Технология обеспечения информационной и кибербезопасности в учреждениях высшего образования

Александр Сергеевич Олейник
студент
Национальный исследовательский ядерный университет «МИФИ»
Москва, Россия
sasha010698z@yandex.ru
0000-0002-8021-3799

Виктор Михайлович Герасимов
студент
Национальный исследовательский университет ИТМО
Москва, Россия
my.virus.kaspersky@gmail.com
0000-0002-3830-5155

Фарид Надирович Халилуллин
студент
МГТУ им Н.Э Баумана (Московский государственный технический университет имени Н.Э Баумана)
Москва, Россия
fkhalilullin@gmail.com
0000-0000-0000-0000

Юлия Муслимовна Гайнулова
студент
Санкт-Петербургский государственный университет
Санкт-Петербург, Россия
julia12111990@mail.ru
0000-0000-0000-0000

Денис Станиславович Калинин
студент
Национальный исследовательский университет «Московский государственный строительный университет»
Москва, Россия
denis312578465@mail.ru
0000-0000-0000-0000

Поступила в редакцию 16.04.2022
Принята 07.05.2022
Опубликована 20.06.2022

10.25726/v6109-4146-3543-s

Аннотация

Сегодня, в условиях широкой доступности интернета и стремительного развития средств связи, существует очень заметный разрыв в ожиданиях студентов и теми возможностями, которые могут предложить им учреждения высшего образования (вуз) России. При этих условиях формы и методы образовательной деятельности в отечественных вузов должны постоянно обновляться в зависимости от

информационных потребностей и технологического развития общества. В то же время не последнее место в этом процессе должно занимать обеспечение информационной и кибербезопасности как образовательных материалов и другой информации ограниченного доступа, так и самой ИТ-инфраструктуры от случайных или направленных атак. Реализация указанных задач осложняется тем, что вузы России переживают сейчас период адаптации не только к объективным процессам информационного общества, но и к новым социально-политическим условиям с разноплановыми проявлениями конкурентной борьбы.

Ключевые слова
обеспечение, кибербезопасность, вуз, информация.

Введение

При таких условиях создание эффективных механизмов управления информационными и ИТ-ресурсами вуза в современных условиях невозможно без:

– выработка и совершенствование комплекса согласованных организационных, нормативно-правовых и технологических мер, направленных на защиту информации;

– формирование и обеспечение системы информационной и кибербезопасности (ИКБ);

– координации деятельности структурных подразделений при проведении работ по соблюдению требований обеспечения информационной и кибербезопасности.

Для их практической реализации в вузе должен быть: во-первых, проведен комплекс превентивных мер по защите информации, в том числе конфиденциальных и персональных данных (Глушков, 2017) с учетом рекомендаций общего регламента о защите данных в странах Евразии относительно законности, ограниченности цели, минимизации данных и их точности, ограничение срока хранения данных, их целостности и подотчетности (Колмогоров, 2015), а также информационных процессов, которые содержат требования к персоналу, менеджеров и технических служб, анализ информационных потоков, рисков и оценки защищенности информации; во-вторых, построена система информационной и кибербезопасности с подсистемой управления, которая будет отвечать требованиям нормативно-правовых документов и рекомендаций международных стандартов в сфере защиты информации, а также результатам информационного и технического обследования системы управления информационными и IT ресурсами вуза и тому подобное.

В то же время следует учитывать, что безопасность вуза как объекта информационной деятельности (ОИД) не существует в выделенной среде и/или в отрыве от жизнедеятельности самого объекта – отдельных корпусов вуза в пределах контролируемых зон их деятельности.

Материалы и методы исследования

Безопасность вуза как объекта информационной деятельности должна быть плотно интегрированной к этому объекту.

Преодолению этих проблем может способствовать создание в вузе системы информационной и кибернетической безопасности (СИКБ), которая была бы способна обеспечить идентификацию и аутентификацию пользователей, управлять их доступом к информации и ресурсам информационно-телекоммуникационной системы (ИТС) вуза, блокировать несанкционированные действия и предотвращать возможности реализации угроз нарушения конфиденциальности, целостности и доступности информации, предотвращать инфицирование АРМ ИТС компьютерными вирусами и тому подобное (Шеннон, 2013).

