ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004.056
DOI 10.37468/2307-1400-2025-3-25-35

Алгоритм принятия риска в информационных системах

Овсянников Данил Вячеславович[1]
Ягнина Ольга Андреевна[2]
Якушина Анна Евгеньевна[1]

[1] *Донецкий национальный технический университет, Донецк, Россия*

[2] *Южно-Российский государственный политехнический университет (НПИ) имени М.И. Платова, Новочеркасск, Россия*

Аннотация
Безопасность информационных систем в высших учебных заведениях является критически важной в связи с возрастающей сложностью и координацией кибератак, направленных на персональные данные и критическую инфраструктуру. В данном исследовании рассматриваются требования к защите персональных данных в информационных системах ДонНТУ с акцентом на соответствие российским нормативным стандартам, таким как рекомендации ФСТЭК и четвертый уровень безопасности (УЗ-4).
Предложена многоуровневая архитектура защиты, включающая контроль доступа пользователей, защиту на уровне приложений, системного программного обеспечения и сетевой инфраструктуры. В исследовании представлен алгоритм оценки уязвимости активов на основе вероятности угроз и существующих средств защиты, а также алгоритм определения приемлемого уровня риска, который определяется экспертными группами для баланса затрат на защиту и стоимости активов. Ключевые меры защиты включают многофакторную аутентификацию, шифрование данных, регулярное резервное копирование и обнаружение аномалий для обеспечения целостности, конфиденциальности и доступности данных. В исследовании также подчеркивается важность импортозамещения для снижения зависимости от иностранных технологий в условиях геополитических ограничений. Количественные оценки уязвимости получены с использованием статистических данных и взвешенных коэффициентов для оценки частоты угроз и эффективности защиты.
Будущие направления исследований включают совершенствование внутренних инструментов безопасности и отработку методологий оценки рисков для противодействия эволюционирующим киберугрозам, обеспечения надежной защиты.

Ключевые слова: защита персональных данных, импортозамещение, оценка уязвимости активов, приемлемый риск.

Введение

Состояние информационной безопасности характеризуется постоянным повышением сложности защиты, увеличением масштабов и ростом скоординированности компьютерных атак на объекты критической информационной инфраструктуры, усилением разведывательной деятельности иностранных государств, а также нарастанием угроз применения информационных технологий в целях нанесения ущерба суверенитету и территориальной целостности государства [1].

Защита информации на объектах информатизации (ОИ) с целью противодействия кибернетической преступности является составной частью обеспечения национальной безопасности [2]. Решение данной задачи в современных условиях актуально для всех ОИ.

Наиболее частыми целями атак злоумышленников являются государственные и муниципальные учреждения, банки и коммерческие организации. В настоящее время отмечается рост количества хакерских атак на образовательные и научные учреждения Министерства науки и высшего образования Российской Федерации, т.к. в информационных системах этих учреждений циркулирует информация, содержащая сведения о персональных данных (ПДн) работников и обучающихся, научных исследованиях, антитеррористической защищённости объектов.

Импортозамещение в сфере информационной безопасности представляет собой стратегическое направление, имеющее целью уменьшение зависимости от иностранных технологий, программного обеспечения и оборудования, а также развития отечественных аналогов и альтернативных решений. Это становится особенно актуальным в контексте возрастающей угрозы кибератак и киберпреступности, а также в условиях геополитических ограничений и санкций [3, 4].

Исходя из вышеизложенного, возникает необходимость при построении системы защиты ПДн, обрабатываемой в информационных системах «ДонНТУ» («ИС ДонНТУ»), использовать программные продукты и программно-аппаратные комплексы отечественных производителей средств защиты информации.

Согласно постановлению Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», уровень защищенности «ИС ДонНТУ» определяется исходя из категории и количества ПДн, а также актуальности угроз различных типов. К «ИС ДонНТУ» предъявляются требования по защите ПДн четвёртого уровня защищенности (УЗ-4).

Для обеспечения 4-го уровня защищенности ПДн необходимо выполнение следующих требований:

- организация режима обеспечения безопасности помещений, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;
- обеспечение сохранности носителей персональных данных;
- определение перечня лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;
- использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз [5].

Учитывая состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, определенные Приказом ФСТЭК России от 18.02.2013 № 21, а также структурно-функциональные характеристики и актуальные угрозы безопасности информации, для «ИС ДонНТУ» необходимо провести и определить состав и содержание мер по обеспечению безопасности.

Оценка рисков

Для решения задачи проектирования системы защиты баз данных на объектах информатизации необходимо учитывать специфику работы современных систем управления данными, их интеграцию с прикладными решениями и взаимодействие с внешними интерфейсами. Как правило, базы данных являются ядром информационных систем, и защита БД требует комплексного подхода, который предполагает интеграцию технических, организационных и правовых мер.

