DOI 10.37882/2223–2966.2021.12.12

ГЕОИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ И ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

THREATS OF INFORMATION IMPACT ON INFORMATION SYSTEMS OF EDUCATIONAL INSTITUTIONS

S. Ivliev
S. Krilova
A. Kvaskov
Abdul-Karim Umyarov

Summary. The widespread use of open cartographic services in the information systems of educational organizations leads to an increase in the list of current threats to personal data processed in these systems. The danger of reducing the level of protection of personal data processed in the information systems of educational organizations is shown in the light of the growing threats of informational psychological impact on the population of Russia through social engineering and information technology impact. Research in the field of GIS information security has shown insufficient security of data transmission protocols and the client part. The purpose of this study is to analyze information security threats implemented through publicly available mapping services. As a result of the study, the following were identified: a number of technical and organizational vulnerabilities related to the use of third-party mail services and services provided by social networks, the use of WEB developments that have not passed the verification procedure for undocumented capabilities, vulnerabilities in system and application software, violation of password management rules and related violation of information access rules, insufficient measures to counter access blocking.

Keywords: information systems, information security, cartographic services.

Ивлиев Сергей Николаевич
К.т.н., доцент, ФГБОУ ВО «Мордовский Государственный Университет им. Н.П. Огарёва», Саранск
ivliev_ibis@mrsu.ru
Крылова Светлана Львовна
Старший преподаватель, ФГБОУ ВО «Мордовский Государственный Университет им. Н.П. Огарёва», Саранск
krilova_ibis@mrsu.ru
Кваскov Алексей Александрович
Аспирант, ФГБОУ ВО «Мордовский Государственный Университет им. Н.П. Огарёва», Саранск
unholy_str@mail.ru
Умяров Абдул-Карим Рафаэлевич
ФГБОУ ВО «Мордовский Государственный Университет им. Н.П. Огарёва», Саранск, Россия
umiarov.karim@yandex.ru

Аннотация. Широкое использование открытых картографических сервисов в информационных системах образовательных организаций приводит к увеличению перечня актуальных угроз для персональных данных, обрабатываемых в этих системах. Показана опасность снижения уровня защищенности персональных данных, обрабатываемых в информационных системах образовательных организаций, в свете нарастающих угроз информационного психологического воздействия на население России посредством социальной инженерии и информационно-технического воздействия. Исследования в области информационной безопасности ГИС показали недостаточную защищенность протоколов передачи данных и клиентской части. Целью настоящего исследования является анализ угроз информационной безопасности, реализуемых через общедоступные картографические сервисы. В результате исследования были выявлены: ряд уязвимостей технического и организационного характера, связанных с использованием сторонних почтовых сервисов и сервисов, предоставляемых социальными сетями, использованием WEB-разработок, не прошедших процедуру проверки на наличие недокументированных возможностей, уязвимости в системном и прикладном программном обеспечении, нарушение правил управления паролями и связанное с ним нарушение правил доступа к информации, недостаточность мероприятий противодействия блокированию доступа.

Ключевые слова: информационные системы, информационная безопасность, картографические сервисы.

Введение

В век информационных технологий, когда информация стала критически важным ресурсом, особую актуальность приобретают проблемы информационной безопасности. При этом данная проблема не имеет однозначного простого решения, а носит комплексный характер. Это подтверждается в Доктрине информационной безопасности Российской Федерации: «Обеспечение информационной безопасности — осуществление взаимоувязанных правовых, организационных, оперативно-розыскных, разведывательных, контрразведывательных, научно-технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления». К сожалению, при реализации и продвижении проектов, связанных с информатизацией различных сторон общественной, научной и производственной деятельности, обеспечению безопасности при генерации, обработке, хранении и удалении информации иногда уделяется недостаточно внимания. На наш взгляд реализация Национальных проектов «Здравоохранение», «Образование», «Демография», «Экология», «Жилье и городская среда» невозможна в отрыве от Национального проекта Российской Федерации «Цифровая экономика», содержащего федеральный проект «Информационная безопасность».

Уязвимости использования геоинформационных систем при реализации национальных проектов «Здравоохранение», «Образование», «Демография», «Экология», «Жилье и городская среда» обуславливают возможности реализации угроз конфиденциальности, целостности и доступности при удаленном подключении к сервисам сторонних производителей и поставщиков картографического контента. Причем, это в большей степени касается информационных систем персональных данных (ИСПДн). Целью атак на ИСПДн может быть как получение конфиденциальной информации о субъекте, так и информационно-психологическое воздействие на население. Ряд исследователей указывает на наличие существенных уязвимостей в информационных системах. В частности, это относится информационным системам образовательных организаций. На кафедре информационной безопасности и сервиса ФГБОУ ВО «Национальный исследовательский Мордовский государственный университет имени Н.П. Огарева» проводятся исследования проблем защиты персональных данных в информационных системах различного назначения. Целью настоящего исследования является анализ угроз информационной безопасности, реализуемых через общедоступные картографические сервисы.

