УДК 004.056

Л. П. Вовк, д-р техн. наук, Ю. А. Логвиненко

Автомобильно-дорожный институт
ГОУВПО «Донецкий национальный технический университет», г. Горловка

РИСКИ И УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЙ

В статье рассматриваются риски и угрозы информационной безопасности высших учебных заведений. Составлена классификация данных АДИ ГОУВПО «ДОННТУ», а так же для оценки данных рисков применен метод экспертных оценок. Исходя из этого выявлены наиболее важные риски. Предложен ряд рекомендаций по устранению рисков и их минимизации.

Ключевые слова: *риски, угрозы, безопасность, институт, данные, метод, эксперты, оценки, ранг*

Введение

Высшие учебные заведения – это учреждения, которые выполняют множество различных ролей, однако наиболее фундаментальными ролями являются исследования и образование. Они строятся вокруг информации: ее получения, хранения, обмена и применения. Это означает, что они сильно зависят от использования информационной системы. Многие университеты приняли во внимание важность информационных систем для выполнения своих обязанностей и включили их в свои учебные планы (Университет штата Сан-Франциско; Университет Лестера). Важность информации для университетов в целом хорошо известна [1]. Для эффективной и действенной работы учреждения такой обмен информацией следует поощрять и развивать.

Вопросы эффективного управления безопасностью в ИТ секторе занимались такие ученые, как С. Эллиот, У. Хасслер, Г. Стамен, В. А. Герасименко, А. А. Грушо, Е. Е. Тимонина, А. Ю. Щербаков, С. П. Расторгуев и другие [2].

В результате проведенного анализа было выявлено, что наряду с достаточно глубокой проработанностью данного вопроса недостаточно изучен механизм оценки угроз и рисков в Автомобильно-дорожном институте ГОУВПО «Донецкий национальный технический университет». В связи с этим данная работа в современных условиях является важной и актуальной задачей.

Цель исследования – классифицировать угрозы и оценить риски информационной безопасности высших учебных заведений на примере Автомобильно-дорожного института ГОУВПО «Донецкий национальный технический университет».

Основная часть

В таблице 1 показана матрица классификации данных Автомобильно-дорожного института ГОУВПО «Донецкий национальный технический университет», находящегося в г. Горловка (ДНР, Российская Федерация).

Большинство угроз часто попадают в одну из следующих четырех категорий [3]:

1. Вредоносная активность (кража оборудования; физический взлом; подслушивание; вредоносное сканирование; нарушение процесса; физическое нападение, такое как вандализм, мародерство).

2. Неисправность (неисправность программного обеспечения; аппаратная неисправность; сбой процесса; сбой питания).

3. Человеческая ошибка (потеря оборудования; недопонимание; ошибка реализации).

4. Относящийся к окружающей среде (огонь, экстремальные температуры и влажность, наводнение, молния, ущербный ветер).

Таблица 1 – Классификация данных в АДИ ГОУВПО «ДОННТУ»

	Конфиденциальные данные (самый высокий уровень безопасности)	Чувствительный/критический (умеренный уровень безопасности)	Общедоступный (низкий уровень безопасности)
Правовые требования. Отраслевые правила	Защита данных требуется по закону или отраслевым нормам	Университет имеет обязательства по защите данных	
Репутационный риск	Высокий	Средний	Низкий
Примеры данных	– информация о банковском счете; – номера кредитных карт; – доход; – налоговые декларации	– информационные ресурсы с доступом к конфиденциальным данным; – контрактные и библиотечные операции; – студенческие записи	– данные справочника персонала; – данные, опубликованные учреждением

Риски исходят от самых разных лиц. Это могут быть преподаватели, сотрудники, студенты, посетители, подрядчики, гости или лица, не имеющие причин находиться в институте [4]. Причины, по которым может быть осуществлена попытка получить доступ к информации:

– ради политической или экономической выгоды;

– из-за личной неприязни или несогласия (по отношению к учреждению или конкретному индивиду).

В Автомобильно-дорожном институте ГОУВПО «ДОННТУ» могут существовать следующие риски:

1) похищение конфиденциальных сведений;

2) утрата или недоступность определенной информации;

3) внешние атаки на информационные системы;

4) размещение в открытом доступе сведений, оказывающих негативное влияние на репутацию;

5) получение информации при помощи технических средств;

6) использование нелицензионных программных решений, зачастую содержащих недекларируемые возможности.

Для оценки данных рисков можно применить метод экспертных оценок [5]. Была сформирована выборка из оценок экспертов, задачей которых являлось оценить по 5-балльной шкале риски (таблица 2). Далее распределяем «Вес» между параметрами таким образом, чтобы в сумме он был равен 1. Наиболее приоритетные параметры выделяются большим значением.

