

Информационная безопасность для педагогических работников

Образовательный процесс касается наименее защищенных от пропаганды членов общества – детей и подростков. В связи с этим система информационной безопасности образовательной организации должна не только обеспечивать сохранность баз данных и содержащихся в них массивов конфиденциальных сведений, но и гарантировать невозможность доступа в стены колледжа любой пропаганды, как незаконного характера, так и безобидной, но предполагающей воздействие на сознание учащихся в заведениях среднего профессионального образования.

Педагогическому работнику крайне важно иметь навыки медиаграмотности и «информационной гигиены», уметь работать с современным программным обеспечением, знать основные аспекты информационной безопасности, а также применять указанные навыки не только в повседневной жизни, но и в образовательном процессе. Информационная безопасность образовательной организации включает систему мер, направленных на защиту информационного пространства и персональных данных от случайного или намеренного проникновения с целью хищения какой-либо информации или внесения изменений в конфигурацию системы. Вторым аспектом данного понятия является защита образовательного процесса от любых сведений, носящих характер запрещенной законом пропаганды, или любых видов рекламы.

В составе массивов охраняемой законом информации, находящейся в распоряжении образовательной организации, можно выделить три группы:

- персональные сведения, касающиеся обучающихся и преподавателей, оцифрованные архивы;
- ноу-хау образовательного процесса, носящие характер интеллектуальной собственности и защищенные законом;
- структурированная учебная информация, обеспечивающая образовательный процесс (библиотеки, базы данных, обучающие программы).

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

Обязанностями лиц, ответственных за защиту информации, должно стать сохранение данных в целостности и неприкосновенности и обеспечение их:

- доступности в любое время для любого авторизованного пользователя;
- защиты от любой утраты или внесения несанкционированных изменений;
- конфиденциальности, недоступности для 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 злему умыслу или ошибочно способных повредить компьютерное оборудование или

внести вирус. Выделяются пять групп объектов, которые могут подвергнуться намеренному или ненамеренному воздействию:

1. компьютерная техника и другие аппаратные средства, которые могут быть повреждены в результате механического воздействия, вирусов, а также по иным причинам;
2. программы, используемые для обеспечения работоспособности системы или в образовательном процессе, которые могут пострадать от вирусов или хакерских атак;
3. данные, хранимые как на жестких дисках, так и на отдельных носителях;
4. сам персонал, отвечающий за работоспособность информационных систем;
5. обучающиеся, подверженные внешнему агрессивному информационному влиянию.

Угрозы, направленные на повреждение любого из компонентов системы, могут носить как случайный, так и осознанный преднамеренный характер. Среди угроз, не зависящих от намерения персонала, обучающихся или третьих лиц, можно назвать:

- любые аварийные ситуации, например, отключение электроэнергии или затопление;
- ошибки персонала;
- сбои в работе программного обеспечения;
- выход техники из строя;
- проблемы в работе систем связи.

Все эти угрозы информационной безопасности носят временный характер, предсказуемы и легко устраняются действиями сотрудников и специальных служб.

Намеренные угрозы информационной безопасности носят более опасный характер и в большинстве случаев не могут быть предвидены. Их виновниками могут оказаться обучающиеся, сотрудники, третьи лица, имеющие умысел на совершение киберпреступления. Для подрыва информационной безопасности такое лицо должно иметь высокую квалификацию в отношении принципов работы компьютерных систем и программ. Наибольшей опасности подвергаются компьютерные сети, компоненты которых расположены отдельно друг от друга в пространстве. Нарушение связи между компонентами системы может привести к полному подрыву ее работоспособности. Важной проблемой может стать нарушение авторских прав, намеренное хищение чужих разработок. Компьютерные сети редко подвергаются внешним атакам с целью воздействия на сознание детей, но и это не исключено. Самой серьезной опасностью в подобном случае станет использование оборудования образовательной организации для вовлечения ребенка в совершение преступлений экстремистской и террористической направленности.

