Внутренние факторы информационной безопасности военного вуза

Яна Ивановна Бодина
студент
Волгоградский государственный университет
Волгоград, Россия
Yaboiv@ya.ru
0000-0000-0000-0000

Дмитрий Анатольевич Мясоедов
студент
Ивановский государственный энергетический университет имени В. И. Ленина
Иваново, Россия
tagri.200@yandex.ru
0000-0000-0000-0000

Антон Андреевич Васильев
студент
Московский Политехнический университет
Москва, Россия
Vasantadr@ya.ru
0000-0000-0000-0000

Михаил Васильевич Кудрин
студент
Национальный исследовательский университет ИТМО
Москва, Россия
Kudrinmva@ya.ru
0000-0000-0000-0000

Леон Артурович Лисикян
студент
Кубанский государственный медицинский университет
Краснодар, Россия
leonlisikan1263@gmail.com
0000-0000-0000-0000

Поступила в редакцию 10.04.2022
Принята 12.05.2022
Опубликована 20.06.2022

10.25726/c4914-3637-2087-d

Аннотация

Активное развитие глобальной экономической среды и национальных систем происходит в условиях интенсивного внедрения инновационных технологий. Интеграция высокотехнологичных электронных устройств в различные процессы на уровне стран, видов экономической деятельности, отдельных предприятий и в частном жизни населения приводит к генерации значительных объемов информации. Отдельное место в качестве источника генерирования данных занимает сеть Интернет, что служит инструментом создания, накопления и передачи информации. В указанных условиях

информация выступает в виде ресурса, который можно оценить в денежной форме исходя из специфики данных и спроса среди отдельных групп пользователей. Отдельные государства пытаются завладеть секретной информации других стран, компании используют промышленный шпионаж для получения секретной информации конкурентов, во многих случаях фиксируются случаи похищения персональной информации граждан с целью получения определенной выгоды и тому подобное. Приведенная ситуация приводит к разработке национальных стратегий защиты в сфере информационной безопасности и активной разработке специализированных продуктов, позволяющих с помощью аппаратного и программного обеспечения минимизировать потерю информационных ресурсов стран, компаний, граждан и тому подобное. Рынок представленных продуктов активно развивается и имеет значительный потенциал для роста, поскольку происходит непрерывная эволюция методов, которые нацелены на незаконное завладение коммерческой и частной информации.

Ключевые слова
военный вуз, ВВУЗ, защита информации, безопасность.

Введение

В отдельных случаях главной целью незаконно доступа к информации является блокирование доступа к ней владельцев или полное уничтожение данных, что негативно влияет на функционирование компании в целом или отдельных систем.

Исходя из международного опыта и ситуации в России, в первую очередь речь идет о хакерской атаке в 2017 г. через специализированное бухгалтерское программное обеспечение M.E.Doc, следует отметить активизацию государственных мер, которые ориентированы на предотвращение незаконного нарушения информационной безопасности.

Например, после хакерских атак в 2017 г. был создан Ситуационный центр обеспечения кибернетической безопасности. Правительством РФ 11 июля 2018 г. введено в действие распоряжение «Об утверждении плана мероприятий на 2018-2020 год по реализации Стратегии кибербезопасности РФ», а с сентября 2018 г. начинают рассматриваться предложений к плану мероприятий на 2019 год. Наряду с этим, важно уделять внимание решению вопросов информационной безопасности в отдельных видах экономической деятельности, в том числе в сфере образования.

Специфика функционирования учебных заведений предусматривает генерирование персональной информации учащихся, студентов и педагогических работников, баз данных с учебными материалами, текущей документации и тому подобное (Кашкароева, 2021). Для обеспечения эффективного функционирования учебных структур необходимо создать действенную систему защиты информации, которая позволит минимизировать риски потери или повреждения соответствующих данных.

Материалы и методы исследования

Анализ кибербезопасности ВВУЗА позволяет определить такие основные внутренние факторы, которые влияют на нее, а именно:

1. Подготовленность (обученность) личного состава.
2. Политика киберзащиты.
3. Топология (архитектура) информационного пространства.
4. Аппаратное обеспечение.
5. Программное обеспечение.