При проектировании системы защиты баз данных необходимо придерживаться следующих требований.

1. **Простота и оперативность внедрения.** Выбранное решение должно быть интегрировано в существующую инфраструктуру без длительной адаптации.
2. **Гибкость и масштабируемость.** Система должна адаптироваться к изменяющимся требованиям и объёму обрабатываемой информации.
3. **Прогнозирование перспектив развития.** Необходимо учитывать динамику эволюции угроз и тенденций в области кибербезопасности.
4. **Простота управления и адаптивность.** Решение должно предусматривать возможность оперативного контроля, аудита и обновления мер защиты [6].

На основе требований информационной безопасности и специфики функционирования баз данных проектирование системы защиты опирается на рекомендации следующих нормативных документов:

1. Указ Президента Российской Федерации от 01.05.2022 г. № 250.
2. Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры».
3. «Требования к средствам криптографической защиты информации, предназначенным для обеспечения некорректируемой регистрации информации, не содержащей сведений, составляющих государственную тайну» от 07.10.2019.
4. Приказ ФСТЭК РФ от 11.02.2013 №17.
5. Отечественная серия стандартов ГОСТ Р ИСО/МЭК 27000-2021.
6. Методический документ «Методика оценки угроз безопасности информации» ФСТЭК от 5 февраля 2021 года.

В Методике оценки угроз безопасности информации, утвержденной ФСТЭК России 5 февраля 2021 г., приводятся рекомендации по построению системы защиты информационных систем с учетом их архитектуры и предполагается применение сквозного, многоуровневого подхода (рис. 1). Такая архитектура подразумевает разделение системы на несколько слоёв защиты: уровень пользователей (управление доступом и аутентификация), прикладной (системы управления базами данных, веб-приложения, серверы приложений), системный (операционные системы, системное программное обеспечение), а также сетевой уровень (маршрутизация, шифрование трафика, контроль сетевых соединений) [7].

Это позволяет детализировать составные компоненты системы на каждом уровне, обеспечивая изоляцию рисков, упрощение процессов мониторинга, управления и оперативного реагирования на инциденты. Такой подход гарантирует защиту данных и инфраструктуры, минимизируя вероятность угроз для всех уровней взаимодействия.

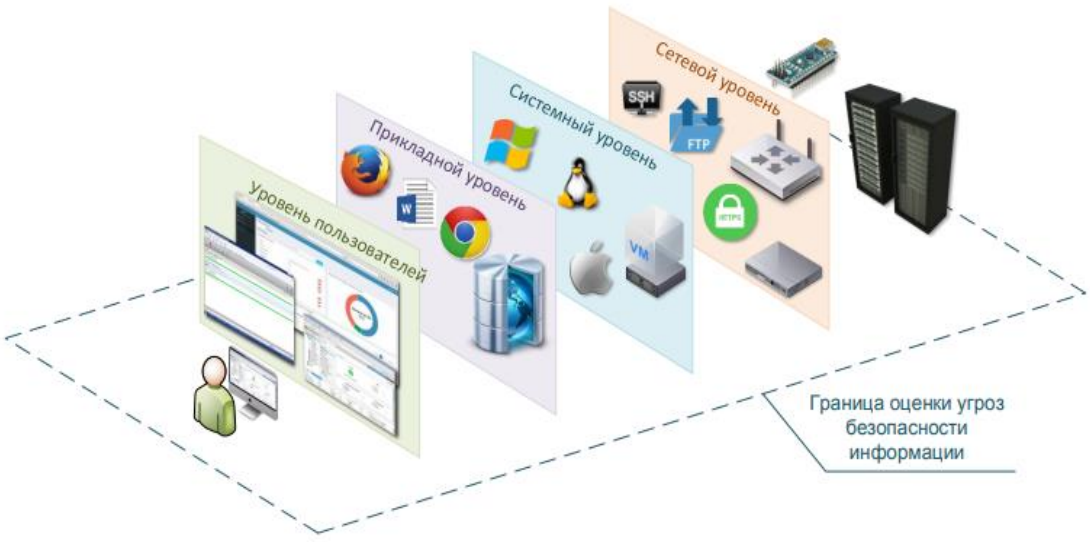

Рисунок 1 – Архитектура защиты систем, обеспечивающих связь между оконечными устройствами

На исходном этапе разработки системы защиты баз данных следует руководствоваться рекомендациями стандарта ГОСТ Р ИСО/МЭК 27000-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология», предусматривающего идентификацию активов с точки зрения их значимости и уязвимостей, способных повлиять на уровень защищенности системы. Для этого целесообразно выделить следующие плоскости защиты баз данных [7, 8]:

1. Управление и администрирование. Реализуется посредством применения ролевых моделей и политик минимизации прав, что гарантирует возможность осуществления взаимодействия с БД только уполномоченными субъектами.

