

Вестник Евразийской науки / The Eurasian Scientific Journal <https://esj.today>

2024, Том 16, № s4 / 2024, Vol. 16, Iss. s4 <https://esj.today/issue-s4-2024.html>

URL статьи: <https://esj.today/PDF/28FAVN424.pdf>

5.2.6. Менеджмент (экономические науки)

**Ссылка для цитирования этой статьи:**

Верещагин, И. Ю. Современные угрозы и риски информационной безопасности корпоративных систем в условиях импортозамещения / И. Ю. Верещагин // Вестник евразийской науки. — 2024. — Т. 16. — № s4. —

URL: <https://esj.today/PDF/28FAVN424.pdf>

**For citation:**

Vereshchagin I. Yu. Modern threats to information security of corporate database management systems in the context of import substitution. *The Eurasian Scientific Journal*. 2024;16(s4): 28FAVN424. Available at:

<https://esj.today/PDF/28FAVN424.pdf>. (In Russ., abstract in Eng.)

УДК 339.562; 004

**Верещагин Илья Юрьевич**

ФГБОУ ВО «Финансовый университет при Правительстве Российской Федерации», Москва, Россия

E-mail: [verestchagin.ilya@mail.ru](mailto:verestchagin.ilya@mail.ru)

## Современные угрозы и риски информационной безопасности корпоративных систем в условиях импортозамещения

**Аннотация.** В деятельности любого коммерческого предприятия важное значение имеет защита информации и активов. Потеря конфиденциальной информации может не только нанести ущерб самой компании, но и раскрыть данные клиентов, что приведет к административным санкциям и репутационным потерям.

С развитием цифровых технологий возможности злоумышленников растут, что требует от компаний внимания к управлению рисками и обеспечению информационной безопасности. Эффективное управление рисками информационной безопасности требует точной оценки рисков, что обосновывает инвестиции в средства защиты. Разработано множество количественных методик для анализа рисков, включая статистический анализ, байесовские сети, имитационное моделирование, нечеткую логику и нейронные сети. Однако они часто сталкиваются с трудностями в описании информационной среды и формализацией процедур оценки рисков, что вынуждает привлекать экспертов и может приводить к приблизительным и неточным результатам.

Отсутствие общепризнанных методов решения этих проблем сохраняет актуальность разработки универсальных методов оценки рисков. Несмотря на прогресс в сфере информационной безопасности, информационные системы по-прежнему не могут быть полностью защищены. Анализ рисков информационной безопасности определяет характеристики рисков в отношении информационных систем и активов компании, выбирая средства защиты или переноса рисков. Основными факторами при оценке рисков являются ценность активов, оценка влияния угроз и уязвимостей, эффективность существующих средств защиты, предполагаемое время простоя и восстановления, величина штрафов и санкций. Результаты анализа рисков позволяют принять решение по поводу их снижения, переноса, устранения, страхования или принятия. Процесс оценки рисков информационной безопасности включает этапы идентификации, описания объектов защиты, угроз и уязвимостей, а также формирует базу для выбора адекватных средств защиты.

**Ключевые слова:** информационная безопасность; конкурентоспособность; утечка данных; цифровые технологии; управление рисками; санкции; регуляторы

## Введение

Эффективное управление рисками требует их корректной оценки. Высокоточная оценка также помогает обосновать инвестиции в средства обеспечения информационной безопасности. Существуют большое количество методик и программного обеспечения, как отечественного, так и зарубежного, для проведения анализа рисков. Широкое применение имеют количественные методики, однако, их недостаточно для оценки эффективности инвестиций в контрмеры. Специалистами предложено большое количество моделей и методов количественной оценки рисков, которые основаны на статистическом анализе, байесовских сетях, имитационном моделировании, нечеткой логике, нейронных сетях, линейном программировании.

Вместе с тем существуют проблемы, связанные с количественной оценкой, такие как трудности, возникающие при описании информационной среды и связи активов компаний, недостаточная формализация процедур оценивания рисков, что вынуждает компании привлекать экспертов. Как результат, полученные значения могут являться приближенными с недопустимой степенью точности.

## 1. Материалы и методы

При написании автором использовались следующие методы: сравнительный анализ, анализ данных и статистики.

Целью исследования является всесторонний анализ рисков и угроз, связанных с информационной безопасностью в контексте импортозамещения.