Таблица 2 – Распределение «Веса» между рисками

Номер риска	Вес	Эксперт 1	Эксперт 2	Эксперт 3	Эксперт 4	Средняя оценка
1	0,15	4	3	1	2	2,5
2	0,15	5	5	4	5	4,75
3	0,10	3	2	3	3	2,75
4	0,25	1	4	5	2	3
5	0,20	2	1	2	1	1,5
6	0,15	2	3	2	2	2,25
Сумма	1					

Далее баллы умножаем на вес данного параметра. В предпоследний столбец вносится максимальное значение получившихся чисел и рангов. В строке «Сумма» складываем сумму «весов» параметров для риска (таблица 3).

Таблица 3 – Получение максимального числа, исходя из весовых коэффициентов

Номер риска	Вес	Эксперт 1	Эксперт 2	Эксперт 3	Эксперт 4	Мах число	Ранг
1	0,15	0,60	0,45	0,15	0,30	0,60	3
2	0,15	0,75	0,75	0,60	0,75	0,75	2
3	0,10	0,30	0,20	0,30	0,30	0,30	6
4	0,25	0,25	1,00	1,25	0,50	1,25	1
5	0,20	0,40	0,20	0,40	0,20	0,40	5
6	0,15	0,30	0,45	0,30	0,30	0,45	4
Сумма	1	2,60	3,05	3	2,35		

Результирующие ранги объектов ранжирования по данным опросов определяются как сумма рангов для каждого объекта. Исходя из этого, были выявлены наиболее важные риски (таблица 4).

Таблица 4 – Перечень наиболее важных рисков

№ п/п	Код риска	Сущность риска
1	3	Внешние атаки на информационные системы организации
2	2	Утрата или недоступность определенной информации
3	6	Использование нелицензионных программных решений, зачастую содержащих недекларируемые возможности
4	1	Похищения конфиденциальных сведений
5	5	Получение информации при помощи технических средств
6	4	Размещения в открытом доступе сведений, оказывающих негативное влияние на репутацию

Исходя из этого, можно сделать вывод, что наиболее важный риск – это внешние атаки на информационные системы организации.

Для демонстрации эффективности рекомендаций можно использовать матрицу рисков (таблица 5).

Таблица 5 – Матрица рисков

Вероятность, баллы	Ущерб, баллы				
	Очень низкий	Низкий	Средний	Высокий	Крайне высокий
Очень низкая	1	2	3	4	5
Низкая	2	4	6	8	10
Средняя	3	6	9	12	15
Высокая	4	8	12	16	20
Крайне высокая	5	10	15	20	25

– диапазон 1–2 относительного значения риска крайне низкий, такие риски можно принять без компенсационных мер;

– диапазон 3–5 соответствует низким рискам, обрабатывать которые можно в последнюю очередь;

– 6–15 – средние риски;

– 16–20 – высокие риски;

– 25 – крайне высокие риски, обработка которых является первоочередной задачей.

Общим же и основным преимуществом подобного вида визуализаций является их наглядность и доступность для понимания сотрудниками в случае, если необходимо визуально представить более детальный анализ по конкретному риску.

Используя матрицу риска, можем оценить риск, оценив вероятность использования угрозы или уязвимости. Это позволит расставить приоритеты в защите (таблица 6).

Таблица 6 – Матрица рисков, исходя из ущербов

Вероятность, баллы	Ущерб, баллы				
	Очень низкий	Низкий	Средний	Высокий	Крайне высокий
Очень низкая					
Низкая					
Средняя		5	2	3	
Высокая		6		1	
Крайне высокая					4

Для АДИ ГОУВПО «ДОННТУ» следует предложить ряд рекомендаций по устранению рисков и их минимизации [6]:

1. Обучение сотрудников современным знаниям. Персонал должен знать, что уязвимости от вмешательства хакеров/взломщиков обнаруживаются до того, как они станут проблемами, а не после.
2. Правильно сконфигурированные информационные системы с хорошей безопасностью пользователя/пароля (всегда менять пароли по умолчанию).
3. Эффективный мониторинг и оценка трафика интернета.
4. Поддерживать антивирусное программное обеспечение в актуальном состоянии (чтобы не отставать от последних разработок вирусов).
5. Обслуживание и резервное копирование всех ключевых систем.
6. Хранение критически важных данных на защищенных серверах [5].

Выводы

Проведенные исследования показали, что в процессе анализа были выявлены угрозы и риски в Автомобильно-дорожном институте ГОУВПО «ДОННТУ». А так же были предложены рекомендации по минимизации рисков информационной безопасности. Процедура обработки рисков помогает не только выявить и устранить существующие уязвимости и минимизировать вероятность реализации существующих угроз информационной безопасности, но и повысить уровень грамотности сотрудников организации, участвующих в процессе оценки и обработки рисков.