2. Контроль доступа и аутентификация. Многофакторная аутентификация (сочетание паролей, биометрии, токенов) обеспечивает проверку подлинности пользователей и сервисных процессов, подтверждая, что доступ получают именно те, кто имеет на него право.

3. Защита хранения и целостности данных. Меры по защите данных от несанкционированного изменения, утраты или искажения, включая регулярное резервное копирование, создание контрольных сумм и использование систем обнаружения аномалий. Применение криптографических методов для шифрования информации, как при хранении (at rest), так и при передаче (in transit), а также чётко выстроенная система контроля доступа к данным. Физическая и программная защита серверных помещений, применение шифрованных носителей информации и средств виртуализации для ограничения доступа на уровне оборудования. Обеспечение достоверности и неизменности информации через использование транзакционных журналов, контроль версий, цифровых подписей и механизмов валидации данных. Гарантия оперативного доступа к необходимой информации посредством резервирования ресурсов, использования кластерных архитектур, отказоустойчивых решений и систем балансировки нагрузки.

4. Аудит и мониторинг активности. Внедрение средств логирования, мониторинга активности пользователей, анализа системных событий и своевременного обнаружения аномальных действий для оперативного реагирования на инциденты.

В соответствии с поставленными задачами для каждой плоскости определяются активы. Далее для каждого актива проводится анализ имеющихся уязвимостей, источники угроз и актуальные угрозы безопасности информации.

На следующем этапе принятия решения по защите информации оценивается вероятность реализации существующих угроз. Алгоритм оценки уязвимости активов, с учетом принятых мер защиты, представлен на рис. 2. На основании проведенного анализа принимается решение об эффективности или недостаточности принятых мер защиты.

Необходимо отметить, что одним из ключевых моментов при построении системы защиты, является принятие решения по уровню приемлемого (остаточного) риска при реализации угрозы безопасности информации.

Условно, решение о принятии приемлемого уровня риска представлено на рис. 3 [9].

Данное решение, как правило, принимается группой экспертов, обладающих знаниями и опытом работы в сфере деятельности организации. Алгоритм процесса принятия приемлемого риска представлен на рис. 4.

В процессе оценки риска анализируется, удовлетворяет ли результат критериям оценки. В случае приемлемого результата производится принятие риска. В случае неудовлетворительного результата происходит принятие мер по снижению риска. При помощи средств защиты информации (СЗИ) риск либо снижается, либо вовсе избегается. После принятия соответствующих мер производится повторный анализ на предмет удовлетворения требуемым результатам принятых мер. В случае приемлемых показателей риск принимается. Если же результаты не достигают требуемых – производятся повторные меры по снижению риска до тех пор, пока результаты не достигнут ожидаемых показателей.