Для достижения поставленной цели в работе были поставлены следующие задачи:

- Определить и описать все возможные риски и угрозы, связанные с информационной безопасностью корпоративных систем, включая активы и уязвимости, а также их потенциальное влияние.
- Анализ различных методик для анализа идентифицированных рисков, включая статистический анализ, байесовские сети, имитационное моделирование, нечеткую логику и нейронные сети, чтобы предоставить точные оценки для управления рисками информационной безопасности.
- Разработать и рекомендовать эффективные меры защиты и управления рисками, основываясь на проведенном анализе, чтобы компании могли направлять свои инвестиции на наиболее критические аспекты информационной безопасности.

В основу исследования легли научные труды учёных по вопросам импортозамещения в сфере информационной безопасности: Г.Г. Витязев [1], В.А. Довгаль, Д.И. Шередько [2], А.О. Патрашов [3], В. Филипенков, Е.Л. Кузьмин [4], Д.Р. Хлестова, К.Г. Попов [5].

Особое внимание также было уделено работам в сфере управления информационными рисками ряда авторов: Е.Н. Бояров [6], Д.С. Исламова [7], В.Н. Максименко, Е.В. Ясюк [8], Н.А. Тишина [9], М.А. Польшенко [10].

Методы и модели обеспечения информационной безопасности: И.И. Баранкова [11], М.М. Добрышин [12], С.К. Варлатая [13], Т.А. Мызникова, Е.В. Родина [14]. Также были

рассмотрены работы, акцентирующие внимание на информационную безопасность в контексте экономической безопасности: Е.Е. Ершова [15], Л.А. Уточкина [16].

## 2. Результаты и обсуждения

В деятельности любого коммерческого предприятия очень большую важность имеет защита информации и активов. Активы компании, как материальные, так и нематериальные — ценный ресурс, от которого зависит как функционирование предприятия в целом, так и его конкурентоспособность [17]. Из-за некорректно проведенного анализа рисков и выбора контрмер, компания может лишиться не только собственной конфиденциальной информации, которая даст преимущество конкурентам, но и данных своих клиентов, утечка которых ведет административные санкции и репутационный ущерб. Возможности для злоумышленников продолжают расти с развитием цифровых технологий, что расширяет масштаб угроз в условиях импортозамещения. Именно поэтому руководства компании, а также менеджеры и отделы по обеспечению информационной безопасности, проявляют интерес к теме управления рисками и обеспечения информационной безопасности [17].

Несмотря на все больший прогресс в сфере обеспечения информационной безопасности, до сих пор ни одна информационная система не может быть абсолютно и полностью защищена. Частота появления новостей об очередной утечке данных или взломе не уменьшается со временем. Отечественные информационные системы становятся все более и более значимыми для бизнеса, а некоторые из них и вовсе считаются обязательными для работы объектов критической информационной инфраструктуры.<sup>1</sup>

Можно утверждать, что все компании являются цифровыми по умолчанию. Даже если фирма не предоставляет свои продукты, каталоги или сервисы в цифровом формате, ее операционная работа, бизнес-процессы и внутренняя организация тесно и напрямую связаны с цифровыми технологиями и информационными системами.

Всемирный экономический форум вносит крупномасштабную утечку данных в пятерку наиболее серьезных рисков, существующих в современном мире. Масштаб угрозы стремительно возрастает: ожидается, что глобальный ущерб от утечек данных и нарушений информационной безопасности составит 6 триллионов долларов США.<sup>2</sup> В дополнение к крупным потерям утечки данных влекут за собой административные и юридические меры.

В связи с постоянно расширяющимся ландшафтом угроз остается актуальной проблема своевременной идентификации рисков информационной безопасности, их оценки, и, как следствие, управления этими рисками.

Целью анализа рисков информационной безопасности является определение характеристик этих рисков по отношению к информационным системам компании и к ее активам. В результате проведения анализа рисков выбираются необходимые средства защиты или переноса рисков.

Основными факторами, которые учитываются при оценивании рисков информационной безопасности, являются:

---

<sup>1</sup> Указ Президента РФ от 30 марта 2022 г. № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» (с изменениями и дополнениями).

<sup>2</sup> РИА Новости. Путин оценил ущерб от киберпреступности в мире. Режим доступа — <https://ria.ru/20201120/kibeprestupnost-1585566903.html> (дата обращения: 28.07.2024).

