Научная статья
УДК 621.391
DOI: 10.25688/2072-9014.2023.63.1.03

АНАЛИЗ УГРОЗ И РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ВУЗЕ

Оксана Николаевна Ромашкова[1],
Андрей Игоревич Каптерев[2] ✉

[1] Российская академия народного хозяйства и государственной службы при Президенте РФ, Москва, Россия,
ox-rom@yandex.ru, https://orcid.org/0000-0002-1646-8527

[2] Московский городской педагогический университет, Москва, Россия,
kapterevai@mgpu.ru ✉, https://orcid.org/0000-0002-2556-8028

Аннотация. Актуальность проблемы исследования обусловлена растущим воздействием угроз информационной безопасности эффективному и устойчивому функционированию информационных систем университетов. Современные информационные системы имеют достаточно сложную объектную структуру, а также предполагают многогранность понятий информационной безопасности. Цель исследования — выявление угроз информационной безопасности, присутствующих в информационных системах университетов. Задачи исследования: 1) проанализировать четыре категории данных угроз; 2) выделить потенциальные риски; 3) предложить модель потенциального нарушителя системы информационной безопасности вуза; 4) на основе построенной модели предложить контрмеры, снижающие риски до допустимых уровней.

Ключевые слова: информационная безопасность; потенциальные угрозы и риски; модель потенциального нарушителя; контрмеры, снижающие риски.

Original article
UDC 621.391
DOI: 10.25688/2072-9014.2023.63.1.03

ANALYSIS OF THREATS AND RISKS OF INFORMATION SECURITY AT THE UNIVERSITY

Oxana N. Romashkova[1],
Andrey I. Kapterev[2] ✉

[1] The Russian Presidential Academy of National Economy and Public Administration,
Moscow, Russia,
ox-rom@yandex.ru, https://orcid.org/0000-0002-1646-8527

[2] Moscow City University,
Moscow, Russia,
kapterevai@mgpu.ru ✉, https://orcid.org/0000-0002-2556-8028

Abstract. The relevance of the research problem is due to the growing impact of threats to information security to the effective and sustainable functioning of university information systems. Modern information systems have a rather complex object structure, and also assume the versatility of the concepts of information security. The purpose of the study is to identify threats to information security present in the information systems of universities. Research objectives: 1) analyze four categories of these threats; 2) identify potential risks; 3) to propose a model of a potential violator of the information security system of the university; 4) on the basis of the constructed model to propose countermeasures that reduce risks to acceptable levels.

Keywords: information security; potential threats and risks; the model of a potential violator; countermeasures that reduce risks.

Для цитирования: Ромашкова, О. Н., Каптерев, А. И. (2023). Анализ угроз и рисков информационной безопасности в вузе. *Вестник МГПУ. Серия «Информатика и информатизация образования», 1*(63), 37–47. DOI: 10.25688/2072-9014.2023.63.1.03

For citation: Romashkova, O. N., & Kapterev, A. I. (2023). Analysis of threats and risks of information security at the university. *MCU Journal of Informatics and Informatization of Education, 1*(63), 37–47. https://doi.org/10.25688/2072-9014.2023.63.1.03

Введение

В настоящее время технологии анализа рисков информационной безопасности в России развиты недостаточно. Это связано с тем, что в российских нормативных документах аспект угроз информационной безопасности, рисков, их допустимый уровень и ответственность за принятие определенного уровня рисков разработаны мозаично, а не системно. Современные информационные системы имеют достаточно сложную объектную структуру, а также предполагают многогранность понятий информационной безопасности. Для описания модели угроз целесообразно

использовать различные методологии автоматизации данного процесса. В зависимости от своего класса информационная система должна обладать подсистемой безопасности с определенными формальными требованиями. Переход российской экономики к шестому технологическому укладу оказывает значительное влияние на различные сферы жизнедеятельности человека, особенно на образование и науку.

Развитие общества в целом и различных стран в частности неразрывно связано с применением цифровых технологий. С одной стороны, информационные, цифровые технологии позволяют значительно повысить эффективность производства и деятельности организаций, с другой — накладывают свои ограничения, а также вызывают новые риски для отдельного человека, организации и государства. Спектр возможностей и инструментарий злоумышленников в киберсреде неуклонно расширяются [1].