Соответственно, рассмотрим внутренние факторы более подробно.

Подготовленность (обученность) личного состава. В связи с геометрическим роста кибератак во всем мире перед различными субъектами государственных институтов, в том числе и ВВУЗ встает задача, по поиску рациональных решений по повышению эффективности их киберзащищенности.

К тому же проведенный анализ свидетельствует, что неосознанные действия (неосторожность и невнимательность) различной категории личного состава, которые прямо или косвенно влияют на

кибербезопасность ВВУЗ являются одной из главных причин снижения ее уровня (Правовое, 2008). При этом анализ неосознанных действий личного состава по отношению к киберзащите ВВУЗ свидетельствует, что предпосылкой их проявления были следующие причины:

– отсутствие ценностей и мотивации к соблюдению правил киберзащиты (отсутствие со стороны руководства действий по формированию у личного состава ВВУЗА ценностей и мотивации к выполнению правил киберзащиты при применении ИКТ в научно-педагогической деятельности, а также отсутствие понимания важности диагностика их уровня сформированности (Доктрина, 2016; Галатенко, 2008));

– низкий уровень образовательного, научного и методического обеспечения кибербезопасности образовательно-научной деятельности (фрагментированный подход к формированию у личного состава ВВУЗА компетентности киберзащиты или его отсутствие вообще; отсутствие исследований по проблемным вопросам связанных с обеспечением кибербезопасности личного состава в их образовательно-научной деятельности; отсутствие методической литературы с практическими примерами по киберзащите).

Рассмотрев причины неосознанных действий личного состава по отношению к киберзащите ВВУЗ, необходимо отметить, что без обеспечения ценностно-мотивационной подготовки личного состава достичь киберзащищенности не удастся (ФЗ «Об информации, 1995).

Результаты и обсуждение

Кроме того, вопросы подготовки по киберзащите являются системообразующим элементом обеспечения кибербезопасности ВВУЗ.

В частности, это связано с тем, что:

– во-первых, за внедрение ИКТ в образовательно-научную деятельность и обеспечение киберзащиты ВВУЗ отвечает отдельное техническое подразделение, от уровня подготовленности (компетентности) которого зависит качество выполнения задания по разработке политики киберзащиты ВВУЗ, которая должна учитывать организационно-правовые и инженерно-технические мероприятия, в частности: утверждение руководств, правил, ограничений, рекомендаций и инструкций на основе которой строится киберзащита ВВУЗ; возложение ответственности за развертывание и функционирование информационного пространства ВВУЗ; определение топологии (архитектуры) информационного пространства ВВУЗ и аппаратно-программного обеспечения которое будет установлено);

– во-вторых, от уровня подготовленности (компетентности) личного состава зависит кибербезопасность информационного пространства ВУЗА, а именно осознание или не осознание действий в отношении использования ИКТ в образовательно-научной деятельности, что может привести к киберугроз.

Отсюда можно сделать вывод, что проблема подготовки (обученности), как личного состава, так и специалистов в сфере киберзащиты ВВУЗА, актуальна как никогда и этому вопросу необходимо уделять первоочередное внимание.

Политика киберзащиты. Стоит отметить, что политика киберзащиты определяет совокупность установок, правил, ограничений, рекомендаций и инструкций, на основе которой строится киберзащита НЕМ, в частности, она должна учитывать организационно-правовые и инженерно-технические меры, а именно:

– юридическую ответственность определенного круга специалистов за развертывание и функционирование информационного пространства ВВУЗ;

– топологию (архитектуры) информационного пространства ВВУЗ, и аппаратно-программного обеспечения которое будет установлено;

– модель киберзащиты ВВУЗ;

– порядок использования информационного пространства ВВУЗ пользователями и соблюдение требований (правил) по киберзащите;

– порядок предоставления и использования прав доступа пользователей в системе информационного пространства ВВУЗ;

– требования отчетности пользователей информационного пространства ВВУЗ по возникновению киберинцидентов;

– план реагирования (мероприятий) пользователей информационного пространства ВВУЗ на случай киберинцидентов и т.д.