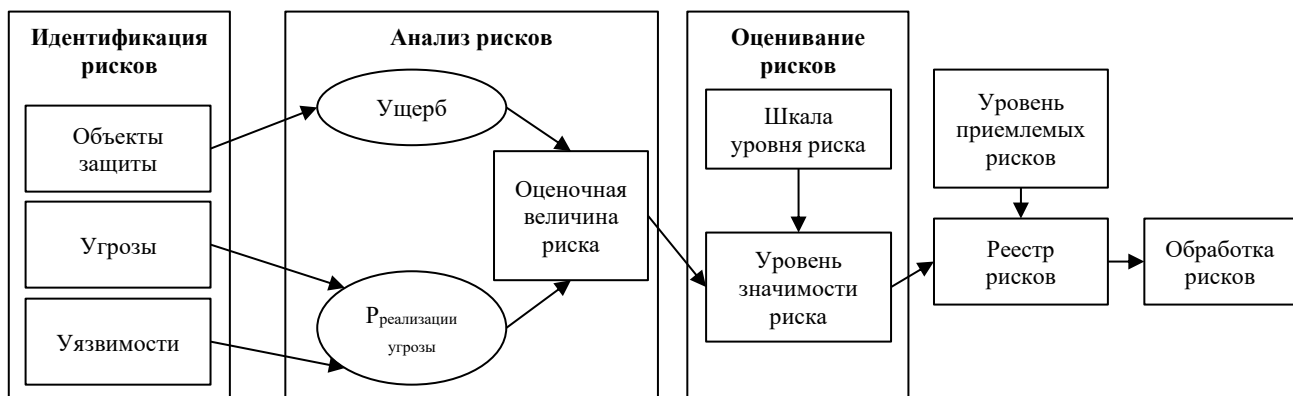
- ценность активов (ресурсов);
- оценки влияния угроз;
- оценки значимости уязвимостей;
- эффективность существующих средств защиты;
- предполагаемое время простоя и восстановления после атаки;
- величина штрафов и санкций со стороны регулирующих органов в случае утечки данных.

Во многих странах введены стандарты информационной безопасности, которые определяют необходимый минимальный уровень защищенности информационных систем компании. Такой уровень защищенности называется базовым, и соответствует требованиям, изложенным в стандартах (для России это требования ФСТЭК и международного стандарта ISO).

Базовый анализ рисков проводится в соответствии с требованиями базового уровня защищенности. Как правило, при таком анализе не рассматривается ценность ресурсов и не оцениваются меры эффективности тех или иных средств защиты, поэтому такой базовый анализ не подходит для эффективного управления рисками.

Для эффективного управления рисками и повышения защищенности компании стоит проводить так называемый полный анализ рисков информационной безопасности. Он включает в себя определение ценности как материальных, так и нематериальных активов, оценку влияния угроз, уязвимостей, а также определение эффективных контрмер. Такой анализ предъявляет повышенные требования в области информационной безопасности.

Процесс оценки рисков информационной безопасности схематично представим в виде схемы на рисунке 1.



**Рисунок 1.** Процесс оценки рисков информационной безопасности (разработано автором)

На этапе идентификации рисков составляется список рисков с их описаниями: объекты защиты, угрозы и уязвимости. Определим угрозы как факторы, повышающие риск.

Угрозы различаются по их источникам и результатам их реализации. Сами источники можно разделять более поверхностно — на внутренние и внешние, а можно рассматривать непосредственную причину возникновения и существования угрозы.

Рассмотрим эту классификацию. Угроза может возникнуть в результате природного или техногенного явления, может быть связана непосредственно с цифровым ландшафтом компании и его уязвимостями, может являться следствием несанкционированного физического доступа:

- Цифровые угрозы используют различные типы вредоносного ПО, фишинговые письма и сообщения в программах-мессенджерах, вредоносные вложения и др., а также различные схемы социальной манипуляции. Это также угрозы, создаваемые недостатками в проектировании, разработке, развертывании, обновлении и обслуживании приложений.

- Природно-техногенные угрозы — это угрозы, связанные с климатическими и природными условиями. Примером реализации такой угрозы может быть потеря данных ввиду разрушения центра обработки данных ураганом. Техногенной угрозой могут быть перебои в работе электрического обеспечения ЦОД или офиса, в результате которой произойдет временная остановка деятельности или потеря данных. Реализация таких угроз имеет случайный характер, их частота является достаточно малой, по сравнению с другими видами угроз.

