УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ПОЛУЧЕНИИ ДИСТАНЦИОННОГО ОБРАЗОВАНИЯ

Богатко М.П., Богатко И.Н., Качан Д.А.

Главный информационно-аналитический центр Министерства образования Республики Беларусь, г. Минск, Беларусь, bogatko@unibel.by

Abstract. The article presents the main threats of information security and measures for their prevention in the information systems that provide distance education.

В соответствии с Кодексом Республики Беларусь об образовании [1] дистанционная форма получения образования – вид заочной формы получения образования, когда получение образования осуществляется преимущественно с использованием современных коммуникационных и информационных технологий.

Использование современных коммуникационных и информационных технологий при дистанционном обучении позволяет получить образование в любом вузе страны и мира; реализовать непрерывное самообразование без каких-либо ограничений; получить образование людям, для которых затруднено перемещение, например, инвалидам; получить второе высшее или дополнительное образование всем желающим, повысить квалификацию по любой профессии в любое удобное время и/или пройти переподготовку.

Одним из наиболее распространенных видов дистанционных образовательных технологий является использование глобальной компьютерной сети Интернет для обучения и обеспечения обучающихся учебно-методическими материалами.

Данная форма получения образования предусматривает использование специального программного обеспечения (программы обмена быстрыми сообщениями, организация общения посетителей информационных ресурсов), сервисов, базирующихся на системе протоколов Интернет (почтовые, гипертекстовые, телекоммуникационные, передачи файлов) и социальных сервисов (безопасный поиск, размещение информации, фото, презентаций, реализация проектов и т. п.).

Используемые информационные ресурсы, средства, системы и сервисы в общем виде представляют собой информационные системы, обеспечивающие сбор, предоставление и хранение информации, в том числе (зачастую) персональных данных лиц, получающих образование дистанционно.

Анализ [2,3,5] демонстрирует, что нормативно-правовые акты Республики Беларусь в области информационной безопасности и защиты информации отражают основные требования, методы и средства обеспечения информационной безопасности в информационных системах.

На основании [2] информация о частной жизни физического лица и персональные данные относятся к категории информации, распространение и (или) предоставление которой ограничено.

Потенциальные злоумышленники, с целью получения доступа к персональным данным, неправомерного изменения данных о лицах, получающих образование дистанционно и затруднения или полного ограничения доступа к ресурсам информационной системы, могут подвергать информационные системы следующим видам угроз информационной безопасности:

– угрозы конфиденциальности (неправомерный доступ к информации);

– угрозы целостности (неправомерное изменение данных);

– угрозы доступности (осуществление действий, делающих невозможным или затрудняющих доступ к ресурсам информационной системы).

Под доступом к информации понимается возможность получения информации и её использования [2]. Доступ к конфиденциальной информации лиц, не имеющих доступа к этой информации на законных основаниях, всегда носит неправомерный характер.

Неправомерный доступ к информации может быть осуществлён путём:

– перехвата информации с использованием технических средств (утечки информации по техническим каналам);

– хищения носителя информации;

– несанкционированного доступа к информации (далее – НСД).

Для информационных систем, обеспечивающих получение образования дистанционно, характерным типом угрозы конфиденциальности является НСД к информации, обрабатываемой в таких системах.

Согласно Хореву, чаще всего используются следующие способы НСД [4]:

– маскировка под зарегистрированного пользователя;

– непосредственное обращение к объектам доступа;

– использование программных средств, выполняющих обращение к объектам доступа в обход средств защиты;

– использование программных средств для модификации средств защиты, позволяющих осуществить НСД;

– внедрение в информационную систему вредоносных программ для осуществления НСД к информации или её копирования.

Как отмечает Хорев А. А., к угрозам целостности информации относятся факторы (явление, действие или процесс), результатом которых могут быть неправомерное уничтожение или неправомерное модифицирование (искажение, подмена) информации, а к угрозам доступности информации – факторы, резуль-

татом которых может быть неправомерное блокирование доступа к информации [4].

Угрозы целостности и доступности информации можно разделить на преднамеренные и непреднамеренные.

К преднамеренным угрозам можно отнести [4]:

– диверсию в отношении информационной системы, в результате которой произошло разрушение, уничтожение информации, носителя информации;

– использование специальных программных воздействий на информацию (вредоносных программ, программных закладок и компьютерных вирусов), вызывающих модифицирование (искажение, подмену), уничтожение информации или блокирование доступа к ней;

– использование специальных программных воздействий на программное обеспечение (вредоносных программ, программных закладок и компьютерных вирусов), вызывающих блокирование доступа к информации, сбои в работе функционировании носителя информации.