Информационные, цифровые технологии, используемые любой организацией, со временем становятся ее главной ценностью. При этом большая доля инцидентов информационной безопасности связана с нарушением таких ее ключевых атрибутов, как целостность, конфиденциальность и доступность. К наиболее распространенным видам воздействий относятся: фишинговые атаки; выдача себя за сотрудника организации; применение вирусного и другого вредоносного программного обеспечения. Потеря или хищение данных, в том числе персональных, приводит к репутационным и финансовым потерям: материальному ущербу и утрате доверия со стороны контрагентов как к самой организации, так и к ее инновациям, что может крайне негативно сказаться на деятельности организации.

Проблема цифровой трансформации образования и внедрения новых информационных технологий в отечественных вузах стоит особенно остро в связи с возрастающими требованиями к качеству, объему и темпам образовательного процесса и неудовлетворенностью существующей структурой квалификаций в высшем образовании. В процессе внедрения и функционирования механизмов дистанционного образования первостепенной является задача обеспечения информационной безопасности. Практическая значимость нашего исследования состоит в том, что его результаты могут быть применены для обеспечения информационной безопасности образовательного процесса с использованием дистанционных технологий в вузе, а также для разработки и оценки эффективности соответствующих информационных систем.

Методы исследования

В последние годы ученые интенсивно изучают проблемы цифровизации и цифровой трансформации образования [2–4]. Это принципиально новое явление в развитии современного социума, перспективы и риски которого изучены в недостаточной степени. Для адекватной оценки данного феномена его необ-

ходимо рассматривать в неразрывном единстве с изменениями, происходящими в важнейших сферах социального функционирования: экономике, политике, науке, культуре. В целом в условиях высокой цифровой взаимозависимости между различными экономическими агентами создание защищенной информационной среды становится важным фактором формирования устойчивой цифровой экономики [5–6] и сохранения конкурентоспособности. Правильно выстроенная стратегия информационной безопасности позволяет сохранить конкурентоспособность компании, обеспечивает защищенность протекающих в ней процессов, а значит, способствует повышению эффективности ее деятельности.

Для современных условий идеальная система информационной безопасности, с одной стороны, не должна быть помехой для основных бизнес-процессов организации, способствуя их развитию, а с другой — должна надежно выявлять и блокировать все неэффективные и убыточные процессы.

Таким образом, современная система информационной безопасности должна отвечать следующим основным требованиям:

1. ***Интеграция.*** Надежная система информационной безопасности должна быть интегрирована в информационную инфраструктуру и систему управления предприятием. Навесные системы удовлетворительно работают при защите инфраструктуры, но для защиты процессов необходима интеграция. Таким образом, информационная безопасность превращается не в отдельную функцию, а в качественное свойство бизнес-процесса. Подобная трансформация информационной безопасности потребует от специалистов глубокого понимания не только технологий защиты информации, но и знания предметной области, в которой реализуется процесс, будь то финансы, производство, исследования, логистика или продажи.

2. ***Адаптация.*** Цифровизация предполагает постоянные изменения автоматизированных процессов, быструю их адаптацию под требования бизнеса. Поэтому информационная безопасность как свойство процесса должна перестраиваться не апостериорно, а непосредственно в ходе изменений. Сегодня при обеспечении информационной безопасности сначала создается объект защиты (например, бизнес-приложение), потом тестируется его защищенность, далее исправляются замечания, снова тестируется объект и т. д. Столь долгий путь не удовлетворяет требованиям стремительно происходящих изменений.

