DOI 10.37882/2223-2966.2024.8.10

УПРАВЛЕНИЕ СОСТОЯНИЕМ ЗАЩИЩЁННОСТИ ИНФОРМАЦИИ В ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЯХ НА ОСНОВЕ ЕГО ОЦЕНКИ

MANAGEMENT OF THE STATE OF INFORMATION SECURITY IN HIGHER EDUCATIONAL INSTITUTIONS BASED ON ITS ASSESSMENT

I. Bulygin

Summary. This article covers the issues of assessing the level of information security for infrastructure and elements of information educational environments in higher educational institutions. The objectives of this article are: 1) justify the importance of conducting an assessment; 2) describe the main security violators in higher education institutions, dividing them according to the degree of interest in committing malicious acts, based on primary motives and authority; 3) highlight the key areas to be assessed; 4) describe approaches to determining the weighting coefficients of areas and individual measures within areas; 5) identify a basic set of threats to which institutions are exposed; 6) identify the main risks associated with violation of information security requirements and best practices for maintaining the level of infrastructure security.

As a result, the article proposes to link the assessment results with the threats and, therefore, the risks that the institution is exposed to, which will allow the organization's management to build a prioritized plan to increase the level of security.

Keywords: information educational environment, information security, intruder model, threats to information security, information security risks, assessment of the state of security, level of security.

Булыгин Иван Максимович
Аспирант, АОЧУ ВО «Московский финансово-юридический университет (МФЮА)»
ftivanbulygin@gmail.com

Аннотация. Настоящая статья освещает вопросы оценивания уровня защищенности информации для инфраструктуры и элементов информационных образовательных сред в высших учебных заведениях. Целями данной статьи ставится: 1) обосновать важность проведения оценки; 2) описать основных нарушителей безопасности в высших учебных заведениях, разделив их по степени заинтересованности в совершении злонамеренных действий, основываясь на первостепенных мотивах и наличии полномочий; 3) выделить ключевые, подлежащие оценке направления; 4) описать подходы к определению весовых коэффициентов направлений и отдельных мер внутри направлений; 5) выделить базовый набор угроз, которым подвержены институты; 6) определить основные риски, связанные с нарушением требований информационной безопасности и лучших практик по поддержанию уровня защищённости инфраструктуры.

Как итог, в статье предлагается связать результаты оценки с угрозами и, как следствие, рисками, которым подвергается учреждение, что позволит руководству организации строить приоритезированный план по повышению уровня защищённости.

Ключевые слова: информационная образовательная среда, информационная безопасность, модель нарушителя, угрозы информационной безопасности, риски информационной безопасности, оценка состояния защищённости, уровень защищённости.

Введение

В условиях осложнения геополитической обстановки, усиления информационной войны, участившихся попыток кибератак на информационные ресурсы коммерческих и государственных организаций Российской Федерации дополнительную актуальность приобретают вопросы обеспечения защиты информации и противодействия киберпреступникам, а также несанкционированному распространению чувствительной с точки зрения конкретной организации информации, к внедрению в информационный контур сведений, нацеленных на пропаганду и популяризацию экстремистской идеологии.

Согласно публикации [1] государственные и коммерческие организации, а в частности и высшие учебные заведения, столкнулись с многократным ростом злонамеренного воздействия, начиная с 2022 года. В первую очередь в источнике описываются внешние воздействия, направленные на отказ в обслуживании сервисов институтов, доступных через сеть Интернет. При этом внешние атаки на учебные заведения реализуются и с другими целями, например, — кража персональных данных обучающихся и сотрудников [2]. В дополнение к внешним воздействиям повышаются и внутренние угрозы информационной безопасности высших учебных заведений. Это связано с общим повышением навыков и знаний студентов, обучающихся по направлениям информационных технологий и компьютерной безопасности с использованием прогрессивных подходов [3], а также самостоятельно интересующихся вопросами воздействия на защищённость информационной среды, стремлением студентов отработать практические навыки в контуре образовательного учреждения и тем самым получить выгоду в процессе аттестации или нанести вред инфраструктуре (киберхулиганство).

