Министерство образования Республики Беларусь

Белорусский государственный университет

информатики и радиоэлектроники

Институт Информационных Технологий

**ЛАБОРАТОРНАЯ РАБОТА**

**Концепция информационной безопасности web-сайтов**

Выполнил:

**Слушатель гр.** 10422

**Ф.И.О.** Минцевич В.В.

Минск 2022

**Введение**

Настоящая Концепция обеспечения безопасности информации определяет систему взглядов на проблему обеспечения безопасности информации web-сайтов и представляет собой систематизированное изложение целей и задач защиты, основных принципов построения, организационных, технологических и процедурных аспектов обеспечения безопасности информации.

**Объекты защиты**

Основными объектами информационной безопасности web-сайта являются:

1. информация с ограниченным доступом, составляющая коммерческую, банковскую тайну, а также открытая (общедоступная) информация, представленные в виде документов и массивов данных, независимо от формы и вида их представления;
2. процессы обработки информации – информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации, а также защита;
3. информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены чувствительные компоненты

**Цель и задачи**

Цель web-безопасности – предотвращении различных видов атак. Разработка способов защиты web-сайта от несанкционированного доступа, использования, изменения, уничтожения или нарушения работы.

Задачи:

1. защита от вмешательства в процесс функционирования сайта;
2. разграничение прав доступа к информации, компьютерам, средствам защиты;
3. регистрация происходящих событий (SIEM), процедуры обеспечения целостности и достоверности информации, а также методы ее восстановления;
4. защита от несанкционированных действий;
5. авторизация и аутентификация пользователей;
6. мониторинг возможных угроз и информационной защищенности; действия для минимизации и локализации ущерба от неправомерных действий;
7. сканирование на возможность проникновения.

**Основные угрозы web-безопасности**

**XSS (Cross-Site Scripting - Межсайтовый скриптинг)** – тип атак, которые позволяют злоумышленнику внедрять вредоносный код через web-сайт в браузеры других пользователей. Поскольку внедрённый код поступает в браузер с сайта, он является доверенным и может выполнять такие действия, как отправка авторизационного файла cookie пользователя злоумышленнику. Когда у злоумышленника есть файл cookie, он может войти на сайт, как если бы он был пользователем, и сделать все, что может пользователь, например, получить доступ к данным кредитной карты, просмотреть контактные данные или изменить пароли. Вредоносный код может быть вставлен в страницу как через [уязвимость](https://ru.wikipedia.org/wiki/%D0%A3%D1%8F%D0%B7%D0%B2%D0%B8%D0%BC%D0%BE%D1%81%D1%82%D1%8C_(%D0%BA%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C)) в [веб-сервере](https://ru.wikipedia.org/wiki/%D0%92%D0%B5%D0%B1-%D1%81%D0%B5%D1%80%D0%B2%D0%B5%D1%80), так и через уязвимость на компьютере пользователя.

**SQL-инъекции** позволяют злоумышленникам выполнять произвольный код SQL в базе данных, позволяя получать, изменять или удалять данные независимо от разрешений пользователя. Успешная инъекционная атака может подделать удостоверения, создать новые удостоверения с правами администратора, получить доступ ко всем данным на сервере или уничтожить / изменить данные, чтобы сделать их непригодными для использования. Атака типа внедрения SQL может быть возможна из-за некорректной обработки входных данных, используемых в SQL-запросах.

**Подделка межсайтовых запросов (CSRF).** CSRF-атаки позволяют злоумышленнику выполнять действия, используя учётные данные другого пользователя, без его ведома или согласия.