Следовательно, система киберзащиты ВВУЗ будет эффективной, если будут выполняться требования (правила) политики киберзащиты. Кроме того, прежде всего необходимо определить главную цель построения системы киберзащиты ВВУЗ, что должно выражаться через влияние совокупности внешних и внутренних факторов, которые влияют на нее (Указ Президента, 2000). Совокупность внешних и внутренних факторов является базисом (основой) для определения требований к системе киберзащиты ВВУЗ.

Без сомнения, разработка политики киберзащиты ВВУЗ является нетривиальной задачей. Эксперты (специалисты) киберзащиты должны не только знать соответствующие стандарты, иметь высокий уровень подготовленности (компетентности) и хорошо разбираться в комплексных подходах к обеспечению киберзащиты информационного пространства, но и, например, проявлять детективные способности при выявлении особенностей его построения (ФЗ «О персональных, 2006).

Кроме того, необходим постоянный анализ соответствия политики киберзащиты ВВУЗ реальному положению вещей, что крайне важно. По этой причине необходимо по совокупности показателей киберзащиты определить соответствующие критерии (отобрать своего рода «контрольные точки») и провести оценку состояния кибербезопасности, по результатам которого установить соответствие (несоответствие) политики киберзащиты заданным требованиям киберзащищенности и сделать соответствующие изменения в нее (Абрамова, 2020).

Топология (архитектура) информационного пространства. Построение информационного пространства ВВУЗ невозможно без определения ее топологии (архитектуры), которая будет определять способ размещения и соединения элементов ИКТ.

При этом, построение той или иной топологии (архитектуры) информационного пространства ВВУЗ влияет на (Зубалова, 2018):

– количество необходимого аппаратного (сетевого оборудования) и программного обеспечения для организации линий (каналов) связи;

– способ соединения аппаратных (сетевого оборудования) и различных по назначению элементов ИКТ;

– функциональные возможности аппаратного (сетевого оборудования) и программного обеспечения;

– возможность расширения информационного пространства;

– сегментацию (зоны) информационного пространства;

– способ управления информационным пространством;

– модель киберзащиты информационного пространства;

– финансовые расходы по закупке аппаратного (сетевого оборудования) и программного обеспечения.

Исходя из вышесказанного, можно сделать вывод, что чем сложнее топология (архитектура) информационного пространства ВВУЗ, тем сложнее задача обеспечения ее киберзащищенности, что в свою очередь влияет на кибербезопасность ВВУЗ в целом (Клевцова, 2018).

Аппаратное обеспечение. В настоящее время информатизация образовательно-научной деятельности ВВУЗ требует современного аппаратного обеспечения. Под аппаратным обеспечением будем понимать – специализированные вычислительные средства (устройства) или электронные (механические) его составляющие. Кроме того, современные тенденции свидетельствуют о необходимости иметь производительное аппаратное обеспечение, которое будет способно выполнять сложные нагрузки в условиях создания, обработки, передачи, хранения и киберзащиты циркулирующей информации (данных) в информационном пространстве ВУЗА.

Проведенный анализ аппаратного обеспечения позволяет определить следующие основные характеристики (показатели) его влияния на кибербезопасность ВВУЗ, а именно:

– установка (наличие) аппаратного обеспечения;
– актуальность (современность) аппаратного обеспечения;
– исправность аппаратного обеспечения;
– настройку аппаратного обеспечения.

При этом несоответствие хотя бы одной из характеристик влияния аппаратного обеспечения на кибербезопасность ВВУЗ создает предпосылки для снижения киберзащищенности ВВУЗ, то есть созданию уязвимости в информационном пространстве.

Поэтому, при оценке кибербезопасности ВВУЗ необходимо учитывать все вышеперечисленные характеристики влияния аппаратного обеспечения на кибербезопасность ВВУЗ.