Список литературы

1. Северцев, А. Г. Введение в безопасность / А. Г. Северцев, А. В. Бецков ; 2-е изд., перераб. и доп. – Москва : Юрайт, 2019. – 177 с. – ISBN 978-5-534-05710-2.
2. Сотов, А. И. Компьютерная информация под защитой. Правовое и криминалистическое обеспечение безопасности компьютерной информации : монография / А. И. Сотов. – Москва : Русайнс, 2022. – 128 с. – ISBN 978-5-4365-9078-3.
3. Сычев, М. П. Киберустоичивость информационной инфраструктуры: модели исследования : монография / М. П. Сычев, В. В. Гайфулин, В. М. Сычев [и др.] ; под общ. ред. С. В. Скрыля. – Москва : РУСАЙНС, 2022. – 254 с. – ISBN 978-5-4365-9632-7.
4. Воронцовский, А. В. Оценка рисков : учебник и практикум для бакалавриата и магистратуры / А. В. Воронцовский. – Москва : Юрайт, 2019. – 179 с. – ISBN 978-5-534-02411-1.
5. Коваленко, Ю. И. Методика защиты информации в организациях : монография / Ю. И. Коваленко, Г. И. Москвитин, М. М. Тараскин. – Москва : РУСАЙНС, 2022. – 164 с. – ISBN 978-5-4365-9349-4.
6. Пименов, Н. А. Управление финансовыми рисками в системе экономической безопасности : учебник и практикум для академического бакалавриата / Н. А. Пименов ; 2-е изд. перераб. и доп. – Москва : Юрайт, 2018. – 326 с. – ISBN 978-5-534-04539-0.

Л. П. Вовк, Ю. А. Логвиненко
Автомобильно-дорожный институт
ГОУВПО «Донецкий национальный технический университет», г. Горловка

Риски и угрозы информационной безопасности высших учебных заведений

В настоящее время актуальным является анализ угроз безопасности информации в связи с внедрением IT-технологий, новых аппаратных и программных средств, и, соответственно, новых уязвимостей у них.

В статье рассматривалась классификация данных в Автомобильно-дорожном институте ГОУВПО «ДОННТУ». А так же рассмотрены угрозы и риски в данной организации. Для оценки данных рисков применялся метод экспертных оценок. Было выявлено, что наиболее важный риск – это внешние атаки на информационные системы организации.

Предложены рекомендации по минимизации рисков информационной безопасности такие, как обучение сотрудников современным технологиям; правильно сконфигурированные информационные системы с хорошей безопасностью пользователя/пароля; эффективный мониторинг и оценка трафика интернета; поддержка антивирусного программного обеспечения в актуальном состоянии; обслуживание и резервное копирование всех ключевых систем; хранение критически важных данных на защищенных серверах. Процедура обработки рисков помогает не только выявить и устранить существующие уязвимости и минимизировать вероятность реализации существующих угроз информационной безопасности, но и повысить уровень грамотности сотрудников организации, участвующих в процессе оценки и обработки рисков.

РИСКИ, УГРОЗЫ, БЕЗОПАСНОСТЬ, ИНСТИТУТ, ДАННЫЕ, МЕТОД, ЭКСПЕРТЫ, ОЦЕНКИ, РАНГ

L. P. Vovk, Yu. A. Logvinenko
Automobile and Road Institute of Donetsk National Technical University, Gorlovka

Risks and Threats to the Information Security of Higher Educational Institutions

At present, it is relevant to analyze the threats to the information security in connection with the introduction of IT technologies, new hardware and software, and, accordingly, new vulnerabilities in them.

The article considers the classification of data at the Automobile and Road Institute of Donetsk National Technical University. Threats and risks at this organization are also considered. To assess these risks, the method of expert assessments was used. It was found that the most important risk is external attacks on the information systems of the organization.

Recommendations for minimizing information security risks such as training employees in modern technologies; correctly configured information systems with good user/password security; effective monitoring and evaluation of the Internet traffic; keeping anti-virus software up to date; maintenance and backup of all key systems; storing critical data on secure servers are proposed. The risk treatment procedure helps not only to identify and eliminate existing vulnerabilities and minimize the likelihood of existing information security threats, but also to increase the level of literacy of the organization's employees involved in the risk assessment and treatment process.

RISKS, THREATS, SECURITY, INSTITUTE, DATA, METHOD, EXPERTS, ASSESSMENTS, RANK

Сведения об авторах:
Л. П. Вовк
SPIN-код РИНЦ: 9860-6682
Телефон: +7 (949) 301-98-55
Эл. почта: lv777@list.ru
Ю. А. Логвиненко
Телефон: +7 (949) 338-19-48
Эл. почта: yulya.logvinenko.01@mail.ru

Статья поступила 17.03.2023

Рецензент: В. Л. Николаенко, канд. техн. наук, доц., АДИ ГОУВПО «ДОННТУ»