- Физические угрозы — угрозы, возникающие в результате несанкционированного физического доступа к оборудованию компании. В отличие от цифровых угроз, где несанкционированный доступ является логическим, нарушитель при реализации такой угрозы не может действовать удаленно. Стоит заметить, что сам факт получения физического доступа к оборудованию может быть результатом реализации цифровой угрозы (взлома). Например, коды доступа к серверной могут быть получены в результате нарушения конфиденциальности переписки в корпоративном мессенджере. Основным же отличием физической угрозы от природно-техногенной (часто происходит некорректное объединение этих групп) является преднамеренность, наличие злоумышленника.

Далее рассмотрим возможные результаты реализации угроз вне зависимости от их источника. В результате реализации данные могут быть потеряны, работа компании или филиала может быть остановлена ввиду поломок оборудования, информация может быть разглашена или похищена. Таким образом, можно разделить угрозы на следующие:

- Угрозы конфиденциальности — угрозы несанкционированного доступа к данным (например, получение посторонними лицами сведений о состоянии счетов клиентов). Реализация таких угроз несет за собой не только финансовые потери для компании, но и, в большинстве стран, административные санкции ввиду действия законов о защите персональных данных. Для компаний потребительского сектора дополнительную угрозу составляет то, что они работают не только с персональными данными клиентов, но и данными кредитных и дебетовых карт. Нарушение конфиденциальности таких данных влечет за собой дальнейшее мошенничество со счетами клиентов, что, в свою очередь, повлечет дальнейшие выплаты компенсаций, зачастую большие, чем потери в результате взлома.

- Угрозы целостности — угрозы несанкционированной модификации, дополнения или уничтожения данных (например, внесение изменений в бухгалтерские проводки с целью хищения денежных средств). Для компаний такие угрозы могут быть связаны с деятельностью магазинов и филиалов, которые контролируются удаленно. Несанкционированная модификация или удаление данных может, например, привести к разнице между заявленной и фактической выручками и дальнейшей краже денежных средств или товара) [17].

- Угрозы доступности — угрозы ограничения или блокирования доступа к данным (например, невозможность подключиться к серверу с базой данных в результате DDoS-атаки). Эти угрозы связаны не только с данными, но и с оборудованием. Так, потеря доступа к серверу критичного для операционной деятельности приложения (например, системы ERP) может привести к остановке или замедлению деятельности предприятия. Потеря доступа может привести к тому, что данные о продажах, наличии о складах, выручке, остатках товара будут некорректными, что может привести к нарушению работы торговой точки [17].

Вернемся к простейшей классификации по источникам угроз.

Она не требует подробного описания, так как является очевидной, поэтому в работе будут приведены лишь примеры для каждой категории.

К внутренним угрозам относятся [17]:

- ошибки пользователей и системных администраторов;
- ошибки в работе ПО;
- сбои в работе компьютерного оборудования;
- нарушение сотрудниками компании регламентов по работе с информацией;
- намеренные мошеннические действия со стороны сотрудников компании.

К внешним угрозам относятся [17]:

- несанкционированный доступ к информации со стороны заинтересованных организаций и отдельных лиц (промышленный шпионаж конкурентов, сбор информации спецслужбами, атаки хакеров и т. п.);
- компьютерные вирусы и иные вредоносные программы;
- стихийные бедствия и техногенные катастрофы (например, ураган может нарушить работу телекоммуникационной сети, а пожар уничтожить сервера с важной информацией).

Уязвимости информационной безопасности возникают на следующих уровнях [17]:

- веб-серверы (соединение через сеть Интернет);
- вычислительные сервера приложений (находится в головном офисе);
- рабочие станции;
- платежные терминалы;
- базы данных;
- мобильные компьютеры (с приложениями программ лояльности);
- персонал.