3. ***Ориентация на бизнес-задачи.*** Кибербезопасность оперирует следующими техническими характеристиками: мощность DDoS-атаки; количество вирусов, уязвимостей, инцидентов. Для бизнеса такая информация не является внятной, поскольку ее нельзя конвертировать в величину убытков или упущенной выгоды. Поэтому подходы информационной безопасности должны быть трансформированы с ориентацией в первую очередь не на источники угроз, а на защищаемый объект. Это не только смещение фокуса, но и смещение самой парадигмы информационной защиты: при таком подходе для бизнеса неважно, кто или что может нарушить процесс — хакер, инсайдер, мошенник, неквалифицированный оператор или сбой компьютера. Ответственные

за информационную безопасность должны будут отвечать за полное плановое выполнение процесса вне зависимости от причины нарушения.

Результаты исследования

Модель потенциального нарушителя. Важным этапом анализа угроз является создание модели потенциального нарушителя и сценариев его поведения: описание категорий лиц, к которым может принадлежать нарушитель; его мотивы; квалификация; характер возможных действий. К внутренним нарушителям относятся лица из числа сотрудников организации, к внешним — клиенты, поставщики, конкуренты [7]. Список потенциальных нарушителей зависит от сферы деятельности организации. Цели у нарушителей могут быть различными, например угроза экономической, информационной или физической безопасности организации. Соответственно, учет потенциальных угроз различного характера позволяет организации подготовиться к их предотвращению, реагированию на непредвиденные инциденты, а также выработать у сотрудников необходимые нормы поведения, обеспечивающие безопасное функционирование организации в условиях потенциальных опасностей.

Действия злоумышленника по добыванию информации, так же как и других материальных ценностей, определяются поставленными целями и задачами, его мотивами, квалификацией и технической оснащенностью. При моделировании системы защиты необходимо выяснить с максимально возможной достоверностью, кому нужна защищаемая информация.

Методика выявления и анализа существующих рисков информационной безопасности. Поскольку циркулирующие в подразделениях вуза сведения об обучающихся, а также о тьюторах представляют собой персональные данные, текущие принципы их хранения и передачи могут привести к их утере или хищению, что является фундаментальным нарушением, которое чревато репутационными потерями для вуза в целом. Помимо этого, подобный механизм обработки информации может привести к нарушению ее целостности и, следовательно, к ошибкам в работе подразделений. Также необходимо осуществить качественную защиту хранимых данных от вредоносных кодов и программ. Для предотвращения нарушения конфиденциальности и целостности информации, циркулирующей в подразделениях вуза, необходимо внедрение и использование в бизнес-процессах защищенной информационной системы.

Мы проанализировали информацию, циркулирующую в подразделениях вуза. Нами были выделены следующие виды данных, требующих защиты от нарушения конфиденциальности[1]:

[1] Путин, В. (2006, 28 июля). Федеральный закон о персональных данных. Дата подписания: 27.07.2006. Опубликован: 28.07.2006. Вступает в силу: 26.01.2007. *Российская газета.* Федеральный выпуск. 2006. 28 июля. URL: https://rg.ru/documents/2006/07/29/personaljnye-dannye-dok.html (дата обращения: 10.08.2022).

– сведения об обучающихся;
– сведения о тьюторах.

Также были выделены виды данных, требующих защиты от нарушения целостности:

– сведения об обучающихся;
– сведения о тьюторах;
– отчеты об экспертизах;
– федеральные государственные образовательные стандарты;
– информационно-образовательные ресурсы;
– учебно-методические рекомендации;
– учебно-методические материалы;
– сведения об учебных модулях и учебных курсах;
– результаты проверки знаний обучающихся.

Модель нарушителя информационной безопасности представлена в таблице 1.

Таблица 1

Модель нарушителя информационной безопасности

Тип	Категория	Подготовленность		Осведомленность
		Психофизическая	Техническая	
Внешний	Первая	Высокая	Высокая	Высокая
	Вторая	Средняя	Средняя	Средняя
	Третья	Низкая	Низкая	Низкая
Внутренний	Четвертая	Средняя	Средняя	Высокая

Тип нарушителя определяется в зависимости от его отношения к объекту защиты. Мы выделили четыре категории нарушителей информационной безопасности.

