**Дмитриев Михаил Сергеевич**, доктор технических наук, профессор кафедры автомобильного транспорта, информационных технологий и методики обучения техническим дисциплинам

*Южно-Уральский государственный гуманитарно-педагогический университет*

*(Россия, 454080, г. Челябинск, пр. Ленина, 69, e-mail:* [*dmitrievms@cspu.ru*](dmitrievms@cspu.ru)*)*

**Руднев Валерий Валентинович**, кандидат технических наук, доцент, заведующий кафедрой автомобильного транспорта, информационных технологий и методики обучения техническим дисциплинам

*Южно-Уральский государственный гуманитарно-педагогический университет*

*(Россия, 454080, г. Челябинск, пр. Ленина, 69, e-mail:* [*rudnevvv@cspu.ru*](mailto:rudnevvv@cspu.ru)*)*

**Куприянов Кирилл Александрович**

*Южно-Уральский государственный гуманитарно-педагогический университет*

*(Россия, 454080, г. Челябинск, пр. Ленина, 69, e-mail:*[*kuprijanovk@mail.ru*](kuprijanovk@mail.ru)*)*

**Завоеванов Александр Сергеевич**

*Южно-Уральский государственный гуманитарно-педагогический университет*

*(Россия, 454080, г. Челябинск, пр. Ленина, 69, e-mail:*[*a.zavoevanov@mail.ru*](mailto:a.zavoevanov@mail.ru)*)*

**Обеспечение конфиденциальности доступа к информационным системам образовательной организации**

*Данная статья посвящена вопросам обеспечения защиты информации в образовательных учреждениях. Подчеркивается, что защита персональных данных работников образовательных учреждений является прямой задачей руководства этих организаций.* *Указаны методические разработки, позволяющие построить защиту образовательного учреждения на необходимом уровне.*

*Ключевые слова: образовательная организация, данные, информационная безопасность, обеспечение защиты информации, Постановление Правительства, информационное пространство.*

*Kupriyanov Kirill Alexandrovich*

*(Chelyabinsk State University, Chelyabinsk, Russia)*

*Zavoevanov Alexander Sergeevich*

*(Chelyabinsk State University, Chelyabinsk, Russia)*

**ENSURING CONFIDENTIALITY OF ACCESS TO THE SITE OF AN EDUCATIONAL ORGANIZATION**

*This article is devoted to the issues of ensuring information protection in educational institutions. It is emphasized that the protection of personal data of employees of educational institutions is a direct task of the management of these organizations. Methodological developments are indicated to build the protection of the educational institution at the required level.*

*Key words: educational organization, data, information security, ensuring information protection, government decree, information space.*

Современные информационные технологии диктуют нам свои требования, которые необходимо интегрировать в образовательный процесс. Несмотря на то, что внедрение информационных технологий в этот процесс облегчает его и делает его более понятным, использование этих технологий может нанести непоправимый вред обществу [3].

Образовательные учреждения среднего и высшего образования стремительно внедряют информационные системы, обеспечивающие обработку персональных данных сотрудников, перевод имеющихся документов в электронный вид. Целью этих систем является создание и ведение базы данных студентов, преподавателей, а также расширение административных возможностей в управлении учебным процессом. Работа с таким набором информации требует от учреждения, с одной стороны, соблюдения новейших требований, касающихся скорости доступа и обработки существующего набора информации внутри данной организации, а с другой стороны, нужно соблюдать нормы и правила нормативно-правовой базы в области обработки данных. Современные образовательные учреждения испытывают потребность в защите информации, так как помимо возможности обеспечения обработки данных в образовательных учреждениях присутствует другая информация различного характера [2].

Соответственно, проблема обеспечения защиты персональных данных в образовательных учреждениях сегодня является весьма актуальной.

Термин «информационная безопасность» используется для обозначения двух различных понятий. В первом случае, информационная безопасность (ИБ) рассматривается как практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации. Это универсальное понятие применяется вне зависимости от формы, которую могут принимать данные (электронная или, например, физическая). Основная задача обеспечения информационной безопасности в данном контексте — сбалансированная защита конфиденциальности, целостности и доступности данных, с учетом целесообразности применения и без какого-либо ущерба производительности организации. Когда речь заходит об информационной безопасности, обычно мы начинаем думать о компьютерах, сетях, интернете и хакерах. Но для образовательной среды проблема стоит шире: в ограждении учащегося от информации, которая может негативно повлиять на его формирование и  развитие, то есть о пропаганде различной направленности [2].