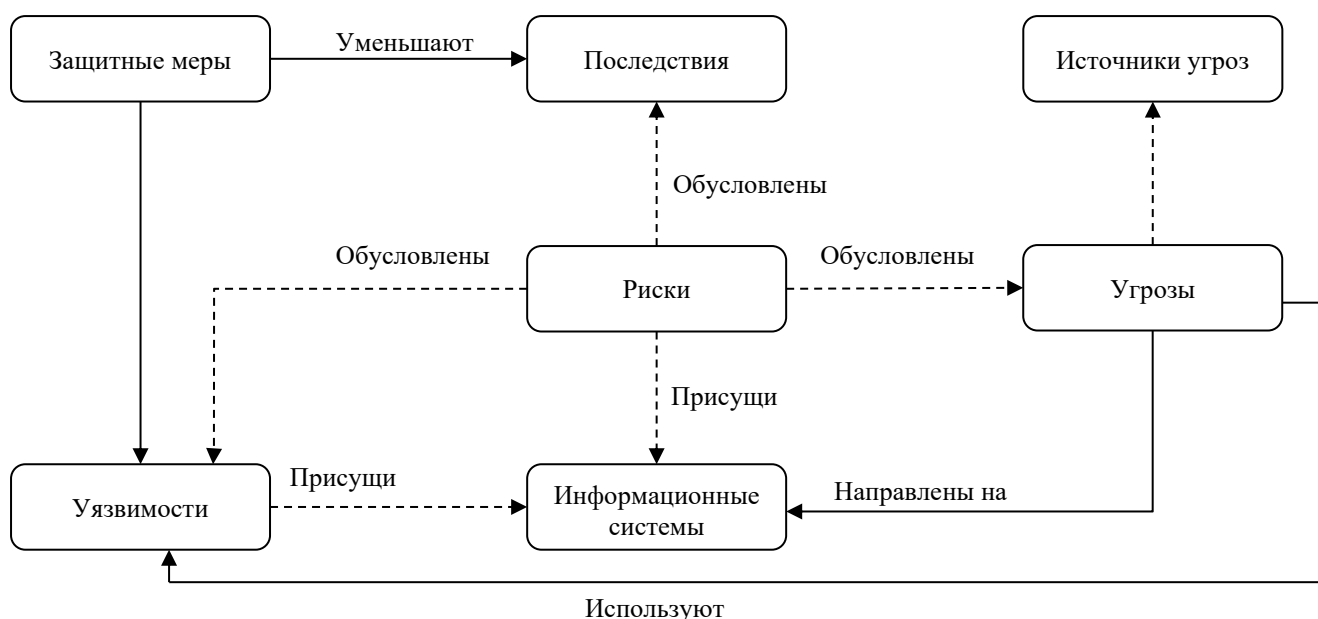
Таким образом, область анализа рисков информационной безопасности можно представить в виде схемы (рис. 2).

Пунктирными линиями на диаграмме показаны ассоциативные связи, а непрерывными — непосредственные фактические.

Из представленных диаграмм процесса оценки риска и предметной области нам видно, что анализ рисков информационной безопасности является сложным процессом, затрагивающим различные аспекты работы компании.

Так же существует большое количество областей, в которых компании может быть нанесен вред в результате реализации одной или нескольких угроз информационной безопасности.

Поэтому для успешного функционирования недостаточно проведения базового анализа рисков. Это приводит к необходимости проведения полного анализа рисков, для осуществления которого существует набор программных комплексов.



**Рисунок 2.** Предметная область анализа рисков информационной безопасности (разработано автором)

Все известные методики оценки рисков информационной безопасности можно разделить на три группы:

- Методики качественной оценки рисков (например, с помощью лингвистических переменных, таких как «низкий», «высокий», «средний»).

К таким методикам относится, например, методика FRAP.

- Методики количественной оценки (для оценки риска используются числовые значения, например, ожидаемый размер материального ущерба оборудованию, размер ожидаемых потерь в прибыли).

К этому классу относится такая методика, как RiskWatch.

- Смешанные методики оценки, такие как CRAMM, MSAT.

При выборе методики учитываются бизнес-потребности предприятия, масштаб компании, а также то, насколько методика соответствует лучшим практикам и описывает требуемые действия и процессы.

На практике более распространены методики качественной оценки рисков. В них значения параметров определяются по заранее составленным шкалам, которые являются качественными. Недостатки качественных методик оценки состоят в том, что они дают весьма грубые, приближенные результаты. Из-за этого возникают трудности в том, чтобы, например, аргументировать нужные размеры инвестиций в меры защиты и оценить их эффективность.

Количественные оценки риска как правило определяются по формулам, основывающимся на следующей:

$$Risk = P * Loss, \quad (1)$$

$P$  — вероятность возникновения рисковогого события;  $Loss$  — величина ущерба.

В итоге количественным значение риска является величина ожидаемого ущерба. Вероятность возникновения рисковогого события, или реализации угрозы, определяется при помощи статистических, экспертных или прочих методов. Величина потерь в результате наступления рисковогого события определяется в показателях стоимости.