Категория нарушителя в общем виде определяет его положение:

✓ к первой категории относятся лица, имеющие профессиональные навыки в области несанкционированной добычи и хищения защищаемой информации. Действуют как в интересах государства, так и в собственных интересах;

✓ ко второй категории принадлежат лица, нанятые злоумышленником, намеренно осуществляющие несанкционированные действия по получению доступа к защищаемой информации;

✓ к третьей категории причисляются лица, преследующие корыстные или вандальные цели. Чаще всего они не обладают специальными навыками и не подготовлены к проникновению предварительно;

✓ к четвертой категории относятся лица, являющиеся непосредственными сотрудниками объекта защиты и взаимодействующие со злоумышленником либо по своей воле, либо по принуждению [8].

Проанализировав полученные данные, можно заключить, что самую большую угрозу несет внешний нарушитель первой категории в связи с высокой подготовленностью и осведомленностью. Однако относительно защищаемых данных, циркулирующих в вузе, гораздо большую значимость имеет угроза

со стороны внешнего нарушителя второй категории и внутреннего нарушителя четвертой категории.

Проведенный анализ показал, что основными угрозами информационной безопасности являются следующие:

– угроза автоматического распространения вредоносного кода в грид-системе;
– угроза внедрения вредоносного кода в BIOS;
– угроза внедрения кода или данных;
– угроза воздействия на программы с высокими привилегиями;
– угроза деструктивного изменения конфигурации / среды окружения программ;
– угроза доступа к защищаемым файлам с использованием обходного пути;
– угроза изменения компонентов информационной (автоматизированной) системы;
– угроза искажения вводимой и выводимой на периферийные устройства информации;
– угроза использования альтернативных путей доступа к ресурсам;
– угроза использования информации идентификации/аутентификации, заданной по умолчанию;
– угроза неправомерного ознакомления с защищаемой информацией;
– угроза неправомерных действий в каналах связи;
– угроза несанкционированного доступа к аутентификационной информации;
– угроза несанкционированного копирования защищаемой информации;
– угроза несанкционированного удаления защищаемой информации;
– угроза перехвата вводимой и выводимой на периферийные устройства информации;
– угроза преодоления физической защиты;
– угроза утраты носителей информации;
– угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации;
– угроза распространения «почтовых червей»;
– угроза фишинга;
– угроза несанкционированной модификации защищаемой информации;
– угроза внедрения вредоносного кода через рекламу, сервисы и контент;
– угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет;
– угроза утечки информации с неподключенных к сети Интернет компьютеров;
– угроза несанкционированного доступа к системе при помощи сторонних сервисов.

На основе проведенного анализа угроз были выявлены основные риски информационной безопасности [9]. Мы выделили и проанализировали шесть групп рисков:

1. Риски сред и инфраструктуры:

– отсутствие физической защиты зданий, дверей и окон (риск кражи защищаемой информации);

– неправильное или халатное использование физических средств управления доступом в здания, помещения (риск намеренного повреждения);

– нестабильная работа электросети (риск колебаний напряжения).

2. Риски аппаратного обеспечения:

– подверженность колебаниям напряжения (риск возникновения колебаний напряжения);

– подверженность температурным колебаниям (возможен, например, риск возникновения экстремальных значений температуры);

– чувствительность к воздействию электромагнитного излучения (возможен, например, риск воздействия электромагнитного излучения).

3. Риски программного обеспечения:

– отсутствие механизмов идентификации и аутентификации, например аутентификации пользователей (риск нелегального проникновения злоумышленников под видом законных пользователей);

– отсутствие аудиторской проверки (риск использования программного обеспечения несанкционированным способом);

– плохое управление паролями (легко определяемые пароли, хранение в незашифрованном виде, недостаточно частая замена паролей);

– неправильное присвоение прав доступа (риск использования программного обеспечения несанкционированным способом);

– неконтролируемая загрузка и использование программного обеспечения (риск столкновения с вредоносным программным обеспечением);

– отсутствие документации (возможен, например, риск ошибки операторов);

– отсутствие резервных копий (риск воздействия вредоносного программного обеспечения или пожара).

4. Риски коммуникаций:

– незащищенные линии связи (риск перехвата информации);

– отсутствие идентификации и аутентификации отправителя и получателя (риск нелегального проникновения злоумышленников под видом законных пользователей);

– незащищенные потоки конфиденциальной информации (риск перехвата информации).