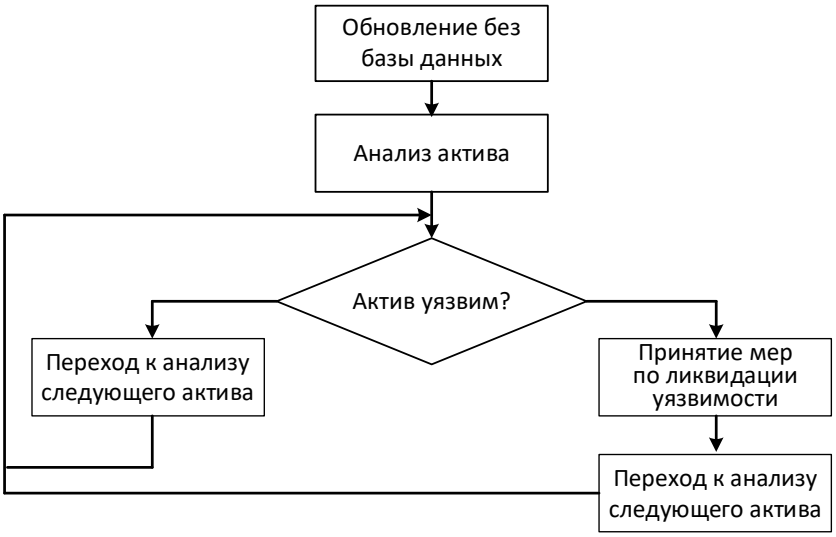

Рисунок 2 – Схема оценки уязвимости активов от вероятных угроз

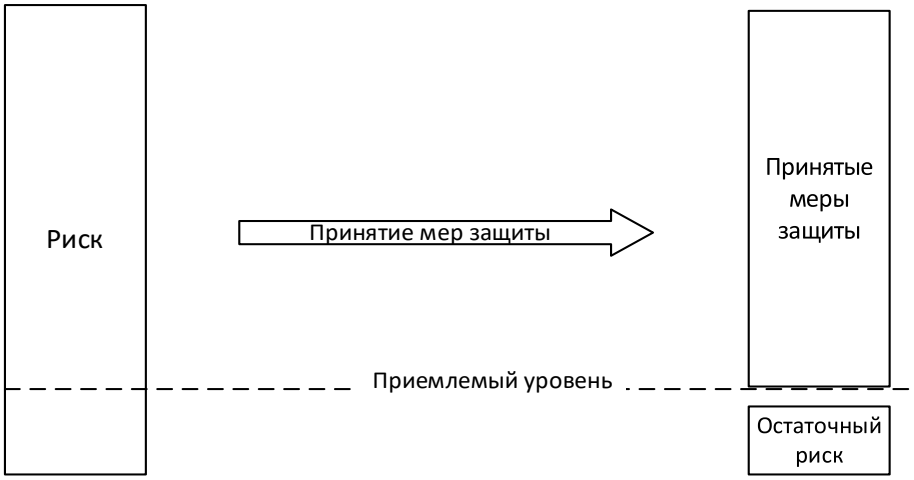

Рисунок 3 – Принятие приемлемого уровня риска

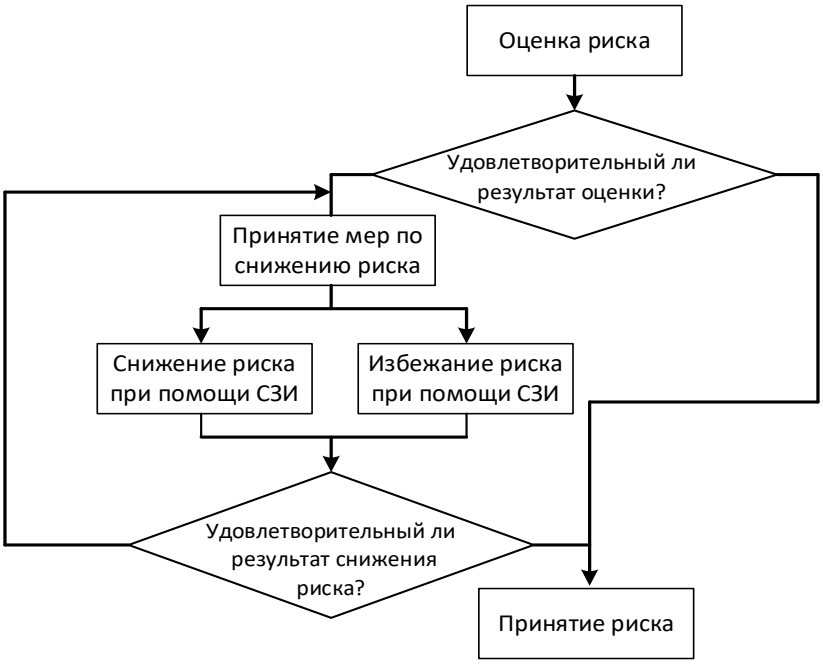

Рисунок 4 – Схема алгоритма принятия рисков

В дальнейшем, на основании решения о принятии приемлемого риска, возможно принятия решения о применении защитных мер, которые должны быть сопоставимы по затратам, исходя из принципа – стоимость защиты объекта не должна превышать стоимость объекта защиты.

Каждое из этих измерений играет ключевую роль в обеспечении комплексной защиты, позволяя минимизировать последствия успешной атаки, которая может нарушить:

- целостность данных;
- доступность сервисов;
- конфиденциальность информации;
- управляемость системы;
- возможность своевременного обнаружения инцидентов.

На основании проведённого анализа разрабатывается количественная оценка уязвимости конкретных активов, что помогает определить оптимальный уровень риска и принять решение о корректировке выбранных мер защиты. При этом, применение комплекса технических мер должно сочетаться с регулярным аудитом и анализом системных событий.

Для каждой плоскости защиты выделяют активы, относящиеся к соответствующему уровню: инфраструктуры, услуг, применяемых программ.

Учитывая важность начального этапа принятия решения, к данному процессу должен быть привлечен персонал, имеющий соответствующую квалификацию и опыт работы.

Такие требования к экспертам, например, сформулированы в рекомендации в области стандартизации банка России [10]:

- наличие высшего образования;
- опыт работы в данной профессиональной области не менее четырех лет;
- систематическое повышение квалификации;
- способность идентифицировать людей, способных предоставить необходимую информацию;
- владение навыками делового и управленческого взаимодействия.

Следующим шагом оценки рисков активов является определение угроз для идентифицированных активов. Угрозы для информационно-телекоммуникационной системы (ИТС) по своей природе делятся на природные и техногенные, последние в свою очередь делятся на случайные и преднамеренные. На данном этапе также определяется источник угроз и «область» действия угрозы, то есть, на какие составные части ИТС может влиять данная угроза.

Этап оценки уязвимости активов схематически представлены на рис. 5.