Это предполагает наличие в корпоративной информационной среде вуза таких основных компонентов, необходимых для обеспечения его безопасного функционирования, например (Эшби, 2019):

– оборудования вычислительной сети, каналов и линий передачи данных, рабочих мест пользователей, системы хранения данных;

– операционные системы, сетевые службы и сервисы по управлению доступом к ресурсам, программному обеспечению среднего слоя;

– прикладное программное обеспечение, информационные сервисы и среды, ориентированные на пользователей.

Целостная система управления указанными ресурсами в существующей ИТС вуза или такой, которая создается, должна строиться на концепции единого системного подхода, который будет обеспечивать политика информационной и кибербезопасности (ПИКБ вуза), разработанная и утвержденная вузом (Винер, 2018).

Нормативно-правовой основой создания такой системы должны быть Федеральные Законы «Об информации», «О защите информации в информационно-телекоммуникационных системах», «О защите персональных данных», «О доступе к публичной информации», «О научно-технической информации», «Об авторском праве и смежных правах» и другие.

Несмотря на то, что ИТС вуза строятся на концепциях системного подхода, они в условиях «мизерного финансирования» не имеют, как правило, стратегических целей развития (Макарова, 2000).

Для решения таких глобальных задач, как обеспечение образовательной и научной деятельности, а также управление образовательным и научным процессами в ИТС вуза имеются несколько автоматизированных подсистем, которые одновременно работают в рамках одной системы управления. Такими подсистемами ИТС вуза могут быть:

– подсистема авторизации пользователей в ИТС вуза для доступа к интернету;

– подсистема электронного документооборота вуза;

– подсистема бухгалтерского и планово-финансового учета вуза;

– подсистема организации дистанционного обучения и тестирования студентов.

Вместе с этим, учитывая, что создаются такие системы в течение длительного времени и предназначены для решения различных задач, технологии обеспечения безопасности в них или вообще отсутствуют, или же являются слишком устаревшими (Фишер, 1985).

Ввиду этого, вуз стремится к созданию надежной и эффективной системы защиты собственных ресурсов. К системе защиты вуза прежде всего относятся информационные ресурсы, в том числе и поступающие из сети Интернет (Малюк, 2004).

В то же время вуз стремится к созданию эффективной системы защиты информации, которая накапливается, обрабатывается и хранится с использованием технических возможностей ИТС вуза и подлежит защите в соответствии с требованиями действующего законодательства России (например, персональных данных научно-педагогических работников, обслуживающего персонала и студентов от несанкционированных действий) (Петров, 2017).

Результаты и обсуждение

С учетом этого технология создания в вузах России системы ИКБ, на наш взгляд, должна сочетать следующие основные этапы:

1) во-первых, проведение обследования вуза как объекта информационной деятельности;

2) во-вторых, разработка технорабочего проекта СИКБ вуза;

3) в-третьих, создание комплекса технической защиты информации, проведение предварительных испытаний и опытной эксплуатации СИКБ вуза;

4) в-четвертых, проведение государственной экспертизы СИКБ вуза (как для АС класса “3”) и сопровождение СИКБ вуза в течение ее жизненного цикла.

Обследование вуза, как ОИД проводится с целью проверки их на предмет наличия:

– планов ОИД с элементами электропитания, заземления, размещения АТС, телефонных кабелей и аппаратов, пожарной и охранной сигнализации по этажам;

– документов по системе охраны и контроля доступа к ОИД;

– документов, содержащих описание общей структурной схемы ИТС вуза: перечень и состав оборудования, технических и программных средств; оборудования связи, технических и

программных средств; особенности конфигурации, архитектуры и топологии ИТС; таблицы адресации ресурсов и компонент ИТС, таблицы маршрутизации и коммутации (Белов, 2006);

– документов, которые определяют виды и характеристики каналов связи ИТС;

– документов, определяющих особенности взаимодействия отдельных компонентов ИТС (взаимное влияние друг на друга, взаимное влияние при взаимодействии с ресурсами глобальной сети Интернет);

– документов на существующие средства контроля доступа к помещениям, где циркулирует (находится) информация, которая подлежит защите, а также системы и технологии, ограничивающие доступ пользователей ИТС к определенным ресурсам ИТС и наружных сетей; − документов на подсистемы и компоненты ИТС (технические, программные, программно-аппаратные и тому подобное), которые являются средствами защиты информации и/или содержат механизмы защиты информации, потенциальные возможности этих средств и механизмов, их свойства и характеристики (Бриллюэн, 1966);