Материалы и методы

Теоретическому исследованию угроз информационного воздействия на население в последнее время уделяется все большее внимание [1–5]. Предлагаются методики построения моделей угроз информационно-технического и информационно-психологического воздействий [6]. Учитывая огромное значение защиты от негативного информационного воздействия для молодежи, следует отметить ряд работ, посвященных оценке защищенности информационных систем образовательных организаций [7–10].

Как отмечалось выше, для достижения информационного превосходства могут быть использованы информационно-техническое (ИТВ) и информационно-психологическое (ИПВ) воздействия. Особую опасность представляет их комплексное использование. Наибольшую известность приобрели теории Джона Уордена и Джона Бойда, являющихся идеологами и разработчиками стратегии современных войн и военных конфликтов [1,11].

Проблемам защиты геоинформационных систем в последнее время уделяется достаточно много внимания. Но, следует отметить, большинство работ связывают информационную безопасность в этой области с безопасностью серверов геоинформационных систем. На наш взгляд недостаточно внимания уделяется информационной безопасности клиентской части [12]. Особенно это касается некоммерческого использования картографических сервисов. Например, большинство образовательных организаций используют общедоступные картографические сервисы (Яндекс карты, Google map и др.) для указания своего местоположения.

На кафедре информационной безопасности и сервиса Мордовского государственного университета была разработана общая модель угроз информационной системы образовательной организации [7, 8]. К наиболее характерным уязвимостям подобного класса ИС относятся:

Уязвимости в системном и прикладном программном обеспечении. Основным источником данной группы уязвимостей является использование программного обеспечения, не прошедшего процедуру подтверждения отсутствия не декларированных возможностей.

Нарушение правил управления паролями и связанное с ним нарушение правил доступа к информации. Т.е. в большинстве образовательных организаций отсутствуют удостоверяющие центры. Регламентирующие документы, касающиеся порядка генерации, распространения и утилизации паролей и прав доступа, в ряде

Таблица 1. Перечень актуальных угроз

Угроза	Наименование угрозы
УБИ.23	Угроза изменения компонентов информационной (автоматизированной) системы
УБИ.30	Угроза использования информации идентификации/аутентификации, заданной по умолчанию
УБИ.34	Угроза использования слабостей протоколов сетевого/локального обмена данными
УБИ.90	Угроза несанкционированного создания учётной записи пользователя
УБИ.167	Угроза заражения компьютера при посещении неблагонадёжных сайтов
УБИ.186	Угроза внедрения вредоносного кода через рекламу, сервисы и контент
УБИ.192	Угроза использования уязвимых версий программного обеспечения

случаев не соответствуют требованиям и рекомендациям регуляторов в области информационной безопасности.

Использование сторонних почтовых сервисов создает предпосылки для несанкционированного обмена информацией. При этом резко повышается вероятность загрузки вредоносного кода.

Использование для пересылки сообщений сервисов, предоставляемых социальными сетями и мессенджерами, так же открывает возможности для несанкционированного обмена информацией и внедрения вредоносного кода.

Использование собственных web-сайтов отдельных подразделений образовательного учреждения (чаще всего разработанных кустарно), не отвечающих требованиям безопасности, для несанкционированного не контролируемого размещения внутренней (в том числе и конфиденциальной) информации на этих ресурсах.

Отсутствие или малая эффективность системы периодического создания, обновления и хранения резервных копий информационных ресурсов.

Результаты и обсуждение

Дальнейшим этапом исследований было построение уточненной модели угроз, учитывающей подключение общедоступных картографических сервисов к сайтам образовательных организаций. На основании рекомендаций ФСТЭК России по моделированию угроз информационной безопасности был составлен перечень возможных угроз для информационной системы образовательного учреждения. Далее с учетом вероятности (возможности) реализации угроз, возможностей потенциальных нарушителей и серьезности последствий от реализации угроз (ущерба) были определены актуальные угрозы. Актуальными были признаны угрозы, источниками которых может быть внутренний и внешний нарушитель с низким потенциалом (bdu.fstec.ru).

Перечень актуальных угроз безопасности для информационной системы образовательного учреждения приведен в таблице 1.

Далее, применяя нормативные документы, были определены меры для компенсации актуальных угроз безопасности, представленные в таблице 2.

На основании проведенного анализа можно отметить, что использование картографических общедоступных сервисов приводит к возникновению дополнительных угроз безопасности для общедоступных персональных данных, размещенных на сайтах образовательных организаций. Это связано как с наличием уязвимостей сетевых протоколов передачи картографической информации, так и вероятностью загрузки вредоносного кода из источников с низким уровнем доверия. Для обеспечения необходимого уровня защищенности требуется обновление модели угроз.