Для принятия осознанных управленческих решений по повышению уровня защищённости руководству выс-

ших учебных заведений требуется информация о релевантных для организаций данного типа потенциальных угрозах информационной безопасности, об источниках таких угроз, о факторах, от которых зависит их реализация, о технических и организационных аспектах текущего состояния защищённости, вероятных последствиях. А для приоритезации принимаемых решений источники угроз должны быть ранжированы по степени опасности, а направления и меры по обеспечению информационной безопасности — по степени важности и с учётом рисков, которые несет организация в случае их нереализации.

Методы

В начале работы для дополнительного обоснования актуальности исследуемой темы управления уровнем защиты информации в высших учебных заведениях была проанализирована нормативно-правовая база, регламентирующая вопросы защиты информации в организациях, осуществляющих деятельность на территории Российской Федерации.

В условиях наличия в информационных хранилищах образовательных организаций персональных данных обучающихся, их родственников, а также профессорско-преподавательского состава и иных работников организации, данные организации попадают под требования ФЗ «О персональных данных».

Помимо этого, согласно ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», к субъектам критической инфраструктуры Российской Федерации относятся государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере науки. Это определение применимо и к образовательным организациям, на базе которых осуществляется научная деятельность.

Было принято во внимание, что в рабочих группах по внесению изменений в законодательство о критической информационной инфраструктуре (КИИ) обсуждаются планы по добавлению всех образовательных организаций в контур КИИ.

Первоначальным этапом для определения угроз и вероятных векторов атак для реализации таких угроз, является построение модели нарушителя, характерной для организаций рассматриваемого типа [4].

Для построения собственной модели были проанализированы результаты работ, содержащие исследования и разработки моделей нарушителя для университетов [5], определены критерии, влияющие на степень опасности нарушителей, а также привлечены работники из числа профессорско-преподавательского состава института для экспертных оценок.

На основе практического опыта автора по проведению аудитов информационной безопасности в организациях различных сфер деятельности, а также с учётом работ, рассматривающих основные стандарты построения и оценки систем обеспечения информационной безопасности в организациях [6], был сформирован перечень направлений для оценивания уровня защищённости организаций и предложен перечень конкретных мер, входящих в одно из описанных направлений.

В каждое из верхнеуровневых направлений перед началом проведения оценивания должен входить набор конкретных организационных и технических мер, подлежащих оцениванию внутри данных направлений. Для каждого направления и меры внутри направления целесообразно определить весовые коэффициенты важности, определяемые с учётом специфики сценариев атак в образовательных организациях, опасности нарушителей, особенностей построения системы обеспечения информационной безопасности (СОИБ) в оцениваемой организации.

В работе [7] отмечается, что для описания понятий, имеющих многозначные или неточные оценки, применимы алгоритмы нечетких множеств, формируемых на основе экспертных знаний. Исключительно экспертных знаний может быть недостаточно в связи с отсутствием у отдельно взятых экспертов всеобъемлющих знаний об оцениваемой системе обеспечения информационной безопасности. В связи с этим целесообразно построение самонастраивающихся моделей оценки весовых коэффициентов значимости оцениваемых направлений и мер, а также рисков в СОИБ, основываясь на объективных данных о системе, к которым относятся результаты измерений входов и выходов системы. Источниками объективных входных данных могут выступать отчёты различных средств защиты, использующиеся в контуре оцениваемой организации, например таких, как сканеры уязвимостей, сканеры конфигураций параметров по информационной безопасности для использующихся в периметре технологических платформ, антивирусные средства защиты, системы учёта инцидентов и другие классы средств [8, 9].

В публикации [10] отмечается, что способностью извлечения знаний из пар входных и выходных данных и аппроксимации исходных зависимостей обладают нейронные сети.

При оценке важности параметров по информационной безопасности в высших учебных заведениях, а также

последующей оценке рисков целесообразно, как один из перспективных, использовать совмещенный подход перевода нечётких множеств в нейро-нечеткую сеть, ее настройку и использование для получения объективных механизмов повышения уровня защищённости.

Результаты

В таблице 1 представлена информация о возможных нарушителях информационной безопасности информационных образовательных сред (ИОС) высших учебных заведений и оценка опасности нарушителя, основанная на степени интереса к совершению злонамеренных действий и наличия специализированных навыков у потенциальных категорий нарушителей, где 3 — высокая опасность, 2 — средняя опасность, 1 — низкая опасность.

Таблица 1.