– документов, регламентирующих схемы информационных потоков каждого элемента ИТС, состав информационных объектов, режим доступа к ним, возможное влияние на него элементам среды пользователей, физической среды;

– документов об учете и порядке использования носителей информации в ИТС;

– описания специальных программных средств (подсистемы антивирусной защиты, подсистемы электронного документооборота и т. д) по регламенту технологии обработки информации в ИТС и обращения электронных документов;

– действующих лицензий на программные средства, используемые в ИТС;

– проектной и эксплуатационной документации на ИТС, в частности на установленное гетерогенное сетевое оборудование и системы его защиты (межсетевые экраны), а также другие программно-аппаратные средства системы (Конахович, 2021).

По результатам обследования должно быть:

1) восстановлены недостающие / утраченные документы, планы и описания или же внесены изменения в устаревшие;

2) сформирован «Перечень сведений, подлежащих автоматизированной обработке и соответственно норм права нуждается в защите».

3) сформирован «Перечень служебной информации, персональных данных и открытой информации, которая накапливается, обрабатывается и хранится в структурных подразделениях вуза»;

4) сформирован «Перечень угроз информации, обрабатываемой в ИТС вуза».

5) формализованы требования к перспективной СИКБ вуза. Определены условия и пути реализации: оперативно-тактических и системотехнических требований к СИКБ вуза в целом, а также требований к подсистемам СИКБ вуза;

6) разработан проект варианта концепции СИКБ вуза, ключевыми элементами которого должны быть:

a) во-первых, требования по базовому обеспечению ИКБ в вузе, а именно к:

– авторизованных и неавторизованных программно-аппаратных средств и средств управления уязвимостями;

– защищенных конфигураций мобильных устройств, ноутбуков, рабочих станций и серверов и т. п;

b) во-вторых, требования по применению лучших практик в сфере ИКБ отношении:

– защиты электронной почты и Web-бразера;

– защиты от воздействия вредоносных программ;

– обследование и контроля сетевых портов;

– возможности восстановления потерянных данных;

– защищенных конфигураций для сетевых устройств (файерволов, роутеров, коммутаторов);

– защиты периметра и данных;

– контроля доступа и контроля учетных записей и тому подобное;

с) в-третьих, требования в отношении организационных процессов и административных мер, связанных с обеспечением информационной и кибербезопасности вуза, а именно к:

– процедур контроля уровня осведомленности персонала и прикладного программного обеспечения;

– технологий реагирования на инциденты и процедур тестирования на проникновение и тому подобное.

Угрозы информации в ИТС вузы могут иметь как субъективную, так и объективную природу. Источником угроз субъективного характера могут быть преднамеренные или непреднамеренные действия лиц, которые могут иметь удаленный доступ к ресурсам ИТС с использованием канала доступа к сети Интернет или физический доступ в помещения, где размещена ИТС или к ее машинным носителям информации.

К угрозам объективного характера относятся:

– изменение условий физической среды (влажность, запыленность, колебания температуры). Источник угрозы-природные явления. Последствия-нарушение целостности, доступности;

– сбои и отказы в работе оборудования и технических средств. Источник угрозы-аппаратура.

Последствия – нарушение целостности, доступности, наблюдения.

Политика безопасности должна доказательно давать гарантии того, что в вузе обеспечивается:

– адекватность уровня защиты информации уровню ее критичности;

– рентабельность реализации мер защиты информации;

– оценка и проверка уровня защищенности информации;

– персонификация положений политики безопасности (в отношении субъектов вуза);

– отчетность (Регистрация, аудит) для всех критических с точки зрения безопасности ресурсов;

– доступ персонала и пользователей ко всем документам, которые регламентируют порядок защиты информации и обеспечивают их строгое соблюдение;

– непрерывная работа средств ИТС и возможность ее возобновления в случае возникновения непредвиденных ситуаций.

Политика информационной безопасности является частью общей ПБ вуза. Ее построение предполагает определение структуры ценности и проведение анализа риска, а также определение правил для любого процесса пользования определенным видом доступа к элементам информации, которые охватывают круг вопросов, связанных с оценкой ценностей (Ярочкин, 2018).

Подэтап №2.2. Разработка Технического задания на создание СИКБ вуза.

