УДК 681.518

**Е. Ю. Царегородцева***

# ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЯХ

*Современные технологии обеспечения информационной безопасности в высших учебных заведениях можно охарактеризовать как недостаточно развитые. Это обусловлено тем, что в российских нормативных документах аспекты, связанные с угрозами информационной безопасности, рисками, их допустимым уровнем и ответственностью за принятие определенных уровней рисков, изложены фрагментарно, а не в системной форме. Кроме того, значительную проблему представляет дефицит квалифицированных специалистов в области информационной безопасности в университетах.*

*Целью статьи является определение уровня защищенности информации от злоумышленников в учебных заведениях в современных условиях. В связи с поставленной целью необходимо решить ряд задач: 1) изучение основных трудностей, с которыми сталкиваются учебные заведения при защите информации; 2) анализ количества инцидентов со взломом информации, способов распространения вредоносного программного обеспечения в успешных атаках на высшие учебные заведения; 3) формулирование новых мер по противодействию угрозам информационной безопасности в учебных заведениях высшего образования.*

КЛЮЧЕВЫЕ СЛОВА: *информационная безопасность, методы защиты, высшие учебные заведения, новые методы защиты.*

**E. Yu. Tsaregorodtseva**

# INFORMATION SECURITY IN HIGHER EDUCATION INSTITUTIONS

*The current state of information security technologies in higher education institutions can be characterized as underdeveloped. This is due to the fact that in Russian regulatory documents, aspects related to information security threats, risks, their acceptable level and responsibility for accepting a certain level of risks are developed fragmentarily, rather than systematically. Another big problem is the lack of high-quality personnel in the field of information security in universities.*

*The purpose of the article is to study information security in educational institutions from intruders in modern conditions. In connection with the set goal, the tasks will be:*

* ***Царегородцева Елена Юрьевна**, кандидат экономических наук, доцент Иркутского государственного университета путей сообщения.*

*1) study the main difficulties that educational institutions face when protecting information; 2) consider the number of incidents of information hacking, methods of malware distribution in successful attacks on higher education institutions; 3) suggest new countermeasures to information security threats in higher education institutions.*

KEYWORDS: *information security, protection methods, higher education institutions, new protection methods.*

В современных условиях информационные системы характеризуются сложными понятиями, которые связаны с информационной безопасностью. Для эффективного выявления угроз информационной безопасности необходимо применять различные методики. В зависимости от типа информационной системы в анализ следует включать подсистему безопасности, отвечающую определенным формальным характеристикам.

На сегодня цифровые технологии сделали информацию ценным активом в образовательном процессе. При этом, несмотря на стремительное развитие технологий внутривузовской защиты информации, информационные угрозы весьма затруднительно распознать полностью. В таком случае следует рассмотреть основные трудности, с которыми сталкиваются учебные заведения при защите информации (рис. 1).

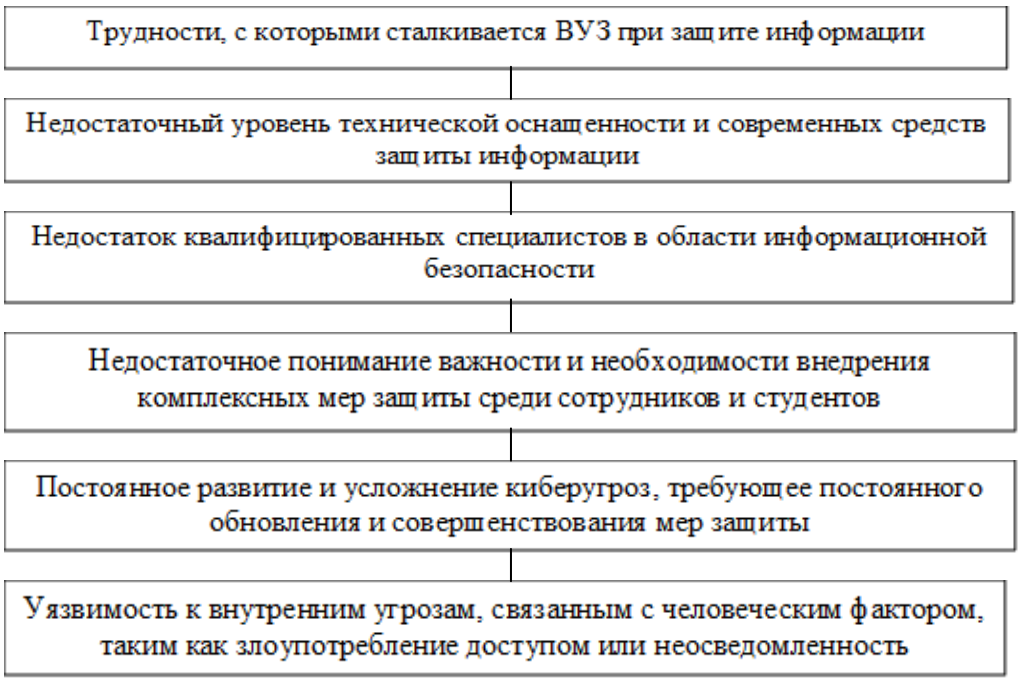


***Рис. 1. Основные трудности, с которыми сталкивается вуз при защите информации***

Помимо прочего, к проблемам следует отнести недостаточное финансирование внедрения современных систем информационной безопасности и нехватку ресурсов для этого. Также наблюдается ограниченность времени и возможностей для постоянного обучения и повышения квалификации персонала и студентов по вопросам обеспечения информационной безопасности в вузе.