Программное обеспечение. Следует отметить, что без использования программного обеспечения невозможно реализовать конечную цель-информатизацию образовательно-научной деятельности ВВУЗ. При этом каждый ВВУЗА использует в своей образовательно-научной деятельности такое программное обеспечение, как: операционные системы Microsoft Windows; редактор документов Microsoft Office; модульное объектно-ориентированная динамическая учебная среда Moodle; антивирусные программы ESET и т.д.

Вместе с тем, роль программного обеспечения заключается в управлении аппаратными составляющими разнообразного оборудования (устройств), создании, обработке, передаче, хранении и киберзащите циркулирующей информации (данных) в информационном пространстве ВВУЗ. К тому же аппаратное и программное обеспечение, взаимозависимы и дополняют друг друга (Тимошенко, 2016).

Проведенный анализ программного обеспечения позволяет определить следующие основные характеристики (показатели) его влияния на кибербезопасность ВВУЗ, а именно:

– установка (наличие) программного обеспечения;
– актуальность (современность) программного обеспечения;
– исправность программного обеспечения;
– настройку программного обеспечения.

Так же, как и с аппаратным обеспечение, несоответствие хотя бы одной из характеристик влияния программного обеспечения на кибербезопасность ВВУЗА создает предпосылки для снижения киберзащищенности ВВУЗА, то есть созданию уязвимости в информационном пространстве. Поэтому, при оценке кибербезопасности ВВУЗА необходимо учитывать все вышеперечисленные характеристики влияния программного обеспечения на кибербезопасность ВВУЗА (Шинина, 2019).

Благодаря сделанной декомпозиции можно определить ключевые особенности влияния внешних и внутренних факторов, которые вытекают, в частности:

1. Влияние внешних факторов на кибербезопасность ВВУЗА:

– наблюдается зависимость реализации различных типов кибератак от качества разработки и производства аппаратно-программного обеспечения соответствующего иностранного производителя, а именно наличие уязвимостей (умышленных или неумышленных);
– по критичности влияния внешних факторов на кибербезопасность ВВУЗА, чрезвычайные ситуации (естественная опасность) являются наиболее опасными (снизить эффективность их влияния почти нереально) по сравнению с другими внешними факторами (ФЗ «О защите, 2015).

2. Влияние внутренних факторов на кибербезопасность ВВУЗА:

– наблюдается зависимость всех факторов от подготовки (обученности) личного состава, в частности от компетентности специалистов зависит качество политики кибербезопасности, топологии (архитектуры) информационного пространства, аппаратного и программного обеспечения ВВУЗА. При этом, политика кибербезопасности ВВУЗА в будущем также косвенно может влиять на подготовку (обученность) личного состава, путем закрепления в ней юридического требования относительно постоянного формирования/развития знаний, умений и навыков по вопросам киберзащиты (Шинина, 2006).
– с критичностью влияния внутренних факторов на кибербезопасность ВВУЗА, подготовка (обученность) личного состава также занимает решающее значение, в частности она является

системообразующим элементом (без знаний невозможно решить любые имеющиеся проблемы, тем более вопросы обеспечения кибербезопасности ВВУЗА).

Таким образом, анализ внешних и внутренних факторов, должно стать предпосылкой для понимания текущего уровня кибербезопасности вашего ВВУЗ и принятия соответствующих управленческих решений по его повышению (ФЗ «О персональных, 2006).

Заключение

Проведенный анализ свидетельствует, что на кибербезопасность любого ВУЗА влияют внешние и внутренние факторы. На основе декомпозиции установлена взаимозависимость (критичность) влияния внешних и внутренних факторов на кибербезопасность ВВУЗ, что позволяет системно учесть всю причинно-следственную систему их связей. Обосновано, что заблаговременный анализ влияния внешних и внутренних факторов на кибербезопасность ВВУЗА позволит получить ситуационную осведомленность современного состояния кибербезопасности и принять руководству соответствующие управленческие решения.