5. Риски, связанные с документами и документооборотом:

– хранение в незащищенных местах (риск хищения);

– недостаточная внимательность при уничтожении (риск хищения);

– бесконтрольное копирование (риск хищения).

6. Риски, связанные с сотрудниками вуза:

– недостаточная подготовка персонала по вопросам обеспечения безопасности (риск ошибки операторов);

– отсутствие необходимых знаний по вопросам безопасности (риск ошибок пользователей);

– отсутствие политики правильного пользования телекоммуникационными системами для обмена сообщениями (риск использования сетевых средств несанкционированным способом).

Заключение

Проблема обеспечения защиты информации в целом является одной из важнейших для устойчивого функционирования информационной структуры вуза, а также для минимизации рисков. В целях организации защиты информации необходимо использовать как нормы и правила в области информационной безопасности, так и программно-технические средства. Вопросы эффективной антивирусной защиты сегодня как никогда актуальны для корпоративного сектора и частных пользователей.

Однако проблемы и задачи, стоящие перед организациями, в том числе перед учебными заведениями, намного серьезнее и требуют решений иного уровня. Локальные сети — один из основных источников распространения вирусов [10]. Если не принимать необходимых мер защиты, то зараженная рабочая станция при входе в сеть может заразить один или несколько служебных файлов на сервере. Пользователи при входе в сеть запускают зараженные таким образом файлы. В качестве подобных служебных файлов может выступать программное обеспечение, установленное на сервере; стандартные документы-шаблоны или Excel-таблицы, применяемые в вузе. Решение данного вопроса достигается путем сочетания организационных и программно-технических мер.

Такой подход не требует больших технических и немедленных финансовых затрат, он может быть применен для комплексной антивирусной защиты локальной сети любого предприятия.

В физической модели содержится информация обо всех объектах базы данных. Физическая модель зависит от конкретной реализации системы управления базами данных (СУБД). Следовательно, одной и той же логической модели могут соответствовать несколько разных физических моделей. Если в логической модели не имеет значения, какой конкретно тип данных имеет атрибут, то в физической модели важно описать всю информацию о конкретных физических объектах: таблицах, колонках, индексах, процедурах и др. Разработанная трансформационная модель информационной системы содержит назначенные домены атрибутов сущностей и области допустимых значений, а также типы данных. На основе полученных сведений создана трансформационная модель, которая состоит из сущностей, атрибутов, их типов данных, ограничений контроля целостности и согласованности данных. Разработанные модели базы данных информационной системы далее могут быть реализованы в любой СУБД в зависимости от требований конкретной разработки.

Список источников

1. Каптерев, А. И. (2022). *Социальные эффекты и риски общего образования.* Монография. Москва: Book-expert. 281 с.
2. Pettersson, F. (2018). On the issues of digital competence in educational contexts — a review of literature. *Educ. Inf. Technol., 23,* 1005–1021.
3. Уваров, А. Ю. (2018). *Образование в мире цифровых технологий: на пути к цифровой трансформации.* Москва: Издательский дом ГУ-ВШЭ. 168 с.
4. Никулина, Т. В., Стариченко, Е. Б. (2018). Информатизация и цифровизация образования: понятия, технологии, управление. *Педагогическое образование в России, 8,* 107–113.
5. Асаул, В. В., Михайлова, А. О. (2018). Обеспечение информационной безопасности в условиях формирования цифровой экономики. *Теория и практика сервиса: экономика, социальная сфера, технологии, 34*(38), 5–10.
6. Каптерев, А. И. (2021). *Представление знаний в информационных системах.* Учебное пособие. Москва: Book-expert. 269 с.
7. Тихонов, В. А., Райх, В. В. (2019). *Информационная безопасность. Концептуальные, правовые, организационные и технические аспекты.* Москва: Гелиос АРВ. 528 с.
8. Romashkova, E. D., & Romashkova, O. N. (2021). International Training Programs IT Security System For Specialists in Onboard Systems. *Systems of Signals Generating and Processing in the Field of on Board Communications, Conference Proceedings,* 9416134.
9. Pavlicheva, E. N., & Romashkova, O. N. (2019). Model of Functioning of Information System for Institute of Distance of Specialists of Onboard Communications. *Systems of Signals Generating and Processing in the Field of on Board Communications,* 8706783.
10. Вострецова, Е. В. (2019). *Основы информационной безопасности.* Учебное пособие. Екатеринбург: Издательство Уральского университета. 204 с.

