Информационная безопасность электронных образовательных ресурсов

Гегерь Эмилия Владимировна, ООО «НИЦ ИДТ», Брянск

emiliya_geger@mail.ru

Комплексная система информационной безопасности электронных образовательных ресурсов должна обеспечивать полную сохранность баз данных и содержащейся в ней конфиденциальной информации, иных справочно-информационных источников, а также гарантировать защиту от несанкционированного доступа.

Особенно это становится актуальным в условиях глобального открытого доступа информационных ресурсов.

Выход в глобальное информационное пространство диктует необходимость соблюдения принципов безопасности данных.

Понятие информационной безопасности представляет собой систему мер, которые направлены на защиту информационного пространства и персональных данных от случайного или преднамеренного проникновения с целью хищения данных или внесения изменений в программно-аппаратную конфигурацию системы, а также незаконного распространения информации.

Другим аспектом концепции является защита образовательного процесса от любой информации, носящей пропагандистский характер, который запрещен законом, любого вида рекламы, проникновение которой возможно вместе с информационными источниками открытого доступа.

В массиве охраняемой законом информации, находящихся в распоряжении образовательных учреждений, разумно выделить три группы:

- персональные сведения;
- материалы для образовательного процесса, носящие характер интеллектуальной собственности;
- структурированная учебная информация, поддерживающая образовательный процесс (научные библиотеки, базы данных, образовательные программы и информационно-справочные материалы).

Все сведения образовательного учреждения теоретически могут стать объектом хищения.

Преднамеренное проникновение может нарушить сохранность оцифрованных книг, уничтожить хранилища баз знаний, изменить код программ, используемых для обучения.

Обязанностями лиц, ответственных за защиту информации, должно стать сохранение данных в целостности и обеспечить:

- их доступность для авторизированного пользователя;
- их защиту от любой утраты или внесения несанкционированных изменений;
- их конфиденциальность;
- их недоступность для третьих лиц.

Угрозы информационной безопасности

Особенностью угроз становится не только возможность хищения сведений или повреждение информации хакерами, но и деятельность отдельных лиц, намеренно или ошибочно способных повредить компьютерное оборудование или внести вредоносный вирус.

Целесообразно выделить следующие группы объектов, которые могут подвергнуться как намеренному, так и ненамеренному воздействию:

- аппаратные средства компьютерных систем, которые могут быть повреждены в результате как механического воздействия, так и вредоносных вирусов;
- программные средства, используемые для обеспечения работоспособности системы или в образовательном процессе, которые могут пострадать от вредоносных вирусов или хакерских атак;
- данные, которые хранятся как на жестких дисках, так и на отдельных носителях;
- персонал, отвечающий за работоспособность информационных систем;

- учащиеся, подверженные внешнему особо агрессивному информационному влиянию, которые способны создать в учебной организации криминальную ситуацию.

Угрозы, направленные на повреждение любого из компонентов системы, могут носить как случайный, так и преднамеренный характер.

Среди угроз, не зависящих от намерения персонала, учащихся или третьих лиц, можно выделить:

- аварийные ситуации, например, отключение электроэнергии или затопление;
- ошибки персонала;
- сбои в работе аппаратно-программного обеспечения;
- проблемы в работе систем связи.

Эти угрозы носят временный характер и легко устраняются действиями сотрудников организации и специальных служб.

Намеренные угрозы информационной безопасности носят более опасный характер и в большинстве случаев не могут быть предвидены. Их могут спровоцировать учащиеся, служащие и специалисты организации, конкуренты, третьи лица с намерением на совершение кибер-преступления.

Надо отметить, что для подрыва информационной безопасности данное лицо должно иметь высокую квалификацию и знать принципы работы компьютерных систем и программ.

Наибольшей опасности подвергаются распределенные компьютерные сети организации. Нарушение связи между звеньями системы может привести к полному уничтожению ее работоспособности.

Особой проблемой может стать нарушение авторских прав, намеренное хищение чужих разработок.

И самой серьезной опасностью может стать использование образовательного оборудования для вовлечения учащихся в криминальные ситуации и способствующее террористическим действиям.