Список литературы

1. Абрамова С.В., Бояров Е.Н., Храпаль Л.Р., Рубцова С.Ю. Информационная безопасность современного профессионального образования: проблемы, угрозы, пути решения // Современные проблемы науки и образования. 2020. № 6. http://science-education.ru/ru/article/ view?id=30339
2. Галатенко В.А. Основы информационной безопасности: учебное пособие. Под редакцией академика Ран В.Б. Бетелина. 4-е изд. М.: Интернет-Университет Информационных Технологий; БИНОМ. Лаборатория знаний, 2008. 205 с.
3. Доктрина информационной безопасности Российской Федерации № 646 от 05.12.2016 г.: https://rg.ru/2016/12/06/doktrina-infobezoba snost-site-dok.html
4. Зубалова О.А. Проблемы информационной безопасности образовательной среды в современных условиях // МНКО. 2018. № 3 (70). С. 36-38.
5. Кашкароева А.А., Атаканова Н.Э. Информационная безопасность в системе образования // International Journal of Humanities and Natural Sciences, vol.6, part 1. С. 167-172.
6. Клевцова А.М., Марачева А.В. Информационная безопасность в образовании: проблемы и перспективы // Вестник Калужского университета, 2018. № 3. С. 24-26.
7. Правовое обеспечение информационной безопасности: учебник. 2-изд., доп. М.: Маросейка, 2008. 368 с.
8. Тимошенко В.Н., Романова М.И., Казинец В.А., Стрелова О.Ю. Вакцинация от фальсификации. Хабаровск 2016. 95 с.
9. Указ Президента Российской Федерации от 10.01.2000 г.№ 24 «О Концепции национальной безопасности Российской Федерации» (Собрание законодательства Российской Федерации, 2000, № 2, ст. 170). http:// www.kremlin.ru/acts/bank/14927
10. Федеральный закон «Об информации, информатизации и защите информации» № 24-ФЗ от 20.02.1995 г. http://base.garant.ru/10103678/
11. Федеральный закон «Об информации, информатизации и защите информации «О персональных данных» № 152-ФЗ от 27.07.2006 г. http://www.consultant.ru/ document/cons_doc_LAW_61801/
12. Федеральный закон «Об информации, информатизации и защите информации «О персональных данных» № 152-ФЗ от 27.07.2006 г. https://base.garant. ru/12148567/
13. Федеральный закон «Об информации, информатизации и защите информации «О защите детей от информации, причиняющей вред их здоровью и развитию» № 438-ФЗ от 29.12.2010 г. (редакция от 29.06.2015 г.). http://www.consultant.ru/document/cons_ doc_LAW_108808/
14. Шинина М.В. Обеспечение информационной безопасности внутри организации // Образование и наука в России и за рубежом, № 10 (Vol. 58), 2019. https://www.gyrnal.ru/statyi/ ru/1659/

Internal factors of information security of a military university

Yana I. Bodina
student
Volgograd State University
Volgograd, Russia
Yaboiv@ya.ru
0000-0000-0000-0000

Dmitriy A. Myasoedov
student
Engineering University named after V. I. Lenin
Ivanovo, Russia
tagri.200@yandex.ru
0000-0000-0000-0000

Anton A. Vasil'ev
student
Moscow Polytechnic University
Moscow, Russia
Vasantadr@ya.ru
0000-0000-0000-0000

Mikhail V. Kudrin
student
ITMO National Research University
Moscow, Russia
Kudrinmva@ya.ru
0000-0000-0000-0000

Leon A. Lisikian
student
Kuban State Medical University
Krasnodar, Russia
leonlisikan1263@gmail.com
0000-0000-0000-0000

Received 10.04.2022
Accepted 12.05.2022
Published 20.06.2022

10.25726/c4914-3637-2087-d

Abstract

The active development of the global economic environment and national systems takes place in conditions of intensive introduction of innovative technologies. The integration of high-tech electronic devices into various processes at the level of countries, types of economic activity, individual enterprises and in the private life of the population leads to the generation of significant amounts of information. A separate place as a source of data generation is occupied by the Internet, which serves as a tool for creating, accumulating and transmitting information. Under these conditions, information acts as a resource that can be evaluated in

monetary form based on the specifics of the data and demand among individual user groups. Individual states are trying to get hold of the secret information of other countries, companies use industrial espionage to obtain the secret information of competitors, in many cases cases of theft of personal information of citizens for the purpose of obtaining certain benefits and the like are recorded. The above situation leads to the development of national protection strategies in the field of information security and the active development of specialized products that allow using hardware and software to minimize the loss of information resources of countries, companies, citizens, and the like. The market of the presented products is actively developing and has significant potential for growth, as there is a continuous evolution of methods that are aimed at the illegal acquisition of commercial and private information.