**Основные положения технической политики в обеспечении web-безопасности**

1. реализация разрешительной системы допуска пользователей к информации;
2. разграничение доступа пользователей к информационным ресурсам;
3. реализация системы сбора и обработки, объективное документирование событий;
4. регистрация действий пользователей и контроль за несанкционированным доступом и действиями пользователей;
5. надежное хранение традиционных и машинных носителей информации;
6. криптографическое преобразование информации, обрабатываемой и передаваемой средствами вычислительной техники и связи;
7. необходимое резервирование технических средств и информационных ресурсов;

**Принципы построения комплексной системы защиты**

**Законность** – предполагает осуществление защитных мероприятий и разработку системы безопасности информации в соответствии с действующим законодательством.

**Системность** – системный подход к построению системы защиты информации предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности информации.

**Комплексность** – комплексное использование методов и средств защиты предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов.

**Непрерывность** – непрерывный, целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла web-сайта. Своевременность – предполагает упреждающий характер мер для обеспечения безопасности информации.

**Преемственность и совершенствование** – предполагают постоянное совершенствование мер и средств защиты информации.

**Разумная достаточность (экономическая целесообразность)** – предполагает соответствие уровня затрат на обеспечение безопасности информации, ценности информационных ресурсов и величине возможного ущерба.

**Персональная ответственность** – предполагает возложение ответственности за обеспечение безопасности информации и системы ее обработки на каждого сотрудника в пределах его полномочий.

**Принцип минимизации полномочий** – означает предоставление пользователям минимальных прав доступа в соответствии с производственной необходимостью.

**Взаимодействие и сотрудничество** – предполагает создание благоприятной атмосферы в коллективах подразделений.

**Гибкость системы защиты** – для обеспечения возможности варьирования уровня защищенности, средства защиты должны обладать определенной гибкостью. Открытость алгоритмов и механизмов защиты – суть данного принципа состоит в том, что защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно давать возможности ее преодоления (даже авторам). Это, однако, не означает, что информация о конкретной системе защиты должна быть общедоступна.

**Простота применения средств защиты** – механизмы защиты должны быть интуитивно понятны и просты в использовании, без значительных дополнительных трудозатрат.

**Научная обоснованность и техническая реализуемость** – информационные технологии, технические и программные средства, средства и меры защиты информации должны быть реализованы на современном уровне развития науки и техники, научно обоснованы с точки зрения достижения заданного уровня безопасности информации и должны соответствовать установленным нормам и требованиям по безопасности информации.

**Специализация и профессионализм** – предполагает привлечение к разработке средств и реализаций мер защиты информации специализированных организаций, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области. Реализация административных мер и эксплуатация средств защиты должна осуществляться профессионально подготовленными специалистами.

**Обязательность контроля** – предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил безопасности.

**Меры, методы и средства защиты**

1. эффективное управление паролями. Реализация двухфакторной аутентификации для сайта, чтобы в дополнение к паролю пользователь должен был ввести другой код аутентификации, например, код в SMS или с помощью стороннего приложения, как например Google Authenticator, также запрет на использование «опасных» ключевых слов(напр. слово script) и удалять их с помощью Web Application Firewall;
2. настройка web-сервера для использования HTTPS и HTTP Strict Transport Security (HSTS). HTTPS шифрует данные, передаваемые между клиентом и сервером. Это гарантирует, что учётные данные для входа, файлы cookies, данные запросов POST и информация заголовка не будут легко доступны для злоумышленников;
3. отслеживание наиболее популярных угроз, и в первую очередь устранение наиболее распространённых уязвимостей;
4. использование инструментов сканирования уязвимостей с постоянной периодичностью;
5. Для защиты от SQL-инъекций используются механизмы **Санитизация** (процесс очистки от управляющих символов), **Валидация** (процесс проверки соответствия данных), **Типизация** (процесс привода данных к нужному нам типу) и **Подготовленный** **запрос** (скомпилированный запрос, передаваемые данные для которого не могут повлиять на сам запрос);
6. Для предотвращения XSS используются SameSite cokie flag и anti-CSRF token. Также завершение сессии должно быть реализовано как на клиенте, так и на серверной части при отсутствии действий пользователя на клиенте по тайм-ауту и по истечении времени жизни сессии.