Количество инцидентов с угрозой информации в образовательных организациях в 2023 и 2024 гг. показано на рис. 2.

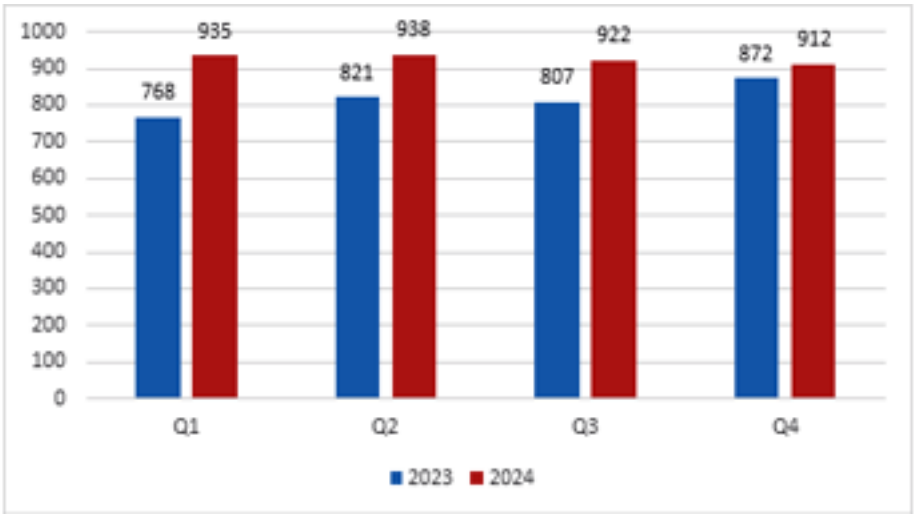


***Рис. 2. Количество инцидентов с угрозой информации в вузах в 2023 и 2024 гг. (по кварталам) [1]***

Из данных, продемонстрированных на рис. 2, очевидно, что в 2024 г. прослеживается явный рост числа инцидентов в сфере информационной безопасности в организациях системы образования. Данные показатели неутешительны. В свою очередь, все это требует активизации усилий по совершенствованию комплекса мер в сфере борьбы с киберпреступностью.

Атаки на информацию со стороны злоумышленников становятся все более распространенными. Мошенники проникают в информационные системы через уязвимости в программном обеспечении поставщиков.

На рис. 3 представлены основные способы распространения информационных угроз в учреждениях сферы образования. В основном они распространяются через электронную почту организаций. Такие угрозы составляют свыше 90 % атак на личные данные [2]. Частные лица становятся уязвимы при посещении фишинговых сайтов. Можно заключить, что фишинговые сайты и рассылки на почту вредоносных писем

для социальных инженеров в целом являются наиболее подходящими методами.

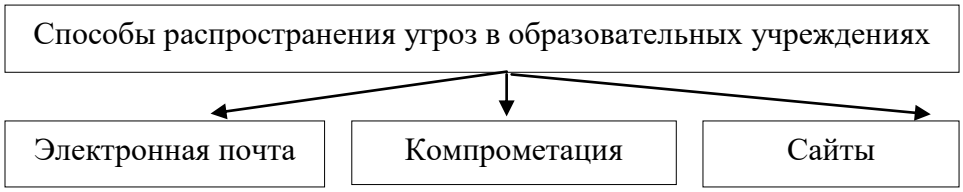


***Рис. 3. Способы распространения информационных угроз в образовательных учреждениях***

В широком смысле информационная безопасность представляет собой состояние общества, при котором обеспечивается комплексная защита как личности, так и государства от различных угроз, связанных с организованными информационными потоками. Узкое понимание информационной безопасности связано непосредственно с защитой самой информации и ее передачи. Для образовательной среды более актуально узкое определение, которое содержит два ключевых аспекта для исследования: безопасность формирующейся личности и безопасность уже сформировавшейся личности [3].

Для защиты от кибератак необходимо реализовывать мероприятия по защите личных данных в учебных заведениях, представленные на рис. 4. Их применение обеспечит сохранность информации и поможет университетам предотвратить репутационные убытки. При оценке угроз для информации необходимо учитывать потенциальные источники опасности.

| **Технологии по защите информации для вузов** |
|---|
| 1. Обеспечение конфиденциальности – защита личных данных обучающихся и сотрудников |
| 2. Сохранение целостности информации – предотвращение искажения или изменения данных в информационных системах вуза |
| 3. Защита от вредоносных кодов – блокировка программ, которые могут повредить систему или украсть данные |

***Рис. 4. Технологии защиты информации в вузах [4, с. 21]***

Тем не менее в высших учебных учреждениях, где доступ к конфиденциальной информации ограничен определенным кругом лиц, внутренние нарушители могут представлять более серьезную угрозу. Знание видов нарушителей способствует разработке эффективных методов защиты конфиденциальной информации, направленных на уменьшение атак с обеспечением безопасности данных (рис. 5).