Как показатели вероятности, так и показатели ущерба могут быть разложены на ряд других показателей, в результате чего появляются и другие формулы оценки риска. Примером такой формулы является оценка риска, полученная путем перемножения показателей вероятности реализации угрозы, вероятности использования уязвимости и значения потерь<sup>3</sup>:

$$R = p_T * p_V * Loss, \quad (2)$$

$p_T$  — вероятность реализации угрозы;  $p_V$  — вероятность использования уязвимости.

Так же можно добавить множитель, равный разности единицы и показателя эффективности защитных мер<sup>3</sup>:

$$R = p_T(1 - E_V) * p_V(1 - E_{Loss}) * Loss, \quad (3)$$

$E_V$  — показатель эффективности защитных мер, которые направлены на предотвращение уязвимости;  $E_{Loss}$  — показатель эффективности защитных мер, которые направлены на минимизацию потерь.

Однако все эти формулы справедливы, только если каждое рисковое событие наступает в виду реализации только одной угрозы и использования только одной уязвимости.

Предположим, что мы имеем  $N$  активов (объектов защиты),  $K$  уязвимостей и  $X$  угроз. Каждая угроза может использовать одну или более уязвимостей. Так же будем считать, что уязвимости независимы, то есть наличие одной из них никак не влияет на наличие другой. Тогда, используя условные вероятности, получаем следующую формулу вероятности того, что  $n$ -ый актив пострадает в результате того, что реализовалась  $x$ -ая угроза.

$$p(n|x) = p_T(x) * [1 - \prod_{k=1}^K (1 - p_V(x|k))], \quad (4)$$

$p_T(x)$  — вероятность того, что возникнет угроза  $x$ ;  $p_V(x|k)$  — вероятность того, что угроза  $x$  использует уязвимость  $k$ .

Предположим, что угрозы, так как и уязвимости, являются независимыми. Тогда величина риска  $n$ -ого актива<sup>3</sup>:

$$R(n) = \sum_{x=1}^X p(n|x) * q(n), \quad (5)$$

$q(n)$  — потери, если будет поврежден (как в физическом, так не нематериальном смысле) актив  $n$ .

Однако стоит заметить, что в этой формуле последствия, которые возникают при наступлении нескольких угроз, учитываются несколько раз. Например, если актив будет поврежден в результате одновременной реализации нескольких угроз, то при расчете по этой формуле, ожидаемый ущерб может оказаться в разы больше реального.

Если ввести предположением о том, что угрозы приводят к одинаковым последствиям, то риск безопасности элемента информационной среды можно определить по формуле<sup>3</sup>:

$$R(n) = (1 - \prod_{x=1}^X (1 - p(n|x))) * q(n), \quad (6)$$

Предположение, что угрозы приводят к одинаковым последствиям, нереализуемо в реальности, поэтому формулы, использующие его, нежизнеспособны. Можно определить степень ущерба для каждого из возможных нарушений свойств актива, и использовать уже вероятности реализации для каждого из этих нарушений.

<sup>3</sup> Нурдинов, Р.А. Модель количественной оценки рисков безопасности корпоративной информационной системы на основе метрик: специальность 05.13.19 «Методы и системы защиты информации, информационная безопасность»: диссертация на соискание ученой степени кандидата технических наук / Нурдинов Руслан Артурович, 2016. — 186 с. — EDN WFLGJE.

Методики MSAT и RiskWatch используют вместо параметра «риск» показатель ожидаемых годовых потерь или ALE.

$$ALE = AS * EF * F, \quad (7)$$

$AS$  — стоимость актива;  $EF$  — коэффициент уязвимости (показывает, какая часть от стоимости актива подвергается риску);  $F$  — частота реализации угрозы, связанной с рассматриваемым активом.

Так же показатель ожидаемых годовых потерь можно рассчитать, перемножив ожидаемую годовую частоту реализации угрозы (ARO) и ожидаемый ущерб от единичного возникновения угрозы (SLE). Ожидаемый единичный ущерб определяется, разностью первоначальной стоимости актива и остаточной стоимости этого актива после реализации угрозы.

Таким образом, очевидно, что проблема анализа рисков информационной безопасности остается одной из самых актуальных в условиях импортозамещения. Неправильное управление этими рисками, или вовсе их игнорирование, может привести к крупным потерям, как материальным, так и нематериальным, для компании. Однако для корректного выбора необходимых мер и определения их эффективности необходимо с достаточной точностью оценить риски информационной безопасности. Качественные методы оценки пользуются достаточно большой популярностью, ввиду сложности количественной оценки, но они дают достаточно грубые результаты, не позволяющие эффективно аргументировать, например, инвестиции в контрмеры.