К непреднамеренным угрозам относятся [4]:

– природные явления, стихийные бедствия (пожары, наводнения, землетрясения, грозовые разряды и т. д.);

– дефекты, сбои, отказы, аварии;

– ошибки обслуживающего персонала информационной системы.

Приведенные выше угрозы нарушают работу информационных систем, и, как следствие, препятствуют обучению и обеспечению обучающихся учебно-методическими материалами с помощью глобальной компьютерной сети Интернет.

На рисунке 1 приведено угрозы информационной безопасности на дистанционное образование.

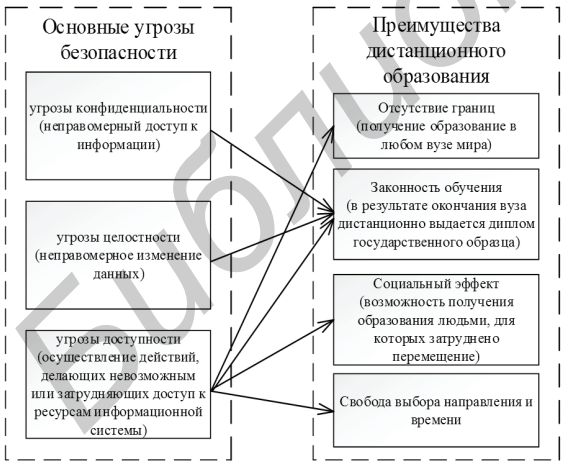

Рисунок 1 – Угрозы информационной безопасности и влияние их на дистанционное образование

При получении неправомерного доступа к информации, обрабатываемой в информационных системах, возникает угроза кражи персонифицированных данных и как следствие «кража личности».

После получения доступа к информации возможно осуществление неправомерного воздействия на неё, в результате которого могут быть созданы угрозы целостности и доступности информации.

В качестве примера, можно смоделировать ситуацию. При изменении данных злоумышленник вносит изменения в персональные данные физического лица и диплом об окончании вуза будет выдан другому лицу.

Таким образом, противодействие угрозам информационной безопасности следует осуществлять непрерывно и целенаправленно на всех этапах ее жизненного цикла с комплексным применением всех имеющихся методов и средств.

Типом угроз информационной безопасности влияющим в целом на получение образования дистанционно, являются угрозы доступности. При осуществлении действий, делающих невозможным или затрудняющих доступ к ресурсам информационной системы, обучающиеся не в состоянии получить доступ к материалам в любое время и из любой точки мира, отсутствует возможность получения образования людьми, для которых затруднено перемещение и т. п.

С учетом всего вышесказанного в информационных системах, на основании [3], целесообразна техническая защита информации, которую обязана обеспечить организация-собственник (владелец) информационных систем путем проведения мероприятий по созданию систем защиты информации, путем выполнения комплекса мероприятий по технической защите информации, подлежащей обработке в информационной системе, представленного в [5], позволяет обеспечить требуемый уровень защищенности информации.

Литература

1. Кодекс Республики Беларусь об образовании: Кодекс Республики Беларусь, 13 янв. 2011 г. № 243-З // Нац. реестр правовых актов Респ. Беларусь. – 2011. – №13. – 2/1795.

2. Об информации, информатизации и защите информации: Закон Респ. Беларусь, 10 нояб. 2008 г. №455-З: в ред. Закона Респ. Беларусь от 11.05.2016 г. // Нац. реестр правовых актов Респ. Беларусь. – 2008. – №279. – 2/1552.

3. О некоторых мерах по совершенствованию защиты информации: указ Президента Республики Беларусь, 16 апр. 2013 г. №196 // Нац. реестр правовых актов Респ. Беларусь. – 2013. – 1/14225.

4. Хорев А. А. Угрозы безопасности информации// Специальная техника. – М.: 2010. – № 1 – С.50-63.

5. О внесении изменений в некоторые приказы Оперативно-аналитического центра при Президенте Республики Беларусь: приказ Оперативно-аналитического центра при Президенте Республики Беларусь, 11 окт. 2017 г. №64 // Нац. реестр правовых актов Респ. Беларусь. – 2017. – 7/3911.