Модель нарушителей в ИОС ВУЗа

Нарушитель	Опасность	Пояснение к выбранной оценке
Преподавательский состав	1	Обычно не заинтересованы в совершении деструктивных действий. Редко имеют набор необходимых навыков для совершения деструктивных действий
Обучающиеся	3	Заинтересованы в искажении информации в автоматизированных системах организации с целью ложного прохождения аттестации, хулиганства.
Администраторы	2	Чаще не заинтересованы в совершении деструктивных действий, но в силу повышенных привилегий более склонны, чем другие работники организации
Иные работники	1	Обычно не заинтересованы в совершении деструктивных действий. Редко имеют набор необходимых навыков для совершения деструктивных действий
Внешние пользователи (хакеры)	3	Заинтересованы в краже персональных данных, нанесении финансового и репутационного ущерба, распространении пропаганды. Имеют требуемую для совершения деструктивных действий подготовку.
Провайдеры, и поставщики	1	Могут быть заинтересованы в совершении деструктивных действий, но несут собственные репутационные риски, поэтому имеют низкую опасность

С целью описания основных аспектов, требующих внимания при оценке уровня защищённости, в настоящей статье в таблице 2 представлен набор направлений мер, применимых и влияющих на состояние защищённости образовательной организации от возможных нарушителей, описанных ранее.

Таблица 2.

Верхнеуровневые направления оценки (I уровень)

№	Название направления
1	Система менеджмента информационной безопасности университета
2	Управление доступом персонала и обучающихся
3	Физическая безопасность образовательных объектов
4	Обеспечение ИБ на стадиях жизненного цикла систем и прикладного программного обеспечения
5	Обеспечение сетевой безопасности инфраструктуры
6	Управление уязвимостями
7	Обеспечение безопасности автоматизированных рабочих мест обучающихся и эксплуатационного персонала
8	Обеспечение безопасности серверов
9	Обеспечение антивирусной защиты
10	Предотвращение утечек защищаемой информации
11	Криптографическая защита информации
12	Управление событиями ИБ
13	Управление инцидентами ИБ
14	Защита среды виртуализации
15	Взаимодействие с третьими лицами (включая обеспечение ИБ при использовании внешних сервисов)
16	Обеспечение ИБ персональных данных обучающихся и работников
17	Обеспечение непрерывности функционирования прикладного обеспечения и сервисов
18	Осведомленность в вопросах обеспечения ИБ преподавателей и обучающихся
19	Работа с конфиденциальной информацией — исследования, научные работы, интеллектуальная собственность, бухгалтерская отчётность и финансовая информация

В таблице 3 приведены меры второго уровня, предлагаемые для оценки в рамках раздела «Обеспечение безопасности автоматизированных рабочих мест (АРМ) обучающихся и эксплуатационного персонала». Данный раздел был выбран, поскольку в нем затрагиваются вопросы безопасности устройств, непосредственно доступных для нарушителей с высокой и средней оценкой безопасности (обучающиеся — 3, эксплуатационный персонал — 2).

Определен и представлен наиболее распространённый перечень мер внутри направлений, который может быть дополнен и изменен с учётом специфики построения инфраструктуры высшего учебного заведения. Основная цель при этом — непротиворечивость, отсутствие дублирования мер в смежных тематических направлениях для получения объективной совокупной картины.

Таблица 3.

Меры для направления оценки (II уровень)

№	I уровень	II уровень
1	Обеспечение безопасности автоматизированных рабочих (АРМ) мест обучающихся и эксплуатационного персонала	Использование централизованного управления учётными записями обучающихся
2		Аутентификация на АРМ только под персонифицированными доменными учетными записями с запретом использования стандартных учётных записей («Гость», «Администратор»)
3		Запрет использования на АРМ обучающихся учётных записей с правами локального администратора
4		Ограничение прав обучающихся на доступ к системным файлам АРМ
5		Запрет на внесение изменений обучающимися в конфигурации прикладного и системного прикладного обеспечения
6		Обеспечение парольной защиты BIOS
7		Использование актуальных поддерживаемых версии операционных систем
8		Установлены обновления и патчи, закрывающие известные CVE (Common Vulnerabilities and Exposures)
9		На АРМ отсутствуют уязвимости системного и прикладного пограммного обеспечения выше 4.0 по шкале CVSS (Common Vulnerability Scoring System)
10		Запрет загрузки операционной системы с внешних носителей
11		Опломбирование АРМ для обеспечения целостности аппаратной части
12		Запрет подключения к АРМ съемных устройств