Keywords
military university, university, information protection, security.

References

1. Abramova S.V., Bojarov E.N., Hrapal' L.R., Rubcova S.Ju. Informacionnaja bezopasnost' sovremennogo professional'nogo obrazovanija: problemy, ugrozy, puti reshenija // Sovremennye problemy nauki i obrazovanija. 2020. № 6. http://science-education.ru/ru/article/ view?id=30339
2. Galatenko V.A. Osnovy informacionnoj bezopasnosti: uchebnoe posobie. Pod redakciej akademika Ran V.B. Betelina. 4-e izd. M.: Internet-Universitet Informacionnyh Tehnologij; BINOM. Laboratorija znanij, 2008. 205 s.
3. Doktrina informacionnoj bezopasnosti Rossijskoj Federacii № 646 ot 05.12.2016 g.: https://rg.ru/2016/12/06/doktrina-infobezoba snost-site-dok.html
4. Zubalova O.A. Problemy informacionnoj bezopasnosti obrazovatel'noj sredy v sovremennyh uslovijah // MNKO. 2018. № 3 (70). S. 36-38.
5. Kashkaroeva A.A., Atakanova N.Je. Informacionnaja bezopasnost' v sisteme obrazovanija // International Journal of Humanities and Natural Sciences, vol.6, part 1. S. 167-172.
6. Klevcova A.M., Maracheva A.V. Informacionnaja bezopasnost' v obrazovanii: problemy i perspektivy // Vestnik Kaluzhskogo universiteta, 2018. № 3. S. 24-26.
7. Pravovoe obespechenie informacionnoj bezopasnosti: uchebnik. 2-izd., dop. M.: Marosejka, 2008. 368 s.
8. Timoshenko V.N., Romanova M.I., Kazinec V.A., Strelova O.Ju. Vakcinacija ot fal'sifikacii. Habarovsk 2016. 95 s.
9. Ukaz Prezidenta Rossijskoj Federacii ot 10.01.2000 g.№ 24 «O Koncepcii nacional'noj bezopasnosti Rossijskoj Federacii» (Sobranie zakonodatel'stva Rossijskoj Federacii, 2000, № 2, st. 170). http:// www.kremlin.ru/acts/bank/14927
10. Federal'nyj zakon «Ob informacii, informatizacii i zashhite informacii» № 24-FZ ot 20.02.1995 g. http://base.garant.ru/10103678/
11. Federal'nyj zakon «Ob informacii, informatizacii i zashhite informacii «O personal'nyh dannyh» № 152-FZ ot 27.07.2006 g. http://www.consultant.ru/ document/cons_doc_LAW_61801/
12. Federal'nyj zakon «Ob informacii, informatizacii i zashhite informacii «O personal'nyh dannyh» № 152-FZ ot 27.07.2006 g. https://base.garant. ru/12148567/
13. Federal'nyj zakon «Ob informacii, informatizacii i zashhite informacii «O zashhite detej ot informacii, prichinjajushhej vred ih zdorov'ju i razvitiju» № 438-FZ ot 29.12.2010 g. (redakcija ot 29.06.2015 g.). http://www.consultant.ru/document/cons_ doc_LAW_108808/
14. Shinina M.V. Obespechenie informacionnoj bezopasnosti vnutri organizacii // Obrazovanie i nauka v Rossii i za rubezhom, № 10 (Vol. 58), 2019. https://www.gyrnal.ru/statyi/ ru/1659/