Несанкционированный доступ необходим для проникновения в периметр информационной безопасности и совершения хищения информации или повреждения работоспособности компьютерных систем.

Способы несанкционированного доступа

1. Человеческий. Информация может быть похищена путем копирования на резервные или съемные носители, отправлена по электронной почте. Кроме того, наличие доступа к серверу позволяет вносить изменения в базы данных вручную.
2. Программный. Специальные программы для хищения сведений обеспечивают копирование паролей, копирование либо перехват информации, перенаправление трафика, дешифровку информации, внесение изменений в работу иных программных систем.
3. Аппаратный. Он взаимосвязан либо с использованием специальных технических средств, либо с перехватом электромагнитного излучения по различным каналам, в том числе, телефонным.

Меры защиты

Борьба с различными видами атак на информационную безопасность должна носить комплексный характер и максимально предотвращать возможные угрозы. Существующие методические разработки позволят построить информационную защиту образовательного учреждения на необходимом уровне.

Нормативно-правовой способ защиты информационной безопасности

В Российской Федерации существует нормативно-законодательная база, определяющая возможную стратегию действий, вероятную степень угроз, а также комплекс мер по защите информационной безопасности.

Защита информации основывается на действующих в данной сфере законодательных документах, определяющих подлежащую защите информацию.

Они выделяют те сведения, которые по разным причинам должны быть недоступны третьим лицам (конфиденциальная информация, персональные

данные, коммерческая, служебная или профессиональная информация, не подлежащая распространению).

Порядок защиты персональных данных определяется, в том числе, Федеральным законом от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Трудовым кодексом. Эти документы и Гражданский кодекс помогают разработать методику для обеспечения защиты сведений, относящихся к неподлежащей разглашению коммерческой тайне.

Кроме законов необходимо выделить действующие в этой сфере ГОСТы, определяющие порядок защиты данных, и применяемые в этих целях методики и аппаратные средства.

В образовательных учреждениях организация информационно-телекоммуникационной сети осуществляется в соответствии с Приказом Федеральной службы по надзору в сфере образования и науки от 29 мая 2014 г. N 785 «Об утверждении требований к структуре официального сайта образовательной организации в информационно-телекоммуникационной сети «Интернет» и формату представления на нем информации».

Административно-организационные меры

Этот комплекс мер построен на создании внутренних для учреждения документов и регламентов, определяющих порядок работы с информацией. Это внутренние методики, посвященные информационной безопасности, должностные инструкции, перечни тех сведений, которые не подлежат передаче.

Дополнительно должен быть разработан регламент, определяющий порядок взаимодействия с компетентными органами по запросам о предоставлении им тех или иных данных и документов, а также документально определен перечень данных ограниченного пользования.

Физические меры

За данную систему мер и ее внедрение должно отвечать руководство образовательного учреждения, а также сотрудники информационных и инженерных служб.

Среди физических мер необходимо предусмотреть пропускную систему в помещения, где находятся носители информации, организацию контроля доступа посетителей, установления различных степеней допуска. Кроме того, к мерам физической защиты может быть отнесено обязательное копирование всей значимой информации на диски компьютеров, которые не должны иметь доступ к сети Интернет. Обязательно не только установление паролей, но и их регулярная замена.

Технические меры

Комплексную систему защиты компьютерной сети должны обеспечивать специализированные программы, например, DLP-системы и SIEM-системы, позволяющие выявлять возможные угрозы безопасности и применяющие меры по борьбе с ними.

Если финансовые возможности образовательного учреждения не позволяют внедрение профессиональных систем, необходимо использование рекомендуемых программных мер защиты, в том числе, лицензионных антивирусных программ.

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 учащихся на определенные сайты (контент-фильтры).

Все меры должны применяться в комплексе, для чего необходимо определить лица, отвечающие за реализацию всех аспектов информационной безопасности.

Заключение.

Электронные образовательные ресурсы, особенно информационное пространство открытого доступа, требуют к себе пристального внимания.

Использование информационных ресурсов в условиях глобализации становится все более актуальным.

Поэтому в развитии информационных ресурсов в образовательном учреждении на первом плане должна находиться их защита.