Выполнение каждой меры j каждого верхнеуровневого направления i можно оценить по следующей шкале

$$E_{i,j} = \begin{cases} 0 - \text{мера полностью не выполнена} \\ 0{,}5 - \text{мера выполнена частично} \\ 1 - \text{мера выполнена в полном объеме.} \end{cases} \quad (1)$$

Для обеспечения гибкости оценки руководством организации может быть сформировано несколько уровней защищённости от более низкого к более высокому, характеризующиеся обязательностью выполнения тех или иных мер для достижения соответствующего уровня

$$a_{1,i,j} = \begin{cases} 0, \text{ неприменима к уровню защиты } 1 \\ 1, \text{ применима к уровню защиты } 1. \end{cases} \quad (2)$$

Вычисление средней оценки для направления на основе конкретных оценок мер с учетом весовых коэффициентов даст количественную оценку состояния защищённости ресурсов информационной образовательной среды по определенному направлению на отрезке от 0 до 1

$$E_i = \frac{\sum_{j=1}^{M_i} E_{i,j} \cdot a_{I,i,j} \cdot t_{i,j}}{\sum_{j=1}^{M_i} a_{I,i,j} \cdot t_{i,j}}, \quad (3)$$

где M_i — общее количество мер защиты информации по направлению i;

I — выбранный уровень защиты организации.

Весовой коэффициент $t_{i,j}$ определяет значительность результата оценки меры при подсчете итогового количественного значения оценки направления E_i.

В зависимости от стратегии управления руководителя он сможет оценить для себя и качественное состояние информационной безопасности, проинтерпретировав полученные количественные оценки по направлениям.

С участием экспертов по информационной безопасности и консультантов по учебным и ИТ-процессам в институте, а также с учётом сформированного набора направлений оценки, был разработан перечень релевантных для университетов угроз:

- угроза внедрения вредоносного кода;
- угроза распространения вредоносного кода;
- угроза искажения защищаемых данных: персональных, финансовых данных, результатов авторских научных исследований;
- угроза кражи защищаемых данных;
- угроза удаления защищаемых данных;
- угроза блокировки защищаемых и общедоступных данных, функционала систем;
- угроза искажения общедоступных данных: данных об аттестации студентов, иных данных, определяющих учебный процесс;
- угроза отсутствие обеспечения защитных мер при проектировании и разработке систем;
- угроза внесения изменения в целостность программного обеспечения, конфигурации программного обеспечения и средств защиты;
- угроза отказа работоспособности внешних сервисов;
- угроза отказа работоспособности внутренних сервисов;
- угроза несанкционированного проникновения на объекты учебного заведения;
- угроза неконтролируемых почтовых рассылок от имени студентов и работников организации;
- угроза внедрения пропагандистской информации с использованием фишинга и социальной инженерии;
- угроза неконтролируемого доступа в сеть Интернет;

— угроза нарушения требований законодательства Российской Федерации.

Автором предлагается связать реализацию каждой меры с набором угроз, на минимизацию которых направлена каждая мера

$$y_{k,i,j} = \begin{cases} 1, \text{мера направлена на снижение угрозы } У_k \\ 0, \text{мера не направлена на снижение угрозы } У_k \end{cases}, \quad (4)$$

где k — номер типовой угрозы;

i — порядковый номер направления оценки;

j — порядковый номер меры внутри направления.

Тогда каждой оцениваемой мере защиты информации $E_{i,j}$ соответствует связанный с ней вектор $\{y_{1,i,j}, y_{2,i,j}, y_{3,i,j}, \ldots, y_{N,i,j}\}$.