### Заключение

Современные угрозы и риски информационной безопасности корпоративных систем управления базами данных, особенно в условиях импортозамещения, требуют тщательного управления и активных мер по их минимизации. Основные выводы, сделанные в рамках данного исследования, подчеркивают необходимость проведения всестороннего анализа рисков с использованием различных количественных методик, таких как статистический анализ, байесовские сети, имитационное моделирование, нечеткая логика и нейронные сети.

Несмотря на разнообразие доступных подходов, остается проблема с их применением из-за трудностей в описании информационной среды и формализованности процедур оценки рисков. Данная проблема актуализирует задачу разработки универсальных методик и повышает значение привлечения экспертов для проведения анализа. Частота утечек данных и кибератак продолжает расти, что требует от компаний постоянного совершенствования своих систем защиты и управления рисками.

Анализ рисков информационной безопасности, включающий определение ценности активов, влияние угроз и уязвимостей, позволяет компаниям принять взвешенные решения по снижению, переносу, устранению, страхованию или принятию рисков. Ключевыми шагами в этом процессе являются идентификация и описание объектов защиты, анализ угроз и уязвимостей, а также выбор адекватных средств защиты.

Таким образом, выводы исследования подчеркивают необходимость непрерывного мониторинга и совершенствования систем информационной безопасности как ключевого элемента успешного функционирования и устойчивости коммерческих предприятий в условиях импортозамещения и развития отечественных цифровых технологий.

## ЛИТЕРАТУРА

1. Витязев, Г.Г. Информационная безопасность бизнеса в контексте импортозамещения / Г.Г. Витязев // Вестник науки и образования. — 2018. — № 9(45). — С. 43–47. — EDN XVQSPZ.
2. Довгаль, В.А. Обеспечение информационной безопасности веб-сайта в условиях импортозамещения / В.А. Довгаль, Д.И. Шерedyкo // Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. — 2022. — № 2(301). — С. 67–77. — DOI 10.53598/2410-3225-2022-2-301-67-77. — EDN MVVOWD.
3. Патрашов, А.О. Как повлияли изменения внешней политики РФ на процесс управления информационной безопасностью / А.О. Патрашов // Актуальные проблемы авиации и космонавтики: сборник материалов VIII Международной научно-практической конференции, посвященной Дню космонавтики: в 3 т., Красноярск, 11–15 апреля 2022 года. Том 2. — Красноярск: Федеральное государственное бюджетное образовательное учреждение высшего образования «Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева», 2022. — С. 290–292. — EDN OJGOEW.
4. Филипенков, А.В. Сравнение существующих систем управления базами данных в целях выбора наилучшей при реализации требований по сокращению затрат и импортозамещению / А.В. Филипенков, Е.Л. Кузьмин // Газовая промышленность. — 2018. — № 4(767). — С. 24–29. — EDN YWRMKQ.
5. Хлестова, Д.Р. Проблемы импортозамещения в сфере информационной безопасности / Д.Р. Хлестова, К.Г. Попов // Символ науки: международный научный журнал. — 2016. — № 4-3(16). — С. 138–140. — EDN VVWTSD.
6. Boyarov, E.N. Analysis of information risks in education / E.N. Boyarov, S.V. Abramova, P.V. Stankevich, I.V. Korneeva // Perspectives of Science and Education. — 2021. — No. 3(51). — P. 451–464. — DOI 10.32744/pse.2021.3.32. — EDN CTQOAG.
7. Исламова, Д.С. Управление информационными рисками и «уровень зрелости» корпоративных систем / Д.С. Исламова // Экономика и социум. — 2024. — № 5-1(120). — С. 1983–1988. — EDN EBNMGE.
8. Максименко, В.Н. Основные подходы к анализу и оценке рисков информационной безопасности / В.Н. Максименко, Е.В. Ясюк // Экономика и качество систем связи. — 2017. — № 2(4). — С. 42–48. — EDN ZHLBOL.
9. Тишина, Н.А. Оценка рисков информационной безопасности облачных сред на основе нечеткого метода анализа иерархий / Н.А. Тишина, И.А. Щудро, Е.Н. Чернопрудова, Л.Ф. Тагирова // Научно-технический вестник Поволжья. — 2019. — № 7. — С. 149–152. — EDN CSPCGD.
10. Польшенко, М.А. Анализ рисков в информационной среде / М.А. Польшенко // Молодой исследователь Дона. — 2023. — Т. 8, № 3(42). — С. 55–62. — EDN GLXCXU.
11. Добрышин, М.М. Вариант применения диверсионного анализа при разработке систем обеспечения информационной безопасности для корпоративной сети связи / М.М. Добрышин, А.Н. Горшков, А.С. Белов, Н.Ю. Борзова // Известия Тульского государственного университета. Технические науки. — 2021. — № 9. — С. 67–72. — DOI 10.24412/2071-6168-2021-9-67-72. — EDN NNMNFK.

