ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СИСТЕМЕ УПРАВЛЕНИЯ ОБРАЗОВАТЕЛЬНЫМ УЧРЕЖДЕНИЕМ

М.И. Бочаров

Россия, г. Москва

В настоящее время все больше внимания в системе образования уделяется вопросам обеспечения информационной безопасности. При построении системы управления информационной безопасностью в образовательном учреждении возникает целый ряд вопросов, относящихся к администрированию механизмов безопасности, непосредственно не относящихся к безопасности программных средств и данных. В системе образования на первый план выходит человек со своими потребностями в доступе к полноценной информации и его защита от ее негативного воздействия. Эффективное управление сферой информационной безопасности не только ограждает от информационных угроз участников образовательного процесса комплексом специальных средств, но и закладывает фундамент информационно безопасного взаимодействия в социальной среде.

И. В. Роберт отмечает, что специалист в области организации информатизации образования в учебном заведении должен владеть следующими видами профессиональной деятельности [5]:

1) научно-педагогическая;
2) учебно-методическая;
3) организационно-управленческая;
4) информационно-аналитическая;
5) культурно просветительская;
6) диагностическая [5].

Д. А. Новиков выделяет следующие ключевые проблемы управления образованием:

- упорядочить разделение и наладить координацию функций, полномочий и ответственности между различными уровнями управления образованием;
- обеспечить развитие общественной составляющей системы управления;
- преодолеть ведомственность в управлении системой образования;

•создать полноценное информационно-статистическое обеспечение органов управления и учреждений образования, а также общественности и отдельных граждан [2].

В этих проблемах четко можно выделить составляющие понятия информационной безопасности. Это открытость образовательной системы для социума. И защита данных и их передачи между различными уровнями образования.

Система образования, как ни одна другая интегрирована в государство, общество, различные социальные группы, в управлении которыми одним из значимых факторов является информационно-психологическое воздействие.

Основные источники информационно-психологического воздействия на человека в обобщенном виде можно представить следующим образом:

•Государство (в том числе иностранные государства), органы власти и управления и другие государственные структуры и учреждения.

•Общество (различные общественные, экономические, политические и иные организации, в том числе зарубежные).

•Различные социальные группы (формальные и неформальные, устойчивые и случайные, большие и малые по месту жительства, работы, учебы, службы, совместному проживанию и, проведения досуга и т.д.); отдельные личности (в том числе представители государственных и общественных структур, разнообразных социальных групп и т.п.) [2].

В качестве основных средств информационно-психологического воздействия на человека в обобщенном виде выделяются следующие:

•средства массовой коммуникации (в том числе информационные системы, например, Интернет и т.п.);

•литература (в том числе, художественная, научно-техническая, общественно-политическая, специальная и т.п.);

•искусство (в том числе различные направления так называемой массовой культуры и т.п.);

•образование (в том числе системы дошкольного, среднего, высшего и среднего специального государственного и негосударственного образования, система так называемого альтернативного образования и т.п.);

•воспитание (все разнообразные формы воспитания в системе образования, общественных организаций — формальных и неформальных, система организации социальной работы и т.п.);

•личное общение [1].

В соответствии со стандартом ISO ГОСТ Р ИСО/МЭК 17799-2005 основные меры, реализация которых позволяет добиться требуемого уровня информационной безопасности организации, включают в себя:

•разработку и проведение в жизнь политики (регламента) информационной безопасности;

•распределение обязанностей по обеспечению информационной безопасности;

•обучение и подготовку персонала по вопросам поддержания режима информационной безопасности;

•внедрение системы уведомлений о случаях нарушения системы безопасности;

•разработку планов на случай чрезвычайных ситуаций и для обеспечения непрерывности деловой деятельности организации;

•защиту документов организации (в том числе важнейших документов);

•защиту персональных данных и информации, являющейся интеллектуальной собственностью.

Руководитель организации должен:

•понимать значимость проблем информационной безопасности и их взаимосвязь с другими направлениями деятельности, такими, как обеспечение соответствия законодательству и нормативным требованиям, управление качеством, обеспечение непрерывности деловой деятельности и т.д.;

•понимать последствия несоблюдения правил информационной безопасности;

•видеть слабые места в информационной безопасности своей организации.

Разработка официальной политики образовательного учреждения в области информационной безопасности подразумевает определение способа использования вычислительных и коммуникационных ресурсов, а также

разработку процедур, предотвращающих или реагирующих на нарушения режима безопасности с учетом преемственности уровней образования. Решение этой сложной и важной проблемы должно носить системный характер.

Для формирования политики информационной безопасности (ИБ) в образовательном учреждении (ОУ) необходимо, прежде всего, определить субъектов и категории участников информационного обмена. Определить характер и уровень информационных угроз, который может исходить от них.

Так, например, для реализации политики комплексной ИБ в средней общеобразовательной и профессиональной школе выделяем в ней группы работников образовательного учреждения и получаем следующие категории: учащиеся, родители, администрация, учитель информатики, учитель организации безопасности жизнедеятельности, классный руководитель (учитель начальной школы), учителя предметники, сервисно-обслуживающий и технический персонал.

Информационная безопасность – это обеспеченность индивида, организации, общества, государства защищенностью их интересов в реализации конституционных прав и свобод по доступу к официальным нормативно закрепленным и открытым персональным и общественным не противоречащим законодательству информационным ресурсам с соответствующим обеспечением состояния защищенности от информационных угроз организационными, правовыми, инженерно-техническими, социально-педагогическими, информационно-психологическими средствами и технологиями.