Такой подход позволит определить показатель, находящийся в диапазоне от 0 до 1 и показывающий степень реализации мер по отношению к рассматриваемым типовым угрозам (нежелательным событиям) — чем больше мер не реализовано, тем выше данный показатель

$$Y_g = \frac{\sum_{i=1}^{19}\sum_{j=1}^{M_i} y_{g,i,j} \cdot (1 - E_{,i,j}) \cdot a_{I,i,j}}{\sum_{i=1}^{19}\sum_{j=1}^{M_i} y_{g,i,j} \cdot a_{I,i,j}}, \quad (5)$$

где M_i — общее количество мер защиты информации по направлению i;

I — выбранный уровень защиты организации, а для каждой меры посчитать обобщенный показатель связанных угроз суммированием по всем угрозам

$$X_{i,j} = \sum_{g=1}^{N} y_{g,i,j}, \quad (6)$$

где N — общее количество рассматриваемых угроз безопасности.

Наличие таких показателей позволит руководству приоритезировать работы по реализации мер, начиная с тех, которые максимально воздействуют на большее количество угроз.

В завершении на основе приведенного перечня угроз информационной безопасности в высшем учебном заведении были определены и представлены основные риски, которым подвержена организация и ее руководство:

1. Нарушение работоспособности основных сервисов вуза, то есть вынужденная приостановка реализации основных функций организации;
2. Снижение качества выполняемых высшим учебным заведением функций;
3. Коммерческие потери, например, связанные с дополнительными расходами на восстановление функционирования сервисов;
4. Репутационные риски, связанные с попаданием в открытый доступ информации об инцидентах информационной безопасности или сведений ограниченного распространения
5. Риски неисполнения требований регуляторов, результатом чего может стать наложение штрафных санкций и даже временная приостановка права на осуществление деятельности.

Заключение

Проблема обеспечения защиты информации в образовательных учреждениях является актуальной и вызывает вопросы, как у менеджмента организаций, так и у регуляторов Российской Федерации.

В связи с разнообразием используемых технологий и предоставляемых сервисов, попытками нарушить защищённость, как снаружи, так и изнутри, повышением навыков потенциальных нарушителей, организации подвержены разнообразным угрозам информационной безопасности, а процесс оценивания разбивается на большое количество направлений. При этом вклад каждой меры необходимо оценить, избежав субъективности и фрагментарности, используя объективные данные и технологию их анализа.

ЛИТЕРАТУРА

1. Михайлов А.А., Ермаков А.А. Особенности российского рынка информационной безопасности в современных экономических условиях // Московский экономический журнал. — 2023. №3.
2. Romashkova O.N., Romashkova E.D. International Training Programs IT Security System for Specialists in Onboard Systems // 2021 Systems of Signals Generating and Processing in the Field of on-Board Communications, Conference Proceedings, 2021, 9416134.
3. Ponomareva L.A., Chiskidov S.V., Romashkova O.N. Instrumental implementation of the educational process model to improve the rating of the universities // В сборнике: CEUR Workshop Proceedings. 9. Сер. «Selected Papers of the Proceedings of the 9th International Conference Information and Telecommunication Technologies and Mathematical Modeling of High-Tech Systems, ITTMM 2019» 2019. С. 92–101.
4. Корниенко С.В., Пантюхина А.В. Методика выявления потенциальных внутренних нарушителей информационной безопасности // Интеллектуальные технологии на транспорте. — 2023. №2 (34). С. 50–55.
5. Ромашкова О.Н., Каптерев А.И. Анализ угроз и рисков информационной безопасности в вузе // Вестник МГПУ. — 2023. №1(63). С. 37–47.
6. Kapterev A.I., Romashkova O.N. Challengers for Russian Ecosystem of Higher Education for on Board Communications // В сборнике: 2019 Systems of Signals Generating and Processing in the Field of on-Board Communications, SOSG 2019. 2019. С. 8706719.

7. Андрюшкова О.В., Григорьев С.Г. Расчет негэнтропии и весовых коэффициентов многокритериальных оценок на основе нечетких множеств // Информатика и образование. — 2019. № 1. С. 40–49.
8. Бойправ В.А., Утин Л.Л. Методика и программное средство для проведения аудита систем менеджмента информационной безопасности // Информатика. — 2022. №19(4). С. 42–52.
9. Крутофал Г.Е. О необходимости применения сканеров уязвимостей для обеспечения информационной безопасности //Евразийский научный журнал. — 2022. №. 4. С. 41–44.
10. Сагалаева А.И., Ромашкова О.Н., Рудниченко Н.Д. Нечеткая модель для оценки эффективности распределения информационных ресурсов учебного центра // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. 2021. № 10. С. 116–123.