Таким образом, речь идет о защите информации, о мерах, которые принимает образовательная организация по защите разных видов информации. Информационная безопасность образовательного учреждения представляет собой комплекс мер различного характера, направленных на реализацию двух основных целей. Первой целью является защита персональных данных и информационного пространства от несанкционированных вмешательств, хищения информации и изменения конфигурации системы со стороны третьих лиц. Вторая цель ИБ – защита учащихся от любых видов пропаганды, рекламы, запрещенной законом информации.

Информационная безопасность в современной образовательной среде в соответствии с действующим законодательством предусматривает защиту сведений и данных, относящихся к следующим трем группам:

* персональные данные и сведения, которые имеют отношения к учащимся, преподавательскому составу, персоналу организации, оцифрованные архивные документы;
* обучающие программы, базы данных, библиотеки, другая структурированная информация, применяемая для обеспечения учебного процесса;
* защищенная законом интеллектуальная собственность.

Все эти сведения не только могут стать объектом хищения. Намеренное проникновение в них может нарушить сохранность оцифрованных книг, уничтожить хранилища знаний, внести изменения в код программ, используемых для обучения.

В обязанности лиц, отвечающих за информационную безопасность, входит:

* обеспечение сохранности защищаемых данных;
* поддержание информации в состоянии постоянной доступности для авторизованных лиц;
* обеспечение конфиденциальности подлежащих защите сведений, предотвращение доступа к ним со стороны третьих лиц.

Особенностью угроз становится не только возможность хищения сведений или повреждение массивов какими-либо сознательно действующими хакерскими группировками, но и сама деятельность подростков, намеренно, по злому умыслу или ошибочно способных повредить компьютерное оборудование или внести вирус. Выделяются четыре группы объектов, которые могут подвергнуться намеренному или ненамеренному воздействию:

* компьютерная техника и другие аппаратные средства, которые могут быть повреждены в результате механического воздействия, вирусов, по иным причинам;
* программы, используемые для обеспечения работоспособности системы или в образовательном процессе, которые могут пострадать от вирусов или хакерских атак;
* данные, хранимые как на жестких дисках, так и на отдельных носителях;
* сам персонал, отвечающий за работоспособность IT-систем;
* учащиеся, подверженные внешнему агрессивному информационному влиянию и способные создать в образовательном учреждении криминальную ситуацию. В последнее время перечень таких ситуаций существенно расширился, что говорит о возможной целенаправленной психологической атаке на сознание молодых людей.

Борьба с различными видами атак на информационную безопасность должна вестись на пяти уровнях, причем работа должна носить комплексный характер. Существует ряд методических разработок, которые позволят построить защиту образовательного учреждения на необходимом уровне [5].

*Нормативно-правовой способ обеспечения информационной безопасности.*

В России принята «Национальная стратегия действий в интересах детей», определяющая степень угроз и меры защиты их безопасности. Действия по ограничению агрессивного воздействия на сознание учащихся должны стать основными. На втором месте должно оказаться обеспечение безопасности баз данных.

Защита информации опирается на действующие в этой сфере законы, определяющие отдельные ее массивы как подлежащие защите. Они выделяют те сведения, которые должны быть недоступны третьим лицам по разным причинам (конфиденциальная информация, персональные данные, коммерческая, служебная или профессиональная тайна). Порядок защиты персональных данных определяется в том числе федеральным законом «Об информации», Трудовым кодексом. Они и Гражданский кодекс помогают разработать методику для обеспечения защиты сведений, относящихся к коммерческой тайне. Кроме законов необходимо выделить действующие в этой сфере ГОСТы, определяющие порядок защиты данных, и применяемые в этих целях методики и аппаратные средства.

*Морально-этические средства обеспечения информационной безопасности.*

В образовательной сфере большую роль играет система морально-этических ценностей. На ней должна основываться система мер, защищающих обучающихся от травмирующей, этически некорректной, незаконной информации. В целях защиты от пропаганды необходимо применять нормы закона «О защите прав ребенка», определяющие его права на защиту от сведений, которые могут причинить моральную травму. Необходимо создавать перечни документов, программ и иных источников, которые могут травмировать психику человека, в целях недопущения их проникновения на территорию учебного заведения. Это станет одной из основ информационной безопасности.