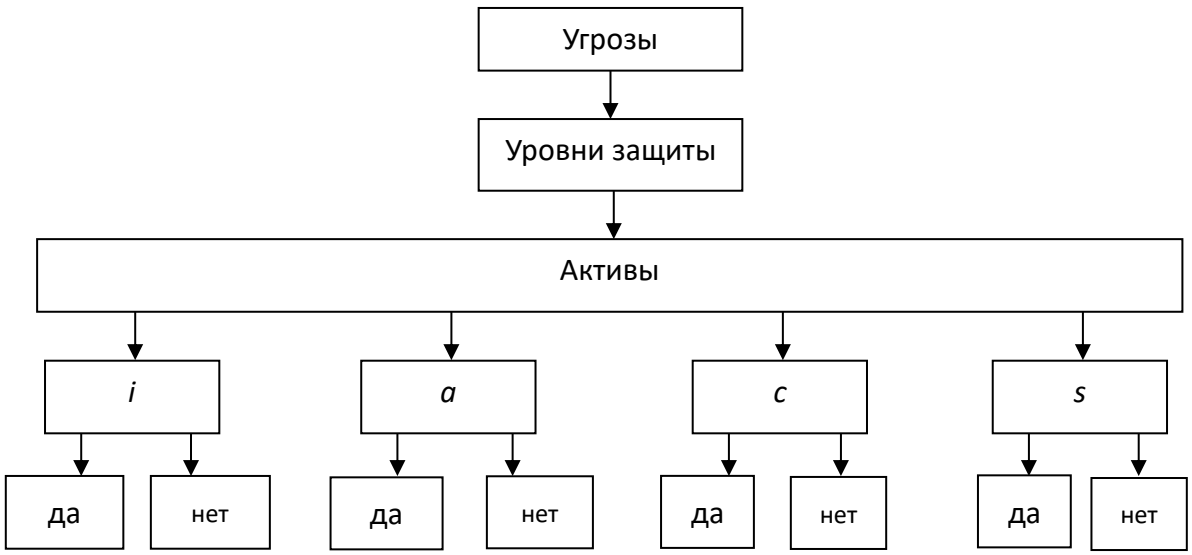

Рисунок 5 – Оценка уязвимости активов от вероятных угроз.

Измерения защиты по своей сути представляют комплекс реализованных мероприятий по защите активов телекоммуникационной системы (ТКС). В случае успешной реализации угрозы активам может быть нанесен ущерб, который может привести к потере свойств информации или управляемости и наблюдаемости ТКС:

- целостность (i);
- доступность (a);
- конфиденциальность (c);
- наблюдаемость и управляемость (s).

Таким образом определяется уровень состояния защищенности ТКС от угроз.

Выделяется восемь основных измерений защиты:

1) управление доступом;
2) аутентификация;
3) сохранность информации;
4) конфиденциальность данных;
5) безопасность связи;
6) целостность данных;
7) доступность;
8) секретность [7].

Результаты оценки уязвимости активов на примере угроз, которые могут быть реализованы с учетом недостатков протоколов межсетевого взаимодействия, приведены в таблице 1.

Таблица 1 – Угрозы для информационной безопасности ТКС

№	Угрозы	Конфиденциальность (confidentiality)	Целостность (integrity)	Доступность (availability)	Наблюдаемость и управляемость (accountability and manageability)	Весовой коэффициент
1	Фишинговые атаки	c_1	i_1	a_1	s_1	p_1
2	Вредоносное программное обеспечение (ВПО)	c_2	i_2	a_2	s_2	p_2
3	Атаки на системы с использованием уязвимостей	c_3	i_3	a_3	s_3	p_3
4	Социальная инженерия	c_4	i_4	a_4	s_4	p_4
5	Применение бот-сетей	c_5	i_5	a_5	s_5	p_5
6	Эксплуатация публичных Wi-Fi сетей	c_6	i_6	a_6	s_6	p_6

Используя полученные данные, можно получить количественную оценку уязвимости конкретного актива от одной угрозы по следующей формуле:

$$T_k = \frac{(c_k + i_k + a_k + s_k)}{4} * z_k * p_k. \quad (1)$$

Весовой коэффициент pk определяет частоту появления данной угрозы относительно совокупности возможных угроз и вычисляется на основе анализа статистических данных или с использованием известных методик. Коэффициент zk определяет вероятность защиты актива ТКС с помощью установленного средства защиты от угрозы pk [11].

Определение уязвимости актива от всех вероятных угроз Ql определяем следующим образом:

$$Q_l = \sum_{i=1}^{k} \frac{(c_k + i_k + a_k + s_k)}{4} * z_k * p_k. \quad (2)$$

Каждый из уровней защиты (программ, услуг, инфраструктуры), представленный на рисунке 1, состоит из ограниченного количества активов. Поэтому для определения общей оценки защиты одного уровня Qp воспользуемся следующей формулой:

$$Q_p = \sum_{j=1}^{l} \sum_{i=1}^{k} \frac{(c_k + i_k + a_k + s_k)}{4} * z_k * p_k. \quad (3)$$

В предложенных формулах весовой коэффициент p_k – это частота появления k угрозы относительно совокупности возможных угроз и коэффициент; z_k – вероятность защиты актива ТКС с помощью установленного средства защиты от k угрозы (определяется на основе анализа статистических данных или с использованием известных методик).