Техническое задание должно определять требования:

1) в организационных мерах и комплекса средств защиты (КСЗ) ИТС вуза, обеспечивающих безопасность информации на всех этапах ее жизненного цикла, а также требования к порядку их разработки, создания и внедрения;

2) в отношении разработки и реализации политики информационной безопасности в ИТС вуза, то есть такого функционального профиля защищенности информации от НСД, который за счет применения КЗЗ и набора определенных правил будет отвечать критериям гарантий, например, на уровне Г-2 и обеспечит ОИД необходим и/или достаточный уровень услуг по конфиденциальности информации в доступности.

Этапы №3 - №5. Создание комплекса технической защиты информации, проведение предварительных испытаний, опытной эксплуатации и государственной экспертизы СИКБ вуза (как для АС класса “3”)

Этапы №6 - №7. Проведение государственной экспертизы СИКБ вуза (как для АС класса “3”) и ее сопровождение в течение жизненного цикла.

Заключение

В статье рассмотрена технология создания в вузе системы ИКБ, направленной на комплексное управление состоянием защиты информационных и ИТ-ресурсов вуза от несанкционированных действий, которые могут привести к нарушению их целостности и доступности, в том числе с использованием компьютерных вирусов, а также всестороннего обеспечения процесса функционирования системы.

С этой целью в работе предложено:

- во-первых, проводить обследование вуза как объекта информационной деятельности;
- во-вторых, разрабатывать технорабочий проект СИКБ вуза;
- в-третьих, создавать комплекс технической защиты информации, проводить предварительные испытания и опытную эксплуатацию СИКБ вуза;
- в-четвертых, проводить государственную экспертизу СИКБ вуза (как для АС класса “3”) и сопровождать СИКБ вуза в течение ее жизненного цикла (Романец, 2011).

Система информационной и кибербезопасности вуза, созданная с соблюдением предложенной технологии, обеспечит: идентификацию и аутентификацию пользователей; управление и контроль доступа пользователей к ресурсам ИТС вуза; блокирование несанкционированных действий и предотвращения возможностям реализации угроз нарушения целостности и доступности информации; предотвращения инфицирования АРМ ИТС вуза компьютерными вирусами и их дальнейшего распространения с использованием съемных носов информации; обеспечение регистрации данных о событиях, происходящих в системе и касаются безопасности информации.

Дальнейшие исследования будут ориентированы на формирование общей модели построения системы ИКБ вуза с учетом: рекомендаций GDPR как стандарту ЕС по защите персональных данных; организационно-технических аспектов взаимодействия элементов системы ИКБ вуза по доступу к авторизованных и Web-ресурсов; ротации контингента студентов и сотрудников вуза; необходимости защиты критически важных сегментов вуза, прежде всего таких, как бухгалтерия, отдел кадров, режимно-секретный орган и др; необходимость мониторинга новых угроз, определение рисков и уровней их интенсивности.

Вместе с этим планируется рассмотреть возможность адаптации к применению в системе ИКБ вуза подсистемы передачи и архивации изображений PACS (Picture Archiving and Communication System) как потенциально возможного предохранителя несанкционированного доступа к сети на территории вуза.

Список литературы

1. Белов Е.Б. и др. Основы информационной безопасности. Учебное пособие для вузов. - М.: Горячая линия-Телеком, 2006. 544 с.
2. Бриллюэн Л. Научная неопределенность и информация. М., 1966. 271 с.
3. Винер Н. Кибернетика или Управление и связь в животном и машине /2-е изд. М.: Советское радио, 2018. 201 с.
4. Глушков В.М. Основы безбумажной информатики. М.: Наука, 2017. 552 с.
5. Колмогоров А.Н. Три подхода к определению понятия «количество информации» // Проблемы передачи информации. 2015. Т. 1. Вып. 1. С. 25-38.
6. Конахович Г.Ф., Климчук В.П., Паук С.М., Потапов В.Г. Защита информации в телекомуникационных системах. К.: «МК-Пресс», 2021. 288 с.
7. Макарова Н.В. Информатика, М.: Финансы и статистика, 2000. 768 с.
8. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб. пособие для вузов. М.: Горячая линия-Телеком, 2004. 280 с.
9. Петров А.А. Компьютерная безопасность. Криптографические методы защиты. М.: ДМК, 2017. 448 с.
10. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях // Под ред. В. Ф. Шаньгина. М.: Радио и связь, 2011. 376 с.
11. Фишер Р. Статистические методы для исследователей, М. 1985. 276 с.