*Административно-организационные меры.*

Этот комплекс мер целиком построен на создании внутренних правил и регламентов, определяющих порядок работы с информацией и ее носителями. Это внутренние методики, посвященные информационной безопасности, должностные инструкции, перечни сведений, не подлежащих передаче. Дополнительно должен быть разработан регламент, определяющий порядок взаимодействия с компетентными органами по запросам о предоставлении им тех или иных данных и документов.

Кроме того, эти методики должны определять порядок доступа учащихся к сети Интернет в компьютерных классах, возможность защиты некоторых ресурсов неоднозначного характера от доступа индивидума, запрет на пользование собственными носителями информации. Должно быть предусмотрено использование системы родительского контроля над ресурсами сети Интернет.

*Физические меры.*

За данную систему мер и ее внедрение должно отвечать руководство образовательного учреждения и сотрудники IT-подразделений. Перекладывать организацию мер физической защиты компьютерной сети и носителей на сотрудников наемных охранных подразделений недопустимо. Среди физических мер должна быть предусмотрена пропускная система защиты в помещения, содержащие носители информации, организация контроля доступа посетителей, установления различных степеней допуска. Кроме того, к мерам физической защиты может быть отнесено обязательное копирование значимой информации на диски компьютеров, не имеющих доступа к сети Интернет. Обязательно не только установление паролей, но и их регулярная замена.

*Технические меры.*

Комплексную систему защиты всего периметра компьютерной сети должны обеспечивать специализированные программные продукты, например, DLP-системы и SIEM-системы, выявляющие все возможные угрозы безопасности и применяющие меры по борьбе с ними. Для тех учебных заведений, бюджет которых не позволяет внедрение профессиональных систем, необходимо использование разрешенных и рекомендуемых программных мер защиты, в частности антивирусов [5].

Электронная почта, к которой имеют доступ сотрудники и учащиеся, должна быть контролируема. Оптимально также ввести полный запрет на копирование любой информации с жестких дисков компьютеров образовательного учреждения.

Кроме того, должно быть предусмотрено программное обеспечение, ограничивающее доступ ребенка на определенные сайты (контент-фильтры).

Все меры должны применяться в комплексе, при этом необходимо определение одного или нескольких лиц, отвечающих за реализацию всех аспектов информационной безопасности. На основании анализа его поиска можно вносить изменения в перечень сайтов, доступ к которым ограничен с компьютеров, установленных в учебном заведении.

Таким образом, в рамках модернизации организации защиты информации в образовательных учреждениях необходимо ввести так называемые парольные протоколы и учитывать доступ к рабочему месту, использовать встроенный или программный межсетевой экран и установить лицензионные средства контроля доступа сотрудников [5].

Также необходимо организовать установку сертифицированного программного комплекса, что обеспечит контроль над процессом защиты информации. Дополнительной мерой по повышению эффективности защиты информации в образовательных учреждениях является разработка типового плана защиты информационных данных в этой организации и назначение лица, ответственного за обеспечение защиты информации.

Рассмотренные в статье положения и предлагаемые меры помогут повысить надежность и эффективность систем информационной безопасности образовательных учреждений в соответствии с их конкретными эксплуатационными и организационными требованиями и рекомендациями.

**Библиографический список**

1. Бариев А. А. Внедрение современных информационных технологий в образовательный процесс // Актуальные вопросы современной педагогики: материалы VI Междунар. науч. конф. (г. Уфа, март 2015 г.). Уфа: Лето, 2015. С. 228–230.
2. Васильев Д. А. Подход к модернизации системы защиты информации в образовательных учреждениях среднего общего полного образования // Auditorium. 2017. № 1 (13). С. 85–92.
3. Винник, Е. А. Обеспечение защиты информации в образовательных организациях / Е. А. Винник. — Текст : непосредственный // Молодой ученый. — 2023. — № 7 (454). — С. 3-6.
4. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных: утв. заместителем директора ФСТЭК России 14 февр. 2008 г. Доступ из справ.-правовой системы «Гарант».
5. Методические рекомендации по ограничению в образовательных организациях доступа обучающихся к видам информации, распространяемой посредством сети Интернет, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования: утв. Министерством просвещения РФ, Министерством цифрового развития, связи и массовых коммуникаций РФ, Федер. службой по надзору в сфере связи, информ. технологий и массовых коммуникаций 16 мая 2019 г. Доступ из справ. правовой системы «Гарант».