С точки зрения проникновения в периметр информационной безопасности и для совершения хищения информации или создания нарушения в работе систем необходим несанкционированный доступ.

Можно выделить несколько видов несанкционированного доступа:

1. Человеческий. Информация может быть похищена путем копирования на временные носители, переправлена по электронной почте. Кроме того,

при наличии доступа к серверу изменения в базы данных могут быть внесены вручную.

2. Программный. Для хищений сведений используются специальные программы, которые обеспечивают копирование паролей, копирование и перехват информации, перенаправление трафика, дешифровку, внесение изменений в работу иных программ.

3. Аппаратный. Он связан или с использованием специальных технических средств, или с перехватом электромагнитного излучения по различным каналам, включая телефонные.

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 образовательной организации на необходимом уровне.

Указом Президента Российской Федерации от 1 июня 2012г. №761 утверждена Национальная стратегия действий в интересах детей, определяющая степень угроз и меры защиты их безопасности. Действия по ограничению агрессивного воздействия на сознание ребенка должны стать основными. На втором месте должно оказаться обеспечение безопасности баз данных.

Защита информации опирается на действующие в этой сфере нормативные правовые акты, 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 Гражданским кодексом Российской Федерации, Трудовым кодексом Российской Федерации, федеральными законами «Об информации, информационных технологиях и о защите информации» и «О персональных данных». На основании данных законодательных актов разрабатываются методики для обеспечения защиты информации.

Педагогическим работникам необходимо помнить, что в образовательной сфере большую роль играет система морально-этических ценностей. На ней должна основываться система мер, защищающих подростка от травмирующей, этически некорректной, незаконной информации. В целях защиты от пропаганды необходимо применять нормы федеральных законов «О защите детей от информации, причиняющей вред их здоровью и развитию», «Об основных гарантиях прав ребенка в Российской Федерации», определяющие права несовершеннолетних на защиту от сведений, причиняющих вред здоровью и (или) развитию детей. К таким сведениям относится информация:

- побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству;
- способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;
- обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным;
- отрицающая семейные ценности, пропагандирующая нетрадиционные сексуальные отношения и формирующая неуважение к родителям и (или) другим членам семьи;

- оправдывающая противоправное поведение;
- содержащая нецензурную брань;
- содержащая информацию порнографического характера;
- представляемая в виде изображения или описания жестокости, физического и (или) психического насилия, преступления или иного антиобщественного действия;
- вызывающая у детей страх, ужас или панику, в том числе представляемая в виде изображения или описания в унижающей человеческое достоинство форме ненасильственной смерти, заболевания, самоубийства, несчастного случая, аварии или катастрофы и (или) их последствий.

Педагогическому коллективу необходимо регулярно принимать меры по предотвращению распространения в колледже информации, которая может травмировать психику детей. Это станет одной из основ информационной безопасности. Указанный 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 детей к сети Интернет в компьютерных классах, возможность защиты некоторых ресурсов неоднозначного характера от доступа ребенка, запрет на пользование собственными носителями информации. Кроме того, в образовательной организации должно быть предусмотрено использование системы родительского контроля над ресурсами сети Интернет. За данную систему мер и ее внедрение должно отвечать руководство образовательной организации.

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

Все перечисленные меры должны применяться в комплексе, при этом необходимо определение одного или нескольких лиц, отвечающих за реализацию всех аспектов информационной безопасности. Желательно привлечение к этой проблеме родителей (законных представителей) студентов, ведь в ряде случаев они помогут провести аудит мер безопасности и порекомендовать современные решения. Кроме того, на родителей (законных представителей) должны быть возложены обязанности и по ограничению информации, которую ребенок может получить дома. Необходимо просматривать страницы, посещаемые ребенком. На основании анализа его поиска можно вносить изменения в перечень сайтов, доступ к которым ограничен с компьютеров, установленных в учебном заведении.

Реализация комплекса перечисленных мер позволит обеспечить информационную безопасность образовательного процесса, сохранить здоровье обучающихся и гарантировать их гармоничное духовно-нравственное воспитание.