Определение весовых коэффициентов a_k, c_k, i_k, s_k должно осуществляться группой назначенных экспертов.

На основании полученной количественной оценки защищенности активов системы принимается решение о принятии риска. Подробный алгоритм принятия риска представлен на рис. 6.

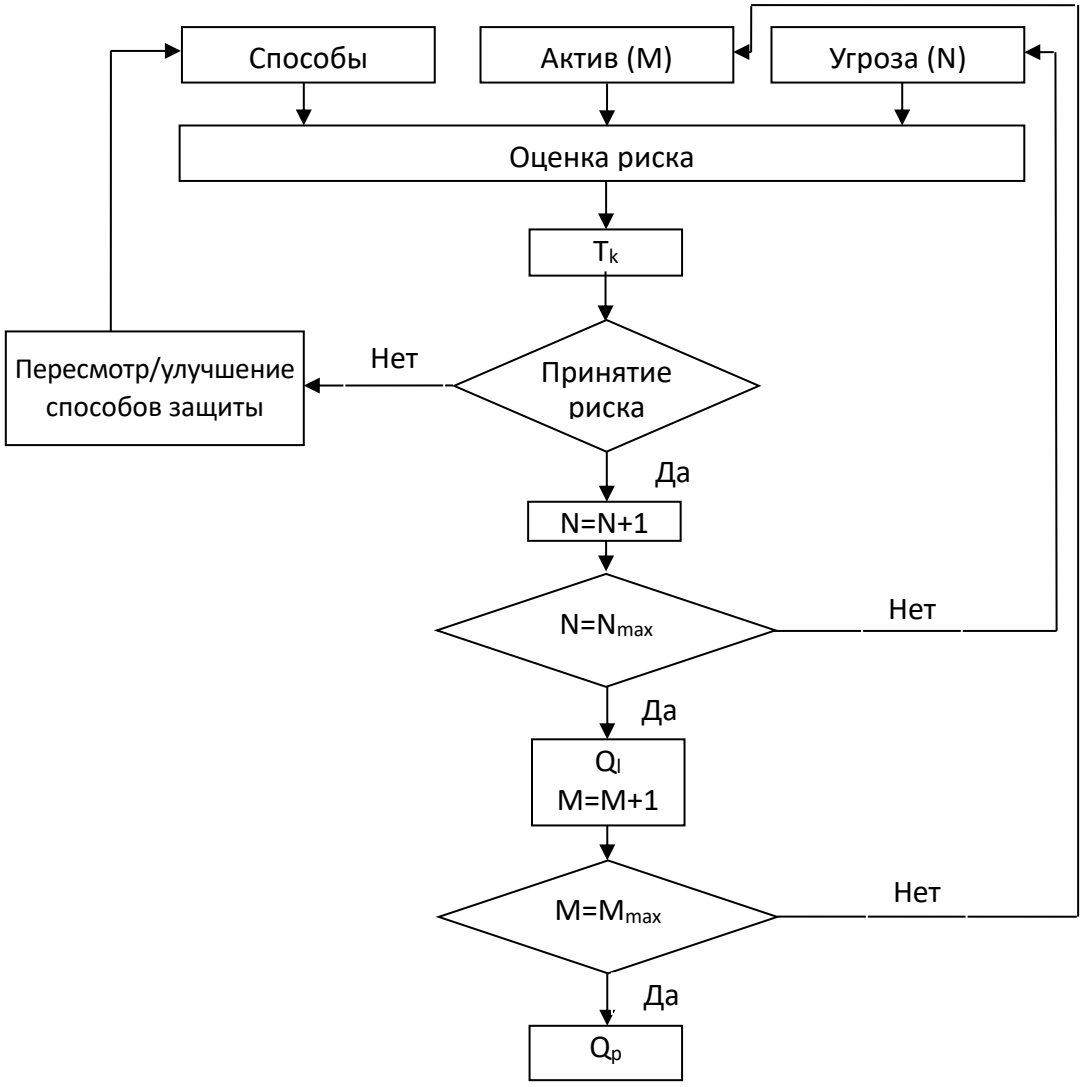

Рисунок 6 – Подробный алгоритм принятия риска.

Предложенный алгоритм оценки и принятия риска может быть применен для всех рассмотренных уровней защиты (программ, услуг, инфраструктуры) всех трех плоскостей защиты (управления, контроля, конечного пользователя).