Выводы

Для обеспечения выполнения требований регуляторов по защите персональных данных в случае использо-

Таблица 2. Меры по обеспечению безопасности

Описание угрозы	Мера по обеспечению безопасности
УБИ.23 Угроза заключается в возможности получения нарушителем доступа к сети, файлам, внедрения закладок и т.п. путём несанкционированного изменения состава программных или аппаратных средств информационной системы, что в дальнейшем позволит осуществлять данному нарушителю (или другому — внешнему, обнаружившему несанкционированный канал доступа в систему) несанкционированные действия в данной системе.	ОЦЛ.1 Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации. УПД.17 Обеспечение доверенной загрузки средств вычислительной техники. ЗИС.5 Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств
УБИ.30 Угроза заключается в возможности прохождения нарушителем процедуры авторизации на основе полученной из открытых источников идентификационной и аутентификационной информации, соответствующей учётной записи «по умолчанию» дискредитируемого объекта защиты.	ИАФ.2 Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных
УБИ.34 Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к передаваемой в системе защищаемой информации за счёт деструктивного воздействия на протоколы сетевого/локального обмена данными в системе путём нарушения правил использования данных протоколов.	ОЦЛ.1 Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации. ЗИС.11 Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов
УБИ.90 Угроза заключается в возможности создания нарушителем в системе дополнительной учётной записи пользователя и её дальнейшего использования в собственных неправомерных целях (входа в систему с правами этой учётной записи и осуществления деструктивных действий по отношению к дискредитированной системе или из дискредитированной системы по отношению к другим системам).	ОЦЛ.1 Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации.
УБИ.167 Угроза заключается в возможности нарушения безопасности защищаемой информации вредоносными программами, скрытно устанавливаемыми при посещении пользователями системы с рабочих мест (намеренно или при случайном перенаправлении) сайтов с неблагонадёжным содержимым и запускаемыми с привилегиями дискредитированных пользователей.	ЗИС.16 Выявление, анализ и блокирование в информационной системе скрытых каналов передачи информации в обход реализованных мер или внутри разрешенных сетевых протоколов
УБИ.186 Угроза заключается в возможности внедрения нарушителем в информационную систему вредоносного кода посредством рекламы, сервисов и (или) контента (т.е. убеждения пользователя системы активировать ссылку, код и др.) при посещении пользователем системы сайтов в сети Интернет или установкой программ с функцией показа рекламы.	ОЦЛ.6 Ограничение прав пользователей по вводу информации в информационную систему. ОЦЛ.8 Контроль ошибочных действий пользователей по вводу и (или) передаче персональных данных и предупреждение пользователей об ошибочных действиях
УБИ.192 Угроза заключается в возможности осуществления нарушителем деструктивного воздействия на систему путем эксплуатации уязвимостей программного обеспечения.	РСБ.4 Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти

вания на сайтах ресурсов общедоступных картографических сервисов ИТ-подразделения образовательных организаций должны обеспечивать посредством технических мер выполнение следующих требований:

- контроль целостности программной среды;
- контроль и реагирование на ошибочные действия пользователей;
- выявление скрытых каналов передачи информации.

Ряд необходимых мер по защите данных может носить организационный характер:

- ограничение прав пользователей по вводу информации в информационную систему;
- определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных;
- установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов.

В заключение необходимо отметить, что для повышения эффективности системы защиты информации в образовательных учреждениях необходимо: во-первых, перед началом эксплуатации сегментов информационных систем их качественно классифицировать; во-вторых, при изменении состава информации, или подключении дополнительных сегментов и сервисов — проводить повторную классификацию ИС

ЛИТЕРАТУРА

1. И.И. Брянцев, О.В. Брянцева, Среднерусский вестник общественных наук, 14~<203 (2019)
2. О.В. Брянцева, Информационные технологии в юридической науке и образовании: сборник научных статей по материалам II Всероссийской научной конференции.— Саратов: Изд-во ФГБОУ ВО «Саратовская государственная юридическая академия», 16 (2018)
3. О.В. Брянцева, И.И. Брянцев, Вестник Поволжского института управления.—18~<4 (2018)
4. М.Ю. Зеленков Теоретико-методологические проблемы теории национальной безопасности Российской Федерации (2013)
5. О.Ю. Макеев Каспийский регион: политика, экономика, культура. 4~<132 (2013).
6. С.Г. Антонов, С.В. Гордеев, С.М. Климов, Б.С. Рыжов Информационные войны 46~<83 (2018)
7. С.Н. Ивлиев Интеграция образования. 69~<27 (2012)
8. С.Н. Ивлиев Картография и геодезия в современном мире. Материалы второй Всероссийской научно-практической конференции 187 (2014)
9. А.Н. Привалов, Т.В. Гореликова Актуальные проблемы методики обучения информатике в современной школе Международная научно-практическая интернет-конференция 352 (2016)
10. Т.Н. Чиркова, С.Л. Крылова Материалы XX научно-практической конференции молодых ученых, аспирантов и студентов Национального исследовательского Мордовского государственного университета им. Н.П. Огарёва 288 (2016)
11. McGregor Knox and Williamson Murray, Eds. The Diplomat 13 (2015)
12. С.В. Булгаков, В.Я. Цветков Информационная безопасность ГИС и инфраструктуры. Saarbrucken (2013)

Журнал «Современная наука: актуальные проблемы теории и практики»