Литература
1. Способность к самоуправлению (ССУ) [Электронный ресурс]. – Режим доступа: https://psytests.org/emvol/ssu.html. [Дата обращения: 11 сентября 2023].
2. Основы психологии [Текст] : практикум / Ред.-сост. Л.Д. Столярснко. – 7-е изд. – Ростов н/Д : Феникс, 2006. – 704 с.

УДК 004.056

СОВРЕМЕННЫЕ ПОДХОДЫ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ И ИНФОРМАЦИОННЫХ СИСТЕМ УНИВЕРСИТЕТА

Мишук Е.С.
Компания «BITRIVER», г. Москва

Цель защиты информации – защита и минимизация рисков информационной безопасности (ИБ) университета от возможного нанесения материального, физического или иного ущерба посредством случайного или преднамеренного воздействия на его информационную систему (ИС).

Основные сервисы и автоматизированные системы управления учреждения высшего образования, как известно, следующие:

−главный сайт университета;
−абитуриент;
−учебный процесс;
−факультеты, кафедры, Центры, отделы и другие подразделения;
−электронная библиотека;
−система дистанционного образования;
−бухгалтерский учет;
−локальная сеть университета;
−наука:
−повышение квалификации и переподготовка кадров;
−телефонный справочник;
−учебно-воспитательная работа и другие.

Здесь хранится и обрабатывается большой объем различных материалов не только связанных с обеспечением учебного процесса, но и с персональными данными студентов, аспирантов, профессорско-преподавательского состава и других работников, служебная, коммерческая информация и другие сведения конфиденциальности. Неправомерные взлом и проникновение в те или иные сферы деятельности учреждения (научно-исследовательская деятельность, образовательные услуги, бухгалтерский учет и др.), несанкционированное удаление информации и баз данных, администрирование оперативной системы, сканирование сетей, портов и т.п., наносят колоссальный вред репутации вуза и снижают его конкурентную способность. Риски также связаны с возможной установкой вирусных и программ, вредоносного программного обеспечения, так называемых троянских коней, DDoS, XSS атаки, запуск игровых программ и др.

Минимальная обязательная защита:

−применение роутера от атак из глобальной сети;
−наличие прокси-сервера;
−постоянная поддержка и совершенствование корпоративной сети;
−комплектование информационного центра профессиональными кадрами;
−формирование высоких морально-этических норм поведения пользователей корпоративной сети в информационных системах, ограничение посещения агрессивных информационных пространств.

Кроме этого должен осуществляться многоступенчатый контроль прав доступа, постоянный мониторинг внешних и внутренних угроз информации, регулярное тестирование системы. Кибератаки из вне направлены на получение несанкционированного доступа (хищения) конфиденциальной информации или навязывания ложной информации при ее передаче. Надежной мерой противодействия таким атакам является использование средств криптографической защиты информации (СКЗИ), которые обеспечивают шифрованную имитозащищенную передачу информации по каналам связи. Необходимо создать несколько уровней защиты, каждый из которых будет включать организационные, программно-аппаратные и технические меры по обеспечению безопасности информации. В процессе эксплуатации ИС осуществляются: контроль за соблюдением требований, установленных локальными правовыми актами университета в области ИБ; контроль за порядком использования ИС; мониторинг функционирования ИС и СЗИ; выявление угроз (анализ журналов аудита), которые могут привести к сбоям, нарушению функционирования ИС; резервное копирование информации, содержащейся в ИС; выявление и фиксация инцидентов ИБ, принятие мер по своевременному реагированию на инциденты ИБ, выполнению мероприятий по недопущению инцидентов ИБ.

Обеспечение целостности и конфиденциальности информации и информационных ресурсов ИС достигается: управлением доступом пользователей к информации; резервным копированием информации и резервированием инфраструктуры; контролем действий пользователей, в частности действий, производимых с критическими ресурсами, влияющими на работоспособность ИС; наличием антивирусной защиты в составе СЗИ; средствами криптографической защиты информации.

Доступность информационных ресурсов и услуг ИС пользователям обеспечивается: резервированием аппаратных и программных средств ИС; наличием регулярно актуализируемых и проверенных на практике планов обеспечения непрерывной работы и восстановления ИС; наличием соглашения с оператором сети Интернет об уровне предоставления сервиса, содержащим описание услуги, права и обязанности сторон, согласованный уровень качества предоставления услуги (доступность, надежность, безопасность и управляемость); наличием документированных процедур, регламентирующих процессы жизненного цикла программно-технических средств, направленных на обеспечение непрерывности функционирования ИС. Подлинность пользователя ИС достигается за счет средств аутентификации ИС. Сохранность информационных ресурсов и услуг ИС достигается за счет системы хранения данных и реализации резервного копирования. Физический доступ к комплексу программно-технических средств (КПТС) обеспечивается в соответствии с Инструкцией о порядке организации доступа в серверные помещения университета. Технические средства защиты оборудования должны включать в себя источники бесперебойного питания, трансформаторы и кондиционеры.

Для дистанционной работы профессорско-преподавательскому составу (ППС) предоставляется автоматической ИС «Персональный кабинет работника БГАТУ» при помощи технологии VPN. Организация дистанционной работы при помощи технологии VPN согласование удаленного доступа при помощи технологии VPN к ИС университета осуществляет Центр информационных технологий (ЦИТ). Если есть возможность рисков ИБ, то ЦИТ вправе отказать в удаленном доступе к ИС.

Литература

1. Закон Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации».
2. Постановление Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1 «О концепции информационной безопасности Республики Беларусь».
Указ Президента Республики Беларусь от 9 декабря 2019 г. № 449 «О Совершенствовании государственного регулирования в области защиты информации».