиях и о защите информации : Федеральный закон от 27 июля 2006 г. N 149-ФЗ // КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_61798/?ysclid=m8hvpzon29462760230 (дата обращения: 17.01.2025).

В системе морально-этических ценностей предусматривается создание комплекса мер, направленных на защиту обучаемых от информации этически некорректного, травмирующего, противозаконного характера.

Административно-организационные меры строятся на базе внутреннего распорядка и правил образовательной организации. Они регламентируют порядок обращения с информацией и ее носителями, в том числе разработку должностных инструкций, внутренних методик по ИБ, перечней данных, не подлежащих передаче сторонним лицам, установление порядка взаимодействия с уполномоченными государственными органами по запросам о предоставлении информации и др.

Разработанными методиками определяется порядок доступа обучаемых в интернет во время занятий в компьютерных классах, меры по предотвращению доступа к определенным ресурсам, предотвращение использования ими своих носителей информации и др.

К физическим мерам относятся:

• установление пропускного режима для доступа в помещения, в которых находятся носители данных;

• создание системы контроля и управления доступом;

• определение уровней допуска;

• создание правил копирования критически важных данных на жесткие диски ПК, не подключенных к интернету;

• создание паролей и их периодическая замена.

Ответственность за организацию защиты компьютерной сети и физических носителей информации несет непосредственно руководитель образовательной организации и IT-персонал.

Технические меры защиты предусматривают использование специализированного ПО, в том числе DLP- и SIEM-систем, рекомендованных и разрешенных антивирусов и другие виды специального софта, установку ограничений на копирование данных с жестких дисков, использование контент-фильтра, с помощью которого ограничивается доступ обучаемых к определенным ресурсам в интернете.

Применяемое для технической защиты ПО должно гарантировать контроль электронной почты обучаемых и персонала образовательной организации.

Конфиденциальность как показатель качества образовательного процесса

Целью защиты информации, накладывающей ограничения на процесс обучения и существенно влияющей на качество образовательного процесса, является конфиденциальность. Анализ образовательного процесса как специфичной для классической информатики деятельности, позволил установить характерные для информационного и образовательного процесса свойства конфиденциальности [6–8]. В классическом понимании конфиденциальность информации – это обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

В соответствии с существующей классификацией свойства информации подразделяются на атрибутивные, динамические и прагматические (см. Рисунок).

Вестник Российского нового университета
Серия «Сложные системы: модели, анализ и управление», выпуск 1 за 2025 год

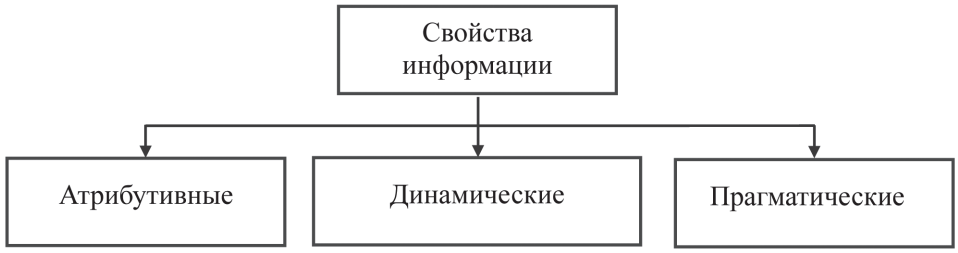

Рисунок. Классификация свойств информации

Конфиденциальность относится к прагматическим свойствам информации и в соответствии с теоретическими основами информатики определяется как состояние, при котором с требуемой вероятностью обеспечивается защита данных от утечки, хищения, утраты, несанкционированного копирования.

Исходя из вышеизложенного дадим определение аналогичным показателям конфиденциальности информационного и образовательного процесса.

Конфиденциальность информационного процесса – это способность обеспечивать защиту данных от утечки, хищения, утраты, несанкционированного копирования.

Под *конфиденциальностью образовательного процесса* будем понимать степень защищенности информации от ее разглашения.

Показателями, характеризующими конфиденциальность образовательного процесса, являются информационный объем закрытых учебных дисциплин и его минимальное значение, соответствующее возможности раскрытия информации, содержащейся в этих дисциплинах. Для практического применения показателя конфиденциальности при оценке качества профессиональной подготовки специалистов в высших учебных заведениях составим его математическое выражение.

Математическое выражение показателя конфиденциальности образовательного процесса

С целью формирования математического (аналитического) выражения, которое может быть использовано в качестве показателя конфиденциальности образовательного процесса, определим следующие параметры:

$V_{(п)}$ – объем перехватываемой конфиденциальной информации, который может быть получен в результате реализации нарушителями соответствующей угрозы безопасности в сфере образовательной деятельности;

$V_{(н)}$ – объем информации, который необходим для раскрытия ее содержания.

Формально условием обеспечения конфиденциальности образовательной деятельности будет являться неравенство

$$V_{(п)} < V_{(н)}. \quad (1)$$

Величина $V_{(п)}$, входящая в неравенство (1), по своей природе является случайной. Отсюда следует, что событие, соответствующее неравенству (1), может быть оценено соответствующей вероятностью, которую следует рассматривать как показатель конфиденциальности образовательного процесса:

$$К = P(V_{(п)} < V_{(н)}). \quad (2)$$

Согласно теоретическим основам информатики [8], измеряемые базовые информационные характеристики – объем и время реализации информационного процесса – связаны линейным преобразованием α.