References

1. Kapterev, A. I. (2022). *Social effects and risks of general education.* Monograph. Moscow: Book-expert. 281 c. (In Russ.).
2. Pettersson, F. (2018). On the issues of digital competence in educational contexts — a review of literature. *Educ. Inf. Technol., 23,* 1005–1021. (In English).
3. Uvarov, A. Yu. (2028). *Education in the world of digital technologies: on the way to digital transformation.* Moscow: Publishing House of the Higher School of Economics. 168 p. (In Russ.).
4. Nikulina, T. V., & Starichenko, E. B. (2018). Informatization and digitalization of education: concepts, technologies, management. *Pedagogical Education in Russia, 8,* 107–113. (In Russ.).
5. Asaul, V. V., & Mikhailova, A. O. (2018). Ensuring information security in the context of the formation of the digital economy. *Theory and practice of the service: economy, social sphere, technology, 34*(38), 5–10. (In Russ.).
6. Kapterev, A. I. (2021). *Knowledge representation in information systems.* Textbook. Moscow: Book-expert. 269 p. (In Russ.).
7. Tikhonov, V. A., & Reich, V. V. (2019). *Information security. Conceptual, legal, organizational and technical aspects.* Moscow: Helios ARV. 528 p. (In Russ.).

8. Romashkova, E. D., & Romashkova, O. N. (2021). International Training Programs IT Security System For Specialists in Onboard Systems. *Systems of Signals Generating and Processing in the Field of on Board Communications, Conference Proceedings,* 9416134. (In Russ.).

9. Pavlicheva, E. N., & Romashkova, O. N. (2019). Model of Functioning of Information System for Institute of Distance of Specialists of Onboard Communications. *Systems of Signals Generating and Processing in the Field of on Board Communications,* 8706783. (In Russ.).

10. Vostretsova, E. V. (2019). *Fundamentals of information security.* Textbook. Ekaterinburg: Publishing House of the Ural University. 204 p. (In Russ.).

Статья поступила в редакцию: 26.09.2022;
одобрена после рецензирования: 01.11.2022;
принята к публикации: 05.12.2022.

The article was submitted: 26.09.2022;
approved after reviewing: 01.11.2022;
accepted for publication: 05.12.2022.

Информация об авторах / Information about authors:

Оксана Николаевна Ромашкова — доктор технических наук, профессор, профессор кафедры системного анализа и информатики, Институт экономики, математики и информационных технологий, Российская академия народного хозяйства и государственной службы при Президенте РФ, Москва, Россия.

Oxana N. Romashkova — Doctor of Technical Sciences, Professor, Professor of the Department of System Analysis and Informatics, Institute of Economics, Mathematics and Information Technology, The Russian Presidential Academy of National Economy and Public Administration, Moscow, Russia.

ox-rom@yandex.ru, https://orcid.org/0000-0002-1646-8527

Андрей Игоревич Каптерев — доктор социологических наук, доктор педагогических наук, профессор, профессор департамента информатизации образования, Институт цифрового образования, Московский городской педагогический университет, Москва, Россия.

Andrey I. Kapterev — Doctor of Sociological Sciences, Doctor of Pedagogical Sciences, Professor, Professor of the Department of Informatization of Education, Institute of Digital Education, Moscow City University, Moscow, Russia.

kapterevai@mgpu.ru ✉, https://orcid.org/0000-0002-2556-8028

Вклад авторов: все авторы сделали эквивалентный вклад в подготовку публикации. Авторы заявляют об отсутствии конфликта интересов.

Contribution of the authors: the authors contributed equally to this article. The authors declare no conflicts of interests.