Заключение

Таким образом, создание системы защиты ПДн в информационных системах высших учебных заведений является многоступенчатым процессом, предусматривающим интеграцию управленческих и технических мер. Постоянный анализ уязвимостей, оперативное внедрение новых методов контроля и использование современных рекомендаций позволяют поддерживать высокий уровень защищенности данных, обеспечивая целостность, доступность и конфиденциальность информации.

Методология исследования основывается на сравнительном анализе отечественных СЗИ с учётом их функциональных возможностей, системных требований и соответствия нормативным документам, таким как требования и нормативы ФСТЭК России. Такой подход позволяет не только объективировать эффективность рассматриваемых средств защиты, но и проводить их соотнесение с конкретными потребностями системы университета, что особенно важно для образовательных учреждений, являющихся центральными звеньями информационной инфраструктуры.

При этом, с учётом возрастающего количества кибератак на информационные системы госучреждений, а также в условиях геополитических ограничений и санкций в отношении РФ, применение отечественных средств защиты, совершенствование методов и алгоритмов принятия решений на организацию защиты являются актуальной задачей и представляют собой направление дальнейших исследований авторов.

Список литературы

1. Доктрина информационной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. N 646.

2. *Ягнина О.А., Щербов И.Л., Якушина А.Е.* Принятие решения по организации защиты информации на объектах информатизации // Информатика, управляющие системы, математическое и компьютерное моделирование (ИУСМКМ-2022): Материалы XIII Международной научно-технической конференции в рамках VIII Международного Научного форума Донецкой Народной Республики, Донецк, 25–26 мая 2022 года. – Донецк: Донецкий национальный технический университет, 2022. – С. 390. – EDN FAKABI.

3. *Абрамова О.В., Микрюков А.А.* Актуальные вопросы информационной безопасности при реализации технологии больших данных // XXXV международные Плехановские чтения : сборник статей участников : в 4 т., Москва, 22–24 марта 2022 года. Том 1. – Москва: Российский экономический университет имени Г.В. Плеханова, 2022. – С. 120-125. – EDN PWERHL.

4. *Емдиханов Р.А., Смирнов Ю.Н.* Основные этапы и стратегии успешной цифровой трансформации // Технологический суверенитет и цифровая трансформация: Международная научно-техническая конференция, Казань, 05 апреля 2023 года. – Казань: Казанский государственный энергетический университет, 2023. – С. 216-218. – EDN ZFGTWO.

5. Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

6. Национальный стандарт РФ ГОСТ Р 50922-2006 "Защита информации Основные термины и определения" (утв. приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. N 373-ст).

7. Методика оценки угроз безопасности информации, методический документ, утвержден ФСТЭК России 5 февраля 2021 г.

8. ГОСТ Р ИСО/МЭК 27000-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология»

9. ГОСТ Р ИСО/МЭК 13335-1 — 2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. [Электронный ресурс]. — Режим доступа: https://ohranatruda.ru/upload/iblock/925/4293846603.pdf

10. Рекомендации в области стандартизации банка России РС БР ИББС-2.9-2016

11. *Воропаева В.Я., Щербов И.Л., Хаустова Е.Д.* Управление информационной безопасностью информационно-телекоммуникационных систем на основе модели «plan-do-check-act» // Научные труды Донецкого национального технического университета. Серия: вычислительная техника и автоматизация. – 2013. – № 25. – С-104-110.

Статья поступила в редакцию 17 апреля 2025 г.
Принята к публикации 26 июня 2025 г.

Ссылка для цитирования: Овсянников Д.В., Ягнина О.А., Якушина А.Е. Алгоритм принятия риска в информационных системах // Национальная безопасность и стратегическое планирование. 2025. № 3(51). С. 25-35. DOI: https://doi.org/10.37468/2307-1400-2025-3-25-35

Risk acceptance algorithm in information systems

Ovsyannikov Danil V. [1]
Yagnina Olga A. [2]
Yakushina Anna E. [1]

[1] *Donetsk National Technical University, Donetsk, Russia*

[2] *South-Russian State Polytechnical University (NPI) named after M.I. Platov, Novocherkassk, Russia*

Abstract
The security of information systems in higher education institutions is critical due to the increasing complexity and coordination of cyberattacks targeting personal data and critical infrastructure. This study examines the requirements for protecting personal data within the information systems of DonNTU, emphasizing compliance with Russian regulatory standards, such as FSTEC guidelines and the fourth level of security (UZ-4).
A multi-layered protection architecture is proposed, encompassing user access control, application-level security, system software, and network infrastructure. The research introduces an algorithm for assessing asset vulnerabilities based on threat likelihood and existing safeguards, alongside an algorithm for determining acceptable risk levels, which is decided by expert groups to balance protection costs against asset value. Key protection measures include multi-factor authentication, data encryption, regular backups, and anomaly detection to ensure data integrity, confidentiality, and availability. The study also highlights the importance of import substitution to reduce reliance on foreign technologies amid geopolitical constraints. Quantitative vulnerability assessments are derived using statistical data and weighted coefficients to evaluate threat frequency and protection efficacy.
Future research directions include enhancing domestic security tools and refining risk assessment methodologies to address evolving cyber threats, ensuring robust protection for educational institutions' information systems.