С учетом этого выражение (2) можно записать как

$$К = P(V_{(п)} < V_{(н)}) = P(\tau_{(п)} < \tau_{(н)}), \quad (3)$$

где $\tau_{(п)} = \alpha_{(п)}$ – время перехвата нарушителем объема информации $V_{(п)}$;

$\tau_{(н)} = \alpha_{(н)}$ – время, необходимое для раскрытия нарушителем объема информации $V_{(н)}$.

Выводы

Таким образом, для обеспечения адекватности оценки качества образовательного процесса, предусматривающего использование информации, содержащей государственную тайну, необходимо применять методики, учитывающие показатель конфиденциальности оцениваемого процесса.

Литература

1. *Григораш О.В., Багута Н.А.* Методика оценки эффективности образовательной деятельности вуза // Высшее образование сегодня. 2024. № 6. С. 11–16. EDN HHTKEG. DOI: 10.18137/RNU.HET.24.06.P.011

2. *Горюнова Е.С., Иванова А.С., Степаненко А.А., Фещенко А.В.* Опыт применения инструментов оценки и практик управления качеством электронного обучения (кейс Томского государственного университета) // Открытое образование. 2022. Т. 26. № 4. С. 4–18. EDN EJTLSQ. DOI: 10.21686/1818-4243-2022-4-4-18

3. *Поначугин А.В.* Современный подход к мониторингу успеваемости обучающихся с применением информационно-коммуникационных технологий // Информационные и математические технологии в науке и управлении. 2021. № 4 (24). С. 125–131. DOI: 10.38028/ESI.2021.24.4.012

4. *Сайфутдинов Р.А., Белогрудова Д.Ю., Иматдинов Р.Р., Иматдинов Р.Р.* Защита информации и информационная безопасность в образовательных учреждениях // Вестник Ульяновского государственного технического университета. 2022. № 4 (100). С. 40–45. EDN MIZNXA.

5. *Авсентьев О.С., Прийма В.Н., Малышев А.А., Дураковский А.П.* Системные аспекты проблематики подготовки специалистов в области информационной безопасности // Информация и безопасность. 2009. Т. 12. № 4. С. 621–622. EDN KYIBFL.

6. *Скрыль С.В., Авсентьев О.С., Карпычев В.Ю.* Применение образовательных технологий при подготовке специалистов по защите информации: основные понятия и определения // Безопасность информационных технологий. 2006. № 2. С. 70–73. EDN HVXDYB.

7. *Авсентьев О.С.* Особенности системного представления процессов подготовки специалистов по защите информации для органов внутренних дел // Безопасность информационных технологий. 2006. № 3. С. 35–38.

8. *Трофимов В.В.* Информатика : учебник для вузов. 4-е изд. М. : Юрайт, 2024. 752 с. ISBN 978-5-534-20227-4.

References

1. Grigorash O.V., Baguta N.A. (2024) Methodology for evaluating the effectiveness of educational activities of the university. *Higher Education Today.* No. 6. Pp. 11–16. DOI: 10.18137/RNU.HET.24.06.P.011 (In Russian).

2. Goryunova E.S., Ivanova A.S., Stepanenko A.A., Feshchenko A.V. (2022) Experience in using assessment tools and e-Learning quality management practices (Case study of Tomsk State University). *Open Education*. Vol. 26. No. 4. Pp. 4–18. DOI: 10.21686/1818-4243-2022-4-4-18 (In Russian).
3. Ponachugin A.V. (2021) A modern approach to monitoring the progress of students with the use of information and communication technologies. *Informational and mathematical technologies in science and management.* No. 4 (24). Pp. 125–131. EDN EIIQFB. DOI: 10.38028/ESI.2021.24.4.012 (In Russian).
4. Saifutdinov R.A., Belogrudova D.Yu., Imatdinov R.R., Imatdinov R.R. (2022) Information protection and information security in educational institutions. *Bulletin of Ulyanovsk State Technical University.* No. 4 (100). Pp. 40–45. (In Russian).
5. Avsentiev O.S., Priima V.N., Malyshev A.A., Durakovskii A.P. (2009) System aspects of the problems of preparation of experts in the field of information security. Information and security. Vol. 12. No. 4. Pp. 621–622. (In Russian).
6. Skryl' S.V., Avsent'ev O.S., Karpychev V.Yu. (2006) Application of educational technologies in training specialists in information security: Basic concepts and definitions. *IT Security (Russia)*. No. 2. Pp. 70–73. (In Russian).
7. Avsentiev O.S. (2006) Features of the systemic representation of the processes of training specialists in information security for internal affairs agencies. *IT Security (Russia)*. No. 3. Pp. 35–38. (In Russian).
8. Trofimov V.V. (2024) *Informatika* [Computer science] : Textbook for universities. 4th edition. Moscow : Yurait Publ. 752 p. ISBN 978-5-534-20227-4. (In Russian).

Поступила в редакцию: 20.01.2025	Received: 20.01.2025
Поступила после рецензирования: 14.02.2025	Revised: 14.02.2025
Принята к публикации: 27.02.2025	Accepted: 27.02.2025