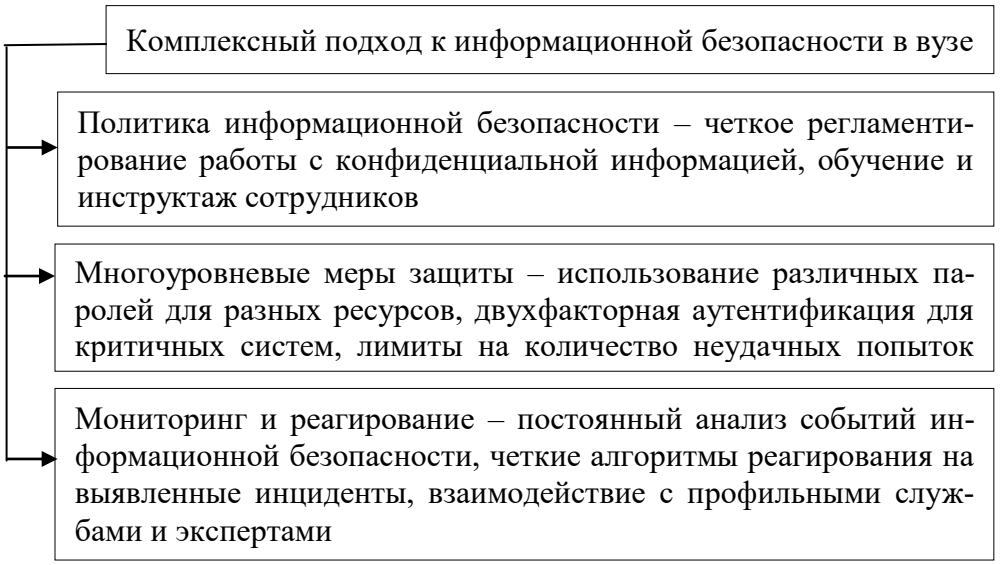


***Рис. 5. Комплексный подход к обеспечению информационной безопасности в вузе [5]***

Представленные на рис. 5 мероприятия позволят объединить технические, организационные и поведенческие методы, значительно сократить вероятность успешных взломов информации, которые основаны на социальной инженерии.

Таким образом, обучение в области информационной безопасности в высших учебных заведениях помогает не только выявлять, но и минимизировать потенциальные угрозы информационных атак [6, с. 143].

Защита информации играет важную роль в стабильной работе университетов и снижении уровня потенциальных угроз для них. В целях ее обеспечения требуется использование комплексного подхода, сочетающего организационные меры с техническими средствами (программное обеспечение). В современном контексте особое значение придается антивирусной защите, особенно в корпоративной сфере, включая образовательные учреждения. Локальные сети могут служить источником вирусных заражений, что может привести к атаке на серверные файлы и впоследствии – к инфицированию пользователей.

Для предотвращения подобных угроз требуется применение комбинированных мер, объединяющих организационные и технические подходы. Такой метод, не предполагающий значительных финансовых затрат, может быть эффективно реализован для обеспечения комплексной антивирусной защиты любой локальной сети в высших учебных заведениях [7].

СПИСОК ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

1. *Винник Е. А.* Обеспечение защиты информации в образовательных организациях / Е. А. Винник // Молодой ученый. 2023. № 7 (454). С. 3–6.
2. *Агеева Е. Л.* Основные аспекты информационной безопасности в образовательной среде / Е. Л. Агеева, О. Ю. Вдовина, А. Ю. Костюнин // Проблемы современного педагогического образования. 2021. № 85-4. С. 10–12.
3. *Бабурин В. В.* Причины и условия преступлений, совершаемых в сфере информационно-коммуникационных технологий / В. В. Бабурин // Вестник Карагандинской академии Министерства внутренних дел Республики Казахстан им. Баримбека Бейсенова. 2022. № 4. С. 140–143.
4. *Вавилова Е. Ю.* Векторы защиты информации в современном обществе / Е. Ю. Вавилова, А. В. Кузин // Исследования молодых ученых : материалы IX Междунар. науч. конф. (г. Казань, апр. 2020 г.). Казань : Молодой ученый, 2020. С. 19–21. URL: https://moluch.ru/conf/stud/archive/368/15712.
5. *Павлова А. А.* Особенности динамики компьютерной преступности и проблемы ее латентности / А. А. Павлова, Т. И. Игнатьева // Право и государство: теория и практика. 2023. № 7 (223). С. 411–415.
6. *Царегородцева Е. Ю.* Значение информационных систем для современного общества / Е. Ю. Царегородцева // Культура. Наука. Образование. 2024. № 2 (71). С. 143–148.
7. О Министерстве цифрового развития, связей и массовых коммуникаций : постановление Правительства РФ от 2 июня 2008 г. № 418 : (ред. от 13 мая 2021 г.). URL: http://www.consultant.ru/document/cons_doc_LAW_77387.