Под информационной безопасностью ОУ следует понимать состояние защищенности информационных ресурсов, технологий их формирования и использования, а также прав субъектов информационной деятельности [3, 4].

Под политикой безопасности, понимают совокупность руководящих принципов, правил, процедур и практических приемов в области безопасности, которые регулируют управление, защиту и распределение ценной информации. Политика безопасности зависит: от конкретной технологии обработки информации; от используемых технических и программных средств; от расположения организации [6].

Политика ИБ ОУ должна содержать следующие компоненты подсистем обеспечения ИБ.

Под инженерно-технической защитой подразумеваются:

1. *Физические средства* (различные средства и сооружения, препятствующие физическому проникновению злоумышленников на объекты защиты и к материальным носителям конфиденциальной информации);

2. *Аппаратные средства* (приборы, устройства, приспособления и другие технические решения, используемые в интересах защиты информации);

3. *Программные средства* (специальные программы, программные комплексы и системы защиты информации в информационных системах различного назначения и средствах обработки данных);

4. *Криптографические средства* (специальные математические и алгоритмические средства защиты информации, передаваемой по системам и сетям связи, хранимой и обрабатываемой на ЭВМ с использованием разнообразных методов шифрования).

Обеспечить все эти компоненты инженерно-технической защиты из выделенных нами групп учителей способен только хорошо подготовленный специалист в области информационных технологий, при дополнительной подготовке по ИБ им может быть учитель информатики.

Правовая защита. Правовая защита информации как ресурса признана на международном, государственном уровне и определяется межгосударственными договорами, конвенциями, декларациями и реализуется патентами, авторским правом и лицензиями на их защиту.

Организационная защита – это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающей или существенно затрудняющей неправомерное овладение конфиденциальной информацией и проявление внутренних и внешних угроз.

Правовой и организационной защитой обеспечения ИБ образовательного учреждения должны владеть все группы учителей для обеспечения ИБ в рамках своих предметов.

Информационно-психологическая защита. Обеспечение ИБ РФ в сфере духовной жизни имеет целью защиту конституционных прав и свобод человека и гражданина, связанных с развитием, формированием и поведением личности, свободой массового информирования, использования культурного, духовно-нравственного наследия, исторических градаций и норм общественной жизни;

Наибольшую опасность в сфере духовной жизни представляют следующие угрозы ИБ РФ:

- деформация системы массового информирования;
- ухудшение состояния и постепенный упадок объектов российского культурного наследия;
- возможность нарушения общественной стабильности;
- использование зарубежными специальными службами средств массовой информации.

Блоком обеспечения информационно-психологической защиты должны владеть все учителя для обеспечения ИБ на своем уроке, т.к. информационно-психологическое воздействие, связанное со СМИ (в тои числе и Интернет), в силу широкого использования компьютерной техники в современной школе присутствует в преподавании практически каждого предмета.

Информатизация образования подразумевает не только использование программно-технических средств для организации учебного процесса. Она изменяет сущность и организацию процессов обучения и развития человека. Цель информатизации образования – приведение всех элементов информационной среды образования в такое состояние, когда информационные потребности субъектов удовлетворяются своевременно в необходимом объеме при соблюдении условий безопасности вне зависимости от расстояния и использования технических средств. Продуманная и взвешенная информационная политика образовательного учреждения реализуемая, в том числе, и в глобальной сети, имеет особое значение для духовного развития учащихся, для предотвращения размывания духовно-нравственных ценностей, российских культурно-исторических традиций, гражданско-патриотического сознания.

Стандарты по ИБ рекомендуют создать в учреждении отдельную службу по ИБ. Анализ же состояния ИБ в системе образования показывает, что большинство вопросов успешно решается существующими структурными элементами ОУ при исполнении их основных обязанностей. Поэтому для обеспечения ИБ ОУ необходимо налаживать совместную согласованную работу имеющихся структур, причем для решения не только проблем организационных, но и информационно-психологических. Таким координатором может стать заместитель директора, ректора по информационным технологиям, по безопасности жизнедеятельности, по воспитательной работе и возможно другие схожие по функциям руководители структурных подразделений.

Литература

1. Грачев Г. В. Информационно-психологическая безопасность личности: состояние и возможности психологической защиты. М.: Изд-во РАГС, 1998. 125 с.

2. Новиков Д. А. Введение в теорию управления образовательными системами. М.: «Эгвес», 2009.156 с.

3. Парфенов А. А. Информационная безопасность школы // Справочник руководителя образовательного учреждения. 2009. №1. http://menobr.ru/material/default.aspx?control=15&id=6317&catalogid=18

4. Пилипенко В. Ф., Ерков Н. В., Парфенов А. А. Обеспечение комплексной безопасности в образовательном учреждении. Теория и практика /М.: Из-во «Айрис-пресс», 2006. 192 с.

5. Роберт И. В. Теория и методика информатизации образования (психолого-педагогический и технологический аспекты): 3-е изд. М: ИИО РАО, 2010. 356 с.

6. Храмов В. В. Информационная безопасность школы: от защиты информации к политике безопасности // Материалы X южно-российской межрегиональной научно-практической конференции «Информационные технологии в образовании» («ИТО-РОСТОВ-2010»). http://ito.edu.ru/2010/Rostov/IV/IV-0-29.html