12. Баранкова, И.И. Минимизация рисков информационной безопасности на основе моделирования угроз безопасности / И.И. Баранкова, У.В. Михайлова, М.В. Афанасьева // Динамика систем, механизмов и машин. — 2019. — Т. 7, № 4. — С. 60–66. — EDN XRТАUD.
13. Варлатая, С.К. Агентный подход к оценке информационной безопасности корпоративных систем / С.К. Варлатая, Ю.С. Москаленко, С.В. Ширяев // Научный вестник Новосибирского государственного технического университета. — 2014. — № 1(54). — С. 66–71. — EDN SMYRDF.
14. Мызникова, Т.А. Разработка модели угроз информационной безопасности организации / Т.А. Мызникова, Е.В. Родина // Системы управления, информационные технологии и математическое моделирование: Материалы I Всероссийской научно-практической конференции с международным участием, Омск, 21–22 мая 2019 года / Ответственный редактор В.Н. Задорожный. — Омск: Омский государственный технический университет, 2019. — С. 73–78. — EDN JKHBY5.
15. Ершова, Е.Е. Информационная безопасность как элемент экономической безопасности / Е.Е. Ершова // Управление образованием: теория и практика. — 2022. — № 6(52). — С. 225–230. — DOI 10.25726/v8343-7232-2832-p. — EDN PTTSSD.
16. Уточкина, Л.А. Информационная безопасность как элемент экономической безопасности организации / Л.А. Уточкина // Инновационная экономика: перспективы развития и совершенствования. — 2021. — № 6(56). — С. 103–109. — DOI 10.47581/2021/IU-01/IE.6.56.17. — EDN PGLLIP.
17. Актуальные проблемы и перспективы развития экономики в современных условиях: Сборник научных трудов X Международной студенческой научно-практической конференции, Оренбург, 25 апреля 2018 года / Оренбургский филиал РЭУ имени Г.В. Плеханова. — Оренбург: Общество с ограниченной ответственностью «Научно-инновационный центр», 2018. — 406 с. — ISBN 978-5-906314-88-8. — DOI 10.12731/REA/AP.2018.406. — EDN XVNGMH.

**Vereshchagin Ilya Yurievich**

Financial University under the Government of the Russian Federation, Moscow, Russia  
E-mail: verestchagin.ilya@mail.ru

## **Modern threats to information security of corporate database management systems in the context of import substitution**

**Abstract.** In any business enterprise, protecting information and assets is important. The loss of confidential information can not only damage the company itself, but also reveal customer data, which will lead to administrative sanctions and reputational losses. Leaks of payment information in retail pose a particular threat, which can lead to large-scale fraud. With the development of digital technologies, the capabilities of attackers are growing, which requires companies to pay attention to risk management and information security. Effective information security risk management requires accurate risk assessment to justify investment in security controls. A variety of quantitative techniques have been developed for risk analysis, including statistical analysis, Bayesian networks, simulation modeling, fuzzy logic, and neural networks. However, they often encounter difficulties in describing the information environment and formalizing risk assessment procedures, which forces them to involve experts and can lead to approximate and inaccurate results. The lack of generally accepted methods for solving these problems remains relevant for the development of universal risk assessment methods. Despite progress in the field of information security, information systems still cannot be completely protected. The frequency of data leaks and attacks is increasing, especially in digital companies, which include retailers. Information security risk analysis determines the risk characteristics of a company's information systems and assets, selecting means to protect or transfer risks. The main factors in assessing risks are the value of assets, assessment of the impact of threats and vulnerabilities, the effectiveness of existing protection measures, expected downtime and recovery time, the amount of fines and sanctions. The results of risk analysis allow decisions to be made regarding risk reduction, transfer, elimination, insurance or acceptance. The process of assessing information security risks includes the stages of identification, description of objects of protection, threats and vulnerabilities, and also forms the basis for selecting adequate means of protection.

**Keywords:** information security; competitiveness; data leakage; digital technologies; risk management; sanctions; regulators