Keywords: personal data protection, import substitution, asset vulnerability assessment, acceptable risk.

References

1. Doctrine of Information Security of the Russian Federation. Approved by the Decree of the President of the Russian Federation dated 5 December 2016. N 646.
2. *Yagnina O.A., Shcherbov I.L., Yakushina A.E.* Making Decisions on Organizing Information Security at Information Technology Facilities // Informatics, Control Systems, Mathematical and Computer Modeling (IUSMKM-2022): Proceedings of the XIII International Scientific and Technical Conference within the Framework of the VIII International Scientific Forum of the Donetsk People's Republic, Donetsk, May 25–26, 2022. – Donetsk: Donetsk National Technical University, 2022. – P. 390. – EDN FAKABI.
3. *Abramova O.V., Mikryukov A.A.* Current Issues of Information Security in the Implementation of Big Data Technologies // XXXV International Plekhanov Readings: Collection of Articles by Participants: in 4 volumes, Moscow, March 22–24, 2022. Volume 1. – Moscow: Plekhanov Russian University of Economics, 2022. – Pp. 120–125. – EDN PWERHL.

4. *Emdikhanov R.A., Smirnov Yu.N.* Key Stages and Strategies for Successful Digital Transformation // Technological Sovereignty and Digital Transformation: International Scientific and Technical Conference, Kazan, April 5, 2023. – Kazan: Kazan State Power Engineering University, 2023. – Pp. 216–218. – EDN ZFGTWO.

5. Resolution of the Government of the Russian Federation of 01.11.2012 No. 1119 'On Approval of Requirements for the Protection of Personal Data when Processing in Information Systems of Personal Data'.

6. National Standard of the Russian Federation GOST R 50922-2006 'Information Protection Basic Terms and Definitions' (approved by the Order of the Federal Agency for Technical Regulation and Metrology dated 27 December 2006 N 373-st).

7. Information Security Threat Assessment Methodology, methodological document, approved by the FSTEC of Russia on 5 February 2021.

8. GOST R ISO/IEC 27000-2021 'Information Technologies. Methods and means of ensuring security. Information security management systems. General overview and terminology'

9. GOST R ISO/IEC 13335-1 - 2006 Information technology. Methods and means of ensuring security. Part 1. Concept and models of information and telecommunication technologies security management. [Electronic resource]. - Access mode: https://ohranatruda.ru/upload/iblock/925/4293846603.pdf

10. Recommendations in the field of standardisation of the Bank of Russia RS BR IBS-2.9-2016

11. *Voropaeva V.Ya., Shcherbov I.L., Khaustova E.D.* Information Security Management of Information and Telecommunication Systems Based on the Plan-Do-Check-Act Model // Scientific Works of Donetsk National Technical University. Series: Computer Engineering and Automation. - 2013. - No. 25. - P-104-110.

For citation: Ovsyannikov D.V., Yagnina O.A., Yakushina A.E. Risk acceptance algorithm in information systems // National security and strategic planning. 2025. № 3(51). pp. 25-35. DOI: https://doi.org/10.37468/2307-1400-2025-3-25-35

Сведения об авторах:

Овсянников Данил Вячеславович – магистрант кафедры «Радиотехника и защита информации», Донецкий национальный технический университет, г. Донецк, Россия
e-mail: neizvestnyy_chelovek_1910@mail.ru

Ягнина Ольга Андреевна – магистрант кафедры «Информационная безопасность», Южно-Российский государственный политехнический университет (НПИ) имени М.И. Платова, г. Новочеркасск, Россия
e-mail: olechkainanna@mail.ru

Якушина Анна Евгеньевна – старший преподаватель кафедры «Радиотехника и защита информации», Донецкий национальный технический университет, г. Донецк, Россия
SPIN-код: 6376-8009
e-mail: yakuann@yandex.ru

Information about authors:

Ovsyannikov Danil V. – Master's student of the Radio Engineering and Information Protection Department, Donetsk National Technical University, Donetsk, Russia
e-mail: neizvestnyy_chelovek_1910@mail.ru

Yagnina Olga A. – Master's student of the Information Security Department, South-Russian State Polytechnical University (NPI) named after M.I. Platov, Novocherkassk, Russia
olechkainanna@mail.ru

Yakushina Anna E. – Senior Lecturer of Radio Engineering and Information Protection Department, Donetsk National Technical University, Donetsk, Russia
SPIN: 6376-8009
e-mail: yakuann@yandex.ru