12. Шеннон К. Работы по теории информации и кибернетике / Под ред Р. Л. Добрушина, О. Б. Лупанова. М.: Изд-во иностр. лит-ры, 2013. 829 с.
13. Эшби У.Р. Введение в кибернетику. М., 2019.
14. Ярочкин В.И. Информационная безопасность. Учебное пособие. М.: Междунар. отношения, 2018. 400 с.

Information and cybersecurity technology in higher education institutions

Alexandr S. Oleinik
student
National Research Nuclear University MEPhI (Moscow Engineering Physics Institute)
Moscow, Russia
sasha010698z@yandex.ru
0000-0002-8021-3799

Viktor M. Gerasimov
student
ITMO University
Moscow, Russia
my.virus.kaspersky@gmail.com
0000-0002-3830-5155

Farid K. Nadirovich
student
Bauman Moscow state technical university
Moscow, Russia
fkhalilullin@gmail.com
0000-0000-0000-0000

Iuliia M. Gainulova
student
Saint Petersburg State University
Saint Petersburg, Russia
julia12111990@mail.ru
0000-0000-0000-0000

Denis S. Kalinin
student
Moscow State University of Civil Engineering
Moscow, Russia
denis312578465@mail.ru
0000-0000-0000-0000

Received 16.04.2022
Accepted 07.05.2022
Published 20.06.2022

10.25726/v6109-4146-3543-s

Abstract

Today, with the widespread availability of the Internet and the rapid development of communications, there is a very noticeable gap in the expectations of students and the opportunities that higher education institutions (universities) in Russia can offer them. Under these conditions, the forms and methods of educational activities in domestic universities should be constantly updated depending on the information needs and technological development of society. At the same time, ensuring information and cybersecurity of both educational materials and other restricted access information, as well as the IT infrastructure itself from accidental or targeted attacks, should not be the last place in this process. The implementation of these tasks is complicated by the fact that Russian universities are currently undergoing a period of adaptation not only to the objective processes of the information society, but also to new socio-political conditions with diverse manifestations of competition.

Keywords

software, cybersecurity, university, information.

References

1. Belov E.B. i dr. Osnovy informacionnoj bezopasnosti. Uchebnoe posobie dlja vuzov. - M.: Gorjachaja linija-Telekom, 2006. 544 s.
2. Brilljujen L. Nauchnaja neopredelennost' i informacija. M., 1966. 271 s.
3. Viner N. Kibernetika ili Upravlenie i svjaz' v zhivotnom i mashine /2-e izd. M.: Sovetskoe radio, 2018. 201 s.
4. Glushkov V.M. Osnovy bezbumazhnoj informatiki. M.: Nauka, 2017. 552 s.
5. Kolmogorov A.N. Tri podhoda k opredeleniju ponjatija «kolichestvo informacii» // Problemy peredachi informacii. 2015. T. 1. Vyp. 1. S. 25-38.
6. Konahovich G.F., Klimchuk V.P., Pauk S.M., Potapov V.G. Zashhita informacii v telekomunikacionnyh sistemah. K.: «MK-Press», 2021. 288 s.
7. Makarova N.V. Informatika, M.: Finansy i statistika, 2000. 768 s.
8. Maljuk A.A. Informacionnaja bezopasnost': konceptual'nye i metodologicheskie osnovy zashhity informacii. Ucheb. posobie dlja vuzov. M.: Gorjachaja linija-Telekom, 2004. 280 s.
9. Petrov A.A. Komp'juternaja bezopasnost'. Kriptograficheskie metody zashhity. M.: DMK, 2017. 448 s.
10. Romanec Ju.V., Timofeev P.A., Shan'gin V.F. Zashhita informacii v komp'juternyh sistemah i setjah // Pod red. V. F. Shan'gina. M.: Radio i svjaz', 2011. 376 s.
11. Fisher R. Statisticheskie metody dlja issledovatelej, M. 1985. 276 s.
12. Shennon K. Raboty po teorii informacii i kibernetike / Pod red R. L. Dobrushina, O. B. Lupanova. M.: Izd-vo inostr. lit-ry, 2013. 829 s.
13. Jeshbi U.R. Vvedenie v kibernetiku. M., 2019.
14. Jarochkin V.I. Informacionnaja bezopasnost'. Uchebnoe posobie. M.: Mezhdunar. otnoshenija, 2018. 400 s.